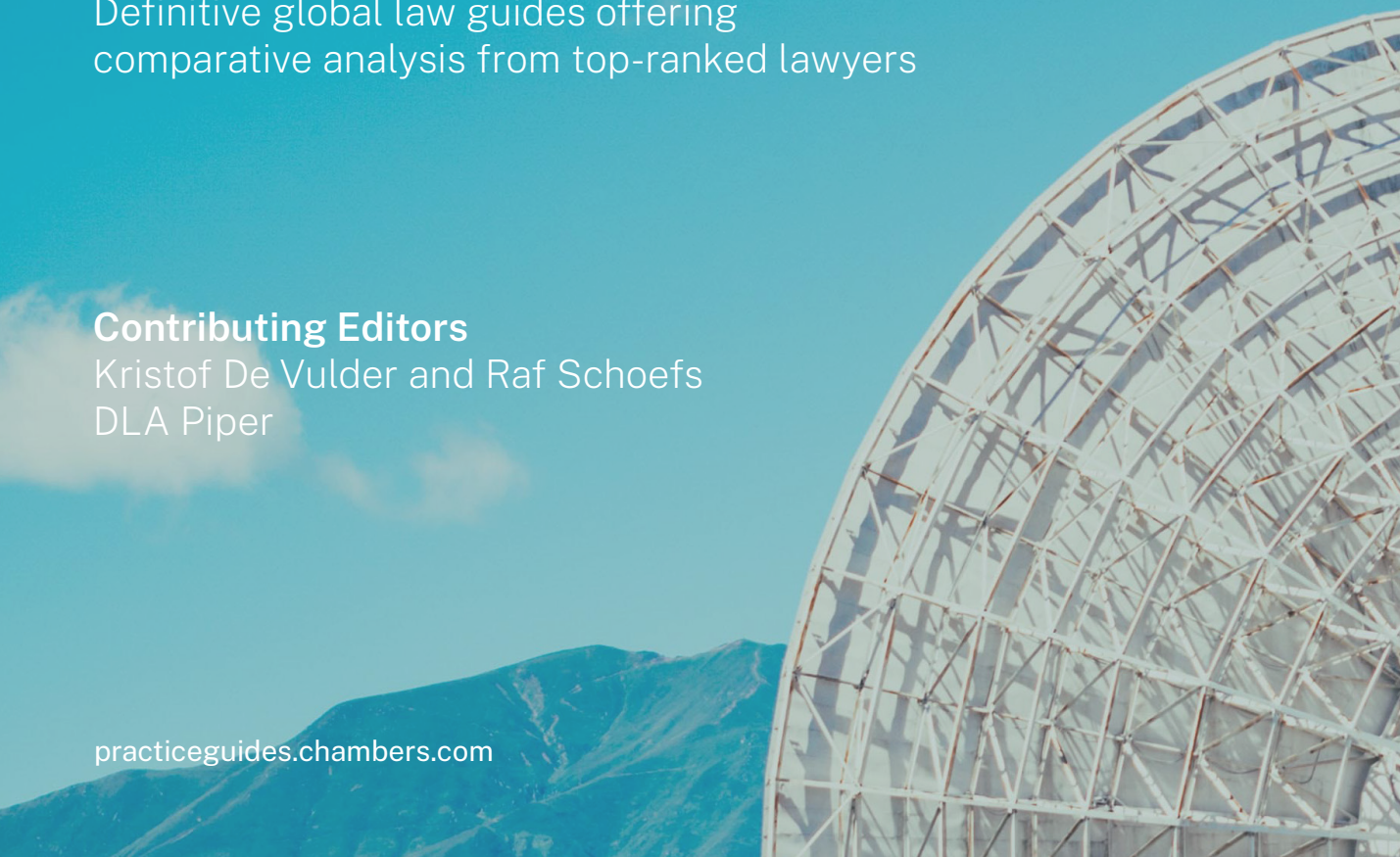

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2023

Definitive global law guides offering
comparative analysis from top-ranked lawyers

Contributing Editors

Kristof De Vulder and Raf Schoefs
DLA Piper



Chambers

Global Practice Guides

TMT

Contributing Editors

Kristof De Vulder and Raf Schoefs

DLA Piper

2023

Chambers Global Practice Guides

For more than 20 years, Chambers Global Guides have ranked lawyers and law firms across the world. Chambers now offer clients a new series of Global Practice Guides, which contain practical guidance on doing legal business in key jurisdictions. We use our knowledge of the world's best lawyers to select leading law firms in each jurisdiction to write the 'Law & Practice' sections. In addition, the 'Trends & Developments' sections analyse trends and developments in local legal markets.

Disclaimer: The information in this guide is provided for general reference only, not as specific legal advice. Views expressed by the authors are not necessarily the views of the law firms in which they practise. For specific legal advice, a lawyer should be consulted.

GPG Director Katie Burrington

Content Management Director Claire Oxborrow

Content Manager Jonathan Mendelowitz

Senior Content Reviewer Sally McGonigal, Ethne Withers

Content Reviewers Vivienne Button, Lawrence Garrett, Dara McCormack, Marianne Page, Heather Palomino and Deborah Sinclair

Content Coordination Manager Nancy Laidler

Senior Content Coordinator Carla Cagnina

Content Coordinators Eleanor Smith and Delicia Tasinda

Head of Production Jasper John

Production Coordinator Genevieve Sibayan

Published by

Chambers and Partners

165 Fleet Street

London

EC4A 2AE

Tel +44 20 7606 8844

Fax +44 20 7831 5662

Web www.chambers.com

Copyright © 2023

Chambers and Partners

CONTENTS

INTRODUCTION

Contributed by Kristof De Vulder and Raf Schoefs,
DLA Piper p.5

AUSTRALIA

Law and Practice p.10

Contributed by Holding Redlich

Trends and Developments p.30

Contributed by Holding Redlich

BELGIUM

Law and Practice p.39

Contributed by DLA Piper

Trends and Developments p.56

Contributed by EDSON

BRAZIL

Law and Practice p.65

Contributed by Azevedo Sette Advogados

CANADA

Law and Practice p.80

Contributed by Fasken

CHINA

Law and Practice p.96

Contributed by DaHui Lawyers

Trends and Developments p.116

Contributed by DaHui Lawyers

EGYPT

Law and Practice p.123

Contributed by Shehata & Partners

FRANCE

Law and Practice p.151

Contributed by White & Case LLP

GERMANY

Law and Practice p.168

Contributed by Orrick, Herrington & Sutcliffe

Trends and Developments p.181

Contributed by Orrick Herrington & Sutcliffe

INDIA

Law and Practice p.187

Contributed by TMT Law Practice

Trends and Developments p.200

Contributed by AnantLaw Solicitors & Advocates

ITALY

Law and Practice p.208

Contributed by Morri Rossetti e Associati

JAPAN

Law and Practice p.230

Contributed by Mori Hamada & Matsumoto

Trends and Developments p.244

Contributed by Nagashima Ohno & Tsunematsu

MACAU SAR, CHINA

Law and Practice p.252

Contributed by Rato, Ling, Lei & Cortés – Advogados
(Lektou)

MALAYSIA

Law and Practice p.267

Contributed by Shin Associates

MALTA

Law and Practice p.289

Contributed by GVZH Advocates

MEXICO

Law and Practice p.305

Contributed by Ruiz Moreno & Asociados

Trends and Developments p.320

Contributed by Santamarina y Steta SC

NETHERLANDS

Trends and Developments p.326

Contributed by Greenberg Traurig, LLP

NIGERIA

Law and Practice p.334

Contributed by Templars

CONTENTS

NORWAY

Law and Practice p.356

Contributed by Advokatfirmaet Haavind

PAKISTAN

Law and Practice p.368

Contributed by RIAA Barker Gillette

PHILIPPINES

Law and Practice p.387

Contributed by Villaraza & Angangco

POLAND

Trends and Developments p.407

Contributed by Sołtysiński Kawecki & Szlęzak

ROMANIA

Law and Practice p.416

Contributed by MPR Partners

Trends and Developments p.431

Contributed by MPR Partners

SPAIN

Law and Practice p.438

Contributed by Asensi Abogados

Trends and Developments p.459

Contributed by Asensi Abogados

SINGAPORE

Law and Practice p.466

Contributed by Drew & Napier LLC

SOUTH KOREA

Law and Practice p.484

Contributed by Yulchon LLC

SWITZERLAND

Law and Practice p.504

Contributed by Lenz & Staehelin

THAILAND

Law and Practice p.521

Contributed by Formichella & Sritawat

Trends and Developments p.536

Contributed by Formichella & Sritawat

USA

Law and Practice p.543

Contributed by Kelley Drye & Warren LLP

Trends and Developments p.562

Contributed by DLA Piper LLP

INTRODUCTION

Contributed by: Kristof De Vulder and Raf Schoefs, DLA Piper

TMT 2023 Global Overview

The past few years have been deeply marked by the COVID pandemic, which for the technology, media and telecommunications (TMT) sector resulted in a rocketing uptake of digital services and technologies – for example, online communication and videoconferencing technologies, streaming services and online shopping.

As of February 2023, the COVID pandemic is somewhat under control, but the world is changing at an unprecedented rate. From supply shocks to war to extreme weather events to recession, there is a historic level of disorder in the market. Looking at the numerous lay-offs at large global tech companies, the TMT sector is not safe from these turbulent times.

Despite the high degree of uncertainty in the world and in the TMT sector, digital evolution has continued at a swift pace. Furthermore, cybersecurity remains very high on the agendas of business leaders and legislators alike. Legislators are also increasingly focusing on the regulation of the digital economy, big tech companies and new disruptive technologies (such as AI), leading to several legislative initiatives and evolutions.

For those outside the sector – and sometimes even for those inside – it is difficult to remain up to date even on the major developments, both technological and legal. This guide is intended to provide a useful outlook on the legal framework applicable to key areas of the TMT sector, helping you to navigate this constantly evolving sector in which law and technology continuously influence each other.

Given the many rapid developments in the TMT field, the Chambers TMT guide 2023 aims not

so much to paint a broad picture covering all possible aspects of the TMT landscape, but to be topic-driven, giving insights into some of the questions with which lawyers and in-house counsel will be most often confronted in this era of permanent change.

Metaverse

The metaverse is a term describing a hypothetical enhanced digital environment in which we will be able to move smoothly between several spheres such as social, work, leisure and retail in one single digital environment. The metaverse could also be seen as the integration of the digital world and the physical world.

It could radically transform the way humans interact with technology and the offerings of technology companies. Meta (Facebook) is a big stakeholder in this respect and has made the metaverse one of its top priorities. No specific laws for the metaverse have been introduced yet, but it raises many questions relating to intellectual property, enforcement, privacy, and cybersecurity.

Digital Economy

Digital economy is an umbrella term that describes how traditional economic activities are being reshaped by the internet. New laws are to be expected, given the recent entry into force of the EU Digital Markets Act (DMA) and the EU Digital Services Act (DSA). It is yet to be seen how these will be implemented in the EU member states and what the practical effect on the TMT sector will be.

Cloud and Edge Computing

Nearly everything is “cloud” nowadays – television, music, wallets, work documents, profes-

INTRODUCTION

Contributed by: Kristof De Vulder and Raf Schoefs, DLA Piper

sional contacts, communications, software, even relationships.

For consumers, there is often a trade-off to be made between availability and control, with licensing replacing ownership. For organisations, a decrease in costs generally goes hand-in-hand with higher security standards – as well as provider-dependency.

The legal implications can be diverse, from sector-specific regulations on availability and liability to broader data protection considerations.

Artificial Intelligence and Big Data

In the past few years, digital assistants have invaded our workplaces and homes. From completing an unfinished symphony by a revered composer to carrying out predictions of shopping patterns and learning board games on their own, an increase in the capabilities of machines has created possibilities deemed unthinkable just a few years ago. With developments such as ChatGPT, the uptake of AI is still accelerating.

For businesses, big data promises a better understanding of their customers and patterns, while for consumers, big data may involve a number of undesired side-effects (for example, being subject to profiling or automated decision-making on the basis of all data gathered).

Big data and artificial intelligence also raise important societal and legal questions on topics such as liability and insurance, data protection and intellectual property, jurisdiction, and even fundamental rights. While a few businesses will already be examining whether algorithms also have fundamental rights, there are more immediate concerns they may well wish to consider.

Internet of Things (IoT)

IoT is a small acronym for something so large. In addition to computers and mobile devices, everything in our home and workplace is becoming “connected”. Energy providers are keen to roll out smart metres, and automobile manufacturers are becoming service providers by adding connectivity to their (manual or self-driving) vehicles.

With many of our devices (eg, fridges, lights and watches) connected to the internet, security risks are increasing because of the vulnerability of such devices. Hackers no longer have to directly target laptops or PCs, which have stronger in-built security features, but can rather attack IoT devices, which are often not properly secured, in order to compromise an entire network and access all devices connected to it.

Aside from data protection, some of the legal key words have become more technical, such as machine-to-machine (M2M) communications, communications secrecy and cybersecurity. Any project in this field requires careful consideration and sound legal review.

Audio-Visual Media Services

Today, every organisation can have a digital communications channel, from podcasts to video channels, a realm once reserved for large content providers. Yet, where this is more than a one-off video, the creation of a structure and frequent addition of content can trigger the need to apply for authorisations with the local regulator.

It is therefore important to know whether rules on audio-visual services also apply to online video channels, even on third-party websites featuring user-generated content.

INTRODUCTION

Contributed by: Kristof De Vulder and Raf Schoefs, **DLA Piper**

Telecommunications

At one time, telecommunications rules would have been considered to apply only to large incumbent telephone and radio operators. Today, voice-over IP (VoIP) and instant messaging solutions have become commonplace in organisations, sometimes even in interactions with customers. Finally, many retailers and product manufacturers have adopted technology-powered labelling in the form of radio-frequency identification (RFID) tags.

However, the use of some of these means of communication or technologies (such as 5G) can trigger the application of a strict regulatory regime for which many different obligations can apply, depending on the electronic communication service or network that is provided. While this regime does not always represent an insurmountable cost or effort, it is important to take these factors into account when providing these kinds of services.

Challenges with Technology Agreements

Technology agreements come in different types and sizes and can cover a myriad of technology products and services.

In a global economy, organisations have a broad range of technology providers to choose from, but when selecting a provider and concluding a contract, it is important to be aware of any specific requirements and restrictions.

If data cannot leave a given provider's country, is it as attractive to work with that provider? Some legal restrictions can be very specific, such as restrictions on price-revision mechanisms. All in all, it is invariably best to be informed of local requirements before making a selection.

Trust Services and Digital Entity

Many transactions are concluded online nowadays. However, this brings forth authentication and identification issues. To battle fraud, trust services, electronic signatures and digital identity schemes have been set up.

Knowing the legal framework applicable to your technology or area of work is fundamental to avoiding unpleasant surprises or undesired obstacles.

INTRODUCTION

Contributed by: Kristof De Vulder and Raf Schoefs, **DLA Piper**

DLA Piper has a global intellectual property and technology (IPT) group consisting of 60-plus offices, around 150 partners and 530-plus fee earners in more than 20 countries, constituting the world's largest IPT team. With over 120 lawyers based in the firm's office in Brussels and its working hub in Antwerp, DLA Piper in Belgium combines DLA Piper's global reach with local know-how. More specifically, the IPT team is part of a global, fully integrated group of IPT teams that operate in the markets of greatest importance to the firm's multinational

clients. The Belgian team continuously develops innovative processes and methodologies to improve the delivery of legal services to its clients, as well as the internal organisation of its clients. The whole IPT team is fully dedicated to advising on IT, media and telecommunications matters, acting for both customers (larger users of IT) and large IT vendors, which gives it invaluable insight at both sides of the negotiation table, translating into better, more commercial and more pragmatic advice for its clients.

Contributing Editors



Kristof De Vulder is country-managing partner of DLA Piper's Belgian offices, and head of the IPT department. He has over 20 years' experience in technology contracts, cyber-incidents,

outsourcing and complex technology transactions. Kristof typically advises both users and suppliers of technology and outsourcing services in relation to all aspects of the procurement process, legal issues arising with the implementation of new technologies and responses to cyber-incidents. He further assists clients during all stages of litigation, including pre-litigation strategies, mediation, arbitration and government courts. His work involves business-critical and strategic projects all over the world. Kristof has received international recognition with respect to his technology sector work and has contributed to numerous publications relating to TMT law.



Raf Schoefs is a counsel in DLA Piper's intellectual property and technology team. He practises in all areas of information technology and intellectual property law, with a particular

focus on technology and outsourcing transactions, and has over 12 years of experience. Raf assists clients in the drafting and negotiating of complex IT and outsourcing agreements. He also advises clients on e-commerce-related topics, such as cloud computing, electronic signatures, intermediary liability, data protection, cookies and consumer protection. He has extensive experience in a wide range of IP-related matters and assists IT providers, buyers of IT services and public sector organisations in all types of technology transactions. Raf has contributed to several publications relating to TMT law.

INTRODUCTION

Contributed by: Kristof De Vulder and Raf Schoefs, **DLA Piper**

DLA Piper

Rue aux Laines 70
1000
Brussels
Belgium

Tel: +32 2 500 15 00
Fax: +32 2 500 16 00
Email: kristof.devulder@dlapiper.com
Web: www.dlapiper.com



Law and Practice

Contributed by:

Angela Flannery, Andrew Hynd,
Dan Pearce and Ian Robertson

Holding Redlich see p.28



Contents

1. Metaverse	p.11
1.1 <u>Laws and Regulations</u>	p.11
2. Digital Economy	p.12
2.1 <u>Key Challenges</u>	p.12
3. Cloud and Edge Computing	p.14
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.14
4. Artificial Intelligence and Big Data	p.16
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.16
5. Internet of Things	p.18
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.18
6. Audio-Visual Media Services	p.20
6.1 <u>Requirements and Authorisation Procedures</u>	p.20
7. Telecommunications	p.22
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.22
8. Challenges with Technology Agreements	p.23
8.1 <u>Legal Framework Challenges</u>	p.23
9. Trust Services and Digital Entities	p.26
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.26

1. Metaverse

1.1 Laws and Regulations

Key legislation regulating metaverse platforms in Australia is:

- the Privacy Act 1988 (Cth) (the “Privacy Act”);
- the Competition and Consumer Act 2010 (Cth) (CCA); and
- the Online Safety Act 2021 (Cth) (the “Online Safety Act”) and proposed codes under that Act.

The Privacy Act

The Privacy Act regulates the collection and management of personal information by most private sector enterprises in Australia. Generally, the Privacy Act imposes obligations that are similar to, but generally seen as less onerous, than the General Data Protection Regulation (GDPR).

The extra-territorial operation of the Privacy Act was expanded by amendments made in late 2022. The Privacy Act now applies to acts or practices of an entity occurring outside Australia, even where the relevant entity is not incorporated or created under Australian law, if an “Australian link” exists. This requires the relevant entity to carry on business in Australia. Australian case law provides that “carry on business in Australia” will be interpreted broadly, and may apply to a digital platform, including a provider of a metaverse platform, that is used by individuals in Australia even where the platform does not have a physical presence in Australia.

The Australian government is part way through a consultation process for reform of the Privacy Act that may have significant implications for the metaverse. The significant changes that are proposed include:

- the imposition of enhanced restrictions in high-risk cases, including where sensitive information, or the information of children, is collected and used on a large scale;
- inclusion of a right of erasure, which is not a right currently provided for under the Privacy Act; and
- rights for individuals to take action in the event of a breach of privacy and the potential for class actions to be permitted in the case of breaches.

The CCA

The Australian competition and consumer protection regulator, the Australian Competition and Consumer Commission (ACCC), has already taken enforcement action against a number of digital platforms for misleading and deceptive conduct, including litigation against Google and Facebook for alleged misleading and deceptive conduct regarding data collection. It would be expected that the ACCC will continue to be vigilant in this area in its supervision of the metaverse.

In addition, the ACCC has proposed that it may recommend to the Australian government to further amend the CCA to clarify that prohibited anti-competitive mergers and acquisitions include so called “killer acquisitions”, where nascent competitors are acquired by existing businesses. This is likely to impact the ability of digital businesses providing metaverse platforms acquiring smaller competitors, which may restrict the ability of those platforms to grow.

The Online Safety Act

The Online Safety Act regulates abuse and harmful content on online platforms. The Online Safety (Basic Online Safety Expectations) Determination 2022 (Cth) was made under the Online Safety Act. That Determination requires,

amongst other measures, that regulated entities, including providers of social media services (the definition of which is broad enough to encompass metaverse platforms), will take reasonable steps to ensure that end-users are able to use those services in a safe manner.

The eSafety Commissioner, the regulator responsible for the enforcement of the Online Safety Act, has already indicated that while the regulator will not mandate the steps that a platform is required to take, addressing safe use of metaverse platforms will be a key area of focus as metaverse platforms develop.

The Online Safety Act also provides for the development and implementation of codes to regulate particular categories of harmful online conduct. Industry bodies are required to develop the codes, which will be registered by the eSafety Commissioner if these meet certain statutory requirements. As at the beginning of 2023, no codes have been registered, however the Commissioner is currently considering codes which have been submitted by industry bodies including for social media, messaging and search engine providers. These initial codes are likely to be registered during the course of 2023.

Further Reforms

As at the beginning of 2023, the Australian government is consulting on regulatory reforms to be applied to digital platforms, which would include the providers of metaverse platforms. These encompass both competition measures, which may include for example requirements restricting the ability of dominant platforms to engage in self-preferencing and consumer protections, such as restrictions on unfair trading practices, which may apply to limit the ability of metaverse platform providers from collecting consumer data.

Other Legal Issues

Businesses operating on any metaverse platform will need to consider other legal issues, including intellectual property laws and cybersecurity. Australia does not have any specific online intellectual property laws, with general laws, such as the Copyright Act 1968 (Cth), the Trade Marks Act 1995 (Cth) and the Patents Act 1990 (Cth) applying equally in an online environment as in the physical environment. Businesses will need to consider whether extra protections (such as trade mark registrations) are required to protect metaverse related assets.

There is no specific cybersecurity laws that currently apply to metaverse platforms or other similar services. However, significantly increased penalties were introduced for breaches of the Privacy Act at the end of 2022, which would apply to future cyber-attacks where the relevant business has not adequately protected the personal information it holds.

2. Digital Economy

2.1 Key Challenges

Leaving aside consideration of Australia's critical infrastructure legislation and the regulation of artificial intelligence and the use of big data, which are discussed in 3. **Cloud and Edge Computing** and 4. **Artificial Intelligence and Big Data** respectively, Australia does not have laws or regulations that focus solely on the digital economy. Digital economy businesses must comply with economy wide laws and regulation. There are, however, a number of specific legislative and regulatory regimes that have significant implications for certain sectors of the digital economy, some of which are discussed in this response.

Consumer Data Right

Part IVD of the CCA contains the regulatory framework for the Australian Consumer Data Right (CDR). At the time the legislation for this relatively new regime was passed in 2019, the then Australian Treasurer commented that the CDR would be an important building block for “Australia’s data revolution”.

The CDR has two key elements. First, the ability for customers (whether individuals or businesses) to require that businesses transfer data held about them either to the relevant customer directly or to an accredited third party. The second element is a requirement for businesses to provide public access to information on specified products that they offer in a standardised format.

Where consumers are able to share data that a business holds about them, this has the potential to assist those consumers to find better products or services, more suited to their needs, from another company. In addition, requiring businesses to provide public data regarding specific products in a standardised format allows consumers to compare products and services more easily.

There are two regulators with primary responsibility for CDR. First, the ACCC which, for example, provides accreditation for CDR data recipients (that is, those entitled to obtain consumer data under the regime) and enforces compliance with the CDR legislation, rules and standards. Secondly, the Office of the Australian Information Commissioner (OAIC) is responsible for enforcing the privacy safeguards and privacy rules that are part of the CDR scheme and providing a complaints resolution service for individuals and small business.

CDR is intended to be applied across all sectors of the economy over time. Since its implementation, CDR has been applied in the banking sector (also known as “open banking”) and, in late 2022, took effect in the consumer energy sector. As at the beginning of 2023, CDR is being rolled out in the telecommunications sector. The Australian government intends to implement CDR in one new sector each year. The next sector to which CDR will be applied after telecommunications is the non-bank lending sector.

The Australian government undertook a review of the effectiveness of the CDR regime in 2022. The review found that CDR is an appropriately supported data-driven innovation with the potential for enhancing competition in the sectors to which CDR is applied. There were, however, concerns raised including for example, that a “sector by sector” roll out may not reflect business models; on occasions friction between the regulators with responsibility for the scheme created difficulties for participants (such as through the receipt of inconsistent advice); and also in relation to the complexity of the scheme, particularly in relation to the process for accreditation of data recipients.

The review made 16 recommendations. These ranged from taking steps to encourage innovative use cases, to banning screen scraping in sectors where CDR is a viable alternative, to focussing on improving functionality and data quality in sectors that are already designated, rather than moving forward too quickly with other designations. The review also suggested that there could be greater interaction between CDR and the broader digital economy, including by avoiding duplication in areas such as digital payments and digital identities.

Regulation of Digital Payments and Digital Wallets

Digital payments and digital wallets are not directly regulated. Nonetheless, the Australian government has been actively considering payment system reforms, including in the context of digital payments and digital wallets. See below for a number of examples.

- On 30 August 2021, the Australian Treasurer released a report of the findings of the Treasury's Payment System Review. This noted, amongst other matters, that digitalisation of payments, while creating many benefits, also resulted in new risks and regulatory challenges. It was, however, beyond the scope of that Review to make any recommendations regarding the manner in which those challenges should be addressed.
- In late 2021, a report on Mobile Payment and Digital Wallet Financial Services was released by the Parliamentary Joint Committee on Corporations and Financial Services. The report pointed to significant market changes, with multinational technology firms becoming very important providers within Australia's payment systems. The report concluded that these market changes meant that Australia's payment systems regulation is no longer fit for purpose and recommended that this be urgently reviewed.
- With the change of government in early 2022, the Treasury commenced consultation in December 2022 on A Strategic Plan for the Payments System. The plan that is to be implemented following the consultation is intended to ensure that Australia's payment systems regulation provides for the security of Australia's systems, promotes competition and protects Australians from harms, particularly scams and fraud. The consultation will look at developments in the broader digital

economy, including but not limited to in the context of digital wallets, buy-now-pay-later (BNPL) businesses and crypto-assets.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Under Australian law, infrastructure used for certain data processing and storage services is considered to be critical infrastructure and such services are subject to additional government oversight. As the Australian government has sought to ensure public trust in the provision of its own services, including to ensure that Australians are willing to provide their data to the government, additional requirements are also imposed on, for example, providers of hosting services to the Australian government. Sector-specific obligations have been imposed by other regulators.

The government has foreshadowed that, as part of the updating of its cybersecurity strategy that will be undertaken over 2023, it is considering implementing additional rules that will impact cloud and edge computing, such as additional data localisation requirements (which would require data to be held in Australia).

The Security of Critical Infrastructure Act 2018 (Cth)

The Security of Critical Infrastructure Act 2018 (Cth) (the "SOCI Act") is Australia's primary critical infrastructure regulation. There are 11 critical infrastructure sectors, and an additional number of categories of critical infrastructure assets. As well as sectors such as transport, water and energy, the regulated sectors include:

- communications (though noting that telecommunications infrastructure remains largely subject to separate telecommunications specific regulation);
- data storage or processing;
- financial services and markets; and
- space technology.

Data storage or processing sector and assets

The critical data storage or processing sector provides services enabling end-users to store or back-up data using information technology or data processing services. Critical data storage or processing assets include enterprise data centres, managed services data centres and the like where the primary business offering is to government or to private sector critical infrastructure asset operators.

Data storage or processing services are critical to maintaining the supply and availability of data and cloud services and are increasingly relied upon by, and facilitate the effective functioning of, government and industry. In introducing the amendments to the SOCI Act to include this sector as a critical infrastructure sector in late 2020, the Australian government indicated that it was concerned not only because cyber breaches impacting this sector may result in the disclosure of highly sensitive and confidential information but also because significant outages may create risks for business continuity.

General obligations

While the SOCI Act defines critical infrastructure sectors, it primarily regulates critical infrastructure assets. The key obligations under the SOCI Act are (though some have not taken effect as at early 2023 and some apply only to particular critical assets categories):

- relevant regulated entities must provide information about critical infrastructure assets to the Australian government for inclusion in a non-public register;
- particular types of cybersecurity incidents involving critical infrastructure assets are required to be reported to the government;
- a government “assistance” regime applies under which, if a regulated entity suffers a cybersecurity incident, the government is able to collect information, direct entities to take particular action and request government agencies to provide support;
- risk management plans are required to be implemented for particular types of critical infrastructure assets; and
- where an asset is a system of national significance, additional cybersecurity obligations may also be applied.

The information that must be provided for the register referred to above will include, where the responsible entity for a particular critical infrastructure asset does not itself maintain certain data (such as personal information, research and development data, operational system data and the like), information about its service providers, including providers of cloud services, and where data is held.

Risk management plans that will be required under the SOCI Act will identify and manage material risks of hazards occurring to the relevant critical infrastructure assets. While the definition of hazards is broad, it does include cyber and information security, for example, risks to digital systems, computers and data sets.

Accordingly, even for critical infrastructure assets outside of the data storage or processing sector, the management of risks related to

cloud computing and data storage services are very important under the SOCI Act.

Hosting Certification Framework

The Digital Transformation Agency (DTA) is the Australian government agency with primary responsibility for strategic advice on whole of government IT and digital services delivery. It has implemented a Hosting Certification Framework, which is essentially a procurement mandate rather than a legislative instrument.

The Framework requires that Australian government agencies must use certified service providers when procuring hosting arrangements for high value government data, whole of government systems or government systems classified as “protected” under the government’s information classification framework. For impacted service providers, certification is therefore a critical pre-condition to dealing with the government.

The categories of service providers that are within the Framework are primarily:

- data centre providers;
- cloud services providers; and
- software-as-a-service providers.

There are two levels of certification, namely (i) strategic and (ii) assured. Strategic is the higher level of certification and therefore providers seeking this certification must meet higher standards. Data sovereignty is a relevant consideration, with providers being required to agree to a level of government control over changes in strategic direction, operation and ownership to obtain certification.

Sector Specific Regulation

Prudential standards issued by the Australian Prudential Regulatory Authority (APRA) impose

information security and outsourcing requirements on APRA regulated entities in the banking and insurance sectors. For example, risks associated with using cloud computing services must be identified, assessed, managed and reported on under Prudential Standard CPS 231 Outsourcing. This Standard is expected to be replaced in early 2023 by a new Prudential Standard CPS 230 Operational Risk Management, which will set out minimum standards for managing operational risk.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

There is surprisingly little direct regulation of either artificial intelligence (AI) or big data under Australian law.

Intellectual Property

Australian copyright law, the Copyright Act 1968 (Cth) (the “Copyright Act”) protects literary, dramatic, musical and artistic works. It does not recognise intellectual property rights in data per se; nor does it protect copyright in computer generated work, and in that respect differs from other jurisdictions such as the United Kingdom.

Under Australian law, to obtain protection, a work must be original and created by a human author. Therefore, even if copyright could subsist in an AI created work, it would not be attributed to the artificial intelligence that created it but to an individual, presumably the creator of the algorithm that generated the work.

There are, in any event, difficulties in obtaining copyright protection for AI created works because of the need for works to be “original”.

A key case which considered this issue was *Telstra Corporation v Phone Directories Company* (2010) 194 FCR 142. That case looked at the question of whether copyright existed in telephone directories created largely by an automated computerised process. The Federal Court rejected the argument that copyright existed in the telephone directories, on the basis that there was not a sufficient element of independent intellectual effort in the creation of those directories to conclude that they were “original”.

Protection for AI generated inventions is also not provided under Australia’s Patents Act 1990. In *Commissioner of Patents v Thaler* [2022] FCAFC 62, the Federal Court held that a human inventor is required for a successful patent application.

AI, Big Data and Australia’s Privacy Act

Australia’s Privacy Act does not contain any provisions that directly regulate the use of personal information in the context of AI or big data. The privacy regulator, the OAIC, has released a “Guide to data analytics and the Australian Privacy Principles” which sets out recommended best practice for data analytics involving personal information. The Guide recommends that de-identified data is used where possible, privacy by design approaches are implemented, privacy impact assessments are undertaken, and a position of openness and transparency is adopted in relation to the use of personal information.

The Australian government is, as at the beginning of 2023, undertaking a review of the Privacy Act, which may result in the introduction or more specific regulation of AI and big data. In the Government’s Privacy Act Review Report, the Government has sought views on whether, to increase transparency, regulated entities should be obligated to state in their privacy policies if personal information collected by the entity will

be used in any automated decision-making process that has a legal or other similarly significant effect.

That Report also proposes that the reformed Privacy Act will include additional protections, for example, rights for individuals to obtain information about how substantially automated decisions with legal or similar significant effects are made.

Other Government Guidance

Though law and regulation in the area of AI and big data is limited, guidance material has been issued which may be used by both the private sector and government agencies.

Each of the Australian government and the New South Wales government ombudsmen have released guides regarding the use of big data and AI. Although aimed at governments, both guides provide useful rules for application in the private sector, including to ensure that appropriate consideration is given in the design stages for the relevant project – to ensure that the types of decisions that are made using AI or big data are suitable for automation, automation processes are unbiased and that the information used is accurate.

The Australian government has also released “Australia’s AI Ethics Principles” which sets out eight principles for the use of AI, including for example that AI systems should be “inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups”.

The federal Department of Industry, Science and Resources is consulting, at the beginning of 2023, to make impact assessments compul-

sory for certain AI or automated decision-making processes used by federal agencies.

Use of AI and Big Data by Government Agencies

The Australian government's own use of AI and big data has in some cases been problematic. In *Katherine Prygodicz & Ors v Commonwealth of Australia* (No 2) [2021] FCA 634, the Federal Court held that the Australian government's use of the so called "Robodebt scheme", which used automated processes to calculate whether overpayments of social security benefits had been made and to claim repayments, was unlawful. The Robodebt scheme is, as at the beginning of 2023, subject to a Royal Commission investigation, and it is likely that the failure of this scheme will limit to some extent the appetite of the Australian government to use AI, at least in the short term.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Australia does not have specific laws that solely govern internet of things (IoT) products and services. Providers of IoT products and services are subject to generally applicable laws and regulations, including the Privacy Act, general consumer protection laws such as prohibitions on misleading and deceptive conduct under the Australian Consumer Law and, where telecommunications services are provided with IoT devices, potentially also regulation as carriage service providers under the Telecommunications Act and other telecommunications laws.

Privacy Act Review

While, as at the beginning of 2023, the Privacy Act does not include specific provisions regulating IoT devices, the review of that legislation which is being undertaken by the Australian government may change this.

In the Privacy Act Review Report released for consultation by the Australian Attorney General in late February 2023, amongst other matters, stakeholder views were sought on the following proposals.

- That the Privacy Act should be amended to require that the collection, use and disclosure of personal information is only permitted where it is fair and reasonable in the circumstances, to bring Australia's privacy legislation more in line with legislation in other jurisdictions, such as the GDPR. It is contemplated this would have the potential to significantly impact businesses that provide IoT products and services. In those cases, a higher standard of privacy protection would be expected by objective reasonable individuals, particularly where sensitive information is collected through IoT devices.
- That regulated entities that undertake certain high risk practices, such as the collection, use or disclosure of sensitive information or children's information on a large scale (which would be likely to include providers of IoT products and services) should be subject to an obligation to undertake a privacy impact assessment prior to the commencement of the high risk activity. This is intended to ensure that privacy risks are identified and appropriate mitigation strategies adopted.

IoT Code of Practice

In September 2020, as specified in Australia's Cyber Security Strategy 2020, the Australian

government released a Code of Practice for “Securing the Internet of Things for Consumers”. The Code of Practice, which was stated by the government to be a “first step” in a process to improve the security of IoT devices, is a voluntary code. It was intended to reflect international approaches, such as the European Telecommunication Standards Institute (ETSI) baseline standard on smart devices, ESTI EN 303 645.

The Code of Practice contains 13 principles, which are very general in nature. At the time of the release of the Code of Practice, the government encouraged industry to prioritise compliance with the following three principles.

- No duplicated default or weak passwords – this principle applies to device manufacturers and requires that IoT device passwords should be strong, not resettable to factory defaults and that web services associated with IoT devices should use multi-factor authentication.
- Implementation of a vulnerability disclosure policy – this principle applies not only to device manufacturers but also to IoT service providers and app developers. It requires the establishment of a public vulnerability disclosure policy.
- Keep software securely updated – like the principle immediately above, this applies to device manufacturers, IoT service providers and app developers. This principle requires that software both on IoT devices and for associated web service should be securely updateable and consumers given express information regarding minimum times for software update commitments.

The Australian government assessed the effectiveness of the Code of Practice after its first six months of operation. The Code was not

viewed favourably. The major manufacturers the government consulted with had largely not implemented even those principles that were fairly straight forward, such as to put in place a vulnerability disclosure policy. Those manufacturers expressed concern that, as the principles were high level, they were difficult to implement. The Australian government was also concerned that, in their assessment process, they had difficulty in obtaining feedback from manufacturers of lower cost IoT devices, suggesting that such providers were even less likely than the major manufacturers to comply with the voluntary Code of Practice.

Given the low levels of compliance with the Code of Practice, the Australian government undertook public consultation on whether the Code of Practice should be replaced with a mandatory standard, which would be likely to be ESTI EN 303 645 (or, at a minimum, the top three requirements of that standard). To implement that approach would require new legislation to be passed. As at the beginning of 2023, no action has been taken following that consultation process.

In late 2022, the Minister for Home Affairs and Cybersecurity, Clare O’Neil, announced that the government would develop a new cybersecurity strategy, with the aim of making Australia the “most cyber-secure” country in the world by 2030. The Minister also indicated that, despite pressure from some stakeholders, no action will be taken to adopt a mandatory standard until that new cybersecurity strategy is in place. The timing for that to occur is not yet clear.

The Minister released a discussion paper on the new cyber security strategy in late February 2023 and it is expected to be finalised in August 2023.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

The Broadcasting Services Act 1992 (Cth) (BSA) is the primary legislation regulating audio-visual media services in Australia, though the Radiocommunications Act 1992 (Cth) (the “Radcomms Act”) and the Online Safety Act are also key.

Scope of the BSA

Commercial free-to-air broadcasters, both television and radio, require licences issued under the BSA to operate. Licences apply in specific areas. In addition to complying with the BSA and licence conditions, each of the television and radio broadcasting sectors have implemented, and must comply with, a code of practice, which is registered by Australia’s communications sector specific regulator, the Australian Communications and Media Authority (ACMA).

It is not possible for a new commercial television broadcaster to commence operation in Australia, given the restrictions imposed under the BSA on the issue of new commercial television broadcasting licences. While it is possible to obtain new commercial radio licences, these are available only in limited circumstances. Commercial broadcasters licensed under the BSA are entitled to licences of spectrum under the Radcomms Act. While fees are not payable for commercial broadcasting licences under the BSA, fees are payable for licences under the Radcomms Act. As at 2023, these fees, which are known as a Commercial Broadcasting Tax, raise in aggregate approximately Australian AUD46 million per annum.

Subscription television broadcasters must also obtain licences under the BSA (and for spectrum the Radcomms Act). Unlike free-to-air

broadcasting licences, these licences are not geographically limited. Generally, these broadcasters are regulated in a similar manner to commercial-free-to-air television broadcasters under the BSA.

The BSA also regulates Australia’s two national broadcasters, the Australian Broadcasting Corporation (or ABC) and the Special Broadcasting Service (or SBS) and community broadcasters.

Providers of online audio-visual media services are currently not required to obtain licences under the BSA and are subject to only very limited obligations under that Act.

Ownership Restrictions

The BSA incorporates the following cross-media ownership restrictions (which apply only to ownership of broadcasters and print media):

- only one television licence and two radio licences may be in common ownership in the one area; and
- metropolitan areas must have five media “voices” (across television, radio and print) and regional areas must have four.

The acquisition of an interest in any Australian media business by a foreign person (including any foreign government entity) requires foreign investment approval under the Foreign Acquisitions and Takeovers Act 1975 (Cth). An Australian business which provides online content services would be considered an Australian media business if it was operated wholly or partly to serve Australian audiences and meets certain other tests.

The ACMA maintains a register of foreign owners holding an interest of more than 2.5% in any Australian media company.

Any mergers or acquisitions in the media sector must also comply with general competition law. Section 50 of the CCA prohibits mergers or acquisitions that would have the effect or likely effect of substantially lessening competition. There is no obligation on merger parties to notify the ACCC, though the ACCC undertakes informal merger reviews and parties may seek a merger authorisation prior to finalising a transaction. If a merger authorisation is granted, the transaction cannot subsequently be challenged by the ACCC under Section 50. On the other hand, if an informal merger review clearance is given the ACCC may still challenge a transaction if the ACCC subsequently changes its view and considers the transaction does in fact infringe Section 50.

Australian Content Obligations

Australian content quotas are imposed on commercial free-to-air television broadcasters and subscription television broadcasters. This is one of the key obligations those broadcasters must comply with. Free-to-air television broadcasters must broadcast at least 55% of defined Australian content between 6am and midnight on their primary channels and 1,460 hours per annum during those time periods on their secondary channels. In addition, the Broadcasting Services (Australian Content and Children's Television) Standards 2020 (Cth) imposes quota requirements (via a points system) on these broadcasters for first release Australian programmes. While there is flexibility regarding the content that may satisfy these quotas, higher points are awarded for Australian drama content.

Subscription television broadcasters are subject to a "new eligible drama expenditure" scheme. This requires that at least 10% of total programme expenditure for each drama channel must be on new Australian drama programmes.

As at the beginning of 2023, no Australian content obligations are imposed on providers of online audio-visual media services. A small number of large streaming services providers (Amazon Prime, Disney, Netflix, Paramount+ and Stan) are required to report their level of investment in Australian content to the ACMA.

The Australian government's new National Cultural Policy, released in late January 2023, provides for Australian content quotas to be imposed on streaming services. Consultation on the form the content quotas will take will be undertaken over the first six months of 2023, with the new regime to be implemented from 1 July 2024.

Advertising and Other Content Restrictions

In some cases, very similar regulation is imposed on content service providers, whether these are broadcasters or streaming services providers. One such case is the regulation of gambling advertising, which is restricted during both live sports broadcasts and, through the operation of Schedule 8 of the BSA, when sports are live streamed.

The Online Safety Act contains an online content scheme which enables the eSafety Commissioner to mandate the take down from regulated services (which includes services provided by a broad range of online content providers) of content that would under Australian law be classified as:

- "RC" (refused classification) or "X 18+" (restricted content which may only be distributed in limited circumstances); or
- R 18+, where access to that content is not subject to a restricted access system that limits access to those over 18 years of age.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Telecommunications Service Providers

Two primary types of telecommunications services providers are regulated under Australian law:

- carriers, that is owners of infrastructure used to provide carriage services to members of the public; and
- carriage service providers (or CSPs), who provide carriage services to others, either on a wholesale or retail basis.

Licences and Approvals for Carriers

Under the Telecommunications Act 1997 (Cth) (the “Telco Act”) before core telecommunications infrastructure (fibre or radiocommunications facilities) may be used to supply carriage services to the public, a carrier licence must be obtained by the owner. Alternatively, a nominated carrier declaration may be obtained. This enables a third-party carrier, that is not the owner of the infrastructure, to act as the carrier for that infrastructure provided that third party agrees to comply with the regulatory obligations imposed on carriers for that infrastructure.

Carrier licences and nominated carrier declarations are granted by the ACMA (with the application fee for a carrier licence set at approximately Australian AUD2,000). Before a carrier licence may be granted, the ACMA must consult with the Communications Access Co-ordinator, which considers national security issues in relation to the grant of such a licence.

In addition, as telecommunications infrastructure is considered to be critical infrastructure under Australian laws, foreign investment approval is

required not only for a foreign person to acquire a direct interest in a carrier (or relevant infrastructure) but is also required to commence a carrier business. There are no monetary thresholds for these approvals.

Commencing Operations as a Carriage Service Provider (CSP)

CSPs are not required to obtain a licence under the Telco Act before commencing operations. However, where a CSP is a nominated CSP under the Telecommunications (Interception and Access) Act 1979 (Cth), meaning that the Attorney General has determined that it is a critical CSP, then the foreign investment approval rules for carriers apply to that nominated CSP.

The definition of CSP in the Telco Act is broad. It is not necessary for a CSP to own either the fixed line, mobile or satellite infrastructure that is used to provide carriage services for a telecommunications services provider to be classified as a CSP. In some cases (which are increasingly common as the IoT sector develops), intermediaries who arrange for another CSP to provide services to a third-party customer will also be considered to be CSPs, where that intermediary receives consideration for the provision of the service to the third-party customer and maintains the ongoing relationship with that third-party customer.

Spectrum Licences for Mobile, Fixed Wireless and Satellite Carriage Services

Under the regime established by the Radcomms Act, the ACMA is responsible for licensing spectrum, by means of spectrum, apparatus and class licences. Carriers are not guaranteed any allocation of spectrum and must acquire any relevant spectrum or apparatus licences, or satisfy the requirements to use any applicable class

licence, to provide mobile, fixed wireless and/or satellite telecommunications services.

Spectrum licences for mobile services apply in specific geographic areas. These are generally auctioned by the ACMA for licence terms of 15 years. Apparatus licences are required for transmitters and receivers and are usually granted for one-year terms on a renewals basis. Class licences may be used by any person, without any separate approvals being required, provided that the licence conditions are satisfied. Class licences are relevant to some telecommunications services, for example, the Radiocommunications (Communication with Space Object) Class Licence 2015 (Cth) is relevant for satellite telecommunications services.

Ongoing Regulatory Obligations Imposed on Carriers and CSPs

The regulatory obligations imposed on carriers and CSPs can broadly be split into four categories:

- technical, for example, interoperability requirements, numbering allocation and the like;
- competition related, for example, certain access obligations may be imposed on carriers;
- customer-focussed obligations; and
- national security and law enforcement related requirements.

In the case of customer-focussed obligations, these are most onerous in relation to services provided to consumers and small businesses. In addition to complying with the economy wide obligations under the Australian Consumer Law, there are telecommunications consumer specific regulations that must be complied with from the time that services are first offered by a CSP

to the public. These rules are incorporated not only in the Telco Act but also codes put in place under the co-regulatory regime established pursuant to the Telco Act. The most important code is the Telecommunications Consumer Protections Code. That Code contains a broad range of rules including in relation to the content of customer contracts, invoicing, financial hardship and dealing with disputes. Telecommunications companies that provide consumer and small business services must report annually on their compliance with the Code and must (as must carriers) join to the Telecommunications Industry Ombudsman scheme, which provides a dispute resolution service.

National security and law enforcement-related regulation must also be complied with from the time that services are first provided. For example, carriers and CSPs must maintain “interception capability” in respect of telecommunications services to allow for lawful interception to occur, unless an exemption is available. These arrangements must be in place from the commencement of service provision.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

There are a variety of challenges that are faced when technology agreements are entered into with Australian government entities or businesses. For governments, typically standard form technology agreements are required to be used and additional obligations may be imposed depending on the nature of the services that are provided. When agreements are entered into with private sector entities, a variety of different obligations are required to be considered,

ranging from directors' duties to small business protections under the Australian Consumer Law.

Sector specific obligations are also imposed, some of which are considered in **3. Cloud and Edge Computing**.

Technology Contracts With Government Entities

At the federal level, there are no general mandated forms of technology agreement that all agencies are required to use. However, there are particular guidelines that are required to be adopted. For example, the Australian Cyber Security Centre (part of the Australian government's Australian Signals Directorate) has guidelines that apply for cyber supply chain risk management which may be applied not only by government agencies but also private sector entities in procuring technology services.

At a state and territory level, it is common for governments to mandate not only an approved list of providers for their agencies but also to specify the forms of contracts that must be used. For example, in the case of New South Wales, the government's procurement agency, Buy NSW, has implemented an ICT Services Scheme that agencies must use when procuring ICT goods and services which aligns with that government's digital strategy.

Directors' Duties

It may be a breach of directors' duties where Australian corporates do not adequately manage cybersecurity-related risks and therefore this is a key issue that Australian corporates seek to manage when entering into technology agreements.

The potential scope of the obligation to manage cyber-risks was highlighted in *Australian Securities*

and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496. While that case did not involve a breach of directors' duties, it indicates the attitude of Australia's corporate regulator, the Australian Securities and Investments Commission (ASIC), to the responsibilities of corporates (and directors) to the management of cyber-risks. In that case, ASIC took action against RI Advice in relation to a number of cyber incidents that impacted RI Advice over the period 2014–20.

There is not an absolute obligation on Australian corporates to avoid any cybersecurity incidents. However, ASIC alleged that the failure of RI Advice to implement a programme to improve its cybersecurity and cyber-resilience policies and procedures to minimise the possibility of such incidents occurring breached the Australian financial services licence (AFSL) that providers of financial advice are required to hold. Consent orders were made under which RI Advice admitted to these breaches.

Data Localisation

The Privacy Act does not require that personal information held by a regulated entity is held in Australia. Instead, it provides that if a regulated entity discloses personal information to a person outside Australia who is not bound by the Privacy Act it must, unless an exemption applies, take reasonable steps to ensure that the offshore recipient does not breach relevant Australian Privacy Principles included in the Privacy Act and will be directly liable for any breaches that may occur.

Importantly, where a regulated entity has outsourced its data storage to a third-party provider, such as a cloud services provider, the OAIC is likely to consider that the regulated entity continues to hold its data (including personal informa-

tion) on the basis that the third-party provider must deal with the data in accordance with the directions of the regulated entity, even though the regulated entity does not physically possess the information. While this may mean that the requirements of the Privacy Act dealing with offshore transfers do not apply, the regulated entity will remain directly liable in relation to the management of the personal information. This means that Australian businesses (and Australian government entities) impose strict requirements in contractual arrangements for the storage of data.

While there are no generally mandated data localisation requirements, there are specific localisation requirements that apply in particular circumstances, which will need to be taken into consideration in technology agreements that involve data storage. For example, most Australian states and territories have privacy legislation that applies to the state or territory public sector and, in some cases, private sector health providers. In some cases, this privacy legislation includes restrictions on disclosing personal information outside the relevant jurisdiction. This applies, for example, under the New South Wales Privacy and Personal Information Protection Act 1998. That Act restricts public sector agencies disclosing personal information to an entity outside New South Wales unless a listed exemption applies.

The Hosting Certification Framework, as discussed in **3. Cloud and Edge Computing**, provides for data sovereignty, but does not impose data localisation requirements. In late 2022, the Minister for Home Affairs indicated that as part of the government's proposed new cybersecurity strategy it will look very carefully at data localisation. Should the Australian government mandate data localisation requirements for the

storage of any particular categories of data in future, it is likely that such requirements will also be more frequently required not only by the public sector but also by private sector entities in their technology agreements.

Other Statutory Requirements: Unfair Contract Terms

Many technology services providers use standard form contracts for providing technology services to small businesses and will not agree to modifications of those contracts. Great care must be taken to ensure that those standard form contracts do not include terms that would breach Australia's prohibition on unfair contract terms.

Under the Australian Consumer Law, both standard form consumer contracts and standard form small business contracts must not contain unfair contract terms. An unfair contract term is one which gives a supplier a significant advantage over the customer, is not necessary to protect the legitimate interests of the supplier and would cause financial or other harm to the customer if enforced.

The ACCC has taken action in relation to unfair contract terms in the technology sector. For example, in 2022, it successfully took action against Fuji in relation to terms of its printer and related software contracts. Those unfair contract terms provided for automatic contract renewal, high termination fees and gave Fuji the ability to unilaterally increase prices.

In late 2023, amendments to the Australian Consumer Law will take effect which will mean that not only are unfair contract terms void, but businesses that include these in their standard form contracts will be subject to penalties. This new penalty regime will make compliance with

the regime by technology providers even more important.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Electronic Signatures and Trust Services

In Australia, legislation exists at both a state/territory and federal level regulating the use of electronic signatures. These laws are on consistent terms with the federal law, the Electronic Transactions Act 1999 (Cth) (the “ET Act”).

Under the ET Act, a requirement under a law of the Commonwealth to sign a document can be met by means of an electronic communication, subject to some specific exceptions. For example, the ET Act does not apply to the submission of documents or evidence to a Commonwealth court or tribunal, which is instead regulated under the Evidence Act 1995 (Cth). Other exclusions from the ET Act include documents relating to passports, voting and the electoral roll.

There is no requirement under the ET Act that an electronic signature take a particular form. The ET Act requires that the person signing, and their intention, are identified using a method that meets particular criteria. The method must be as reliable as appropriate in the circumstances or factually satisfy the requirements of identifying the person and their intention. If the signature is given to a Commonwealth entity, the method used must satisfy the entity’s information technology requirements (if any) or otherwise must have the consent of the recipient of the signature.

Real estate transactions are governed by state and territory laws, and therefore are not regulated under the ET Act. While there are no government endorsed trust services, a national electronic conveyancing scheme has been adopted, known as PEXA (Property Exchange Australia), which allows for agents (solicitors and conveyancers) to digitally sign property transaction documents on behalf of their principals.

Australia’s primary corporations legislation, the Corporations Act 2001 (Cth) (the “Corporations Act”), governs the use of electronic signatures by companies. Amendments to the Corporations Act that took effect in early 2022 enable documents, including deeds, to be executed electronically by companies. The Corporations Act is on the same terms as the ET Act, that is, it does not mandate that an electronic signature take a particular form. Instead, the person signing, and their intention, are required to be identified using a method that meets particular criteria, which are the same as those set out in the ET Act.

While, as noted above, there is no government endorsed trust services specifically for electronic signatures in Australia, the Australian government does operate the Trusted Digital Identity Framework (TDIF) which is an accreditation framework for digital identity services for the Australian government. At the current time, private sector entities cannot obtain accreditation under the TDIF for the provision of digital identity services within the Australian government’s digital identity scheme, which is discussed below.

Digital Identity Schemes

The Australian government has implemented a digital identity scheme known as “myGovID”. As at the beginning of 2023, this scheme enables individuals, following an initial identity verification process, to access approximately

80 Australian government services, such as the Australian Taxation Office and Centrelink (social security services) and a very limited number of state government services, without the need to re-verify their identity.

In its current form, the myGovID scheme has significant limitations as it cannot be used for all Australian government services. It also cannot be used to verify identity for most state and territory government services or for services provided by the private sector. To address this deficiency, and to provide for strengthened protections for individuals and establish clearer governance arrangements, in late 2021 the Australian government commenced consultation on a draft “Trusted Digital Identity Bill”. That Bill (and its supporting instruments) provides for significant enhancements to the myGovID scheme, including by providing:

- an accreditation scheme to allow state and territory governments as well as private sector entities to be accredited to provide digital identity services; and
- the ability for state and territory governments and private sector entities to participate in the digital identity scheme by allowing their customers to verify their identity using the scheme.

The Bill would also create an independent statutory office holder, to be known as the “Oversight Authority” with responsibility under the new regime including for example to accredit entities to provide the digital identity services and to take enforcement action for breach of the law. Additional privacy, security and other protections were provided to consumers under the Bill to seek to promote public confidence in the operation of the new regime.

The new Australian government elected in early 2022 has not explicitly adopted the former government’s approach. In late February 2023 the new government announced proposals for a new digital ID scheme, which will be voluntary and includes both identity and credentials. It will be based on a New South Wales scheme that has been in development over a period of time.

Holding Redlich is a national Australian firm, with significant experience in the areas of technology, media and telecommunications. This experience also covers related areas including data and privacy. The firm acts for a broad range of clients, including government, media companies, communication services providers, technology companies and industry bodies. Its knowledge of the law, and experience of the Australian regulatory environment and relationships with government agencies and regulators, assists it in working with clients to: provide

advice and transactional assistance to ensure clients protect their commercial interests, and comply not only with current law but also future regulatory requirements; engage with Australia's regulators to obtain necessary licences and approvals as well as in engaging to resolve potential regulatory breaches; and develop cutting edge regulatory proposals and carefully balanced submissions to government responding to legislative reform consultation processes, as Australian law continues to evolve to address the challenges of the digital age.

Authors



Angela Flannery is a partner with Holding Redlich. Angela has over 20 years' corporate law experience in both transactional and regulatory matters, with a focus on data,

telecommunications, media and technology. Angela's experience includes assisting clients in making submissions to government consultation processes on regulatory reform (particularly in the area of digital markets), providing advice to government agencies in investigations and regulatory enforcement (including regarding privacy regulation), and advising corporates regarding compliance with the Competition and Consumer Act, the Telecommunications Act, the Broadcasting Services Act and competition, consumer protection and privacy issues relating to telecommunications, technology and ad tech.



Andrew Hynd is a partner in the firm's corporate and commercial group, with specialist experience in IT, innovation and procurement. He has over 20 years' experience acting for a

range of public and private sector organisations on IT projects, especially software licensing, implementation and support, cloud services and privacy and data advice. He also advises local and international clients on privacy compliance issues and matters relating to data, including value capture, management, security and breaches. Andrew is a member of the Local Government Association of Queensland's Data Ethics Panel.



Dan Pearce is a general counsel in the firm's corporate and commercial group, having retired from the partnership after more than 20 years. He has deep experience advising on all

aspects of IT, intellectual property, media and related corporate and regulatory issues, including competition and consumer law, privacy and data governance, broadcasting, defamation and other legislative compliance. Dan is currently a councillor for the Australian Information Industry Association (AIIA), Victorian Branch, and is a member of the Intellectual Property Society of Australia and New Zealand.



Ian Robertson is an experienced corporate, commercial, media and regulatory lawyer who advises Australian and overseas clients across a number of industries, particularly in the

media, entertainment and technology sectors. Ian's expertise includes advising on public policy, governance and regulatory issues, advising advertising agencies on commercial and compliance issues, acting for media businesses in respect of regulatory matters, and advising on all aspects of screen production and distribution. Ian is a member of the Communications and Media Law Association of Australia and a Fellow of the Australian Institute of Company Directors.

Holding Redlich

Level 65
25 Martin Place
Sydney
NSW 2000
Australia

Tel: +61 2 8083 0388
Email: inquiries@holdingredlich.com
Web: www.holdingredlich.com



HOLDING REDLICH

Trends and Developments

Contributed by:

Angela Flannery, Andrew Hynd,
Dan Pearce and Ian Robertson
Holding Redlich see p.37

TMT in Australia: an Overview

2023 will be a year of regulatory upheaval in the communications sector in Australia. The election of a new Australian government in 2022 heralded a renewed focus on reform in a broad range of areas in the sector, including in digital platform services markets, media and cybersecurity.

Digital Platform Services

Background

The Australian Competition and Consumer Commission (ACCC – the economy-wide competition and consumer protection regulator) has undertaken a number of inquiries into digital services markets since 2017. These inquiries have included:

- the ground-breaking Digital Platforms Inquiry (finalised in 2019);
- the Digital Advertising Services Inquiry (also known as the Ad Tech Inquiry), finalised in 2021; and
- the ongoing 5 Year Digital Platform Services Inquiry (5 Year Inquiry), where reports issued every six months set out the results of the ACCC's inquiries in a broad range of different digital platform services markets.

These inquiries have identified a range of different competition and consumer harms in different digital platform services markets. Over time, as a result of these inquiries, the ACCC has recommended a range of different regulatory reforms to address those concerns, some of which have already been implemented.

For example, to address bargaining power imbalances between Australian news media businesses and the largest digital platforms (Google and Facebook), which had resulted in the digital platforms using the content produced by those news media businesses at no cost, the innovative Mandatory News Media Bargaining Code was enacted in 2021. While that Code is not in effect (as no digital platforms have been designated under the regime), its enactment pushed Google and Facebook to the bargaining table, and agreements were subsequently entered into by those platforms that resulted in Australian news media businesses receiving payment for their content for the first time.

On the other hand, some reforms the ACCC has recommended have taken longer, such as the reform of Australia's Privacy Act 1988 (Privacy Act) to address the increasing amounts of data that are collected from Australians online. In that case, the then government commenced the reform process in late 2019, but the complexity of addressing different issues and stakeholder concerns has resulted in delays, although it is expected that the reform may be finalised in the course of 2023.

Ambitious regulatory reform

In November 2022, the ACCC released a report (Regulatory Reform Report), prepared as part of the 5 Year Inquiry, outlining the most ambitious regulatory reforms in the digital platform services sector proposed by the ACCC to date. At the time of the report's release, the Chair of the ACCC, Gina Cass-Gottlieb, noted that, while

digital platform services provide many benefits, the expansion of these services has created risks and harms that Australia's competition and consumer protection laws are not well placed to address.

The ACCC is particularly concerned that enforcement action under the Competition and Consumer Act 2010 (Cth) (CCA – Australia's primary competition and consumer law) is not effective in this sector. Enforcement action takes a long time, with court cases taking many years to resolve, and it is expensive. In addition, because enforcement action may only be taken in relation to specific identified conduct, and in these dynamic markets new forms of harm may arise quickly, enforcement action may not be a sufficient deterrent to anti-competitive conduct.

The reforms that the ACCC has proposed are in the following three areas.

- Consumer protection reforms, such as regulation to reduce the risks to consumers from the scam advertising that proliferates on a majority of digital platform services, particularly social media services, and the introduction of a consumer and small business ombudsman scheme for the resolution of disputes.
- Competition reforms applying to specific digital platform services, with the model recommended by the ACCC being centred on ex-ante regulation in the form of mandatory codes. Those codes would address conduct such as anti-competitive self-preferencing and tying and bundling arrangements, as well as issues such as data advantages and transparency.
- Economy-wide reforms: the ACCC recommended expansion of Australia's unfair contract terms regime, which voids unfair

terms in standard form contracts used for products and services provided to consumers and small business. It also recommended the introduction of a prohibition on unfair trading practices, which would address conduct that does not otherwise currently breach the Australian Consumer Law – eg, action to discourage consumers from exercising their contractual rights. The ACCC concluded that these reforms should be applied economy-wide as the issues the ACCC had identified in digital platform services markets that would be addressed by these reforms are prevalent across the economy.

The reforms proposed by the ACCC in the Regulatory Reform Report do not address mergers, as the ACCC is likely to propose a range of economy-wide merger law reforms to the government later in 2023.

A spotlight on proposed competition law reforms

The ACCC's proposal for competition law reforms in the digital platform services sector recommends the adoption of service-specific codes. In this sense, the ACCC's proposals are an interesting hybrid of the regime established under the European Union's Digital Markets Act (DMA) and the (yet to be enacted) UK digital platform reforms.

The DMA will directly regulate the conduct of designated "gatekeeper" platforms in a number of specific markets. The DMA includes:

- prohibitions on tying arrangements (through the imposition of prohibitions on terms that require business users to also use ancillary services);
- prohibitions on self-preferencing, including in rankings; and

- requirements for certain hardware and software interoperability, so that users are not “locked into” specific digital ecosystems.

While the ACCC’s reforms propose to address similar issues to those covered by the DMA, this will occur through the development and implementation of mandatory codes that are put in place under the CCA. The view of the ACCC is that codes will be more flexible, as required in changing digital platform services markets, and will also be able to be highly targeted by applying only to specific dominant platforms. In this sense, the ACCC’s proposals are closer to the proposed UK regime, which will allow the Digital Markets Unit within the UK’s Competition and Markets Authority to determine conduct requirements for designated platforms with “strategic market status” and also to make targeted pro-competitive interventions.

Next steps for implementation of reforms

The Australian government commenced consultation on the Regulatory Reform Report in late December 2022. There is no stated timeframe for the implementation of any reforms following the completion of that consultation process. However, as both the Australian Treasurer, Jim Chalmers, and the Assistant Treasurer responsible for competition, Andrew Leigh, have spoken of their concerns regarding the actions of the dominant digital platforms, and are keen to promote the growth of a vibrant domestic tech sector, the Australian government is expected to propose a reform package based on the ACCC’s recommendations before the end of 2023.

Media Sector Reforms

In late 2022, the Minister for Communications, Michelle Rowland, made a major speech setting out the priorities of the Australian government for reforms in the media sector. These reforms

were categorised as short-term, medium-term and long-term priorities, as follows.

- In the short term, the government will focus on Australian content regulation. Specifically, it will implement a prominence framework, to:
 - (a) ensure that Australian free-to-air television services are easy to find on connected devices;
 - (b) modernise Australia’s anti-siphoning scheme, which mandates that certain major sporting events must be made available for potential broadcast on free-to-air television; and
 - (c) impose content quotas on streaming services, which are increasingly popular with Australian consumers.
- In the medium term, the Australian government will assess reform of:
 - (a) Australia’s classification scheme for movies, computer games and certain publications;
 - (b) the range of advertising regulation that applies differently to different media (for example, in the areas of election advertising); and
 - (c) consumer safeguards and protections.
- The long-term reform will focus on the “future of television”. This is likely to build on the Media Reform Green Paper released by the former Australian government, “Modernising television regulation in Australia”, which raised, amongst other issues, the prospect of free-to-air television moving to use less radio-frequency spectrum, with existing spectrum being reallocated for other, potentially more profitable, uses. A further reallocation of broadcasting spectrum, following completion of the spectrum restack that moved broadcasters to digital-only television broadcasting in 2014, is viewed as particularly contentious. Accordingly, it is no surprise that the govern-

ment has classified this reform as one to be addressed in the “long term”.

The Australian government has moved very quickly on the short-term reforms, commencing consultation processes in relation to two of the three identified areas in late 2022. Regulatory reform in all three areas is expected to be implemented during 2023.

Prominence framework

Prominence refers to the ability of consumers to locate local television services on connected TVs and other connected devices through which content is consumed.

The free-to-air television broadcasting sector has lobbied strongly for the implementation of a regulatory framework for prominence. Free TV Australia is the industry body for commercial free-to-air broadcasters, and has long called this the “number-one” issue for the sector. The concern of Free TV Australia’s members is that, unless Australian audiences have easy access to their content on smart TVs and other connected devices, audience shares will dwindle as Australians instead consume the content of international streaming service providers that is more prominent on those devices.

The Australian government has determined that a prominence framework is required to support the long-standing policy objective of ensuring that Australian audiences have access to high-quality Australian content. In short, the prominence reforms will address the concern that there is limited benefit in imposing Australian content quotas on commercial free-to-air television broadcasters if Australian audiences are not then viewing the content of those broadcasters because it is difficult to find on their devices.

The consultation undertaken at the beginning of 2023 sought feedback on a number of design elements for the prominence framework, including the following.

- What, and who, should be regulated? That is:
 - (a) what content is important – for example, only linear free-to-air broadcasting or also broadcaster video on demand (BVOD) services;
 - (b) what devices should be regulated – for example, only connected TVs or should other devices such as gaming consoles fall within the new regime; and
 - (c) who should be subject to the obligations – for example, device manufacturers only or a broader range of parties.
- What model should be adopted? The consultation proposed four models, ranging from simply requiring reporting by regulated parties to an onerous “must promote” regime, which would require regulated entities to positively promote the relevant Australian services. It is likely that, ultimately, a mid-ground approach will be adopted – ie, a “must carry” regime that would mandate that relevant devices must include the relevant Australian services, providing a specified level of prominence.
- How should the framework be implemented? Views of stakeholders were sought as to whether the framework should, for example, be included in existing legislation such as the Broadcasting Services Act 1992 (Cth), or implemented by means of a code under the CCA.

The design of the framework is expected to be released in mid-2023, with legislation introduced to parliament shortly after that.

Anti-siphoning

The government has also moved quickly to reform Australia's anti-siphoning regime. At the beginning of 2023, that regime applies only to free-to-air television broadcasters and subscription television broadcasters. In summary, subscription television broadcasters cannot acquire the rights to broadcast sports that are on the anti-siphoning list (such as particular football and cricket competitions, the Olympic Games and similar) until free-to-air broadcasters have had an opportunity to acquire those rights.

The current regime does not apply to streaming services of any type, including the broadcaster video on demand (BVOD) services of free-to-air broadcasters. This means that if, for example, a streaming service wished to acquire the exclusive rights to make available the very popular Australian Open tennis tournament, and if it could negotiate such an agreement with the responsible sports body (Tennis Australia), the Australian Open may only be available on an expensive streaming service and may not be available on free-to-air television in Australia at all. Such an arrangement would not breach the anti-siphoning rules, but would clearly breach the spirit of those rules, which is to increase the likelihood of popular sporting events being made available to be viewed by Australians at no cost.

The Australian government consulted on a number of issues, including, unsurprisingly, whether the scheme should be extended to streaming services. The question of what sporting events should be covered was also raised in that consultation process. This is of concern in part because of the gender disparity in relation to the sports included on the list, many of which, such as football and cricket, are limited to male competitions.

As new regulation to extend the operation of the current anti-siphoning regime is required to be implemented by 1 April 2023, it is expected that any reforms of the scheme will be announced before that date.

Australian content quotas for dominant streaming platforms

The one short-term priority area where the government has moved slowly is in the area of content quotas for streaming services.

Under the law as at the beginning of 2023, no Australian content quotas apply to streaming services. A voluntary reporting regime applies for the larger streaming services (for 2021/22 the services that reported were Amazon Prime, Disney, Netflix, Stan and Paramount+), under which expenditure on Australian productions is reported to the Australian Communications and Media Authority (ACMA), which makes aggregated data publicly available.

Some form of Australian content quota for streaming services, or other form of regulatory intervention to incentivise the production of Australian content, has been on the agenda of successive Australian governments for a decade or more. This issue has become increasingly important as the viewing habits of Australians continue to evolve over time, with more and more Australians accessing content online.

As part of its new National Cultural Policy, released in late January 2023, the Australian government re-affirmed its commitment to ensuring that Australian content is available to Australians, by whichever platform that content is viewed, and proposed regulation to require streaming services to invest in a variety of genres, such as children's content, scripted drama and documentaries.

However, the Policy itself did not specify what form the regulation would take or how it would be implemented. Instead, the Policy stated that consultation on the new regulation would occur over the first half of 2023, with legislation to implement the agreed model to be introduced shortly after that. The new regime would then take effect from 1 July 2024. Given content production lead times, this will not give streaming services long to commence compliance.

A Final Word on Cybersecurity Reforms

Spurred on no doubt by significant data breaches in the final quarter of 2022 involving cyber-attacks on one of Australia's largest telecommunications companies (Optus) and one of Australia's largest health insurers (Medibank), the Australian government is also proposing reform in the area of cybersecurity in 2023.

An initial reaction to those cyber-attacks, which resulted in unauthorised access to the personal information of large numbers of Australians, was that the government amended Australia's Privacy Act to provide for significantly higher penalties. Prior to the amendments being made in late 2022, the maximum penalty for serious or repeated breaches of privacy was AUD2.1 million. The maximum penalties are now set at AUD50 million (or three times the value of the benefit obtained through the misuse of information or 30% of the relevant company's adjusted turnover while the breach continued, if either is higher).

A new Australian cybersecurity strategy

In December 2022, the Minister for Home Affairs, Clare O'Neil, unveiled a range of new proposals in the area of cybersecurity, intended to assist Australia to achieve the aim of becoming one of the world's most cybersecure countries by 2030.

A key plank of the proposals is a revamp of Australia's Cyber Security Strategy.

The former Australian government's Cyber Security Strategy 2020 provides for a package of measures, including an investment of just under AUD2 billion to improve the cyberposture of Australian governments, businesses and individuals. Measures included in that Strategy were diverse, with the following examples:

- increased investment in government cybersecurity capabilities to identify, disrupt and protect against cyberthreats;
- amending the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) to cover a broader range of critical infrastructure sectors and to introduce new obligations on regulated sectors, and introducing other legislative requirements, such as reforms to the Privacy Act and data protection laws;
- progressing the development of an Australia-wide digital identity programme, to allow one form of trusted identification to be used for accessing online services and to limit the number of times Australians will need to provide their personal information online; and
- providing funding to find new ways to improve Australians' cybersecurity skills.

While progress had been made in many of the key areas of the 2020 Strategy, the Australian government believes more work is required. Therefore, it has established a new taskforce to consider a new strategy to achieve the aims of:

- strengthening critical infrastructure and government networks;
- building Australia's cybersecurity capabilities; and
- working with international partners to improve cybersecurity across the Pacific region.

In late February 2023, the government released a discussion paper on the new Strategy, developed by the taskforce. It also announced at the same time that it will establish a Coordinator of Cyber Security, supported by a National Office of Cyber Security within the Department of Home Affairs, to ensure a coordinated response by government on cyber issues. The Strategy is likely to be finalised in August 2023.

Tackling misinformation and disinformation

Amongst the other initiatives announced by the Minister for Home Affairs in late 2022 was work regarding the resilience of Australia's democracy. The terms of reference for the "Strengthening Democracy Taskforce" are somewhat vague, as it is intended to "identify concrete initiatives to bolster Australia's democratic resilience and enhance trust among citizens, and between citizens and governments".

What is clear, however, is that, unsurprisingly, a key focus of the taskforce will be on misinformation and disinformation that is spread online and can be used to weaken trust, particularly in governments.

At the time of announcing the taskforce, the Minister for Home Affairs specifically called out the harmful impacts of misinformation and disinformation, and foreign interference, noting that Australians need tools to reduce their susceptibility to the spread of false information online and that the government needs to work with tech companies to reduce the spread of "polarisation and falsehoods".

It will be interesting to see what the taskforce ultimately recommends in terms of regulation to limit online misinformation and disinformation. There appears to be a significant risk of regulatory overlap with other reforms proposed by the Australian government in this regard. For example, in late January 2023 the Minister for Communications announced that ACMA would be given new powers to obtain information from digital platforms regarding their processes for responding to misinformation and disinformation on their platforms and to investigate those processes. ACMA will be given the power to implement a mandatory standard, binding on digital platforms, if it concludes that voluntary measures implemented by those platforms are not sufficient to respond to the threat from this content.

It would appear that the new ACMA powers could be used to address the dissemination of misinformation and disinformation that the Minister for Home Affairs has identified as being of concern. Close co-ordination on the proposals of the two Ministers will be required to avoid regulatory overlap and inconsistency.

Holding Redlich is a national Australian firm, with significant experience in the areas of technology, media and telecommunications. This experience also covers related areas including data and privacy. The firm acts for a broad range of clients, including government, media companies, communication services providers, technology companies and industry bodies. Its knowledge of the law, and experience of the Australian regulatory environment and relationships with government agencies and regulators, assists it in working with clients to: provide

advice and transactional assistance to ensure clients protect their commercial interests, and comply not only with current law but also future regulatory requirements; engage with Australia's regulators to obtain necessary licences and approvals as well as in engaging to resolve potential regulatory breaches; and develop cutting-edge regulatory proposals and carefully balanced submissions to government responding to legislative reform consultation processes, as Australian law continues to evolve to address the challenges of the digital age.

Authors



Angela Flannery is a partner with Holding Redlich. Angela has over 20 years' corporate law experience in both transactional and regulatory matters, with a focus on data,

telecommunications, media and technology. Angela's experience includes assisting clients in making submissions to government consultation processes on regulatory reform (particularly in the area of digital markets), providing advice to government agencies in investigations and regulatory enforcement (including regarding privacy regulation), and advising corporates regarding compliance with the Competition and Consumer Act, the Telecommunications Act, the Broadcasting Services Act and competition, consumer protection and privacy issues relating to telecommunications, technology and ad tech.



Andrew Hynd is a partner in the firm's corporate and commercial group, with specialist experience in IT, innovation and procurement. He has over 20 years' experience acting for a

range of public and private sector organisations on IT projects, especially software licensing, implementation and support, cloud services and privacy and data advice. He also advises local and international clients on privacy compliance issues and matters relating to data, including value capture, management, security and breaches. Andrew is a member of the Local Government Association of Queensland's Data Ethics Panel.

AUSTRALIA TRENDS AND DEVELOPMENTS

Contributed by: Angela Flannery, Andrew Hynd, Dan Pearce and Ian Robertson, **Holding Redlich**



Dan Pearce is a general counsel in the firm's corporate and commercial group, having retired from the partnership after more than 20 years. He has deep experience advising on all

aspects of IT, intellectual property, media and related corporate and regulatory issues, including competition and consumer law, privacy and data governance, broadcasting, defamation and other legislative compliance. Dan is currently a councillor for the Australian Information Industry Association (AIIA), Victorian Branch, and is a member of the Intellectual Property Society of Australia and New Zealand.



Ian Robertson is an experienced corporate, commercial, media and regulatory lawyer who advises Australian and overseas clients across a number of industries, particularly in the

media, entertainment and technology sectors. Ian's expertise includes advising on public policy, governance and regulatory issues, advising advertising agencies on commercial and compliance issues, acting for media businesses in respect of regulatory matters, and advising on all aspects of screen production and distribution. Ian is a member of the Communications and Media Law Association of Australia and a Fellow of the Australian Institute of Company Directors.

Holding Redlich

Level 65
25 Martin Place
Sydney
NSW 2000
Australia

Tel: +61 2 8083 0388
Email: inquiries@holdingredlich.com
Web: www.holdingredlich.com



HOLDING REDLICH

Law and Practice

Contributed by:

Kristof De Vulder and Raf Schoefs

DLA Piper see p.54



Contents

1. Metaverse	p.40
1.1 <u>Laws and Regulations</u>	<u>p.40</u>
2. Digital Economy	p.40
2.1 <u>Key Challenges</u>	<u>p.40</u>
3. Cloud and Edge Computing	p.41
3.1 <u>Highly Regulated Industries and Data Protection</u>	<u>p.41</u>
4. Artificial Intelligence and Big Data	p.43
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	<u>p.43</u>
5. Internet of Things	p.44
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	<u>p.44</u>
6. Audio-Visual Media Services	p.46
6.1 <u>Requirements and Authorisation Procedures</u>	<u>p.46</u>
7. Telecommunications	p.48
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	<u>p.48</u>
8. Challenges with Technology Agreements	p.49
8.1 <u>Legal Framework Challenges</u>	<u>p.49</u>
9. Trust Services and Digital Entities	p.52
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	<u>p.52</u>

1. Metaverse

1.1 Laws and Regulations

Concept

The metaverse is a term describing a hypothetical, future, enhanced, digital environment where users will be able to move smoothly between several spheres (social, work, leisure, shopping, etc) in one single digital environment. The metaverse could also be seen as the integration of the digital and physical worlds.

In practical terms, the metaverse is an advanced version of the internet that can be accessed through VR headsets, augmented reality appliances and more common devices such as mobile phones and personal computers or laptops. So far, the metaverse is mainly a commercial venture and competition is increasing between major technology companies, all of which are developing their own metaverse offerings.

Laws and Regulations

No specific laws for the metaverse have been introduced. Accordingly, all general laws and principles that apply to the “real world” by default also apply to the metaverse.

For example, general contract law will apply to the transactions concerning non-fungible tokens (NFTs), intellectual property protects works can be generated and enforced in the metaverse, and companies active in the metaverse will have to comply with data protection and consumer laws. Furthermore, all criminal law provisions will also apply to offences committed in the metaverse.

According to established case law relating to online disputes, Belgian law will apply to websites which envisage a public in the Belgian territory.

In many situations the legal framework can be applied seamlessly to the digital situation, but there may be situations where the existing laws are not always adapted to the reality of the metaverse.

Key Legal Challenges

A select number of key legal challenges are outlined below.

Intellectual property rights

The enforcement of intellectual property rights in the metaverse may lead to practical difficulties and challenges, just as it has been in the past for Web 1.0 and Web 2.0 disputes. Therefore, it will be important for businesses to actively monitor the metaverse for possible infringements.

One of the questions that will arise is which jurisdiction will be competent to examine infringement claims that might take place in the metaverse, as the metaverse does not belong to a concrete jurisdiction and as it may be difficult to identify the real identity of the infringer.

Data protection and cybersecurity

Lots of personal data will be processed in the metaverse. This will range from traditional types of personal data to the tracking of movements and activities in the metaverse. Given the cross-border character of the metaverse, many different data protection laws may need to be taken into account when processing personal data.

2. Digital Economy

2.1 Key Challenges

Book XII of the Belgian Code on Economic Law is dedicated to regulating the digital economy. This includes the Belgian implementation of the Directive on electronic commerce.

New Belgian laws are to be expected, given the recent entry into force of the EU Digital Markets Act (DMA) and the EU Digital Services Act (DSA), respectively on 1 November and 16 November 2022.

The DMA targets online platforms which qualify as “gatekeepers” and therefore create a bottleneck in the digital economy. Regulating these platforms will enhance competition and create a fairer business environment for businesses who depend on gatekeepers.

The DSA will introduce a new standard for the accountability of online platforms regarding illegal and harmful content.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Regulations

As there are no contracting laws specifically tailored to cloud and edge computing contracts in Belgium, general contract law applies to such contracts (consumer laws, specific laws for certain kinds of contracts, etc). Contractual arrangements thus need to be heavily relied on in order to cover issues not dealt with under traditional contract law, or dealt with in a way that is not readily applicable to cloud and edge computing. In addition to contract law, a number of other laws and regulations also apply to specific issues or aspects of cloud solutions.

The Directive on Security of Network and Information Systems (the “NIS Directive”) mainly aims to strengthen critical infrastructure in the EU, but also contains provisions regarding cloud computing. Providers of critical infrastructure have to comply with the (national implementation of

the) security requirements of the NIS Directive – ie, the requirement to adopt appropriate security measures.

The NIS Directive was transposed into Belgian law through the Belgian NIS Act of 7 April 2019 (the “NIS Act”), and its executing Royal Decree of 12 July 2019. On 16 December 2020, the European legislator presented a new cybersecurity strategy and published two new proposals: a Directive on measures for high common level of cybersecurity across the Union (NIS 2), and a new Directive on the resilience of critical entities. Both texts have recently been adopted, which illustrates the increased attention paid by the European Union to cybersecurity. Thus, the implementation under Belgian law of both Directives will, in principle, start soon.

Regulations in Specific Industries

To date, there are few sector-specific rules in Belgium in relation to cloud services, as several sectors have rules in relation to outsourcing in general (eg, in the banking and insurance sector).

In 2019, for instance, the National Bank of Belgium (NBB) issued a new circular on outsourcing arrangements (the “Circular”) that applies to a wide number of financial institutions. With the Circular, the NBB has fully integrated the European Bank Authority Guidelines on outsourcing arrangements of 25 February 2019 (the “EBA Guidelines”) into its supervisory practices.

In order to be compliant, financial institutions wishing to outsource part of their activities must, among other things, ensure that the outsourcing contract provides for a range of obligations and must submit a file to the regulator in certain circumstances. Similar but more strict obligations exist for (re)insurance companies.

On 28 November 2022, the European Council adopted the regulation on digital operational resilience for the financial sector (DORA) which aims to ensure that all EU financial entities are subject to a common set of standards to mitigate ICT risks for their operations.

Processing of Personal Data

The General Data Protection Regulation (GDPR) is applicable to all processing of personal data. To the extent that the data uploaded by an organisation includes personal data, the GDPR will also be applicable to cloud solutions and will have to be taken into account by both cloud providers and users. Certain obligations and restrictions under the GDPR can be especially problematic with regard to cloud solutions (eg, data transfers to third countries).

For instance, the GDPR prohibits data transfers to third countries without either being able to rely on an adequacy finding issued for the third country by the European Commission (eg, Japan, Switzerland, New Zealand) or having provided appropriate safeguards (eg, binding corporate rules, standard contractual clauses, an approved code of conduct or certification mechanism). If a cloud provider has data centres in such third countries, this requirement should therefore be taken into account.

In July 2020, the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield in the Schrems II decision, which has created significant uncertainty for many companies. Among other things, it follows from the judgment that one can only rely on appropriate safeguards (eg, standard contractual clauses) for a transfer to a non-adequate third country where an appropriate risk assessment has been carried out to evaluate whether the law of the third country of destination ensures adequate protection of the

transferred personal data and, where necessary, additional safeguards have been implemented. If a cloud provider has data centres in such third countries, or where access from those third countries to personal data in the European Economic Area (EEA) is possible, this requirement should therefore be taken into account.

The European Data Protection Board (EDPB) has issued recommendations on the measures that can be used to supplement transfer tools (No 1/2020), on the European Essential Guarantees for surveillance measures (No 2/2020) and, more recently, also guidelines on the interplay between the GDPR's territorial scope and the data transfer rules (No 5/2021). The latter guidelines define, for the first time at EU level, the concept of "transfers".

The European Commission has also issued modernised standard contractual clauses to remedy some of the deficiencies identified by the CJEU in the Schrems II decision. Until recently, controllers and processors could continue to use the old standard contractual clauses adopted under the previous Directive 95/46 for contracts concluded before 27 September 2021, as long as the processing operations subject to the contract remain unaltered. Since 27 December 2022, this is no longer the case.

Moreover, the obligation to notify data breaches to both data subjects and data protection authorities will typically require more extensive involvement of the cloud service provider than in the case of local IT solutions, given the typically greater reliance on the cloud service provider.

In cloud computing contracts, other aspects have to be carefully planned, such as the question of return or destruction of personal data, the question of liability of the provider, etc. In this

respect, the working group on Switching Cloud Providers and Porting Data (SWIPO) presented two data portability codes of conduct to the European Council and European Commission, which were published in May and July 2020.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights Laws and Regulations

Artificial intelligence and big data will be governed under an array of laws and regulations.

Legal challenges

Liability

As one of the characteristics of AI is that it can take decisions with a degree of autonomy, the question of liability (“who is responsible when an AI system causes damage or breaches the law?”) quickly emerged. In this respect, the European Parliament adopted a resolution with recommendations to the Commission on a civil liability regime for artificial intelligence on 20 October 2020 in which it stated that there is no need for a complete revision of liability regimes, but that the capacity of self-learning and the potential autonomy of AI-systems requires specific and co-ordinated adjustments to the liability regimes. The European Parliament also emphasised that the new common rules for AI-systems should take the form of a regulation.

On 21 April 2021, the European Commission published a proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the “Artificial Intelligence Act”) and amending certain union legislative acts. The proposed Artificial Intelligence Act contains a tiering of regula-

tory requirements depending on the inherent risk associated with the AI system that is being used – namely (i) prohibited AI practices, (ii) high-risk AI systems and (iii) low-risk AI systems. High-risk AI systems are permitted provided the strict controls set out in the regulation to mitigate the risks are in place. Key regulatory controls on high-risk AI systems include the obligation to maintain complete and up-to-date technical documentation and to ensure a high level of accuracy, robustness and security. This Regulation is expected to enter into force in 2023 with a transitional period. As of the second half of 2024, it can be expected that the regulation will be applicable to operators.

Additionally, the Commission has adopted a proposal for an Artificial Intelligence Liability Directive (AILD) on 28 September 2022. The Directive aims at improving the functioning of the internal market by laying down rules for certain non-contractual civil liability for damage caused with the involvement of AI.

For now, liability questions regarding AI are still governed by the general liability framework. Regarding non-contractual liability, Belgian law sets out three conditions that need to be fulfilled for liability to be attributable to a party: fault, damage and a causal link between the two. The burden of proof lies with the claimant. Where an AI system causes harm, however, it may be difficult to determine with precision which action or inaction led to the breach or damage and whether it was a “fault”.

It remains to be seen whether non-compliance with (some of) the obligations set out in the Artificial Intelligence Act will contribute/lead to the determination that the supplier/user has made a “fault”. The AILD would introduce a rebuttable presumption of causality in the case of fault – ie,

the lack of compliance with a duty of care under the AI Act, or any other EU or national law.

Given the current legal uncertainty, organisations working on projects involving AI systems must carefully regulate liability in their contractual arrangements, including matters that have an indirect impact on liability (eg, applicable law and choice of jurisdiction).

Data protection

AI systems process vast quantities of data, including personal data in most cases. In accordance with the requirements of the GDPR, key requirements such as data minimisation and privacy by design have to be taken into account when creating or working with AI systems in Belgium.

Intellectual property

Most relevant in this respect is copyright. The conditions of copyright – namely a “work” that is “original” – have been interpreted by the CJEU and are, to a certain extent, similarly applied throughout the EU. This means that the same issues will be faced by all the countries in the EU – for example, “who will be the author when an AI system makes a work of art?”

The first component of originality, also known as the “objective component”, holds that the work must be the result of an intellectual creation. The second component, known as the “personality requirement” or “subjective component of originality”, holds that a personal touch must be given to the work in order to reach the threshold of originality. From these criteria it can be deduced that human input is a prerequisite for copyright.

As AI systems are not likely to be able to claim copyright protection in the near future, the creator of the AI system (the legal or natural per-

son) should document the process of creation and arrange internal assignment of all IP rights, including copyright, to themselves, following the principle of Belgian property law that “the fruits of a good belong to the owner of the good”.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There is no strict definition of the internet of things (IoT), so for the purpose of this article the collection of devices that have the ability to sense, amass and analyse data, and to communicate through networks will be considered as the IoT.

Data Protection

The first important legal framework that needs to be taken into account is data protection law. Because of the nature and goal of IoT devices (ie, smart mobile applications, smart home units, wearables, home assistants, etc), large amounts of data are being collected and processed, some of which will be considered personal data under the GDPR.

The applicability of this framework has a number of consequences as to how IoT devices should be designed (in particular the overarching principle of “privacy by design”).

Consent

Not all IoT devices and services are organised along the lines of traditional graphical user interfaces, so asking for consent cannot always be worked directly into the functionality. As a result, IoT manufacturers and resellers must think of alternative ways to collect consent, in such a way that it meets the requirements of the GDPR:

consent must be freely given, specific, informed and unambiguous.

Data minimisation

The GDPR requires that the personal data used is relevant and limited to what is necessary in relation to the purpose for which it is processed. This is a direct challenge to the data maximalism that is typical of IoT devices and services. One suggested way to keep this balance is “edge computing”, which allows the devices themselves to select the data necessary for processing further down the line.

Data protection impact assessments

In addition to the scenarios provided in the GDPR, the Belgian Data Protection Authority has set out a number of scenarios in which a data protection impact assessment (DPIA) is mandatory, and one of them specifically concerns the deployment of certain kinds of IoT devices – ie, large-scale processing of data generated by devices with sensors sending data over the internet or any another means for the purpose of analysing or predicting individuals’ economic situation, health, preferences or personal interests, reliability or behaviour, localisation or movements.

Cybersecurity

Cybersecurity is also a major point of attention. Various authorities internationally have expressed concern regarding the security of a lot of IoT devices, as these devices have the potential to enable the misuse of information, unauthorised access or attacks on other systems.

In Belgium, there are no specific minimum-security requirements, but specific sectors have requirements in relation to data breach notifications (eg, telecommunications, critical infrastruc-

ture, finance in specific cases) and data protection rules also provide for notification obligations in relation to personal data breaches.

ePrivacy Directive (M2M)

Under the ePrivacy Directive 2002/58/EC (ePD), a key question is whether machine-to-machine communications (M2M) – eg, the communications between an IoT device and the server of the vendor/service provider – are protected by the ePD’s rule of confidentiality of communications.

This question was not settled based on the wording of the ePD (which refers to “parties” to a communication), or in Belgium based on the wording of the Belgian implementation.

The draft ePrivacy Regulation aims to resolve this by clearly covering IoT services and devices. Current drafts would provide for confidentiality of communications, M2M included, which could impact the way in which certain organisations use IoT devices today. On 10 February 2021, the member states agreed on a mandate for negotiations with the European Parliament and trialogues began on 20 May 2021. It is estimated that, after a transitional period, the Regulation will be applicable in 2025.

Interoperability

Today, most companies creating IoT services or devices do so with their own separate infrastructure. As IoT devices and services become more prevalent, the question of interoperability of devices, networks and platforms will inevitably arise.

Within the ongoing efforts to create a European Digital Single Market, the EU has dedicated publications to interoperability architecture for IoT.

While this is not currently a legal requirement, it is highly recommended to consider the question of interoperability with existing services, whether through adopting an open architecture, integrating a third-party architecture – eg, by way of an application programming interface (API) – or making available a software development kit (SDK) for others to use for interoperability.

There are no particular requirements under Belgian law in this respect.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Legal Landscape

European level

In November 2018, the European Parliament adopted Directive 2018/1808 concerning audio-visual media services (the “AVMS Directive”) and the Directive 2019/790 on copyright and related rights in the Digital Single Market (the “DSM Directive”) in April 2019.

National level

The AVMS Directive has been implemented by the Belgian legislature at four different levels, in four different ways. In Belgium, community-level governments (Flemish, French and German-speaking) are in charge of the regulation of audio-visual media services in their respective territories, based on the place of establishment of the provider. By way of an exception, the federal government has the power to regulate audio-visual media services established in the capital region, Brussels, unless they need to be considered as belonging to the Flemish or French community because of their activities.

In conclusion, the Belgian legal framework is composed of a Federal act, a Flemish decree, a French decree and a German decree. These acts are not always consistent and therefore it is necessary to check, in practice, which requirements apply depending on the establishment of the service provider.

Main Requirements for Providing Audio-Visual Media Services

Requirements common to linear and non-linear providers

The following requirements are to be considered common to linear and non-linear providers:

- Prior Declaration and Registration to the Belgian Institute for Postal Services and Telecommunications (BIPT/IBPT). This notification is subject to the payment of a fixed fee. In addition, an annual fee is charged by BIPT. More information on the amount of the fees can be found in the Royal Decree of 7 March 2007 or the BIPT [website](#).
- For transparency reasons, some information identifying the media provider (the name, the address, the telephone number, etc) should be made available.
- Audio-visual media services shall be continuously and gradually made increasingly accessible to persons with a visual or hearing disability.
- There are requirements for audio-visual commercial communications, sponsoring and product placement.
- There is a prohibition against making available services which incite violence, hatred or terrorism.
- There is a prohibition against making available services likely to seriously impair the physical, mental or moral development of minors.

Linear providers (eg, TV, broadcasters)

Under Flemish radio and TV broadcasting rules, national, regional, network and local radio broadcasting is subject to prior authorisation (by the Flemish government). For other forms of broadcasting, no authorisation is required, but a notification process applies.

Under the French community decree, radio and regional TV broadcasting is also subject to prior authorisation. Other audio-visual media services in the French community must notify the regulator (*Conseil Supérieur de l'Audiovisuel*, CSA) before they start their activity.

Non-linear providers (eg, on demand providers)

Promotion of EU works

At least 30% of the catalogues of on-demand audio-visual media service providers must be European works and such works must be given prominence. In addition to this, there are small nuances according to the decrees. In the French decree a gradual increase to reach 40% is encouraged. The Flemish decree also provides a precision in that, of the 30% of European works, a “significant proportion” must be Dutch-speaking. Finally, providers shall, on an annual basis, provide a report on the achievement of the objectives.

Netflix tax

There is a financial contribution obligation (known as the Netflix tax) according to which the media service provider must contribute financially to the production of European works. The French and Dutch Decree provide for a similar mechanism providing for an option between (i) co-producing or pre-purchasing French/Dutch works or (ii) payment to a Dutch/French local fund. However, the federal act does not contain such an obligation. Nor does the German-speaking community,

at least for audio-visual media services providers established in the same community or the same member state. External providers, on the other hand, may be subject to this financial contribution obligation.

Video-Sharing Platforms

Specifically in relation to online video channels, on the French-speaking side, in March 2012, the CSA published a recommendation on the scope of regulation of audio-visual media services, which seems to suggest that merely putting a few videos online will not fulfil the relevant decree, unless there is a systematic structure to organise videos so as to make them into an audio-visual “programme”.

Since 2018, the scope of the audio-visual media services directive has been extended to include video sharing platforms. The video sharing platform is defined as an economic service whose main purpose, severable section or essential functionality must be to provide programmes, user-generated videos or both, to the general public. The relevant rules are to be found in Article 28b of the AVMS Directive and transposed into the federal act and the respective decrees of the communities.

It should be noted that due to the lack of editorial responsibility of these platforms, it is said that a light regime applies to video sharing platforms. Therefore, they are not subject to all the rules in the same way as “true” audio-visual media services.

They must however take appropriate measures:

- to protect minors from harmful content which may impair physical, mental or moral development – eg, through age verification sys-

- tems, reporting and flagging functionalities and parental control systems;
- to protect the general public from content inciting violence or hatred against a group or member of a group based on the grounds of Article 29 of the Charter;
- to protect the general public from content that constitutes a public provocation to commit terrorist offences, child pornography, racism or xenophobia – eg, through adopting appropriate terms and conditions and reporting and flagging functionalities; and
- to comply with the commercial communication rules (identification principle, sponsorship, product placement, etc).

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The Belgian telecommunication rules are heavily influenced by EU rules. This has become even more the case since the adoption of the Electronic Communications Code Directive, and will be even more so once the EU adopts the long-awaited e-Privacy Regulation. Regarding the latter, however, it does not seem that the current deadlock concerning this piece of reform will be resolved soon, so its future remains uncertain.

With the adoption of the European Electronic Communications Code (EECC), a first step towards a uniform EU-wide telecoms framework had already been taken. This has been reinforced by the adoption in December 2019 of an Implementing Regulation by the European Commission, establishing a template for the contract summary that electronic communications services operators need to provide to consumers within the EU before the conclusion of a contract. This summary must include the main

conditions of the contract (eg, price, services and internet speed).

Although the EECC imposed a transposition deadline of 21 December 2020, the Belgian legislature only implemented the EECC into the Belgian legislative framework on 16 December 2021. The Belgian legislator has stayed as close to the text of the EECC as possible.

The EECC applies to electronic communications services (ECS) and electronic communication networks (ECN). An electronic communications service is defined as a service, normally provided for remuneration, via electronic communications networks, which encompasses – with the exception of services providing, or exercising editorial control over, content transmitted using electronic communications networks and services – the following types of services:

- “internet access service” as defined in point (2) of the second paragraph of Article 2 of Regulation (EU) 2015/2120;
- interpersonal communications service; and
- services consisting wholly or mainly in the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.

An “interpersonal communication service” is defined as “a service normally provided for remuneration that enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s) and does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service”. As a result of this definition, online servic-

es which are functionally equivalent to traditional voice telephony, text messages (SMS) and electronic conveyance services such as voice-over IP, messaging services and web-based email services may also fall under the scope of the EECC. The Belgian draft law transposing the EECC contains identical definitions.

Providers of ECN and ECS are, generally, allowed to carry out their activities in Belgium. Depending on the ECN/ECS that they offer they will have to comply with certain obligations. An example is the notification to the Belgian regulator before starting to provide any public ECN/publicly available ECS on the Belgian territory.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Qualification of Contract

Technology agreement is a broad term that can encompass (and combine) several kinds of technology services, such as licensing, maintenance, outsourcing, cloud computing services or even developing of software. When concluding or reviewing a technology agreement, it is important to qualify it appropriately to specify the applicable legal framework. In particular, it is important to check whether the agreement fits within the framework of one (or several) of the legally defined contracts under Belgian law.

The Belgian Civil Code (BCC) names several kinds of agreements, such as construction agreements or commercial agency agreements, and provides both mandatory rules (ie, those from which one cannot deviate by contract) and implied rules (ie, rules that apply when the agreement does not cover that specific issue) that may apply to these kinds of agreements. If an

agreement does not fit into the framework of any of the legally regulated contracts, parties enjoy a broad contractual freedom, but must ensure that they regulate all the important aspects in detail to avoid any legal gaps.

SLAs

An important part of any technology agreement is the set of service levels applicable to the contract, namely the commitment in practice by the supplier or service provider – eg, to a certain percentage of delivery, accuracy, availability, etc, or to responding within a specific number of days or hours to a request or issues. Service level agreements (SLAs) typically apply to the contractual annexes on service levels.

Nature of obligations

The description of these service levels is crucial for their legal classification under Belgian law, which makes a distinction between obligations to attain a specific result (*obligation de résultat/resultaatsverbintenis*) and “obligations of means” (*obligation de moyens / middelenverbintenis*), the latter often translated into English as a “(commercially) reasonable effort” obligation.

In the case of a result obligation, the simple failure to reach the result will be viewed as a “fault” (ie, non-performance) that can trigger liability; for obligations of means, however, a higher threshold applies and the party claiming liability must be able to demonstrate that the defaulting party did not do all that was (commercially) reasonable.

SLAs: not just an IT matter

In many companies in Belgium and abroad, SLAs are often drawn up by IT teams without properly taking the actual terms and conditions of the agreement into account. One must ensure that an SLA has been checked or drawn up in

consultation with the legal department to avoid legal misunderstandings.

Service levels are presumed to be result obligations, unless stated otherwise in the agreement, but service providers prefer to transform them into obligations of means – for example, by including expressions such as “to the best of its ability” or “strive” in the SLA. In that case, the service provider can only be held liable when non-compliance and fault can be proven by the customer. The customer, on the other hand, will aim for more certainty by using terms such as “ensures” or “result” in the SLA; in which case, the service provider can be held liable if the results and milestones set out in the SLA have not been achieved (except where this is attributable to the customer or to force majeure).

Liability

Contracting parties may limit or exclude their liability in an IT services agreement. This can be done by the incorporation of a liability clause or through the wording of the obligations, the inclusion of assumptions and a broad definition of force majeure.

Under Belgian law, it is allowed and generally accepted to exclude a party's liability for specific losses, on the condition that such exclusions:

- do not (fully) relieve a party from its liability for fraud, its wilful default (“*opzet*”/“*dol*”), its gross negligence or that of its employees or, except in cases of force majeure, for the non-execution of the essential obligations that are the subject of the agreement;
- do not apply to a party's liability for death or personal injury caused by negligence;
- do not lead to a “manifest imbalance” between the rights and obligations of the parties; and/or

- do not unduly exclude or limit the legal rights of one party in the event of a non-performance or improper performance by the other party of any of its contractual obligations.

As a result, liability clauses typically include caveats in this respect. Should there be none, the entire agreement, or at least the liability clause, could be held void, according to the principle that if any of the terms of a contract prove to be inapplicable or contrary to a mandatory provision of the law, the validity of the entire contract must be examined. The risk of such a discussion can be mitigated by including a “severability” clause, stipulating that if any (part of a) provision is or becomes illegal, invalid or unenforceable, this shall not affect or impair the legality of any other (part of a) provision of the IT services agreement.

Intellectual Property

Intellectual property (IP) plays an important role in IT services agreements. IT services often go hand in hand with the use of pre-existing IP of the supplier, pre-existing IP of the customer and third-party IP. Sometimes an IT services agreement involves the creation of something new which might also be protected by IP.

Contrary to what is often believed, there are various options to divide the IP on a new creation between the parties, ranging from full ownership for the supplier to full ownership for the customer. In an IT outsourcing agreement, the pre-existing IP typically remains with each party, with a form of cross-licensing (each party grants a licence to the other for the use of its own pre-existing IP).

In the case of a software as a service (SaaS) agreement, all IP rights on the SaaS solution are reserved for the SaaS provider, but this party

typically grants the customer a non-exclusive, non-transferable, worldwide, limited right to use and access the SaaS solution for internal business purposes.

Step-In Right

A step-in right is a discretionary right for a customer to partially or fully take over services or appoint a third party to deliver services instead of the supplier. The foundations for step-in are in the Civil Code, which case law is interpreted as permitting step-in without prior court intervention, subject to certain cumulative requirements (ie, urgency, a prior determination that there is a contractual breach, a prior notice to remedy the breach, immediate involvement of the third party after expiry of the notice period, and good faith).

The step-in principle is not mandatory law and parties may contractually exclude step-in or alter its conditions by adding scenarios in which step-in is possible (for instance, if the supplier causes material interruption or disruption of services or exceeds service credit levels during a certain period).

B2B Relationships

As from December 2020, a new Belgian Act regulates several aspects of B2B relationships. In essence, it prohibits:

- the abuse of economic dependence;
- misleading and aggressive market practices between companies; and
- unfair terms (including abusive clauses) in B2B relationships.

In the context of IT services agreements, the most relevant part pertains to unfair terms. The Act foresees a black list (presumed to be unlawful without possibility of rebuttal) and a grey list

(presumed to be unlawful until proven otherwise).

The black list targets terms which:

- provide for an irrevocable commitment on the part of the other party, while the execution of the contract is subject to a condition, the realisation of which is entirely dependent on the will of the other contracting party;
- give the company the unilateral right to interpret any term of the contract;
- in the event of a dispute, have the other party waive any right of recourse against the undertaking; or
- irrefutably establish the knowledge or acceptance of the other party by means of stipulations of which it had no actual knowledge prior to the conclusion of the contract.

The grey list targets, among others, terms which:

- give the company the right to unilaterally modify the price, characteristics or terms of the contract without a valid reason;
- unduly exclude or limit the legal rights of one party in the event of total or shared non-performance or improper performance by the other company of any of its contractual obligations;
- relieve the company from its liability for wilful intent, its gross negligence or that of its employees or, except in cases of force majeure, for the non-execution of the essential obligations that are the subject of the agreement; or
- in the event of non-performance or delay in performance of the other party's obligations, determine an amount of compensation which is clearly disproportionate to the prejudice which may be suffered.

New Civil Code

From 1 January 2023, the new Belgian Civil Code applies, introducing a number of modifications that will impact the conclusion of technology agreements. Amongst other things, the new Civil Code foresees:

- updated rules on pre-contractual liability;
- a codification of the battle of form doctrine;
- a hardship provision;
- the introduction of a right to unilaterally terminate a contract out of court;
- the introduction of the concept of anticipatory breach; and
- the introduction of the price reduction as a sanction.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Types of Electronic Signature

Under Belgian law, the electronic execution of contracts can be done using three types of electronic signature, which follows from the eIDAS Regulation (Regulation 910/2014/EU), as incorporated in Book 12 of the Belgian Code of Economic Law.

Normal electronic signatures

A (normal) electronic signature is defined broadly as data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. Examples include a name below an email, a PIN, a password, a scanned signature, symmetric and public key cryptography authentication methods and biometric authentication methods.

A (normal) electronic signature may not be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form and not based upon a qualified certificate. This type of electronic signature, however, does not (automatically) receive the same legal effect as a handwritten signature.

Advanced electronic signatures

An advanced electronic signature is defined as an electronic signature which meets the following requirements: (i) it is uniquely linked to the signatory; (ii) it is capable of identifying the signatory; (iii) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control; and (iv) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

In practice, mainly asymmetric public key cryptography (PKI) systems meet the requirements of this definition. It must, however, be emphasised that the legislation does not confer specific legal effectiveness to this type of electronic signature that would be different from (normal) electronic signatures. The main difference between a (normal) electronic signature and an advanced electronic signature is that the latter generally is considered to be more trustworthy, and that consequently more evidential weight is attached to it.

Qualified electronic signatures

A qualified electronic signature is an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. A certificate is an attestation linking electronic signature validation data to a natural person and confirming at least the name or pseudonym of that person. The certificate must

contain certain mandatory statements and must have been issued by a qualified certification service provider.

A typical example of a qualified electronic signature is the one placed with a Belgian eID card. A qualified electronic signature is automatically assimilated to and legally presumed to be equivalent to a handwritten signature.

Functional Equivalence and Proving the Existence of an Agreement

In Belgium, the principle of consensualism applies to the validity of contracts. Mutual consensus, even verbally, of both parties is thus sufficient to conclude a valid agreement. In deviation from this principle, the Belgian legislature at times imposes certain formal requirements (such as a signature) for the valid conclusion of a contract. In this regard, the principle of “functional equivalence for formal requirements” applies. This means that any legal or regulatory formal requirement for the valid conclusion of contracts by electronic means is fulfilled if the functional qualities of this requirement are safeguarded (Article XII.15 of the Belgian Code of Economic Law). Thus, if some “writing” or a “signature” would be required for the valid conclusion of a contract or an electronic contract, an electronic signature (regardless of which type) will suffice.

In certain circumstances, Belgian law, however, deviates from this principle of “functional equivalence for formal requirements”. For example, within employment law, only a handwritten signature or the equivalent qualified electronic signature can be used. The same applies for a tender in the context of public procurement law.

Furthermore, it is relevant to emphasise that there is a difference between concluding a valid agreement (as described above) and being able to enforce that agreement by proving its existence and contents, which is subject to specific requirements.

For example in a B2B environment, the Belgian law of evidence (incorporated in Book 8 of the new Civil Code), specifies that evidence between and against businesses relies on a free system of evidence. Consequently, the evidence of the existence of a contract in a B2B context may be given by electronically signed contracts. In this regard, courts will grant legal effect to electronically signed contracts as soon as two conditions incorporated in Article 8.1 of Book 8 of the new Civil Code are met. Firstly, as to the document itself, the writing must consist of “a set of alphabetical characters or of any other comprehensible signs affixed to a medium which allows access to it for a period of time appropriate to the purpose for which the information may be used and protects its integrity, whatever the medium and the means of transmission.” Secondly, the signature must consist of “a sign or a sequence of signs by which a person identifies himself and which indicates his intention.”

DLA Piper has a global intellectual property and technology (IPT) group consisting of 60-plus offices, around 150 partners and 530-plus fee earners in more than 20 countries, constituting the world's largest IPT team. With over 120 lawyers based in the firm's office in Brussels and its working hub in Antwerp, DLA Piper in Belgium combines DLA Piper's global reach with local know-how. More specifically, the IPT team is part of a global, fully integrated group of IPT teams that operate in the markets of greatest importance to the firm's multinational

clients. The Belgian team continuously develops innovative processes and methodologies to improve the delivery of legal services to its clients, as well as the internal organisation of its clients. The whole IPT team is fully dedicated to advising on IT, media and telecommunications matters, acting for both customers (larger users of IT) and large IT vendors, which gives it invaluable insight at both sides of the negotiation table, translating into better, more commercial and more pragmatic advice for its clients.

Authors



Kristof De Vulder is country-managing partner of DLA Piper's Belgian offices, and head of the IPT department. He has over 20 years' experience in technology contracts, cyber-incidents,

outsourcing and complex technology transactions. Kristof typically advises both users and suppliers of technology and outsourcing services in relation to all aspects of the procurement process, legal issues arising with the implementation of new technologies and responses to cyber-incidents. He further assists clients during all stages of litigation, including pre-litigation strategies, mediation, arbitration and government courts. His work involves business-critical and strategic projects all over the world. Kristof has received international recognition with respect to his technology sector work and has contributed to numerous publications relating to TMT law.



Raf Schoefs is a counsel in DLA Piper's intellectual property and technology team. He practises in all areas of information technology and intellectual property law, with a particular

focus on technology and outsourcing transactions, and has over 12 years of experience. Raf assists clients in the drafting and negotiating of complex IT and outsourcing agreements. He also advises clients on e-commerce-related topics, such as cloud computing, electronic signatures, intermediary liability, data protection, cookies and consumer protection. He has extensive experience in a wide range of IP-related matters and assists IT providers, buyers of IT services and public sector organisations in all types of technology transactions. Raf has contributed to several publications relating to TMT law.

Contributed by: Kristof De Vulder and Raf Schoefs, **DLA Piper**

DLA Piper

Rue aux Laines 70
1000
Brussels
Belgium

Tel: +32 2 500 15 00
Fax: +32 2 500 16 00
Email: kristof.devulder@dlapiper.com
Web: www.dlapiper.com



Trends and Developments

Contributed by:

Christoph De Preter, Pieter Paepe and Judith Bussé

EDSON see p.63

Introduction

Governmental structure

As was the case prior to 2023, Belgium is governed by a centre-left and generally pro-business coalition on the national level.

Like Germany, Belgium is a federal state. Belgium has a hybrid federated level and is composed of:

- three Communities (Flemish, French and German) that have wide powers over media and cultural matters; and
- three Regions (Flemish, Brussels and Walloon) that have wide powers over economic matters.

This leads to regional differences in policy, regulation and enforcement practice.

Brussels, the capital of Belgium, is also home to the EU Commission, the EU Parliament, the EU institutions and NATO. This international openness is reflected in the government's pro-EU stance and the court system's consistent observance of EU legislation.

Belgium: a stronghold for media and technology

Belgium will remain a location of choice for technology, media and telecommunications and should feature in an investor's top three list for investments in Europe. Belgium is renowned for its vibrant cultural scene with a deep-rooted tradition of comics (eg, the Smurfs, Tintin), art movies, indie video games, music (eg, Stromae, Angèle) and festivals (eg, Tomorrowland). In the

field of technology, Belgium hosts many discrete but highly successful B2B tech companies (eg, Collibra, Odoo), as well as world-leading university faculties in IT, engineering and video game design. The Rijndael algorithm was developed at Leuven University and was identified by the US National Institute of Standards and Technology (NIST) in 2021 as the new Advanced Encryption Standard.

Wages, taxation and government support

Wages in Belgium in the tech sector are average compared to top tech jurisdictions in North America or Northern Europe. Tax pressure is relatively high, but in return Belgian companies and the workforce do enjoy robust infrastructure, as well as top-of-the-line education and healthcare systems at very low cost.

As will be set out in this chapter, Belgium has generous incentive schemes for the creative and technology industries, although some of these have recently been subject to controversy.

A haven for B2B SMEs

Together with the Netherlands and Luxembourg, Belgium is a stable haven for businesses that want to serve international markets in the EU and beyond. It is a politically and economically stable and logistically well-connected hub. What makes Belgium stand out is its high density of universities and research centres, making it a haven for spin-offs and tech- and entertainment-focused SMEs. Tech companies are typically more B2B oriented, and therefore less well known among the public at large.

No capital gains tax

The absence of capital gains tax for private individuals in Belgium is noteworthy. Entrepreneurs that sell their shares in the framework of a full or partial exit are taxed 0% on the proceeds. This has helped a generation of young serial entrepreneurs to found or scale a business, exit and immediately reinvest in the next venture. There is also a visible trend of entrepreneurs relocating to Belgium for this reason.

New Opportunities in Government-Backed Digitisation and e-Authentication Markets

Belgium has historically been a forerunner in e-government and e-authentication. The EU regulatory framework (eg, eIDAS) has been swiftly and correctly implemented. The government-backed and partly privately owned “itsme” remote authentication app now allows Belgian citizens to authenticate and pay online, file tax declarations, get pension calculations, lodge court documents and access notarial documents in a digital vault – all from their smartphone.

Concerns have arisen around the dominance of “itsme”. In 2023 a continued push for alternative technologies is expected. Some are currently under development – both in the private sector and within government. Legal activity is expected to proliferate in this area around matters of compliance, competition and state aid.

In 2023, a rise is forecast in automated negotiation and termination solutions that build on the existing e-authentication infrastructure.

Movement in a Mature VHCN market/ Accelerated 5G Network Roll-Out for Enterprises and Cities/Increased Competition on the Retail E-Communications Market

Historically, Belgium has a strong score on Very High Capacity Networks (VHCN) with very high-speed digital subscriber lines (VDSL) and coax cable being available virtually everywhere. Arguably precisely because of this pre-existing infrastructure, fibre initiatives have started late. As a result, the fibre-to-the-home (FTTH) rollout is among the lowest in Europe, with incumbent operators now making efforts to catch up. A [VHCN-map](#) can be consulted on the regulator’s website. 5G rollout in Brussels – historically a pain point – is also getting closer thanks to a bill passed in parliamentary commission approving a radiation norm of 14.5 volts per metre (V/m).

The start of 2023 has seen a surprising alliance of incumbent operators Telenet and Orange; the companies agreed to provide wholesale capacity to each other on their networks in the north and south of the country respectively – a unique situation and a first in Europe.

Whilst 5G auctions are stranded amidst litigation in other countries, Belgium’s regulator has successfully finalised the auctioning of its 5G spectrum. Spectrum licences were made available in the 700 MHz, 1800 MHz, 2.1 GHz and 3.6 GHz bands. The auction raised a total of EUR1.2 billion.

Aside from the incumbent operators Telenet, Orange and Proximus, Citymesh is emerging as a fourth contender on a national scale. Citymesh is already an established player in setting up 5G networks for enterprises and local city governments. As a fourth player, Citymesh will also give a push to competition on the retail market, where it will operate under the DIGI brand. Cit-

ymesh and DIGI are attracting talent away from the three incumbent operators as well as from smaller existing players and are scaling fast.

Another factor to be reckoned with is the bankruptcy of EDPNet at the end of 2022. The bankruptcy administrators will seek to monetise EDPNet's customer portfolio and it will be interesting to see which (potentially virtual) operator will fill this market space.

Legal activity, including court action, can be expected both on the wholesale and the retail front as a result of these developments. This will range from regulatory and market practices claims between competitors to discussion over non-compete clauses and trade secrets.

Hardware is Hot

Refurbished

The Belgian telecoms regulator is very insistent on strict respect of the EU regulatory framework on terminal equipment and devices. As a result, and despite some small clarifications and improvements in the Commission's Blue Guide and legal initiatives underway on the right to repair, continued complications can be expected in 2023 for the refurbished industry. Although the Belgian regulator is vocal on the EU level and pushes for an adapted set of rules, it remains rigid in the day-to-day application of current rules. Continued seizures and inspections are expected on wholesale and retail level.

Local networks, repeaters and terminal equipment

In the same vein and in the wake of the "All Communication" court litigation back in 2020, litigation in the area of local network repeaters is poised to continue, as businesses (eg, retailers) attempt to achieve indoor coverage, meeting

opposition from the Belgian regulator and from incumbent operators.

Developments in Personal Data Protection

Internal DPA organisation

The Belgian Data Protection Authority (DPA) will continue to be in somewhat of a difficult situation in 2023 with a judicial and EU Commission review underway after the dismissal of two key senior members.

DPA enforcement highlights

On the enforcement side, continued activity is expected and businesses are recommended to carefully revise and audit their data flows and processes.

The DPA published several decisions regarding the main Belgian media websites' use of cookies. Most cases ended up being settled between the parties. The DPA nevertheless reaffirmed that cookies will remain among its main priorities for 2023. Companies should therefore review their cookies policy, with the help of specialised experts.

Also, the DPA will keep investigating data brokers, after already having imposed a EUR50,000 fine in 2022 onto an agency that collected and brokered the data of pregnant women and mothers of newborns under the alleged "cover" of sending a gift box to the data subjects concerned.

The DPA has further announced that in 2023 it encourages preventive action and dialogue with actors working on Smart cities, and further wishes to support and emphasise the role of the data protection officer (DPO) as its "ally" when investigating companies.

In February 2022, the DPA fined IAB Europe EUR250,000 for its Transparency & Consent Framework (TCF), which was held to be GDPR non-compliant. This decision has a broad impact, considering the widespread use of the TCF to facilitate the management of users' preferences for online personalised advertising. IAB Europe appealed the decision before the Brussels Market Court, which consequently referred preliminary questions to the Court of Justice of the European Union. The case (C-604/22) is still pending.

Judicial review

On the contentious side, a swell of appeals is expected before the Brussels Market Court (which has jurisdiction over the review of DPA decisions). This is because at the start of 2023 the Constitutional Court ruled that third parties affected by a decision of the DPA – even where they were not privy to the proceedings before the DPA – should also be able to appeal such DPA decision. Thus, in 2023, businesses and trade organisations are advised to keep an eye on DPA decisions that may affect them.

Developments in (Government) Data Access

Access to government data

The updated public sector information (PSI) Directive together with the Digital Markets Act created a push for data access from governments and gatekeepers. We have seen a lot of activity in this space, in particular around geospatial and location data, and expect this to continue in 2023 as the revised Data Governance Act will enter into force in September 2023. Already, clients have many questions on the rules around data brokerage and government data reuse.

Public access to documents

As regards media access to documents, Belgian newspapers continue to participate in multinational investigative journalism initiatives. There have been a number of favourable EU Ombudsman decisions supporting investigative access to document requests, with the Ombudsman taking a courageously strong stance against the EU Commission. This trend is expected to continue in 2023.

Gig Platforms Under Less Pressure – Law and Behold for Non-Compliant Subcontractors Employed or self-employed?

As opposed to neighbouring countries, Belgium did not see the re-classification of gig workers from independent contractors to employees. In 2021 and 2022, the Brussels Labour Court of First Instance held that both Uber and Deliveroo workers were self-employed. In 2023, legislative initiatives are anticipated to improve the situation of gig workers and to provide clear criteria on their self-employed or employed status. These criteria would, at first sight, allow a number of gig platforms to continue their current mode of operations.

Compliance by subcontractors

Whilst the gig economy is largely left alone by the Belgian court system, there has been a sharp crackdown by government inspection services on subcontractors in the telecoms space (working on FTTH). In 2023, prime contractors or subcontractors should ensure that further down the contracting chain, labour and safety regulations are complied with as they may in some circumstances be held liable for downstream violations of the law.

Beware for Fair and Appropriate Remuneration

Implementation of Article 18 DSM Directive

Over the summer of 2022, the Belgian legislature adopted an Act implementing the DSM Directive. The Act lays down an inalienable right to a fair and appropriate remuneration in favour of authors and performing artists that license or transfer their rights in an “exploitation agreement”. The Act furthermore allows for an audit right and a judicial review of contractual remuneration clauses.

Unanswered questions

The media and technology industries have many unanswered questions on the exact scope of these provisions. Businesses are still assessing the impact of these provisions on their contracts, and how to comply with audit requests. Audit requests and claims for judicial review of remuneration clauses are expected in 2023-24.

Streaming and Online Content Sharing Platforms Need to Pay a Remuneration Right

Constitutional Court litigation ongoing

Although Articles 17 and 18 of the DSM Directive do not foresee this, the above-mentioned implementing act also sets up a remuneration right in favour of authors and performing artists that have contributed to audio-visual works (which in Belgium is generally understood to comprise music, film and video games). The remuneration right is to be paid by streaming service providers (SSPs) and online content sharing service providers (OCSSPs). Belgium’s leading streaming platform Streamz, together with international players such as Google, Meta, Spotify, and Sony Music, have applied for the annulment of this remuneration right with Belgium’s Constitutional Court. As of February 2023, it is anticipated that other industry players will also join suit. A deci-

sion is to be expected at the end of 2023 or in early 2024.

Silence before the storm

This court case will be followed with interest by observers both in Belgium and abroad, as court cases are also pending in other EU jurisdictions. For now, Belgium’s collecting societies seem to have adopted a waiting pattern until the Constitutional Court sheds light on the validity of the new remuneration right.

Cloud and Schrems II – The Story Continues

Risky data export business

Since Schrems II, there has been no substantial change for European businesses. Data exports to the USA remain a problem and this is expected to remain the case at least until halfway through 2023, when the EU Commission is expected to issue a new adequacy decision after President Biden’s Executive Order in October 2022. At least until mid-2023, usage of US-based analytics, marketing and customer relationship management (CRM) tools such as Google Analytics, Mailchimp, or Salesforce should be carefully assessed and based on standard contract clauses where possible, a well-documented data transfer impact assessment and, if possible, technical measures (encryption).

Schrems III?

Even beyond the middle of 2023, the question will remain as to whether the expected adequacy decision will stand the test of an ECJ review that is bound to occur.

Tax Shelters – Attractive Remuneration Schemes for the Creative Industry – Uncertainty for the Software Industry

Tax shelters remain attractive

The Belgian audio-visual tax shelter scheme, famed for having boosted local film production,

has now been extended to the production of video games and EDSON is proud to have assisted the video game industry in this effort. The “cultural test” criterion has been implemented in a pragmatic way and key government players at both federal and federated level collaborate well in making the tax shelter a success.

Belgium also maintains an attractive tax shelter scheme for start-ups, with personal income tax reductions of 30-45% for capital investments in start-ups or crowdfunding platforms.

In addition, regional organisations like Wallimage and VAF continue to provide interesting funding schemes to the video game industry.

Copyright remuneration scheme for the creative industry

The highly attractive Belgian copyright remuneration scheme remains in place for “artistic and literary” authors like novelists, screenwriters and composers. They will continue to be able to pay out a substantial part of their remuneration as a copyright royalty, officially taxed at 15% and (thanks to deductibles) effectively taxed at approximately 7.5-12%.

Designers and other creatives in the video game industry will still be eligible for this tax scheme. The same scheme ought to also remain available to coders and software developers contributing to video games – despite the legal reform that is discussed below.

Uncertainty for the software industry

With a reform of the tax legislation adopted at the end of 2022, the Belgian government had the intention to exclude “non-artistic and non-literary” authors like architects, lawyers and software developers. According to government sources, they will no longer be entitled to benefit

from the above copyright remuneration scheme. However, the last word has not been said in this matter. A number of software companies have announced their intention to take steps against the tax reform before the Constitutional Court, whilst some legal scholars consider that even under the new rules, software companies can still pay out a part of their software developers’ remuneration as copyright royalty. By the end of 2023, or early 2024 at the latest, there should be more clarity on this topic.

E-fulfilment

In the area of e-fulfilment, there has been a surge of Belgian and foreign businesses outsourcing their Western-European logistics operations to Belgium-based fulfilment partners (for instance [BME](#)), especially after the experience during COVID-19 has shown that large marketplaces like Amazon favour their own products’ logistics over third-party products.

In 2023, in the e-fulfilment arena, increased attention is also expected to be directed at the liability aspects around storing and shipping products that are regulated differently between EU member states. Increased attention is also expected with regard to the validity and enforceability of fuel surcharges and price indexations.

New Rules Underway for Gaming Sponsoring

In this chapter, the Belgian legal framework on games of chance will not be discussed in detail. Please see the [Belgium Law and Practice chapter](#) in the Gaming Law guide.

However, in the field of media law, a draft Royal decree is set to significantly change rules on advertising and sponsoring by operators of games of chance in 2023. The Royal decree is still in draft form, so specifics will not be men-

tioned in this chapter, but interested parties can consult legal professionals on the draft's details.

Sports and Entertainment: Existing Rules are Under Fire

Important litigation is underway that may profoundly affect the sports and entertainment industries.

The Court of Appeals of Mons, Belgium has referred questions for a preliminary ruling to the European Court of Justice regarding the validity of FIFA's transfer system rules. The ECJ's ruling may impact the football market not only in Belgium, but in the entire EU.

Belgium has a very rigid market for resale of tickets for events (concerts, matches, etc). Any resale that is done on a structural basis and/or for a profit is prohibited. The Belgian rules on ticket resale affect the entire ecosystem, ranging from platforms to businesses offering event-related package trips. Various challenges of the Belgian legislation are being addressed and decisions can be expected late 2023 or early 2024.

EDSON is an innovative and independent firm with head offices in Brussels. **EDSON** supports businesses, entrepreneurs and governmental organisations in all areas of Belgian business law. The team also handles challenging and complex EU law matters. **EDSON** has a focus on helping clients with their hard data, markets, technology, and innovation (DMTI) problems. **EDSON** is very active in the telecoms, media and technology industries and assists online ticketing platforms, streaming platforms, video game publishers and developers, print publish-

ers, cartoon producers, offline/online gaming and betting operators, as well as companies and executives in the electronic communications business. Recent representations include litigation for Streamz (leading streaming platform) before the Constitutional Court regarding a newly implemented remuneration right, ECJ litigation for Fifpro (the global union of professional football players), EU-level state aid clearing of a national tax shelter scheme, and negotiation of digital twin-related agreements in various jurisdictions.

Authors



Christoph De Preter has over 12 years of experience as a practising lawyer. He also has over ten years of business expertise, having assumed CSO and CCO executive roles in

international software companies and scale ups. Christoph is well versed in IP, technology, contracts and strategic litigation. He is a member of the association of German patent attorneys (VPP), the association of German and European IP specialists (GRUR) and the Legal Action Committee of the European video game sector federation (IFSE). He also has expertise in IT contracts with defence and government organisations.



Pieter Paepe has been advising and assisting clients with their legal matters since 2006. Pieter has ample experience in dealing with competition law and commercial law matters, most

often in a highly regulated context. Furthermore, Pieter has a strong EU law background. He has been involved in various high stakes procedures before the EU courts. Pieter is a member of the Belgian Association of Competition Lawyers (Belgische Vereniging van Mededingingsadvocaten) and of the Legal Action Committee of the European video game sector federation (ISFE). Chambers and Partners has ranked Pieter both in 2021 and 2022 among the Global Market Leaders for Gaming & Gambling.

BELGIUM TRENDS AND DEVELOPMENTS

Contributed by: Christoph De Preter, Pieter Paepe and Judith Bussé, **EDSON**



Judith Bussé is counsel at EDSON and has over 8 years of experience, previously working in the Brussels office of a leading US firm. Judith specialises in IP and technology

and Litigation, assisting clients in the creative (fashion and design) and entertainment industries. She spearheads EDSON's trade mark practice and has also developed particular expertise in ESG. Judith presides over the Belgian chapter of ChIPs (women in IP) and has obtained multiple accolades in leading IP reviews.

EDSON LEGAL

Rue de Laeken 88
1000 Brussels
Belgium

Tel: +32 241 46 190
Fax: +32 241 59 562
Email: christoph.de.preter@edsonlegal.eu
Web: EDSONlegal.eu

EDSON.

Law and Practice

Contributed by:

Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda,
Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto
Azevedo Sette Advogados see p.78



Contents

1. Metaverse	p.66
1.1 <u>Laws and Regulations</u>	p.66
2. Digital Economy	p.67
2.1 <u>Key Challenges</u>	p.67
3. Cloud and Edge Computing	p.69
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.69
4. Artificial Intelligence and Big Data	p.70
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.70
5. Internet of Things	p.71
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.71
6. Audio-Visual Media Services	p.73
6.1 <u>Requirements and Authorisation Procedures</u>	p.73
7. Telecommunications	p.74
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.74
8. Challenges with Technology Agreements	p.76
8.1 <u>Legal Framework Challenges</u>	p.76
9. Trust Services and Digital Entities	p.76
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.76

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

1. Metaverse

1.1 Laws and Regulations

The metaverse is the virtual environment in which people, through various technologies (such as augmented or virtual reality, NFTs, crypto-active, blockchain and avatars), seek to reproduce and interact with the real world. Although the metaverse is at a stage of technological development around the world, when it comes to a regulatory framework, there is still a long way to go.

In Brazil, so far, there are no specific laws or regulations for the metaverse, and no legal cases or court decisions have considered the matter thus far. It is possible that in the coming years there will be discussion about the regulation of the relations performed in the metaverse, besides the application of the already existing laws, such as the following.

- Consumer Protection Code (Law No 8,078/1990), which establishes principles and standards of consumer protection and defence and its Decree No 7,962/2013, which regulated electronic commerce providing for the consumer's right to information about the products and services offered, as well as the registration data of suppliers and the service channels they offer, to facilitate customer service and provide for the right to regret. Thus, in the case of a purchase and sale, or provision of services to a consumer in the metaverse, it is possible that the application of this legislation will be questioned.
- Industrial Property Law (Law No 9,279/1996), which preserves the rights of creators and their inventions, ensuring the registration of patents, industrial and model designs, trade marks, etc. With the increasing popularity and the consequent development of more

advanced tools to access the metaverse, new applications for software and device patents, and the creation of other trade marks may arise.

- Copyright Act (Law No 9,610/1998) providing for protection of the creation, reproduction, publication, distribution, etc., of literary, artistic, or scientific works. With the large-scale distribution of these works within the digital space, the misuse, misappropriation or exploitation of moral and patrimonial rights of digital products may arise.
- Brazilian Internet Act (Law No 12,965/2014), which establishes principles, guarantees, rights and obligations for the use of the internet in the country and its Decree No 8,771/2016 which regulates the law by establishing procedures related to the retention and protection of data by connection providers and applications, and points out transparency and inspection measures regarding personal data and private communications.
- Labour Reform (Law No 13,476/2017), which introduced a new chapter to the Consolidation of Labour Laws (a Brazilian labour regulation) providing for work outside the employer's premises, with the use of information and communication technologies (teleworking) and the recently enacted Law No 14,442/2022 which regulates the details of teleworking in the country. People working in the metaverse can give rise to labour issues.
- Brazilian Data Protection Act (Law No 13,709/2018), which aims to regulate the processing of personal data in the Brazilian territory, including in digital media, by individuals or legal entities, of public or private law, in order to ensure the free development of the personality and dignity of the natural person, protecting their fundamental rights of freedom and privacy. It is very possible that the processing of personal data will have its limits

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

questioned in the metaverse, mainly about where controllers and processors would be located and which laws could be applied.

- Decree No 9,854/2019, which establishes the National Plan for the IoT aiming to implement and develop the IoT in Brazil, based on free competition and free movement of data, subject to information security and data privacy guidelines. The integration of IoT in the metaverse can contribute to an accurate representation of an object or an individual with very specific details collected from the real world.

The metaverse experience will require a series of solutions that aim to deal with some challenges that are already present (and others that will arise), such as:

- interoperability between cryptocurrencies, for the purchase of goods and/or services;
- verification systems and tools for proving personal identities (and their respective representations);
- security, privacy, and data protection, in view of the innovative ways of processing such data;
- issues about intellectual property with regard to territoriality, licensing, unauthorised use, copyright, royalties, patents, etc;
- issues about civil and criminal liability;
- debates about the competent jurisdiction to prosecute a claim related to an obligation contracted in the metaverse;
- social issues about misinformation, racism, misogyny, inappropriate behaviour, harassment, etc; and
- physical and mental health issues caused by prolonged immersion.

2. Digital Economy

2.1 Key Challenges

The digital economy in Brazil results in billions of daily online connections among people, companies, devices, data, and processes. Technological evolution has changed the way society interacts and consumes products and services. The speed at which technology reaches business models and industries means that governments and society need to be brought up to date much faster. There is a need for the legislature to move as fast as the digital economy, as companies often need opinions and solutions that are not regulated in Brazil at a given moment.

Brazil has been moving towards adequate regulation of several digital economy services, as illustrated by the examples below.

- Artificial Intelligence – Bill No 21/2020 proposes regulating the development and use of AI in Brazil. This bill is being analysed by the Brazilian Congress and is eagerly awaited by the digital environment. It is worth noting that AI is one of the subjects in stage 3 (one year – six months) of the Regulatory Agenda of the National Data Protection Authority (ANPD), which is expected to issue guidelines on AI that will also serve as a basis for the development of other rules that may be necessary to discipline the AI system.
- Telemedicine – With the COVID-19 pandemic, teleconsultations were regulated on an emergency basis in Brazil. In view of the modality's efficiency, in May 2022, CFM Resolution No 2,314/2022 was published to regulate telemedicine.
- Start-ups – Complementary Law No 182/2021, also known as the Legal Framework for Start-ups, is aimed at improving innovative entrepreneurship in Brazil and

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

leveraging the modernisation of the business environment.

- **Transportation apps** – Law No 13,640/2018 regulates the operation of paid private individual passenger transportation in Brazil.
- **Data Protection** – The General Data Protection Act (LGPD - Law No 13,709/2018) establishes that the processed data of individuals must be used in compliance with the law.
- **Financial Technology** – Fintechs became regulated in 2018 through Brazilian Central Bank Resolution No 4,656/2018.
- **Internet** – The Brazilian Internet Act (Law No 12,965/2014) disciplines the use of the internet in Brazil by providing principles, guarantees, rights and duties for those who use the network, as well as determining guidelines for state action.
- **E-commerce** – Law No 7,962/2013, known as the E-commerce Law, regulates the Consumer Protection Code in relation to e-commerce; this law contains specific provisions about transactions conducted between an online store and its consumer.
- **Electronic signatures** – Provisional Measure No 2,200-2/2001 regulates the use of electronic signatures in Brazil, establishing the Brazilian Public Key Infrastructure (ICP-Brazil), and Law No 14,603/2020 classifies signatures into simple electronic signature, advanced electronic signature and, finally, qualified electronic signature. The three types of signature characterise the level of trust in the identity and the expression of will of its titleholder, and the qualified electronic signature has the highest level of reliability based on its norms, standards and specific procedures.
- **Software** – Law No 9,609/1998 regulates software protection, its commercialisation, and stipulates rights and duties regarding its use.

Although the Brazilian legislature has approved various laws that touch upon digital economy, technology is always evolving and is innovative by nature. In this context, the absence of regulations for specific sectors may be the biggest challenge in relation to digital economy. This absence signifies legal uncertainty for companies and society, difficulty in applying the law, insecurity for investors, and limitation on guidance for clients and internet users, who are not always aware of the legal changes.

Nonetheless, the Brazilian government has taken steps towards promoting digital transformation in the country, through the implementation of the Brazilian Strategy for Digital Transformation (SinDigital). The purpose is to harmonise the federal executive initiatives linked to the digital environment, to harness the potential of digital technologies towards sustainable social and economic development, innovation, increased competitiveness and productivity, among other objectives.

This initiative is composed of the Brazilian Strategy for Digital Transformation (E-Digital), its thematic pillars (split between enabling and digital transformation pillars) and a governance structure. These are set forth by Federal Decree No 9,319/2018, which implements SinDigital and the Brazilian Strategy. SinDigital is co-ordinated by the office of the President's Chief of Staff.

The digital transformation pillars comprise digital transformation of the economy and of the government. On the other hand, some of the enabling pillars are:

- technology infrastructure and access to information and communication technologies, including increased access for the population to the internet and digital technologies;

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

- trust in the digital environment, relevant for ensuring a safe, trustworthy digital environment for services and consumption, respecting the citizens' rights;
- education and professional capacitation, for educating society in the use of advanced technology and preparation for the future of labour; and
- international dimension, for strengthening Brazil's presence and promoting regional integration in digital economy.

The 2018-22 initial E-Digital agenda ended up getting expedited with the COVID-19 pandemic, and the government issued a 2022-26 update after an evaluation process that included public consultations, meetings with experts and other initiatives.

In the above context, it will be important to follow up on the digital transformation expected to take place in Brazil, based on the governmental initiatives, on the legislation updates, and on the private sector inputs and demands.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Although there are not specific laws about cloud services in Brazil, many local laws refer to this matter, including the following.

The Internet Act (Law No 12,956/2014, MCI), further regulated by Decree No 8,771/2016, provides for principles, rights, and obligations about the use of the internet in Brazil. It sets forth obligations for internet connection and application providers that are relevant for cloud computing solutions in general. Among the main obligations

set out by the MCI regarding cloud are related to data retention by internet application providers.

The Brazilian General Data Protection Act (Law No 13,709/2018, LGPD), which came into force in 2020, provides for the processing of personal data, irrespective of industry or business – as controllers or processors of personal data, cloud service providers shall comply with the referred law. The LGPD impacts cloud computing and its providers, in particular with regard to the requirements for the processing of personal data and for data transfers.

On this matter of personal data processing, it is important to enhance the relevance of data protection in a cloud computing environment, highlighting specific issues in this context:

- in cloud environments, the hosting location of personal data remains relevant with respect to the applicability of national law, which will give guidance on the matter;
- in cloud computing, different players usually co-operate along the end-to-end value chain in order to deliver the service to the customer, and this leads to difficult questions surrounding personal data processing requirements such as security of the data, which may be intensified when new providers are added to the service; and
- cloud computing leads to considerable transfers of personal data, involving many different parties and crossing borders between countries, including outside Brazil, which means that the data controllers and data processors must ensure the compliance of these transfers with data protection rules.

Law No 8,078/1990 (the Consumer Protection Code, CDC) governs all consumer relationships, including cloud computing products or services.

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

Brazilian Central Bank's Resolution No 4,658, replaced in 2021 by Resolution No 4893, establishes requirements for cloud services to financial institutions. This ruling has established important obligations on companies regulated by the Brazilian Central Bank, such as specific rules for internal policies relating to cybersecurity and the cloud environment in general.

The Brazilian Superintendence of Private Insurance (SUSEP) has also published standard cybersecurity rules to be followed by insurance companies and their service providers, which are also applicable to cloud services in general (Circular No 638/2021).

Complementary Norm No 14/IN01/DSIC/GSIPR, established in 2012 and amended in 2018, has the objective of setting guidelines regarding the use of technologies in government agencies. More specifically, it addresses cloud computing and the aspect related to security and data protection. The Norm requires that information classified as secret or top secret cannot be processed on the cloud, for any reason. Also, data and metadata produced by and/or under the responsibility of the agency must be stored in data centres within national territory. In addition, it is important to note that in 2016 the Information Security Cabinet of the President's Office and the Ministry of Planning, Budget, and Management, which is now part of the Ministry of Economy, issued a general guideline with best practices, orientations, and restrictions to be followed by federal entities when contracting cloud computing services. The document outlines some contractual requirements that should be ensured by the agencies contracting cloud services, and the following is worth mentioning.

The data and information of the contracting agency must reside exclusively in the national

territory, including replication and backups. This requirement is justified by the need to provide the contracting agency with all the guarantees of Brazilian law, as the client is responsible for safeguarding the information stored in the cloud:

- the Brazilian jurisdiction must be adopted to settle any legal issues related to contracts signed between the contracting agency and the cloud service provider;
- the contracting agency must ensure the portability of data and applications, as well as the availability of information for location transfer, in an adequate period of time and at no additional cost, in order to ensure business continuity and enable the contractual transition; and
- the contractual provisions must ensure that the information in the provider's custody will be processed with confidentiality and cannot be used by or provided to third parties without authorisation under any circumstances.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

The use of AI is currently being discussed in Brazil through Bill No 5,691/2019, which establishes the "National Policy for Artificial Intelligence", with the goal of stimulating the formation of a favourable environment for the development of technologies in AI. This bill is the result of a union of other previous bills that discussed the topic:

- Bill No 5,501/2019 – intended to establish the principles for the use of AI and regulate its use;

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

- Bill No 872/2019 – intended to provide for the ethical frameworks and guidelines that underlie the development and use of AI; and
- Bill No 21/2020 – intended to create the legal framework for the development and use of artificial intelligence by public authorities, companies, and individuals, and the text established principles, rights, duties, and governance instruments for AI.

The National AI Policy establishes as its core principles:

- inclusive and sustainable development;
- respect for ethics, human rights, democratic values and diversity;
- protection of privacy and personal data; and
- transparency, security, and reliability.

The bill also states that AI should:

- respect people's autonomy;
- preserve people's intimacy and privacy;
- preserve the bonds of solidarity between people and different generations;
- be intelligible, justifiable, and accessible;
- be open to democratic scrutiny and allow for debate and control by the population;
- be compatible with maintaining social and cultural diversity and not restrict personal lifestyle choices;
- contain safety and security tools that allow human intervention where necessary;
- provide traceable decisions without discriminatory or prejudiced bias; and
- follow governance standards that ensure ongoing management and mitigation of potential technological risks.

Pending the regulation of AI in Brazil, since there are no specific laws about the matter, other legislation may impact the way AI is used and

may dictate rules and obligations for the parties involved, such as data privacy rules, internet use, and the Consumer Protection Code, for example.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Decree No 9,854/2019 instituted the National Internet of Things (IoT) Plan, aimed at improving the quality of life, fostering competition, increasing productivity, and integrating Brazil into the international landscape, in addition to other objectives. Health, cities, industries, and rural environments are priorities for IoT solutions.

According to this plan, IoT is the infrastructure integrating the provision of value-added services (VAS) with physical or virtual connection capabilities of things with devices based on information and communication technologies or evolutions thereof, with interoperability. Machine-to-machine (M2M) communications systems, in turn, are telecommunications networks, including access devices, for the transmission of data to remote applications aimed to monitor, measure, and control the device itself, the environment around it, or data systems connected thereto by means of such networks.

The provision of IoT/M2M solutions is not regulated in Brazil. However, the connectivity required for the transmission of data between the solution's devices might have an impact on the activity, since telecommunications services are regulated activities, being subject to the provisions of Law No 4,972/1997 (General Telecommunications Law, LGT) and the regulations issued by the National Telecommunica-

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

tions Agency (ANATEL), requiring a licence from ANATEL for their provision.

As per the LGT, VAS refers to activities that involve adding new utilities related to the access, storage, presentation, movement, or recovery of information to a telecommunications service supporting it, with which it is not confused. The LGT also stipulates that telecommunications services are activities enabling the offer of transmission, emission or reception of symbols, characters, signs, writings, images, sounds or information by wire, radio-electricity, optical means or any other kind of electromagnetic process.

Therefore, two situations should be considered.

- If the solution contracts the necessary connectivity from a third-party telecommunications provider holding the applicable license, the IoT/M2M provider is deemed user of the telecommunications service supporting the application, as such not being subject to telecommunications regulatory rules or to ANATEL's control. In this case, the tax on services (ISS) is due, the rates of which vary according to the applicable municipality.
- In case the solution encompasses both the VAS (related to the IoT/M2M application) and the telecommunications service (related to devices' connectivity), the solution provider is subject to telecommunications regulatory rules and ANATEL's control, and it should hold the relevant authorisation. Moreover, in this case, the state tax on circulation of goods and services (ICMS) is due, which has rates higher than ISS rates.

Furthermore, connected devices are deemed communications products using a radio-electric spectrum for information propagation. As such, they should comply with technical requirements

issued by ANATEL, and be certified and homologated by the same agency.

Prior licensing with ANATEL is also required for radiocommunication transmission stations to operate; however, Law No 14,108/2020 exempted stations integrating M2M communications systems from such prior licensing, and exempted said systems from the payment of certain fees until December 2025.

Importantly, although the implementation and development of IoT in Brazil is based on free competition and circulation of data, there must be compliance with information security and personal data protection guidelines. In this regard, several laws and regulations may apply, including:

- Federal Constitution provisions on privacy, private life, honour, and image of people, as well as the confidentiality of data, are inviolable (except in cases of court orders related to criminal investigations or discoveries);
- Law No 9,296/1996 provides that the interception of information technology, telematics, telephone communications, etc, is a crime;
- Law No 12,737/2012 provides for cyber-crimes and classifies disclosure of proprietary information as a crime;
- Law No 12,965/2014 (Brazilian Internet Act) sets principles and rules for ensuring privacy and data protection in internet use;
- Decree No 8,771/2016 sets security standards for the custody, storage, and processing of personal data and private communications by connections/applications providers;
- Law No 13,709/2018 (General Data Protection Act) regulates personal data protection and processing aspects, among other provisions;
- ANATEL's Resolution 740/2020 (Regulation of Cybersecurity Applied to the Telecommunica-

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

tions Sector) establishes conduct and procedures to promote security in telecommunications networks and services and protect critical structures; and

- ANATEL's Act 77/2021 provides for cybersecurity requirements for telecommunications equipment.

In addition, reliable and stable networks are fundamental for the IoT. In this regard, 5G technology began being implemented in Brazil in 2022, and is expected to boost the IoT market, fostering innovation and impacting local economy and society. Minimum security requirements for 5G networks were set by the Office of Institutional Security of the Republic Presidency's Normative Instruction 4/2020.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Audio-visual and media (broadcasting) services are regulated, maintained and exploited by the Federal Union. However, the Brazilian Telecom Code (BTC) allows individuals to execute broadcasting services through the due concessions, authorisations or permissions to be granted for renewable and successive terms of ten (radio broadcasting) or 15 years (television broadcasting).

The process begins with the publication of a notice; the interested parties present proposals that will be sent to the President of the Republic after the analysis by the competent body and issuing of an opinion. A prior licence is required for broadcasting stations, which must be required after registration of the concession contract by the Public Finance Court. If the sta-

tion is approved, the private licence is to be issued within 60 days.

The authorisation/permission is subject to the following requirements:

- 70% or more of the total and voting capital must belong, directly or indirectly, to native Brazilians or individuals naturalised as Brazilian for more than ten years (this must be proved by documents submitted to the competent bodies on a yearly basis), who will obligatorily carry out the administration activities and establish the content of the programming;
- contractual amendments must be submitted to the executive branch within 60 days;
- the transfer of the concession, authorisation or permission to third parties depends on prior approval by the competent body;
- the broadcasters' information, entertainment, advertising and publicity services are subordinated to the educational and cultural purposes inherent to broadcasting, aiming at the best interests of the country;
- radio stations are obliged to rebroadcast the official information programme of the Brazilian Republic called "A Voz do Brasil" on a daily basis (except on weekends, holidays and other specific occasions);
- the same person cannot participate in the administration or management of more than one concessionaire, licensee or be authorised of the same type of broadcasting service in the same location;
- broadcasting organisations, including television, must allocate at least 5% of their time to the broadcasting of news services; and
- executives or partners cannot have suffered condemnations related to the ineligibility criteria provided for in specific law.

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

The fees to be paid are fixed, taking into account the total costs of the services, the amortisation of the invested capital and the formation of necessary funds for the conservation, replacement and modernisation of the equipment, and extensions of the services.

Application providers, such as platforms on which user-generated content such as videos and photos is posted are regulated by specific law regulating the use of the internet in Brazil, so the above-mentioned requirements do not apply to application providers.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

According to the LGT and complementary rules (eg, those issued by ANATEL), telecommunications services might be:

- provided under the public regime (subject to stricter legal/administrative conditions), or private regime (less regulated); and
- of community interest (provided to any party interested in its enjoyment, under non-discriminatory conditions), or restricted interest (intended for the executor's own use or provided to groups of users selected by the provider, and interconnection to other networks is prohibited).

The following are the main communications technologies currently regulated.

- Fixed-switched telephone service (FSTS) transmits voice and other signals, being intended for communication between fixed determinate points using telephony processes. This is the only service rendered under the

public regime (based on concessions, subject to greater state control), but it can also be provided under the private regime (based on authorisations).

- Personal mobile service enables communication between mobile stations, and between mobile and other stations.
- Multimedia communication service enables the supply of transmission, emission, and receipt capacity of multimedia information (ie, audio, video, data, voice and other sound signals, images, texts, other information of any nature), and allows the provision of internet connection using any media to subscribers thereof. Importantly, transmission, emission or receipt or conditioned access services are not allowed.
- Conditioned access service distributes audiovisual content by means of any technology, process, electronic media and communication protocol, with access based on a paid subscription.
- Private limited service is restricted-interest service which encompasses multiple applications, such as communication of data, video/audio signals, voice and text, and capture/transmission of scientific data (eg, meteorology).

Brazilian and foreign satellites might be used by community-interest services providers to transport telecommunications signals, but this is not intrinsically a telecommunications service.

Provision of FSTS under the public system depends on a concession granted in a bid and the execution of the concession agreement. Law No 13879/2019 stipulates that concessionaires might request ANATEL to adjust the concession into an authorisation, if certain requirements are met by the interested party.

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

Exploitation of telecommunications services in the private regime depends on ANATEL's prior authorisation. However, the following exceptions exist.

- Authorisation is not required for telecommunications activities restricted to the limits of the same construction or movable/immovable property (except if involving the use of radio frequencies by means of radiocommunication equipment not categorised as restricted radiation equipment).
- Authorisation for the exploitation of services is waived if the support telecommunications networks use exclusively confined means and/or restricted radiation radiocommunication equipment, provided no numbering resources are employed, and, in case of community-interest services, there is less than 5,000 users; however, the provider should inform ANATEL prior to the start of the activities.

For an authorisation to be granted, the provider should:

- be organised in accordance with Brazilian laws, with its principal place of business and administration in Brazil;
- be able to contract with public authorities;
- have the technical qualification required to provide the service, good economic/financial standing, and tax regularity;
- be in good standing with the social security; and
- not be responsible for providing the same kind of service in the same location.

The interested party requires the applicable authorisation through ANATEL's information system, providing certain information and documents according to ANATEL Resolution

720/2020. Prior notification to ANATEL regarding the services that will be provided is mandatory. The authorisation's amount due is BRL400 for community-interest services and BRL20 for restricted-interest services. Nevertheless, when the provision of community-interest services can be impacted by many competitors, a bid might be required for the issue of authorisations.

Additionally, the provider should comply with all specific conditions established by regulations applicable to the relevant telecommunications service, which requires a deep analysis.

Services and solutions adding utilities to and not confused with the telecommunications services supporting them (eg, instant messaging – communication between computers connected to the internet with no connection to telephony networks) are deemed VAS and are not subject to telecommunications rules.

However, if they also encompass the provision of telecommunications services, ANATEL's authorisation is required and telecommunications regulations apply. Computers' communication using voice-over-IP (VoIP) to connect with fixed/mobile phones, and VoIP services simultaneously originating and terminating the communication with public telephony networks are examples of this.

Moreover, communications products using radio-electric spectrum for the propagation of information should comply with the applicable technical requirements, in addition to being certified and homologated by ANATEL.

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

As the law and case law in Brazil have not yet addressed the matter in depth, technology agreements must be regulated in detail. The main challenges of these agreements in Brazil are probably related to IP rights, service levels, liability, and data privacy. The continuous development of technologies is essential and agreements shall clearly regulate the ownership of existing intellectual property and future intellectual property developed during the commercial relationship between the parties involved.

Regarding software licence agreements, as software is often provided as a service in Brazil, service level agreements (SLAs) are heavily discussed. In this regard, although there is not specific regulation about SLAs (so this is mostly a commercial matter), general laws and customs provide minimum requirements in terms of uptime, backups, disaster recovery, and business continuity.

Liability is always also a significant issue. Although the Software Law (Law No 9,609/98) expressly says that clauses that “exempt any of the contracting parties from any third-party actions arising from misuse, flaws, or violation of copyrights” are null and void (Article 10), limitation of liability is allowed and case law varies a lot with regard to the possible caps to indemnifications regarding technology contracts.

Data privacy matters are also deeply discussed. Personal data (including sensitive data) is usually stored by IT systems and regulated by IT agreements. Controllers and processors of data (as defined in the LGPD) shall comply with local regulation, subject to legal penalties. In addition,

such agreements constantly involve the international transfer of personal data, a subject that is pending regulation by the Regulatory Authority, mainly regarding the approval of binding corporate rules and the issuance of standard contractual clauses, among other mechanisms provided for in the LGPD.

Finally, note that, as a rule, technology transfer agreements, which include IP licences, know-how licences, and software licences (if the software source code is transferred) shall be registered with the Brazilian National Institute of Industrial Property (INPI) for the following purposes:

- to produce effects in relation to third parties;
- to allow tax deductibility for the licensee of amounts paid as royalties and technical service fees; and
- to legitimise remittances of royalties abroad (if licensor is foreign).

Nonetheless, Law No 14,286/2021, which entered into force on 31 December 2022 and regulates the Brazilian exchange market, actually amends Law No 8,383/91 and, as a result, these so-called “technology transfer agreements” will not need to be registered in order to allow royalty payments abroad.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Brazil has had an advanced digital signature structure since the year of 2001, when it established the Provisional Measure No 2,200-2 (MP 2,200-2), regulating the use of electronic signatures in Brazil and creating the Brazilian Public

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

Keys Infrastructure (ICP-Brasil). The ICP-Brasil is composed of a managing authority and a chain of certifying bodies, which are entities accredited to issue digital certificates.

Through this methodology, each digital certificate belongs to a person and has a pair of encrypted keys, which must be in their exclusive control, use, and knowledge. The rules established by the ICP-Brasil management authority determine that when a document is encrypted with the public key; it can only be decrypted with the corresponding private key, which means that the digital signature associates an entity/person with a pair of encrypted keys, through asymmetric encryption.

According to MP 2,200-2, electronic documents are considered public or private for all legal purposes, and the content of documents electronically produced with the certification of ICP-Brasil are considered authentic regarding the signatories thereof. In addition, it is important to highlight the difference between digital and electronic signatures. Digital signatures use ICP-Brasil infrastructure through a digital certificate issued by the ICP-Brasil. On the other hand, the electronic signature does not use a digital certificate issued by ICP-Brasil. Although the legal presumption of authenticity and integrity is applicable only to documents signed within the ICP-Brasil framework, the MP 2,200-2 states that it does not prohibit the use of other means intended to prove the authorship of documents in electronic format, including those using certificates not issued by the ICP-Brasil, provided that such use is accepted in advance by the parties.

Therefore, agreements and documents in general can be signed with digital or electronic signatures. However, certain entities only accept documents signed using digital certified signatures issued by ICP-Brasil for validation purpose, such as government authorities and boards of trade. In this regard, Law No 14,063/2020 has emerged with the objective of expanding access to digital public services by reducing the bureaucracy of electronic signatures in documents. This Law amends MP 2,200-2 and provides for the use of electronic signatures in interactions with public entities, acts of legal entities, and in health issues, as well as on software licences developed by public entities.

The term “Digital Identity” has no standard definition in Brazil; however, it can be defined as the way in which an individual is represented and documented online. There are several distinct identifiers that can represent a digital identity, such as:

- name;
- date of birth;
- login credentials to online services;
- email;
- passport number;
- social security number;
- browsing behaviour; and
- online shopping.

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**

Azevedo Sette Advogados was founded in 1967 and has a leading market team of over 500 professionals with extensive experience, solid academic backgrounds from distinguished educational institutions in Brazil and abroad. The staff works in Azevedo Sette Advogados' five offices located in São Paulo, Belo Horizonte, Brasília, Rio de Janeiro, and Recife to meet the client needs. In addition, the firm is supported by a broad worldwide network of correspondents and partners. Azevedo Sette Advogados works closely with its clients, providing ethical and effective legal solutions. The firm is always seeking creative and efficient ways to offer complete solutions that help clients reach

their goals in accordance with their needs and strategic planning. The firm assists more than 1,200 active clients monthly with activities ranging from industrial, services and commerce sectors to government, private investors, and investment funds. Azevedo Sette Advogados and its team are recognised as leaders in Brazil in multiple areas of law, in particular M&A, contracts, projects and infrastructure, civil litigation and arbitration, TMT, etc. The authors would like to acknowledge the contribution of Danielle Chipranski Cavalcante, Camila Sabino Del Sasso, Bruna Evellyn Pereira Bigas, Carolina Simioni Perdomo, Ingrid Bandeira Santos and Gabriela Soares Mussalam.

Authors



Ricardo Barretto Ferreira da Silva is a senior partner at Azevedo Sette Advogados. He works in the areas of corporate, tax, M&A, IP, TMT, privacy and data protection. He has held the

following positions, among others: co-founder, Vice President (1989-94) and President (1995-98) of the Brazilian Association of Technology, Information and Telecommunications Law; Chair of the Latin America Committee (1993-95); Member of the Board (1995-2001 and 2003-05), Secretary, Treasurer and Vice-President (2001-03) of the International Technology Law Association; Chairman of the Legislation Committee (1991-92); Member of the Council (1991-93); and legal advisor (1992-93) of the American Chamber of Commerce São Paulo. He has also edited and co-authored numerous publications and articles on varied topics.



Juliana Gebara Sene Santos Ikeda is a partner in the TMT Advisory area of the São Paulo office, focusing on IP. She has over 15 years of experience in providing legal assistance to

national and international clients in consultations involving contractual and brand protection issues. She has co-authored articles and books in the areas of IP, technology and regulation.

Contributed by: Ricardo Barretto Ferreira da Silva, Juliana Gebara Sene Santos Ikeda, Lorena Pretti Serraglio and Sylvia Werdmüller von Elgg Roberto, **Azevedo Sette Advogados**



Lorena Pretti Serraglio is co-ordinator of the privacy and data protection area of the São Paulo office. She is a consultant for the Special Data Protection Commission of the Federal

Council of the Brazilian Bar Association. Lorena is co-author of several articles and books, one of which was elected by the Superior Court of Justice as an essential work for the understanding of privacy and data protection in Brazil. She is a professor of digital law at the Digital Marketing Graduate Programme at Senac São Paulo and is also a speaker on digital law, cybersecurity and data protection. Lorena is a reference for technology companies.



Sylvia Werdmüller von Elgg Roberto is an associate at Azevedo Sette Advogados. She acts in the areas of technology, media and telecommunications, focusing on telecommunications

matters. She has co-authored articles in the area of telecommunications and related subjects.

Azevedo Sette Advogados

1327, Presidente Juscelino Kubitschek Avenue
11th floor
International Plaza II Building
04543-011
São Paulo/SP
Brazil

Tel: +55 11 4083.7600
Fax: +55 11 4083.7600
Email: barretto@azevedosette.com.br
Web: www.azevedosette.com.br

Azevedo Sette
ADVOGADOS

Law and Practice

Contributed by:

Christopher Ferguson, Leslie Milton,
Scott Prescott and Paul Burbank

Fasken see p.94



Contents

1. Metaverse	p.81
1.1 <u>Laws and Regulations</u>	<u>p.81</u>
2. Digital Economy	p.82
2.1 <u>Key Challenges</u>	<u>p.82</u>
3. Cloud and Edge Computing	p.82
3.1 <u>Highly Regulated Industries and Data Protection</u>	<u>p.82</u>
4. Artificial Intelligence and Big Data	p.87
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	<u>p.87</u>
5. Internet of Things	p.89
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	<u>p.89</u>
6. Audio-Visual Media Services	p.90
6.1 <u>Requirements and Authorisation Procedures</u>	<u>p.90</u>
7. Telecommunications	p.91
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	<u>p.91</u>
8. Challenges with Technology Agreements	p.92
8.1 <u>Legal Framework Challenges</u>	<u>p.92</u>
9. Trust Services and Digital Entities	p.93
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	<u>p.93</u>

1. Metaverse

1.1 Laws and Regulations

There are no laws that specifically address the metaverse and associated services and products in Canada. As a result, legal considerations regarding the metaverse arise from the application of existing laws of general application to metaverse services and products, such as private sector privacy laws, consumer protection laws, competition laws, and copyright and other intellectual property laws. The following is an illustrative list of such considerations.

Privacy and Cybersecurity

Canadian private sector privacy laws apply to metaverse products and services. It is possible to comprehensively log and record an individual's activity in the metaverse to an even greater degree than in the physical world. Canada's privacy laws remain consent-based, and potential reforms to federal law and the coming into force of reforms in the province of Quebec will increase the transparency and other requirements for that consent (though in the case of federal reform, new broader exceptions to consent may help the development of the metaverse) and empower regulators to impose significant penalties.

In addition, the coming into force of the new Quebec law will bring new requirements on individual profiling and the collection of personal information through technical means. Organisations operating in the metaverse will have to carefully design their processes for obtaining consent, and ensure their processing of personal information remains within the bounds of that consent and the other requirements of Canadian privacy laws.

Responsibility for Cyber-attacks and Security Breaches

To the extent organisations collect a greater volume of potentially more sensitive personal information in the metaverse, the risks from cyber-attacks and security incidents will increase. The requirements to establish and maintain appropriate safeguards for personal information as required by Canadian privacy laws will be more stringent, and it will be even more critical for organisations to identify, mitigate and ameliorate incidents. It may also be difficult to determine where responsibilities lie in respect of breach notification to users, the Office of the Privacy Commissioner of Canada (OPC) or other applicable regulators.

Artificial Intelligence Regulations

Many human interactions within the metaverse will be enabled by artificial intelligence. Seamless, AI-driven human/system interaction (particularly any AI interpreting or mimicking human behaviour) may fall within future artificial intelligence legislation and regulations as well as automated decision-making provisions in revised privacy laws. These points are discussed in 4. **Artificial Intelligence and Big Data.**

Consumer Protection and Civil Liability

Most Canadian provinces have prescriptive consumer protection laws that regulate marketing practices and consumer contracts. For example, organisations in the metaverse must comply with restrictive requirements on internet contracts, even though interactions in the metaverse may be more akin to in-person interactions. Further, the application of tort and other common and statutory law that applies to in-person public places has not yet been tested in the metaverse.

Commercial Contracting

Metaverse industry participants need to co-operate in order to create a seamless experience for consumers and users moving through different metaverse platforms. Common intellectual property sharing agreements and confidentiality clauses will need to account for these novel circumstances, and metaverse businesses will need to consider how to apportion responsibility for privacy and security risks in contracts.

2. Digital Economy

2.1 Key Challenges

In Canada, digital services and digital markets are not subject to a specific regulatory regime as under the European Union's Digital Services Act and Digital Markets Act. Instead, any legal considerations regarding digital markets arise from the application of general laws to digital services and products such as communications laws, consumer protection laws, competition laws, and private sector privacy laws.

In addition, the Canadian government is proposing to regulate online platforms and digital streaming services as "online undertakings", under a bill currently being considered by Parliament that would revise Canada's broadcasting laws. It remains unclear at this time what conditions Canada's broadcasting and telecommunications regulator – the Canadian Radio-television and Telecommunications Commission (CRTC) – will place on these digital services, but they will likely be required to contribute to the development of Canadian programming through monetary and non-monetary contributions and investments in Canada.

The bill would also allow the CRTC to require online streaming services to carry Canadian

programming services and to regulate the discoverability of Canadian programming on online services. The amendments would also provide the CRTC with the authority to impose penalties for violations of certain provisions of the Broadcasting Act and provide the CRTC with explicit information-gathering powers about these services and platforms. At the time of writing, the amendments have passed third reading in the House of Commons and the Senate, and are expected to become law in early 2023.

Digital assets like cryptographic tokens and NFTs can be classified by securities regulators as a "security". As a result, companies seeking to trade in digital assets may be subject to Canada's provincial securities regulations. In particular, they will need to consider whether their assets meet provincial tests for a "security" and, if so, meet the attendant prospectus requirements.

Any business seeking to trade in digital services or markets in Canada should consult legal experts to determine whether their activity may be subject to existing generally applicable laws and regulations.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Regulations

There are no private sector laws of general application focused specifically on the provision of cloud services to the private sector in Canada, but other Canadian laws of general application and certain sector-specific regulations targeted to cloud services apply to the provision and use of such cloud services. Applicable laws include private sector privacy laws and regulations

which impose industry-specific requirements, such as:

- requirements governing the use of cloud services by federally regulated financial institutions;
- requirements that certain records of federally regulated financial institutions be located in Canada; and
- laws regarding personal health information.

Regulated Industries

The Office of the Superintendent of Financial Institutions (OSFI) is the Canadian federal regulator that supervises and regulates federally regulated banks and insurers, trust and loan companies and private pension plans subject to federal oversight. OSFI has issued Guideline B-10, *Outsourcing of Business Activities, Functions and Processes*, which specifies certain OSFI expectations for federally regulated financial institutions (FRFIs) that outsource one or more of their business activities to a service provider. This Guideline applies to all outsourcing arrangements, including cloud services, under which FRFIs are expected to:

- evaluate the risks associated with all cloud service arrangements;
- develop a process for determining the materiality of cloud service arrangements; and
- implement a programme for managing and monitoring risks, commensurate with the materiality of the cloud service arrangements.

The Guideline also contains a list of specific terms that OSFI expects an FRFI to address in a cloud service contract. While Guideline B-10 is directed to federal entities, it has also been voluntarily adopted by many provincially regulated entities in the financial sector. In 2012, OSFI released a memorandum that confirmed

that Guideline B-10 applies to cloud computing and that FRFIs should pay particular attention to the following in connection with cloud services:

- confidentiality and security;
- contingency planning;
- location of records;
- audit and access rights;
- subcontractors; and
- monitoring material outsourcing arrangements.

In April 2022, OSFI released for comment an updated Draft Guideline B-10, which sets out enhanced expectations for FRFIs in managing an expanded scope of third-party risks and places a greater emphasis on governance and risk management plans, and on specific outcomes and principles. The Draft Guideline expands the application to “third-party arrangements” which include any business or strategic arrangement with external entities. Examples of arrangements that would be subject to the Draft Guideline include:

- use of independent professionals, brokers, and utilities;
- use of financial market infrastructure;
- other relationships involving the provision of services for the storage, use or exchange of data; and
- generally, any outsourced activities, functions, and services.

The Draft Guideline replaces the “materiality” threshold in the current guideline and introduces a new “risk-based approach”, which requires a more comprehensive risk management framework that accounts for the level of risk and the “criticality” associated with individual third-party arrangements. A final, revised Guideline B-10 is expected to be issued in Autumn 2023.

Under the Bank Act, the Trust and Loan Companies Act, the Insurance Companies Act and the Cooperative Credit Associations Act, certain records of federally regulated financial organisations carrying on business in Canada must be maintained in Canada. In addition, an FRFI is expected to ensure that OSFI can access, in Canada, any records necessary to enable OSFI to fulfil its mandate.

In addition to Guideline B-10, OSFI has also released an advisory on *Technology and Cybersecurity Incident Reporting*, which sets out OSFI's expectations in relation to the immediate and ongoing reporting of cybersecurity incidents, which FRFIs should account for in their agreements with cloud providers. These expectations are in addition to the mandatory breach notification requirements under Canadian privacy laws.

In July 2022, OSFI released a final Guideline B-13, *Technology and Cyber Risk Management*, that is intended to serve as a complement to existing guidelines, including Guideline B-10. Guideline B-13 is expected to be read, and implemented, from a risk-based perspective to allow FRFIs to compete effectively, and take full advantage of digital innovation, while maintaining sound technology risk management. Guideline B-13 provides FRFIs with technologically neutral guidance to produce key "outcomes" in three domains:

- Technology and Cyber Governance and Risk Management;
- Technology Operations; and
- Cyber Security.

OSFI determined that Guideline B-13 will become effective on 1 January 2024 in order to

provide FRFIs sufficient time to self-assess and ensure compliance.

Personal Information Processing in Canada – Overview

A comprehensive review of all privacy obligations in Canada is beyond the scope of this summary. However, generally the following applies.

- A private sector organisation that uses third-party cloud services to collect, use, store or disclose personal information of individuals on its behalf will be subject to Canadian privacy legislation if the organisation is based in Canada or has a real and substantial connection to Canada.
- A service provider that provides cloud services and that collects, uses, stores or discloses personal information of individuals will be subject to Canadian privacy legislation if the service provider is based in Canada or has a real and substantial connection to Canada. In addition, Canadian customers of cloud services will seek to have their agreements for cloud services address the requirements of Canadian privacy laws, including on transfers of personal information outside Canada.

In Canada, privacy and personal information are regulated by both federal and provincial legislation.

The Personal Information Protection and Electronic Documents Act (PIPEDA) is the federal privacy law for private sector organisations. The OPC oversees compliance with PIPEDA. The OPC has issued a number of guidelines and case summaries that provide non-binding guidance on the OPC's interpretation of PIPEDA's obligations. As of January 2023, PIPEDA continues to be subject to an adequacy decision by the European Commission, to ensure that data is

processed in accordance with the General Data Protection Regulation (GDPR) and can be transferred from the EU to Canada without requiring additional data protection safeguards such as the use of standard contractual clauses.

PIPEDA applies in all provinces and territories in Canada to organisations engaged in commercial activities, except where a province or territory has enacted substantially similar private sector legislation and is subject to an exemption under PIPEDA (though PIPEDA continues to apply in those provinces in connection with federal “works, undertakings, and businesses” such as airlines, banks, and telecommunications companies and in connection with the interprovincial or international processing of personal information). British Columbia, Alberta and Quebec have their own legislation that regulates the collection, use and disclosure of personal information by private sector organisations in those provinces. In addition, most provinces have provincial legislation that regulates the collection, use and disclosure of personal health information. There are also federal and provincial public sector privacy laws that apply to the public sector.

In September 2021, Quebec’s legislature passed comprehensive reforms to the province’s privacy laws, the bulk of which will come into force in September 2023 (though note that certain requirements are effective as of September 2022, notably new mandatory breach notification requirements and obligations regarding the individual responsible for compliance with the Quebec law).

Quebec’s revised law is the first Canadian private sector privacy law to specifically address de-identification and anonymisation, automated decision-making, technology-based profiling, and data portability. Importantly, it will introduce

significant administrative penalties and fines, with penalties of up to CAD10 million or 2% of worldwide “turnover” and fines of up to CAD25 million or 4% of worldwide turnover, as well as a private right of action. The revised Quebec law will also require organisations to undertake privacy impact assessments prior to transferring personal information outside of Quebec.

In June 2022, the Canadian government tabled Bill C-27, the Digital Charter Implementation Act, 2022 – legislation that would, among other things, enact the Consumer Privacy Protection Act (CPPA) to replace the privacy provisions of PIPEDA. The proposed CPPA retains the principles-based and consent-based approach of PIPEDA. Among other things, the CPPA would:

- provide new regulatory tools and remedies for non-compliance, including significant monetary penalties;
- introduce a plain language standard for obtaining consent, with expanded transparency requirements;
- introduce broader “legitimate interest” and “business activities” exceptions to consent;
- clarify that the “manner” of collecting, using, and disclosing personal information, in addition to the purpose for doing so, must be appropriate in the circumstances, regardless of whether consent is required;
- create new individual’s rights of disposal and mobility;
- clarify the obligations of service providers when personal information is transferred to them for processing;
- provide for transparency requirements for automated decision-making systems and for transfers or disclosure of personal information; and

- define and create standards for the de-identification and anonymisation of personal information.

Bill C-27 would also create a new Personal Information and Data Protection Tribunal that would consider decisions and recommendations of the federal privacy commissioner.

The CPPA would allow the federal privacy commissioner to recommend, and for the Personal Information and Data Protection Tribunal to impose, penalties up to the greater of either CAD10 million or 3% of an organisation's annual global revenues. It would also provide for significantly expanded offences with fines up to the greater of either CAD25 million or 5% of annual global revenues, and a private right of action to permit recourse to the courts in certain circumstances.

Every aspect of privacy legislation might have some impact on the provision or use of cloud services.

The Personal Information Protection and Electronic Documents Act (PIPEDA)

Under PIPEDA, personal information means information about an identifiable individual. PIPEDA provides that an organisation is responsible for personal information in its control, or in its possession or custody, including information that has been transferred to a third party for processing. An organisation that transfers personal information to a cloud service provider remains primarily responsible for that personal information, and will want to ensure that the cloud services contract contains appropriate provisions to address the organisation's responsibilities in relation to the personal information transferred to and processed by the cloud service provider.

OPC guidance clarifies that an organisation must take all reasonable steps to protect personal information from unauthorised uses and disclosures while it is in the hands of the third-party processor, regardless of whether the information is being processed in Canada or a foreign country. An organisation must be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times, as well as an audit right.

PIPEDA requires that personal information be protected by security safeguards appropriate to the sensitivity of the information. The security safeguards must protect personal information against loss and theft, as well as unauthorised access, disclosure, copying, use or modification. The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection, particularly where large volumes of information are involved. The methods of protection should include physical, organisational, and technical measures.

PIPEDA case summaries provide non-binding guidance on the OPC's interpretation of these obligations.

An organisation will want to address the detail of a service provider's security safeguards in the cloud services contract. When it investigates security breaches, the OPC will closely examine the safeguards in place at the time of the breach and the contractual requirements to implement and maintain such safeguards. The cloud provider's obligations in the case of a breach of

security safeguards should be included in the cloud services contract.

In June 2022 (and following an unsuccessful attempt to pass similar legislation in 2020) the Canadian government re-introduced proposed legislation to replace PIPEDA's personal information provisions with a new law, the Consumer Privacy Protection Act.

Cross-border Transfers

PIPEDA does not prohibit an organisation from transferring personal information to an organisation outside Canada for processing. However, the OPC expects that organisations must assess the risks to the integrity, security and confidentiality of personal information when it is transferred to third-party service providers operating outside Canada. The OPC expects that organisations will advise their customers that their personal information may be sent to another jurisdiction for processing and that, while the information is in another jurisdiction, it may be accessed by the courts, law enforcement and national security authorities of that jurisdiction.

Alberta's private sector privacy law requires organisations that transfer personal information outside Canada to maintain policies on:

- the countries outside Canada in which the collection, use, disclosure or storage may occur; and
- the purposes for which the service provider outside Canada has been authorised to collect, use or disclose personal information, and to provide information on such policies on request.

Beginning in September 2023, Quebec's privacy law will soon require organisations, prior to personal information being transferred out of

Quebec, to conduct a privacy impact assessment and to determine whether the transferred information will receive protection in accordance with "generally accepted best practices respecting the protection of personal information" in the target jurisdiction.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights Big Data

Big data initiatives in Canada must balance the need to maximise the value of large data sets with the requirements of Canadian privacy laws. Holding large amounts of personal information can lead to issues surrounding consent, transparency, accountability, and the requirement to limit the collection of personal information to that needed for the purposes identified by the collecting organisation.

Additionally, holding large volumes of personal information requires organisations to implement more stringent safeguards in order for them to be considered appropriate under Canadian privacy laws. Holding greater amounts of personal information about a greater number of individuals also increases the risks of a class action in the event of a data breach, and the liability that would result from a breach.

To limit these risks, organisations are increasingly using anonymised and (in the case of machine learning) synthetic data. Anonymised and synthetic data, where there is no "serious possibility" that the information, alone or in combination with other information, can identify an individual (ie, be re-identified) are not personal information and thus not subject to existing Canadian

privacy laws. However, the potential for re-identification increases as data sets grow and other data sets become available for matching, and statistical and other methods that can re-identify data are becoming increasingly sophisticated.

Canada's federal privacy law does not currently include a definition of de-identified or anonymised data, or define what it means to de-identify or anonymise data. Recent revisions to Quebec's privacy law, effective September 2023, introduce anonymisation and de-identification as separate concepts. Under the new Quebec law, anonymised information is information that:

- no longer allows an individual to be identified directly or indirectly where "it is at all times reasonable to expect in the circumstances" that it will not identify an individual; and
- is anonymised in accordance with "generally accepted best practices".

De-identification is a less stringent standard and is information that no longer allows the direct identification of an individual. A business handling de-identified information will have a requirement to take "reasonable steps to avoid re-identification". Proposed revisions to federal private sector privacy law being considered by Parliament would create a similar distinction between de-identified and anonymised information.

Artificial Intelligence

As mentioned in **3.1 Highly Regulated Industries and Data Protection**, in June 2022 the Canadian government tabled Bill C-27, the Digital Charter Implementation Act, 2022. This legislation would, among other things, enact the Artificial Intelligence and Data Act (AIDA) as well as comprehensive reforms to Canada's federal private sector privacy law regime. Bill C-27 remains in

the legislative process under consideration by the House of Commons at this time (January 2023).

If passed, AIDA would regulate the design, development, and use of AI systems in the private sector with a focus on mitigating the risks of harm and bias in the use of "high-impact" AI systems. AIDA would set out positive requirements for AI systems as well as monetary penalties and new criminal offences on certain unlawful or fraudulent conduct in respect of AI systems.

Some of the issues applicable to big data also apply to AI and machine learning (ML), as both typically rely on large data sets. Canadian privacy law requirements regarding consent, openness, and transparency are areas of concern with regard to AI and ML. Meaningful consent and transparency require that organisations identify the purposes of the collection and use of personal information. This is more difficult in the case of AI and ML, since those purposes can evolve over time as ML algorithms and models make discoveries and predictions based on data.

Beginning in September 2023, Quebec's privacy law will require that individuals be informed when their personal information is used to make a decision about them using automated processing, and that individuals must be offered the opportunity to make observations about the decision.

Organisations that use ML might also encounter issues with Canadian intellectual property laws. Canadian copyright law does not protect databases where the creation of a database or other compilation is not an exercise of "skill and judgement", and it does not protect individual data elements removed from a database or other

compilation (for example, where those data elements are mere facts such as street addresses).

Furthermore, an ML algorithm or model is not considered an “inventor” under the Patent Act or an “author” under the Copyright Act. For Canadian copyright law, the choice of the ML algorithm, training data, and the conduct of the training would have to be an exercise of skill and judgement for the ML model and its output to be potentially considered an original work eligible for copyright protection (subject to the output or model otherwise being the proper subject matter of copyright).

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There are no laws that specifically address internet of things (IoT) services and devices in Canada. As a result, any legal considerations regarding the IoT arise from the application of general laws to IoT services and devices.

Canada’s private sector privacy laws apply to the use of IoT devices and services by individuals that allow organisations to collect personal information. In Alberta, British Columbia (BC), and Quebec, provincial private sector privacy laws will also apply to the use of IoT devices in the workplace, while the federal law (PIPEDA) will apply to federally regulated workplaces (ie, to federal works, undertakings and businesses) across Canada. Alberta, BC, and federal privacy laws are notice-based in connection with employee personal information and the employee-employer relationship, and employers must provide notice to employees of the use of IoT devices that collect employee personal informa-

tion and the subsequent use and disclosure of that information.

Even where employers give notice, however, the processing of personal information must also be for purposes a reasonable person would consider appropriate in the circumstances. Thus, the use of IoT devices to collect employee personal information for inappropriate purposes, for example location tracking or video surveillance where less intrusive measures could be used, may still run afoul of Canadian laws even if employees were provided notice of the tracking.

Other than for limited exceptions, Canada’s private sector privacy laws are consent-based. From a privacy perspective, the IoT poses a challenge in obtaining meaningful consent as it allows passive information collection that may be less obvious to individuals and more difficult to explain. Transparency is particularly important if the IoT service provider is contemplating secondary uses of personal information (ie, uses in addition to providing the services), for example marketing or advertising. The ability of IoT devices to collect large amounts of data must be weighed against requirements to limit the collection of personal information.

The OPC has released guidance targeted towards manufacturers of IoT devices. In particular, the guidance recommends as a best practice that organisations perform a privacy impact assessment before releasing IoT products.

Beginning in September 2023, Quebec law will require organisations that use technologies that can identify, locate, or profile individuals to have this functionality off by default. IoT devices and services will have to comply with this requirement.

IoT devices and services are also seeing growing use in the healthcare sector. Most Canadian provinces have enacted health privacy legislation regulating the use of personal health information by healthcare providers. Depending on the province, health privacy legislation may apply to the healthcare provider, or to both the healthcare provider and its service provider.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Audio-Visual Services

All traditional audio-visual services (television, radio, cable, etc) operating in Canada are required to be licensed or exempt from licensing by the CRTC under the Broadcasting Act. The CRTC issues licences for terms not exceeding seven years and makes those licences subject to conditions related to the circumstances of the licensee that it deems appropriate for the implementation of Canada's broadcasting policy. Licensees are generally subject to a variety of Canadian content, programme expenditure and/or contribution obligations.

Television and radio stations that use radio spectrum are also required to obtain authorisation from the Department of Innovation, Science and Economic Development Canada (ISED) in accordance with the Radiocommunication Act. Applications to obtain a broadcasting licence must be filed with the CRTC, and the CRTC is required to hold a public hearing to consider the application. The process typically takes between eight and 18 months to conclude.

In order to be eligible to hold a broadcasting licence, a company must be owned and effectively controlled by Canadians. Broadcasting

licensees are generally required to pay two types of licence fees (Part 1 and Part 2 fees) under the Broadcasting Licence Fee Regulations:

- the Part 1 fee is a licensee's pro rata share of the annual cost of the CRTC's operations; and
- the Part 2 fee is established by the Canadian government using a complex formula and paid on a pro rata basis by each licensee.

The CRTC also has the authority to exempt classes of broadcasting undertakings from holding a licence, and has exercised this authority in a number of circumstances, including with respect to small satellite-to-cable (discretionary) services and small cable distributors. Exemption orders issued by the CRTC contain terms and conditions that apply to an entire class of broadcasting undertaking and do not require a company to pay any licence fee or to obtain any further authorisation from the CRTC.

Online Video-Sharing Platform Services

Individuals and companies that operate online video-sharing platforms (including user-generated content) and other online streaming services in Canada do so in accordance with a CRTC exemption order called the exemption order for digital media broadcasting undertakings. To operate under this exemption order, an online video channel must comply with minimal obligations, which include a prohibition on granting undue preferences or disadvantages and a requirement to submit to the CRTC's dispute resolution process. There are no licence fees or Canadian ownership and control requirements applicable to online video channels.

In February 2022, the Canadian government introduced legislation in Parliament to amend the Broadcasting Act (Bill C-11, The Online Stream-

ing Act). Bill C-11 will amend the Broadcasting Act to empower the CRTC to impose conditions on online video-sharing platforms, which the legislation calls “online undertakings”, providing the CRTC with express legislative authority to regulate the distribution of programming by digital streaming services and online communications platforms, notably through financial and non-financial measures to support the production and exhibition of Canadian content.

Legislative debate around Bill C-11 indicates that user-generated content will not be regulated, but the platforms that share them may be. Among other reforms, Bill C-11 would also provide the CRTC with the authority to impose administrative monetary penalties (AMPs) for violations of certain provisions of the Act and provide the CRTC with more explicit information-gathering powers.

At the time of writing, Bill C-11 has passed third reading in the House of Commons and the Senate and is expected to become law in early 2023.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Telecommunications

The Telecommunications Act regulates telecommunications common carriers and telecommunications service providers. It does not regulate technologies.

The Telecommunications Act defines a telecommunications common carrier as a person who owns or operates a “transmission facility” used by that person or another person to provide telecommunications services to the public for compensation. A transmission facility means

“any wire, cable, radio, optical or other electromagnetic system, or any similar technical system for the transmission of intelligence between network termination points, but does not include an exempt transmission apparatus”.

A telecommunications service means a service provided by means of telecommunications facilities, which in turn is broadly defined to include any facility or thing that is used or capable of being used for telecommunications or for any operation directly connected with telecommunications, including a transmission facility. A telecommunications service provider (TSP) is defined as “a person who provides basic telecommunications services” and includes telecommunications service resellers.

Telecommunications regulation in Canada is therefore technology-agnostic and there are no restrictions on the use of new technologies by carriers or service providers. Certain services are, however, subject to registration and other regulatory requirements. For example:

- non-dominant carriers and resellers must register with the CRTC, and service providers that carry traffic internationally must obtain a Basic International Telecommunications Services (BITS) licence;
- providers of Voice over Internet Protocol (VoIP) services must obtain approval of their 911 emergency calling arrangements; and
- Competitive Local Exchange Carriers (CLECs) must obtain approval of their interconnection arrangements with other carriers, and are subject to the mandated provision of certain services to persons with disabilities and to privacy and consumer protection provisions, all of which have been standardised.

The CRTC does not charge for registering as a TSP, but it operates a contribution fund to which carriers and TSPs are required to contribute based on a percentage of their Canadian telecommunications revenues once they are generating CAD10 million or more in revenues. Money from this fund is used to finance video relay services and the extension of broadband facilities to rural and remote parts of Canada.

VoIP service providers need to register with the CRTC as a carrier or reseller depending on whether they own transmission facilities. VoIP service providers also require a BITS licence, which entails an application to the CRTC. No fees are applicable for these registrations, approvals or licences other than contribution to the fund referenced above. VoIP service providers that provide access or egress to or from the public switched telephone network (PSTN), and that use North American Numbering Plan (NANP) telephone numbers to route calls, require CRTC approval of their 911 emergency services before providing service in Canada.

The provision of instant messaging is regulated if it involves the use of transmission facilities owned or leased by a carrier or TSP providing the messaging service. Registration as a reseller or non-dominant carrier will be required. A BITS licence will also be required. No fees are applicable other than contribution to the fund referenced above. The provision of an app over the public internet without transmission services is generally not regulated.

Radiocommunications

The Radiocommunication Act regulates spectrum, and the Minister of Innovation, Science and Industry (the “Minister”) is empowered to issue radio or spectrum licences, or to exempt frequencies from the requirement for a licence.

The Minister oversees the department of Innovation, Science and Economic Development Canada (ISED) and is empowered to charge fees for radio or spectrum licences or to hold competitive bidding auctions.

Radio apparatus must meet ISED standards and certification requirements before they can be marketed, sold, offered for sale or imported into Canada. Certifications from specified countries can be used as the basis for obtaining Canadian certification, but certification from foreign regulators like the FCC does not serve as authorisation to market, sell, offer for sale, or import radio apparatus in Canada.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

As with cloud services, there are no private sector laws of general application focused primarily on the provision of IT services to the private sector in Canada, but other Canadian laws will apply to the provision of such services.

Applicable laws include those relating to the processing and protection of personal information (both in the public and private sectors) and industry-specific regulations, such as requirements governing the use of IT services (and outsourcing generally) by federally regulated financial institutions (FRFIs), and requirements that certain records of FRFIs be located in Canada, as well as laws regarding personal health information that apply to healthcare service providers.

All Canadian provinces and territories other than Quebec operate under a common law regime, and the law with respect to contracts will be

broadly similar to those of other common law jurisdictions such as the United States and United Kingdom, subject to Canadian jurisprudence and provincial laws concerning contracts. Quebec is a civil law jurisdiction subject to the Civil Code of Quebec, including provisions of the code that address service contracts.

The issues discussed in **3. Cloud Computing** regarding cloud services also apply to IT services.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Provincial Laws and Regulations Governing the Use of Electronic Signatures

The use of electronic signatures is governed by provincial statute and regulation, and the requirements and conditions for use vary heavily from province to province – as such, this summary is not intended to be comprehensive. As an example, Ontario’s Electronic Commerce Act (the “Ontario ECA”) is generally permissive of the use of electronic signatures, which it defines as “electronic information that a person creates or adopts in order to sign a document and that is in, attached to or associated with the document”.

The Ontario ECA (and other provincial statutes and regulations), however, forbid the use of electronic signatures for particular types of documents, such as wills, powers of attorney, or documents that constitute negotiable instruments (in the case of the Ontario ECA). The Ontario ECA also requires the electronic signature to meet any prescribed technology standards or requirements.

The Ontario ECA does not apply to the use of biometric information as an electronic signature or digital personal identifier, although they can be used if all parties to a transaction agree to their use.

Federal Laws and Regulations related to Financial Institutions

Federal laws and regulations may also apply to financial institutions – or other entities involved in the provision of services involving the transfer of money – and require the identification and validation of the government identification of their customers or users.

For example, the Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations prescribe certain acceptable methods of identity verification that a reporting entity (generally, an entity involved in providing financial services) must use when required to verify the identity of an individual, corporation or entity other than a corporation. These methods include the validation of government-issued photo identification, reliance on the individual’s credit file, or a dual-process method (where information must come from two different reliable sources).

Guidance issued by the Financial Transactions and Reporting Analysis Centre of Canada (FINTRAC), the financial intelligence unit of Canada’s federal Department of Finance, contemplates the use of digital identification and verification services in the context of the government-issued photo identification method of identity verification when an individual is not physically present. At this time, FINTRAC guidance provides few details with respect to the specifications or technical requirements for such services, other than that such services must be able to determine that a government-issued photo identification document is authentic, valid and current.

Fasken is a leading international business law and litigation firm. With over 700 lawyers, the firm has offices in Vancouver, Calgary, Toronto, Ottawa, Montreal, Quebec City, London and Johannesburg. Its TMT practice groups are routinely recognised as top band/tier in Canada, and it advises companies on most major consultation or policy proceedings held by Canada's regulators. Fasken's TMT industry group draws upon the firm's expertise in a broad range of practice areas to advise participants in the TMT industry on important legal issues relating to: technology developments and contracts; regulatory communications (including broad-

casting, telecommunications, spectrum and wireless, copyright, antitrust/competition and marketing, privacy, data security and trade); entertainment and media (including production, distribution, video games, online entertainment and online gaming); business law (including foreign ownership restrictions, start-ups, debt and equity financing, public-private partnerships, specialised commercial agreements, mergers and acquisitions, labour, employment and human rights, intellectual property and tax); and dispute resolution (including public law advocacy, commercial litigation and mediation and arbitration).

Authors



Christopher Ferguson focuses his practice on technology, privacy, and regulatory matters. He regularly advises on IT and technology matters, including: negotiating and drafting

services, outsourcing, and licence agreements; privacy and data protection issues; and legal and regulatory developments in the technology sector. Chris has advised and negotiated services and cloud agreements for essential systems and mission-critical outsourcing arrangements. He has advised on privacy, data protection, the Canadian anti-spam legislation (CASL), consumer protection, communications law, legal compliance, and advocacy before regulators and policymakers. This has included dealings with regulators and participation in proceedings before Canadian courts and tribunals.



Scott Prescott practises primarily in the areas of communications and administrative law. He has specific expertise in the legal, regulatory and policy

frameworks governing the broadcasting and telecommunications industries in Canada. Scott provides complex legal and strategic advice to cable and satellite distributors, television and radio broadcasters, online content providers and Canadian and foreign programming services, as well as to wireline and wireless telecom companies and internet service providers. His clients include a range of leading Canadian and international communications companies. He has been involved in numerous licensing and policy proceedings before the Canadian Radio-television and Telecommunications Commission.



Leslie Milton provides complex legal and strategic advice to Canadian and foreign wireline, wireless and satellite telecommunications service providers on all aspects of

telecommunications and radiocommunications regulation in Canada. She acts for clients in a broad range of proceedings before the Canadian Radio-television and Telecommunications Commission (CRTC) – including concerning international licensing, wholesale and retail tariffs, forbearance, foreign ownership, consumer safeguards, local access and interconnection, internet services, access to support structures and public rights of way, numbering, do-not-call, anti-spam (CASL) and voter contact proceedings. She also acts before Innovation, Science and Economic Development Canada (ISED), representing wireless and satellite operators on spectrum and radio licensing, spectrum policy proceedings, antenna siting and sharing, equipment certification and other regulatory compliance matters. Leslie also advises on Canadian competition law and the Investment Canada Act.



Paul Burbank is a corporate/commercial lawyer that works with Fasken's communications law group to provide advice on telecommunications and broadcasting, as well as other

commercial and regulatory matters related to technology. Paul's work involves supporting client businesses and legal teams with practical, regulatory advice for the launch of new telecommunications services and technology products. His commercial work is IT-focused and includes negotiating and drafting services, licence agreements, assisting in implementing enterprise-wide IT outsourcing arrangements and deployments of physical technology infrastructure, such as fibre optic cable and data centres. He collaborates with Fasken's broader TMT team on market access, privacy, lawful interception and telecommunications-based marketing practices, including anti-spam laws.

Fasken

Bay Adelaide Centre
333 Bay Street, Suite 2400
P.O. Box 20
Toronto, ON
M5H 2T6
Canada

Tel: +1 416 366 8381
Fax: +1 416 364 7813
Email: toronto@fasken.com
Web: www.fasken.com

FASKEN

Law and Practice

Contributed by:

Cloud Li, Joanna Jiang, Zhengwei Yang
and Dimitri Phillips

DaHui Lawyers see p.114

Contents

1. Metaverse	p.97
1.1 Laws and Regulations	p.97
2. Digital Economy	p.100
2.1 Key Challenges	p.100
3. Cloud and Edge Computing	p.102
3.1 Highly Regulated Industries and Data Protection	p.102
4. Artificial Intelligence and Big Data	p.105
4.1 Liability, Data Protection, IP and Fundamental Rights	p.105
5. Internet of Things	p.107
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection	p.107
6. Audio-Visual Media Services	p.107
6.1 Requirements and Authorisation Procedures	p.107
7. Telecommunications	p.109
7.1 Scope of Regulation and Pre-marketing Requirements	p.109
8. Challenges with Technology Agreements	p.110
8.1 Legal Framework Challenges	p.110
9. Trust Services and Digital Entities	p.111
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes	p.111

1. Metaverse

1.1 Laws and Regulations

To date, no laws or regulations that specifically regulate the metaverse have been enacted in the People's Republic of China (PRC). However, metaverse platform providers and participants should pay attention to laws and regulations regarding the PRC telecoms regime, virtual property, personal information (PI) and other data, and intellectual property (IP), including the following:

- the PRC Telecommunications Regulations, the PRC Administrative Measures for the Licensing of Telecommunications Business and the PRC Classification Catalog of Telecommunication Services set out myriad restrictions and requirements on telecoms services in China;
- the PRC Copyright Law, the PRC Trademark Law and the PRC Anti-Unfair Competition Law (AUCL) are key pieces of legislation concerning IP rights in China;
- the PRC Civil Code came into effect on 1 January 2021 and covers a wide range of parties' private rights; Article 127 clearly imparts legal status to virtual property, just the same as any object of civil rights; and
- the various laws of the cybersecurity regime, beginning with the PRC Cybersecurity Law of 2017 and most recently including the PRC Data Security Law and the PRC Personal Information Protection Law (PIPL), set out numerous rules for the collection, transfer and other processing of various kinds of data.

Each of the above areas of law is further specified by national and local regulations and rules, although still not addressing the metaverse specifically.

The metaverse is specifically addressed, however, in development plans of several large cities, including Beijing, Shanghai and Chongqing, in order to attract investments from metaverse companies. Furthermore, in April 2022, an industry association – the Shenzhen Information Service Industry Blockchain Association – released two documents with specifications of terms and technical requirements for their respective areas: “Metaverse Identity Authentication System Based on Blockchain Technology” and “Metaverse Payment Clearing System Based on Blockchain Technology”.

PRC Telecoms Regime

Depending on the business model and the telecoms resources to be used for the metaverse, PRC telecoms regulatory requirements might be triggered. The internet and telecoms sectors in the PRC are subject to a comparatively rigid licensing regime, which might be applicable to companies offering services to PRC customers via an onshore model (with servers, data and other facilities/resources within China).

In particular, if an entity offering services via an onshore model would like to engage in activities that fall under the definition of “basic telecoms services” or “value-added telecoms services”, then it will first need to obtain the relevant licences according to the Catalog of Telecommunications Businesses, issued and regularly amended by the Ministry of Industry and Information Technology (MIIT). As examples, depending on the business model and product features to be implemented, engaging in metaverse activities may require an Internet Content Provider (ICP) licence or a Service Provider (SP) licence (if the services are provided through mobile networks), at least one of which is a prerequisite for metaverse platform operators to provide ser-

vices falling into any one of the following sub-categories:

- Information Publishing Platform and Delivery Services, which usually refer to online services provided by a platform disseminating content in the form of text, video or applications;
- Information Community Platform Services, which usually refer to online services provided by platforms that allow users to exchange information;
- Information Search Services, which usually refer to online services provided by search engines such as Baidu and Bing;
- Information Instant Interaction Services, which usually refer to online services that allow users to exchange information instantly through a service provider's product; and
- Information Protection and Process Services, which usually refer to online services relating to anti-virus functions and information protection services.

Some of the activities (eg, certain basic telecoms services) can only be provided by state-owned entities, while others need at least 50% or 51% local Chinese shareholding (eg, services falling under the requirement for an ICP licence), and some are completely open to any kind of investment – with more and more falling under this last category every year.

IP Protection

The metaverse has created an emerging environment that revolutionised the traditional application of the internet, and is creating a virtual society reflective of the physical world. User-generated content makes infringement of IP more common. Metaverse participants usually create scenes in the virtual world based on their preferences in the real world, transferring, copy-

ing and linking trade marks, signs, designs and other copyrights or works protected under IP law into the virtual world. These activities likely implicate IP protection laws, as the PRC Copyright Law and PRC Trademark Law are quite clear that the author and trade mark registrant enjoy the exclusive right of any given copyright or trade mark, and there are currently no exceptions or special provisions that would clearly apply to metaverse activities.

In late 2022, draft amendments to the AUCL were released and included the new concept of “commercial data”, which is defined as data that is lawfully collected by business operators, has commercial value and employs corresponding technical management measures. The draft amendments would impose additional requirements for business operators processing “commercial data” and prohibit certain related conduct, such as disrupting technical management measures of other business operators, breaching relevant contracts, agreements or protocols, acting contrary to the principle of good faith, etc.

Protection of Virtual Property

Although China does not have any laws or regulations that specifically address the protection of virtual property and assets, Article 127 of the PRC Civil Code has been widely understood and interpreted as providing that rights to virtual property and assets have been officially recognised as legal property rights and are thus subject to protection under the civil law regime, just like physical property rights. However, Article 127 further provides that the protection of virtual property and assets is still subject to further, more detailed regulations.

In a court case in which two parties had reached a series of agreements regarding the purchase of Bitcoin mining services, the Beijing Third Inter-

mediate People's Court ruled that such agreements were void and hence unenforceable, as they mainly concerned Bitcoin mining, which is explicitly and strictly prohibited by PRC law. However, in another case (published as a "Typical Case"), the specialised Hangzhou Internet Court ruled that Bitcoin should generally be deemed a commodity, and therefore should be protected by the relevant laws and regulations regarding personal property. The conclusion was also supported by the Shanghai High People's Court in its comments in another case with a similar factual background.

Regulation of Data and Personal Information

There are no PRC rules on data privacy that relate to the metaverse explicitly. However, an operator – and possibly a user – of the metaverse may be subject to various other PRC laws and regulations relating to data protection and privacy.

In particular, due to the massive volume of PI that they might possess or collect, metaverse platform providers are likely to be subject to numerous rules under the PIPL, including the requirement to obtain consent before processing PI from users (except in certain situations permitted by law) and disclosing the intended use, purpose, means, scope and rules of the processing. Special requirements apply to transferring PI outside the PRC, especially large volumes of PI.

Metaverse platform providers and participants such as PCCW Limited and ZTE who engage in multiple industries including "critical information infrastructure" could be deemed Critical Information Infrastructure Operators (CIIOs) and therefore subject to more strict obligations under the cybersecurity regime. For example, for some such operators of the metaverse, the offshore transfer of PI or other information constitut-

ing "Important Data" collected within mainland China may be subject to even more stringent requirements or even absolute prohibitions. The draft amendments to the AUCL would introduce another category of data, "commercial data", with a range of attached rights and responsibilities.

The PRC Data Security Law imposes data security and privacy obligations on entities and individuals carrying out data activities. It also introduces a data classification and hierarchical protection system based on the importance of data in terms of economic and social development, as well as the degree of harm that would be caused to national security, public interests or the legitimate rights and interests of individuals or organisations if such data were to be tampered with, destroyed, leaked or illegally acquired or used. Appropriate protective measures are required to be taken for each category of data. For example, a processor of "Important Data" must designate personnel and a management body responsible for data security, carry out risk assessments for its data processing activities, and file risk assessment reports with the Cyberspace Administration of China (CAC).

A particularly hot topic that has been gathering steam for a few years is facial recognition technology. Cases started cropping up around 2019, such as that of Guo Bing v Hangzhou Wildlife World Co., Ltd., in which the court ruled that the customer has the right to reject a service provider's requirement to collect and use facial features.

Litigation over such matters has mushroomed recently, since the Supreme People's Court released the Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases involving the

Processing of Personal Information Using Facial Recognition Technology in July 2021. In the case of *Gucheng v Tianjin Branch of Lanzhou Chengguan Property Management Co., Ltd.*, a resident living in an apartment complex refused to provide facial information to the management company as the method of unlocking the complex's entryway. In 2022, the First Intermediate People's Court of Tianjin Municipality supported that the resident has the right to refuse to provide facial information, and the company must provide other methods to unlock the entryway.

2. Digital Economy

2.1 Key Challenges

Laws and Regulations

While digital economies can generally be said to be subject to a wide range of laws, the following are especially pertinent in the PRC:

- the PRC E-Commerce Law, which came into effect on 1 January 2019 and is the first law regulating processes relating specifically to digital commerce;
- the regulations of the PRC telecoms industry, as detailed in **1.1 Laws and Regulations**;
- the PRC Electronic Signatures Law, which was revised and took effect on 23 April 2019, and is another key law governing electronic transactions;
- the AUCL, most recently revised in 2019, and the PRC Anti-Monopoly Law, most recently revised in 2022, are widely regarded as playing an essential role in the regulation of the digital economy – anti-monopoly authorities in particular are increasingly targeting technology giants that have huge market shares in e-commerce and the digital economy even more fundamentally; and

- the laws and regulations of the cybersecurity regime, as detailed in **1.1 Laws and Regulations**, especially as they pertain to “Important Data” (eg, sensitive financial data) and CIOs.

E-Commerce

The PRC E-Commerce Law defines an e-commerce operator as any natural person, legal person or unincorporated association that carries out business activities through information networks such as the internet to sell commodities or offer services, including operators of e-commerce platforms, business operators on e-commerce platforms, and other e-commerce operators that sell commodities or offer services on websites they develop themselves or through other network services. Importantly, this definition could extend to individuals who conduct business activities such as selling second-hand commodities or providing procurement services through Taobao.com or JD.com.

The PRC E-Commerce Law includes a large number of rules covering a wide range of conduct, even addressing customer comments, which the law prohibits operators from removing or modifying. For example, one of the largest platforms for individual customers buying and selling second-hand luxury goods in China, Secoo, was investigated by the Beijing Xicheng Branch of the State Administration for Market Regulation and fined RMB50,000 for deleting one negative review from its platform.

Discriminatory pricing using big data is also regulated by the PRC E-Commerce Law, which prohibits schemes that customise the display of search results of products and services based on consumers' interests, preferences, habits and other personal characteristics.

Although such practices are prohibited by the PRC E-Commerce Law, individual customers generally lack sufficient resources and capabilities to prove that any online platform adopts discriminatory pricing based on algorithms, which results in online platforms rarely being penalised for such conduct. As an example, in litigation where Ctrip (one of the largest online travel agencies in China) was allegedly collecting PI from a user and raised the accommodation price for the user based on analysis of her data, the court ruled that Ctrip infringed upon the user's information rights but remained silent on whether and how Ctrip conducted price customisation based on data analysis. It is challenging under the current legal regime for customers to successfully persuade the court or administrative authorities that the price is different as a result of algorithms based on personal data collected from customers.

PRC Telecoms Requirement on E-commerce

Which telecoms licences and rules will apply to an e-commerce participant will depend on its business and model. Typical licences include those for Electronic Data Interchange (EDI) and ICP. The former is needed for platforms featuring third-party sellers (ie, individuals or entities running online stores on the platform), while the need for the latter depends on whether such platforms enable other services that might fall into sub-categories of information services under the question.

Interestingly, foreign investment in an ICP licence holder is capped at 50%, whereas there is no restriction on foreign shareholding for an EDI licence holder. That said, an e-commerce business featuring the sale of products manufactured or procured by the operator itself generally does not need an ICP (or EDI) licence (although a so-called "ICP filing" is generally required).

Other key rules generally applicable to parties using a website or other online platform to sell their own or third parties' goods or services include requirements that e-commerce platform operators have adequate funds (RMB10 million minimum for national level and RMB1 million for provincial level), specialised personnel and a reputation for long-term service. Foreign and foreign-related telecoms enterprises (FITEs) in China are subject to the same registered capital requirements. In 2022, it was confirmed that FITEs are no longer required to have a "record of good performance and operating experience" prior to being established in China.

Unfair Competition

The current AUCL expressly restricts network-based anti-competitive conduct, but only based on high-level provisions. However, the AUCL is currently undergoing another revision process, with the public comment period having closed at the end of 2022. The draft amendments aim to improve anti-competition rules for the digital economy, with several newly added provisions, including Article 4 as a basic guideline and Articles 15, 17, 18 and 19 targeting anti-competitive conduct in the area of digital economy specifically.

In the version of the AUCL currently in effect, Article 12 prohibits acts impeding or disrupting the normal operation of network products or services, specifically including:

- inserting a link or forcing a URL redirection in a network product or service legally provided by another business operator without the consent of that business operator;
- misleading, deceiving or compelling users into modifying, closing or uninstalling a network product or service legally provided by another business operator; and

- implementing in bad faith an incompatibility with a network product or service legally provided by another business operator.

In the draft amendments of the AUCL, Article 4 would function as a fundamental cornerstone prohibiting business operators from using data and algorithms, technology, capital strength or platform rules to engage in unfair competition practices. More specific to the digital economy, unfair competition activities explicitly prohibited by the draft amendments include:

- disrupting the order of fair competition in the market by influencing user choices by using big data collected from users and algorithms to process it;
- violating industry practices or technical specifications to hinder access to other network products or services;
- acquiring commercial data of other operators in an improper way; and
- customising prices for different users based on analysis of their preferences and other characteristics by using algorithms.

Data and Privacy Protection

Subject to the specific data stored or processed during digital economy activities, service providers could be required to comply with various obligations under the PRC Cybersecurity Law, the PRC Data Security Law and/or the PRC Critical Information Infrastructure Regulations, such as local data hosting and offshore data transfer restrictions (see **1.1 Laws and Regulations**). Ultimately, in some circumstances, CIIOs with offshore components (eg, servers hosted outside China, or networks between PRC subsidiaries and foreign parent companies) might have to restructure entities or operations to comply with these laws and regulations.

Under the PIPL and other regulations (such as the PRC Measures for Cybersecurity Review), an e-commerce platform that processes large volumes of PI or operates a certain type of business will be subject to enhanced requirements for PI protection, including:

- completing cybersecurity review if processing PI of one million or more individuals and applying to go public outside China;
- establishing an independent body mainly composed of external members to supervise protection of PI;
- ceasing the provision of any service to any product or service provider operating on the e-commerce platform who commits a serious violation of any law or administrative regulation in the processing of PI; and
- publishing a social responsibility report concerning PI protection on a regular basis and accepting supervision from the public.

The PRC Consumer Protection Law sets similar requirements for the collection of consumer information by business operators. Other high-level laws provide general privacy protections, such as the PRC Tort Law, the PRC Civil Code and the PRC Criminal Law. Draft amendments to the AUCL would introduce a new category of data, “commercial data”, with new attached rights and responsibilities (as set out in **1.1 Laws and Regulations**).

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Regulations

There are no laws, and only a few regulations, in the PRC specifically addressing cloud and edge computing, but cloud and edge computing

service providers are subject to various general bodies of legislation and regulation, including:

- the PRC Telecommunications Regulations and related regulations, such as the PRC Administrative Measures for the Licensing of Telecommunications Business and the PRC Administrative Measures for Internet Information Services;
- the PRC Cybersecurity Law and related laws and regulations forming the framework for governing data security and privacy protection in China;
- the PRC Cryptography Law;
- the Measures for Security Evaluation for Cloud Computing Services; and
- the Circular on Regulating the Market Operations of Cloud Services (Draft for Comments).

The Standardisation Administration of China (SAC; also known as TC260) also publishes numerous non-binding, recommended standards relating to cloud and edge computing, covering topics ranging from security guidance to data centre requirements and file service application interfaces.

PRC Telecoms Regulations

Depending on the business model and features of cloud computing services, engaging in cloud services within China may trigger value-added telecoms licensing requirements. Cloud services might implicate the requirements for an “internet data centre” (IDC) or “internet resource collaborative” (IRC) licence. An IDC/IRC licence essentially allows a company to directly provide server hosting or cloud storage solutions, as well as other related business activities. Foreign shareholding in any holder of an IDC/IRC licence is completely prohibited (with the exception of qualified service providers under the Mainland and Hong Kong Closer Economic Partnership

Arrangement Agreement on Services Trade, who can own up to 50%).

Circular on Regulating the Market Operations of Cloud Services (Draft)

On 24 November 2016, the MIIT released a draft of a new circular for regulating cloud services, with the following key points, which are at least to some extent already enforced in regulatory practice.

- In any co-operation between a local cloud service provider (who holds a relevant telecoms licence) and a foreign partner, the former is prohibited from:
 - (a) transferring or lending (explicitly or “in disguised form”) any telecoms licence to the partner, or providing any resource, site, facility, etc, for the purpose of assisting any unlawful conduct of the partner;
 - (b) allowing the partner to directly conclude a contract with a user;
 - (c) providing users with services by using the trade mark and brand of the partner only; and
 - (d) illegally providing a partner with network data or user PI.
- Cloud services providers may not independently establish a virtual private network (VPN) or other special connection to the internet, except as authorised by the MIIT.
- When providing services for domestic users, an operator of cloud services must locate service facilities and network data within China and abide by the relevant state provisions for cross-border operations, facility maintenance and data flows.

Special Regulatory Reviews for Cloud and Edge Computing

The PRC Measures for Cybersecurity Review provides that any CIO seeking to procure any

network product or service that affects or may affect national security needs to undergo a so-called “cybersecurity review”. Some cloud and edge computing products and services – such as high-performance computers or servers, mass storage equipment, large databases or applications, and network security equipment – are specifically included in the scope of network products that are subject to the PRC Measures for Cybersecurity Review. Therefore, any CIO procuring such cloud and edge computing products or services, or others that may affect national security, will need to go through a process that may include an application for cybersecurity review being submitted to the Cybersecurity Review Office (CRO), an initial review by the CRO, and potentially a “special review” by the CRO if no agreement can be reached by CRO members after the initial review.

Non-CIOs are unlikely to need to go through a cybersecurity review for procuring cloud or edge computing products or services, although there is a broad catch-all provision that may require any network operator or data handler whose processing activities might impact state security to undergo a cybersecurity review (and any party processing PI of one million or more individuals and applying to go public outside China will need to conduct a review, as detailed in **2.1 Key Challenges**).

The Measures for Security Evaluation for Cloud Computing Services provide that cloud computing service providers supplying the Communist Party of China, government agencies or any CIO may complete a security evaluation of each of their cloud computing platforms providing such services. The evaluation result can be used as a reference to support a supplier’s bid for procurement contracts. As of November 2022, 63 cloud computing service providers had passed

this security evaluation, including cloud computing service providers for more than half of China’s provincial governments. The evaluation may cover the following:

- the credit and operation status of the cloud service supplier;
- the stability of the cloud service supplier’s personnel;
- the security of the technologies, products and service supply chains of the cloud platforms;
- the security management capability of the cloud service supplier and the security protection of the cloud platforms;
- the feasibility and convenience of customer data migration; and
- the business continuity of the cloud service supplier.

Higher Scrutiny Over Cloud and Edge Computing Services Provided for Financial Entities

Cloud and edge computing services provided in financial areas are likely to constitute a “fintech product” and therefore be subject to additional requirements under the PRC Certification Rules for Fintech Products. Regulations promulgated by The People’s Bank of China (PBOC) impose even more requirements on cloud and edge computing services providers, including the “Financial Application of Specification of Cloud Computing Technology-Technical Architectures, Security Technical Requirements, and Disaster Recovery”, which sets out a required standardisation for cloud computing services in the financial area and specifies requirements from the perspective of the establishment of basic structures, technical security, risk assessment and risk management.

With respect to financial personal data and information generated, transmitted and stored during

the course of financial cloud and edge computing services, the PBOC and the China Financial Standardisation Technical Committee provide more requirements, primarily through the PRC Personal Financial Information Protection Technical Specification, which adopts a broad definition of personal financial information and specifies measures required during the life cycle of such information.

Data and Privacy Protection

Cloud and edge computing service providers must generally comply with the requirements of the cybersecurity regime in respect of the collection, use, transfer and other processing of PI and certain other kinds of data. Key requirements on parties, including cloud and edge computing service providers, include obtaining consent from data subjects for the collection and further uses of their PI, undergoing so-called “security assessment” procedures prior to overseas data transfers in certain circumstances, and such further general principles as “legitimacy, rightfulness and necessity” in the collection and use of PI (see also **1.1 Laws and Regulations** and **2.1 Key Challenges**).

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights Laws and Regulations

Artificial intelligence

There are no PRC laws specifically pertaining to the creation, development or use of artificial intelligence (AI), but there are some policies and a few regulations. To incentivise the AI industry, China has formulated a number of broad and aspirational plans, such as the New Generation Artificial Intelligence Development Plan in 2017.

At the national level, China also promulgated some policies specifically to guide the regulation of AI.

The Ministry of Science and Technology (MOST) issued the Ethical Norms for New Generation Artificial Intelligence in September 2021, which provide ethical norms covering the protection of personal data, human responsibility and human control of the AI. The CAC issued the PRC Internet Information Service Algorithmic Recommendation Administration Provisions, which govern market entities that use algorithmic recommendation programs, and mandate them to notify users of such use and provide the users an opt-out.

At the local government level, for example, the Shenzhen government issued the Provisions on Promoting the Artificial Intelligence Industry in the Shenzhen Special Economic Zone (“Shenzhen AI Provisions”) in September 2022, which is the first city-level guideline aimed at facilitating the AI industry. Most of the content of the Shenzhen AI Provisions is simply declaratory (eg, the Shenzhen government will formulate a separate risk classification and management standards for AI-related business activities, and if such activities are categorised as low risk, then the market entities can conduct trials even under no specific local and national norms). The Shenzhen AI Provisions also call for the exploration of specialised insurance to be provided to AI products and services.

Also in September 2022, Shanghai passed provincial regulation regarding the AI industry: the Shanghai Provisions on Promoting the Development of the AI Industry (“Shanghai AI Provisions”), effective from 1 October 2022. The Shanghai AI Provisions call for management systems based on grading and “sandbox” supervi-

sion. Such management intends to leave space and flexibility for the AI industry to develop. In particular, the Shanghai AI Provisions stipulate that minor violations of laws during the development of the AI industry can be tolerated without administrative punishment, subject to specific lists of such minor violations formulated by provincial departments. However, the Shanghai AI Provisions also specify ethical norms for AI development as bottom lines.

As the operation of AI tends to be based on large data sets, service providers obtaining such data will be subject to the requirements of the cybersecurity and privacy protection frameworks. In addition to the rules and requirements detailed in **1.1 Laws and Regulations**, **2.1 Key Challenges** and **3.1 Highly Regulated Industries and Data Protection**, AI may be more likely to trigger stricter ones due to the processing of so-called “sensitive personal information”. For example, biological characteristics (eg, fingerprints, faces, voices, gaits) are not allowed to be used as the sole method for personal ID verification; when they are used, the data processor is required to conduct a risk assessment on the necessity and safety of the use, and is prohibited from requesting the natural person to agree on facial information processing as a precondition to using products or services where the facial information is not necessary for their provision.

With respect to the ownership of IP rights, under Article 9 of the PRC Copyright Law, only natural persons, legal persons or organisations may obtain copyrights. As a result, AI may carry out activities such as editing photographs or even composing music or poetry, but it cannot obtain rights or thus protection as a copyright owner under current PRC law. Similarly, the PRC Patent Law stipulates that a patentee should be either an entity or a natural person. Thus, AI itself can-

not be considered entitled to patent rights for its inventions.

In a case between Tencent and an online financial information provider, in which they disputed the copyrights of an AI-created article, the People’s Court of Nanshan District of Shenzhen confirmed that AI is not qualified for IP rights, but the IP rights of creations and inventions by AI are protected: such IP rights belong to the entity or natural person who developed the AI.

Big data

In addition to the requirements and other rules of the cybersecurity and privacy regimes, big data processing is subject to another special framework: foreign investment restrictions. Most notably, the operation of “Internet Data Centres” (IDCs) – including the businesses of providing major data storage and analyses services – is off limits to foreign and foreign-invested parties. As an example, even the Apple iCloud service in mainland China (which formerly operated via an offshore service provider) is currently operated by Guizhou-Cloud Big Data Industry Development Company, as the holder of an IDC permit.

A company engaging in business related to big data within certain industry sectors might be subject to additional regulatory requirements. For example:

- all health-related data must be stored on a secure and trusted server in China;
- hospital authorisation is a precondition to collecting and processing such data (even anonymised); and
- a security assessment is required before transferring such data offshore.

Finally, a big data service provider may be deemed a CIIO and therefore subject to stricter

compliance frameworks (see **3.1 Highly Regulated Industries and Data Protection**).

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

PRC legislators have taken a relatively broad view of the “Internet of things” (IoT) concept. The State Council’s 2013 Guiding Opinions on Promoting the Orderly and Healthy Development of Internet of Things (“IoT Opinions”) describe IoT as technology “based on the intensive integration and comprehensive application of a new generation of information technology”, and designate IoT as an important strategic emerging industry of the country. The IoT Opinion further emphasises the co-ordinated overall development of IoT applications, technologies, industries and standards. In September 2021, the MIIT issued the Guidelines for the Construction of a Fundamental Security Standard system for IoT, aiming to outline the framework for the development and implementation of standards for IoT, including software security, access authentication and data security.

Although China has yet to promulgate any comprehensive legislation on the security and regulation of IoT, recent legislation and regulation on data-related issues – such as the PRC Data Security Law, the PIPL, the Measures for Security Evaluation for Cloud Computing Services and the Measures for Cybersecurity Reviews (see **1.1 Laws and Regulations**, **2.1 Key Challenges**, **3.1 Highly Regulated Industries and Data Protection** and **4.1 Liability, Data Protection, IP and Fundamental Rights**) – are all applicable to IoT. For example, the PIPL provides that IoT companies that collect PI must obtain prior

consent from the individual, and companies cannot refuse to provide services to individuals that refuse to provide PI, unless the processing of such PI is necessary for providing the product or service.

A number of government departments and regulatory bodies have clearly assumed certain responsibilities over IoT activities. Such government bodies include the MIIT (the key regulator for the telecoms sector and approximately 20 other industries), the CAC (which acts as the main watchdog for information security and content administration), the National Development and Reform Commission, the MOST and the SAC.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

There is no single, unified regulatory regime for all components of the audio-visual media industry as a whole in China. Instead, industry sub-sectors are regulated separately through a variety of laws and regulations, with key areas being cable broadcasting, online audio-visual services (including online video-sharing platforms) and over-the-top (OTT) services. In general, the broadcasting or online transmission of audio-visual content is highly regulated, and is off limits to not only foreign but also most domestic investment, in many cases.

Cable Broadcasting

Cable broadcasting is highly regulated in the PRC and is not open to foreign participation or even new domestic market entrants. Currently, a broadcasting television station may only be set up by central or government branches, such as the National Radio and Television Administration

or the Ministry of Education. The station's establishment will also be subject to the central PRC government's national market plans.

The most central piece of legislation relating to cable broadcasting – ie, offering traditional cable television channels – is the PRC Administrative Regulations for Radio and Television. All cable broadcasters are required to obtain the following two key permits, among others:

- the “Radio and Television Broadcasting Institution Permit”; and
- the “Radio or Television Programme Production Permit”.

PRC law requires applicants for these permits to meet certain requirements, including regarding their location, equipment, technology and personnel, and to complete an application process with the applicable authorities. No application fees are required. As mentioned, however, it is difficult if not impossible in practice for new entities – whether purely domestic or foreign-invested – to obtain either of these permits in China.

Online Audio-Visual Services

Online audio-visual services are primarily regulated through the following:

- the PRC Interim Administrative Provisions on Internet Culture, which is central to the so-called “Internet Culture” sector, regulating online cultural activities;
- the PRC Provisions on the Administration of Private Network and Targeted Communication Audio-visual Program Services; and
- the PRC Administrative Regulations on Internet Audio-Visual Program Services.

To operate an online streaming platform – eg, to provide video on demand services, such as

Youku (the Chinese YouTube) – the most important operating permits are the “Internet Culture Business Permit” and the “Internet Audio-Video Broadcasting Permit” (“IAVB Permit”). The IAVB Permit requires an application process to be completed with local and central government authorities, while the application for the Internet Culture Business Permit involves only provincial level government authorities. No application fees are required. An applicant for an IAVB Permit must be controlled or wholly owned by one of China's state-owned enterprises (SOEs). Neither the Internet Culture Business Permit nor the IAVB Permit may be obtained by an applicant that has any direct or indirect (on a see-through basis) foreign investor, although indirect control structures featuring variable-interest-entity structures established before the requirement that the IAVB Permit must be controlled or wholly owned by SOEs are widely used in this sector.

OTT Services

The most important operating permit for providers of OTT services is the OTT licence. To apply for an OTT licence, a qualified applicant must meet certain requirements, including being controlled by an SOE, along with equipment and personnel requirements. Here too, both local and central government approval are needed. There are no application fees. To date, only 16 OTT licences have been issued, and the regulators have effectively suspended the granting of this licence, with the date of resumption unknown.

Contractual Partnerships/Licensing

Directly operating an online video channel in the PRC is highly regulated and requires the procurement of operating licences/permits (ie, an Internet Culture Business Permit and an IAVB Permit/OTT licence) that are generally only available to companies with SOEs as (controlling) shareholders. As such, it is more common for

content owners outside China to simply license content to domestic entities that hold all required permits – eg, the licensing arrangement between iQiyi and Netflix. Such domestic entities will also ensure that licensed content complies with PRC content/censorship requirements and will potentially self-censor any content as needed.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The PRC Telecommunications Regulations apply to all types of “telecommunications” services. “Telecommunications” is defined broadly as any “act of using wired or wireless electromagnetic or optoelectronic systems to transmit or receive voice, text, data, images, or any other form of information.”

The PRC Telecommunications Regulations categorise telecommunications services as either “basic telecommunications services” (BTS) or “value-added telecommunications services” (VATS), and different operating permits are required to engage in each. BTS include communications services, public data transmission and public network infrastructure, while VATS consist of call centre services, IDC services, CDN services, VPN services and others. A complete list of BTS and VATS can be found in the PRC Catalog of Telecommunications Businesses, as first formulated by the MIIT in 2000 and last updated in 2019.

Therefore, depending on the type of telecommunications services being provided, the telecommunications operator will need to obtain either a “Basic Telecommunications Service Operating Permit” or a “Value-Added Telecommunications Services Operating Permit” prior to bringing a

service to market. Setting aside the fact that numerous BTS and several VATS are off limits to foreign and foreign-invested parties, each permit requires a telecommunications services operator to meet different requirements, as follows.

- **Basic Telecommunications Service Operating Permit:**

- (a) the operator must be a legally established company that specialises in BTS and in which the state has no less than 51% ownership;
- (b) a feasibility study and technical plan for the formation of the network must be completed;
- (c) the operator must have access to funds and specialised personnel commensurate with the business activities to be engaged in;
- (d) there must be a site and corresponding resources to carry out envisioned business activities;
- (e) the operator must have the reputation or the capability to provide long-term service to its subscribers;
- (f) the minimum registered capital for operators engaging in business within a single province is RMB100 million, while the minimum registered capital for operators engaging in business across provinces (including nationwide) is RMB1 billion; and
- (g) the operator must comply with other conditions specified by the state.

- **Value Added Telecommunications Services Operating Permit:**

- (a) the operator must be a legally established company with a minimum domestic shareholding of no less than 50% for most VATS, unless otherwise specified by the state (except for those fully opened up to foreign investment, such as domestic

multi-party communications services, call centres and e-commerce services);

- (b) the operator must have access to funds and specialised personnel commensurate with the proposed business activities;
- (c) the operator must have the reputation or the capability to provide long-term service to its subscribers;
- (d) the minimum registered capital for operators engaging in business within a single province is RMB1 million, while the minimum registered capital for operators engaging in business across provinces (including nationwide) is RMB10 million; and
- (e) the operator must comply with other conditions specified by the state.

The procedure for obtaining the relevant approvals/permits can be complicated and time-consuming, but is increasingly being simplified, especially for foreign and foreign-invested businesses. For example, on 15 October 2020, the MIIT released the Notice on Strengthening Interim and Ex-Post Supervision of Foreign-Invested Telecommunications Enterprises, which confirmed that a separate process for MIIT approval would no longer be required for the establishment of FITEs. Then, on 1 May 2022, the key legal regime governing FITEs – the PRC Administrative Provisions on Foreign-Invested Telecommunications Enterprises – was further amended to remove one of the market entry requirements imposed on FITEs looking to obtain the telecommunication operating permits.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

The fundamental legal regime in the PRC governing technology agreements is the “Technology Contracts” chapter of the Civil Code (which entered into effect on 1 January 2021), which sets forth certain requirements for technology contracts, as well as the rights and obligations of the contracting parties. Because trade secrets are usually involved in technology agreements, technology agreements are also often subject to the PRC AUCL and the Provisions of the Supreme People’s Court on Several Issues concerning the Application of Law in the Trial of Civil Cases of Trade Secret Infringement. Aside from the general laws and regulations above, technology agreements of computer software are subject to the PRC Copyright Law and the PRC Regulations on Computer Software Protection.

Technology Improvements and Ownership

Provisions dealing with technology improvements and ownership are commonly negotiated in China’s technology agreements. As indicated in Articles 850 and 864 of the Civil Code, a technology transfer agreement or technology licensing agreement may not restrict competition or development of the technology, nor illegally monopolise it. Provisions that restrict improvements to the technology received may be held invalid and unenforceable by a PRC court. However, the risk tends to be deal-specific.

With respect to the ownership of the subsequent improvements using the technology received, Article 875 of the Civil Code mandates that, unless the ownership is explicitly specified, the party who develops such improvements shall be the owner of the improvements, and the improvements may not be shared by other

parties. That said, the subsequent improvements will not be automatically granted back to the technology provider. Therefore, a technology provider should carefully draft the relevant clauses to explicitly specify the ownership of any subsequent improvements.

Reverse Engineering

Another challenge routinely encountered when entering a technology agreement with a local organisation is reverse engineering, which is defined by PRC law as the acquisition of technical information on a product obtained from any public channel through disassembly, mapping, analysis and other technical means.

The provisions restricting reverse engineering are widely used in China as a seller protection scheme, and there is no law expressly prohibiting the inclusion of “anti-reverse engineering provisions” in a technology agreement. However, as explained just above, the provisions against reverse engineering cannot explicitly restrict competition or development of the technology, nor promote its illegal monopolisation. Therefore, anti-reverse engineering provisions bear some risk of being deemed invalid or unenforceable by a PRC court, and any provisions relevant to anti-reverse engineering should be carefully drafted to mitigate such risk.

Technology Import/Export

Many technology agreements also implicate import/export issues. For cross-border technology transfers, parties should look into the PRC Catalogue of Technologies Prohibited or Restricted from Export and the Catalogue of Technologies Prohibited or Restricted from Import to determine if the technology involved is prohibited or requires pre-approval. Even for technology that is not prohibited or does not require pre-approval, the technology contracts

need to be filed with the PRC Ministry of Commerce and relevant authorities.

On the other hand, this is another area that China is gradually opening up. In 2020, several clauses implicating forced transfer of technology were removed from the PRC Regulations on the Administration of Import and Export of Technologies. Moreover, the Foreign Investment Law enacted in 2020 made forced technology transfers and unauthorised disclosure of trade secrets by government officials illegal.

Resale Price Maintenance

Furthermore, technology agreements should be carefully drafted to avoid violating provisions in the PRC Anti-Monopoly Law. For example, the Anti-Monopoly Law strictly prohibits fixing the resale price of a product or service. This restriction can be interpreted to include the scenario of fixing the price of sub-licensing in a technology agreement. Therefore, contracting parties must take care to avoid drafting the technology agreements in such a way that might be deemed to create resale price maintenance, although the most recent amendments to the Anti-Monopoly Law (in 2022) did add a safe harbour.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Laws and Regulations

Trust services and electronic signatures are widely used in China, especially in online commerce. The PRC Law on Electronic Signatures (Electronic Signatures Law) was the first PRC law that systematically set forth the requirements on trust services and electronic signatures. China

also issued two other regulations concerning trust services providers:

- the PRC Measures for the Administration of Cipher Codes for Electronic Certification Services; and
- the PRC Measures for the Administration of Electronic Certification Services.

Furthermore, trust services providers must utilise commercial cryptography when providing the relevant services, and therefore are subject to the PRC Cryptography Law. However, China still has no law specifically governing digital identity.

Trust Services

Trust services are highly regulated in China. To become a qualified trust services provider (ie, to provide electronic certification services in China), two permits are required:

- “Permit for Use of Cipher Codes for Electronic Certification Services” (“Cipher Code Permit”); and
- “Permit for Electronic Certification Services” (“Certification Permit”).

The Cipher Code Permit is a prerequisite for the Certification Permit and should be applied for with the competent Cryptography Administration, while the application for the Certification Permit should be completed with the MIIT. In addition, applicants must satisfy several requirements under PRC law, including concerning corporate capacity, technology equipment, technical personnel and registered capital.

Electronic Signatures

The provision of electronic signatures services is a core part of trust services/electronic certification services in China. An “electronic signature” is defined by the PRC Electronic Signatures Law

as data in electronic form identifying the signatory and verifying the signatory’s acknowledgment of the content being signed. For an electronic signature to have the same legal effect as a seal or written signature, the following conditions must be met:

- the data generated by the electronic signature is exclusively used and owned by the signatory;
- the data generated by the electronic signature is exclusively controlled by the signatory at the time of signing;
- any alteration to the electronic signature can be discovered after signing; and
- any alteration to the content and form of the electronic data can be discovered after signing.

The PRC Electronic Signatures Law also specifies certain documents that cannot be legally accepted in electronic format and cannot be signed electronically, such as documents concerning personal relations (eg, marriage, adoption and succession), and documents concerning transfers of real estate rights and interests.

Digital Identity Schemes

Digital identity refers to a set of data stored online that can be used to identify a specific individual. Such data ranges from a personal name to an ID card number. Digital identity (which is also called “E-ID card”) is widely used in China. For example, the Chinese government has been promoting digital identity cards since 2018. Under the digital identity card system, each individual’s identity information is stored online and can be used to access various social services, such as healthcare and public transportation, with a smart device.

Contributed by: Cloud Li, Joanna Jiang, Zhengwei Yang and Dimitri Phillips, **DaHui Lawyers**

While China has yet to promulgate any law specifically governing digital identity, the rules of the cybersecurity regime are generally applicable to the digital identity schemes – particularly the rules regarding the confidentiality and safe-keeping of individuals' PI and the protection of privacy (see **1.1 Laws and Regulations**, **2.1 Key Challenges** and **3.1 Highly Regulated Industries and Data Protection**).

DaHui Lawyers combines in-depth knowledge of China's legal and business landscape with extensive international experience. It has particular strengths in new economy industries and complex cross-border transactions. DaHui has become a go-to firm for multinational companies in the highly regulated Chinese technology, media and internet/telecoms sectors, where its

expertise has led to it becoming a key adviser and strategist to clients of all types and sizes in China's emerging but challenging market, providing the most effective and solution-oriented services tailored to clients' diversified business needs. The firm's TMT team consists of 20 partners and 85 fee earners.

Authors



Cloud Li is a partner in DaHui Lawyers' TMT practice. He has represented European and North American multinationals, large Chinese state-owned and privately held companies, and

numerous private equity funds in various TMT-related M&A, investments, disputes, compliance and general corporate matters. Cloud has acted for some of the largest and most established participants in China's TMT sector.



Zhengwei Yang is a partner in DaHui Lawyers' compliance and crisis management practice groups. His practice mainly focuses on compliance and investigations, cybersecurity,

complex commercial litigation and arbitration, and employment matters. Zhengwei has profound experience in various business sectors, including technology, sports and entertainment, life sciences, manufacturing and real estate. He is recognised by clients for his strategic thinking and quality of service.



Joanna Jiang is a partner in DaHui Lawyers' corporate, TMT and cybersecurity practice groups, and focuses on the IT and telecommunications, media, entertainment and healthcare

industries. She has been deeply involved in each stage of M&A transactions, private equity investments, foreign direct investment and daily corporate matters, in addition to regularly handling myriad market entry and regulatory matters.



Dimitri Phillips is counsel in DaHui Lawyers' dispute resolution, compliance and corporate/M&A practice groups. He handles a range of issues for foreign companies doing or

seeking to do business in China, as well as Chinese companies operating abroad. Dimitri has advised clients on litigation, international arbitration, compliance, inbound and outbound investment and general corporate matters.

DaHui Lawyers

China World Tower A
1 Jianguomenwai Avenue
Beijing
100004
China

Tel: +86 10 6535 5888
Fax: +86 10 6535 5899
Email: info@dahuilawyers.com
Web: www.dahuilawyers.com

The logo for DaHui Lawyers, featuring the word "dahui" in a bold, red, lowercase serif font. The letter 'i' has a small red diamond above it.

Trends and Developments

Contributed by:

Cloud Li, Joanna Jiang, Zhengwei Yang
and Dimitri Phillips

DaHui Lawyers see p.121

TMT in China – an Introduction

While 2022 was a turbulent year in terms of world geopolitics (and China's re-opening to the world at the end of the year brought another wave of COVID-19 to the country), it was relatively quiet on the Chinese legislative front, and the local TMT industry kept going strong and geared up for an even stronger 2023.

This past year did not see the issuance of any major laws or regulations like 2021's Rules on Blocking Unjustified Extraterritorial Applications of Foreign Legislation and Other Measures or Law of the People's Republic of China on Countering Foreign Sanctions. Data and privacy protection were the most active areas in terms of rule-making, but whereas 2021 saw the promulgation of the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), only implementing rules were released in this area in 2022.

The Anti-Monopoly Law (AML) was revised, draft amendments to the Anti-Unfair Competition Law were published, and another draft of revisions to the Company Law was released, but few changes were relevant to TMT businesses (compared to their predecessor versions). Nevertheless, China took several further moves to open up to foreign investment in the TMT industry, even as geopolitical developments point to the possibility of domestic demand and activity strengthening in 2023.

Further opening to foreign investment

The release of the (near-annually) revised Special Administrative Measures (Negative List) for Access to Foreign Investment (ie, the so-called "Negative List") at the very end of 2021 not only confirmed that no new industry sectors would be subject to new foreign-investment prohibitions or restrictions but also removed two former prohibitions (including on the production of ground receivers and key components for satellite television broadcasts), reflecting the TMT market's stance to foreign investment in 2022. According to a MOFCOM press conference, the hi-tech sector's utilised foreign investment rose by 32.3% between January and September 2022, with hi-tech manufacturing growing by 48.6% and hi-tech services increasing by 27.9% compared to the same period in the previous year.

Further foreign investment liberalisation was seen in 2022, most notably including revisions to the Administrative Provisions on Foreign-Invested Telecommunications Enterprises (the "FITE Provisions"), which are the key regulations governing the entry and licensing of foreign-invested telecommunications enterprises (FITEs). These revisions radically eased the market entry requirements for FITEs to obtain PRC telecommunications operating licences. Specifically, they removed a previous requirement placed on FITEs to demonstrate that their principal shareholders/parent companies have a "good track record in the telecommunications business", which may have, among other things, precluded foreign financial investors (eg, USD-denominated funds) from taking significant

stakes in Chinese companies performing internet/telecommunications activities.

Whereas some TMT financial and even strategic investors formerly had to adopt alternative structures to bypass the “good track record” requirement, they and all foreign TMT businesses seeking to establish themselves or obtain financing should now have a much easier and more straightforward experience in obtaining telecommunications operating licences in China. In fact, a report by the China Academy of Information and Communications Technology already shows that the total number of FITEs with one type of such licences (specifically, a licence for value-added telecommunications business) increased from 829 to 1,097 between February and September 2022.

Data and privacy protection

In 2022, PRC regulators released several final and draft rules concerning data and privacy protection as well as related areas, almost all primarily clarifying or elaborating existing law. These are the fastest growing legal areas in China (mirroring to an extent the situation in many other jurisdictions), and TMT businesses are faced with the considerable task of keeping abreast of and in compliance with new or adjusted rules – often substantial – on a quarterly or semi-annual basis. And regulators appear to be equally eager in enforcing these rules, including in several high-profile actions in 2022.

Cybersecurity review

The highlights of 2022, carrying over from 2021, were the conclusion of the investigation of Didi Chuxing (China’s Uber) by the Cybersecurity Administration of China (CAC) and the issuance and coming into effect (in 2021 and 2022, respectively) of the revised Cybersecurity Review Measures (CRM).

The now infamous investigation of Didi Chuxing was launched, apparently under the CRM, shortly after the wildly successful company’s US IPO in the summer of 2021 and concluded in July 2022 with a fine of RMB8.02 billion. Ultimately, no violations of the CRM were included in the CAC’s findings – perhaps because the version of the CRM at the time the investigation was launched did not include a provision requiring cybersecurity review in connection with IPOs – but the findings instead included violations of the Cybersecurity Law, PIPL and DSL (eg, the “illegal collection” of millions of pieces of screenshot information from users’ mobile phone photo albums, “excessive collection” of millions of pieces of passenger facial recognition information, analysis of billions of pieces of passenger information without having clearly notified passengers, and “inaccurate and unclear explanation” of 19 personal information handling purposes).

During the investigation, however, revisions to the CRM were issued and came into effect, broadening the scope of application for the cybersecurity review. They no longer apply only to so-called Critical Information Infrastructure Operators (CIIOs) who purchase network products or services that might affect national security, but also to any party that handles the personal information (PI) of one million or more data subjects and seeks to list securities outside China as well as (using the typical PRC legislative catch-all formula) to any party whose data handling activities might impact national security. The signal importance of cybersecurity review is clear, likely not only in situations involving CIIOs or overseas IPOs, and many businesses have begun the process or anticipatory self-assessments.

Cross-border data transfers

Although the Cybersecurity Law had emphasised cross-border data transfer controls as far back as 2016, such controls did not adopt a concrete form until 2021's PIPL, and the system only crystallised with detailed implementing rules in 2022.

The PIPL provided for three avenues of regulatory compliance for companies to choose from when transferring certain data out of China:

- undergoing a “security assessment”, which involves submissions to regulatory authorities;
- entering in a “standard contract” with the data transfer recipient; or
- obtaining a “certification” from certain government-designated agencies.

In 2022, details were filled in for all three of these approaches, although mostly for the first and likely insufficiently for the last.

The Measures on Security Assessment for Cross-Border Data Transfer (the “SA Measures”) and the Guidelines on the Application of Security Assessment of Cross-Border Transfer of Data (the “SA Guidelines”) are final, effective rules and have sufficient detail for parties to carry out the “security assessment” procedure and thereby obtain approval to transfer data abroad. However, this procedure is only required if the data handler:

- is a CIO seeking to transfer PI offshore;
- seeks to transfer “important data” offshore;
- processes PI of one million or more data subjects and seeks to transfer any PI offshore;
- transfers offshore, on a cumulative basis, PI of 100,000 data subjects within a period commencing 1 January of the preceding year; or

- transfers offshore, on a cumulative basis, the “sensitive personal information” of 10,000 data subjects within a period commencing 1 January of the preceding year.

On the other hand, 2022's rules for the second avenue – which can be followed if the above “security assessment” is not triggered – were released only in draft form: the Personal Information Export Standard Contract (the “Draft Standard Contract”) and the Standard Contract Provisions for the Exit of Personal Information (the “Draft SC Provisions”). These were used as references even in draft form, but on 24 February 2023, the final versions were officially issued (the “Standard Contract” and “SC Provisions”): their effective date is 1 June 2023 and they provide a six-month grace period (ie, until December 2023) for parties who do not meet the relevant requirements to adopt rectification measures (eg, entering into Standard Contracts, conducting data protection impact assessments, and filing them with the CAC).

The releases related to the third way that a domestic PRC party may legally transfer certain sensitive data overseas in some circumstances – namely, undergoing a so-called “PI protection certification” by a professional institution in accordance with CAC requirements – do not appear to sufficiently lay out the framework to be relied upon. As such, and given the string of cybersecurity investigations alongside that of Didi Chuxing, parties transferring or considering transferring data from inside China out of the territory should carefully review and abide by the SA Measures, the Standard Contract and the SC Provisions.

Moreover, it appears that the CAC views the offshore processing of PI of PRC citizens as “cross-border data transfers”, meaning it is theoretically

subject to the above rules, although there is no indication on whether or how the rules would be enforced in such situations, especially against offshore processing by parties that have no onshore presence.

Data processing requirements

PRC regulators have also been issuing more and more rules on specific aspects of data processing other than (offshore) transfers. The majority of such rules seem to aim at protecting consumers against excessive or “manipulative” processing of their PI, and at empowering consumers with rights to review and have a say in the processing that is done.

The most notable example of 2022 is the Internet Information Service Algorithmic Recommendation Management Provisions (the “Algorithm Provisions”), which apply to any party that uses algorithms to “make recommendations” to consumers within China, including the algorithms that e-commerce and other service providers use to retrieve, filter, sort and push search results, and also potentially algorithms used for certain content generation.

This is an area of technology that is undergoing rapid development in China (as elsewhere), and the Algorithm Provisions impose several somewhat substantial obligations on the use of such technology and techniques, including regularly reviewing the principles, models, data and results of the algorithmic recommendation mechanisms to confirm they do not violate laws, regulations or even (generic/unspecified) ethical norms and, of course, formulating and disclosing the rules for the algorithmic recommendations.

Anti-Monopoly Law

The amendments to the AML promulgated in 2022 reflect a trend continuing from 2021:

seeking to bring more M&A deals within regulatory purview – although not necessarily to place them under strict scrutiny – particularly in the platform economy and related industries. On the one hand, the amendments include a new “safe harbour” and other exemption-like rules; on the other hand, they also substantially increase fines for violating various provisions of the AML.

The “safe harbour” rule provides that if a business operator can prove that its market share in the relevant market is lower than the standard set by the AML authorities (and also meets other conditions), a vertical monopoly agreement of the operator will not be prohibited or penalised. Such vertical monopoly agreements may arise especially in sub-licensing and other technology agreements, so the “safe harbour” may give TMT businesses a little more leeway in their commercial arrangements.

However, the revised AML raised the fine for an illegal concentration of undertakings from RMB500,000 to as much as 10% of the sales from the preceding year if the concentration eliminates or restricts competition. The new AML also expands third-party liability and appears to apply it upstream and downstream, among competitors, and among parties to hub-and-spoke agreements. The message is quite clear: while some activities are afforded more leeway, thereby assisting in business and market development, there is less tolerance – and greater penalties – for conduct that does violate the rules.

Company Law

Revisions to the Company Law were first released in draft form at the end of 2021, followed by another round at the end of 2022. Many of the revisions were not altered from the first draft to the second. The key revisions include:

- eliminating the current Company Law's requirement for a shareholder resolution in certain M&A circumstances (and for the consent of a majority of shareholders for a transfer of equity from one shareholder to anyone other than another shareholder);
- expansion of liability for directors and a requirement that companies with 300 or more employees have an employee-representative director;
- specifying liability and circumstances that would allow a company to forfeit the equity of shareholders who fail to pay the subscribed registered capital in time and in full; and

- introducing shares with different shareholder rights.

If the Company Law is formally revised substantially as indicated by these drafts, possibly as early as the first half of 2023, TMT (as well as other) companies should consider numerous changes to corporate structures and governance. Fortunately, most of the revisions reflect liberalising options rather than (restrictive) requirements, further harmonising PRC company law with international standards and fostering innovation in TMT and other industries.

DaHui Lawyers combines in-depth knowledge of China's legal and business landscape with extensive international experience. It has particular strengths in new economy industries and complex cross-border transactions. DaHui has become a go-to firm for multinational companies in the highly regulated Chinese technology, media and internet/telecoms sectors, where its

expertise has led to it becoming a key adviser and strategist to clients of all types and sizes in China's emerging but challenging market, providing the most effective and solution-oriented services tailored to clients' diversified business needs. The firm's TMT team consists of 20 partners and 85 fee earners.

Authors



Cloud Li is a partner in DaHui Lawyers' TMT practice. He has represented European and North American multinationals, large Chinese state-owned and privately held companies, and

numerous private equity funds in various TMT-related M&A, investments, disputes, compliance and general corporate matters. Cloud has acted for some of the largest and most established participants in China's TMT sector.



Zhengwei Yang is a partner in DaHui Lawyers' compliance and crisis management practice groups. His practice mainly focuses on compliance and investigations, cybersecurity,

complex commercial litigation and arbitration, and employment matters. Zhengwei has profound experience in various business sectors, including technology, sports and entertainment, life sciences, manufacturing and real estate. He is recognised by clients for his strategic thinking and quality of service.



Joanna Jiang is a partner in DaHui Lawyers' corporate, TMT and cybersecurity practice groups, and focuses on the IT and telecommunications, media, entertainment and healthcare

industries. She has been deeply involved in each stage of M&A transactions, private equity investments, foreign direct investment and daily corporate matters, in addition to regularly handling myriad market entry and regulatory matters.



Dimitri Phillips is counsel in DaHui Lawyers' dispute resolution, compliance and corporate/M&A practice groups. He handles a range of issues for foreign companies doing or

seeking to do business in China, as well as Chinese companies operating abroad. Dimitri has advised clients on litigation, international arbitration, compliance, inbound and outbound investment and general corporate matters.

DaHui Lawyers

China World Tower A
1 Jianguomenwai Avenue
Beijing
100004
China

Tel: +86 10 6535 5888
Fax: +86 10 6535 5899
Email: info@dahuilawyers.com
Web: www.dahuilawyers.com

The logo for DaHui Lawyers, featuring the word "dahui" in a bold, red, lowercase serif font. The letter 'i' has a small red diamond above it.

Law and Practice

Contributed by:

Nevine El-Shafei and Tasneem El-Naggar

Shehata & Partners see p.149



Contents

1. Metaverse	p.124
1.1 <u>Laws and Regulations</u>	p.124
2. Digital Economy	p.126
2.1 <u>Key Challenges</u>	p.126
3. Cloud and Edge Computing	p.133
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.133
4. Artificial Intelligence and Big Data	p.135
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.135
5. Internet of Things	p.136
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.136
6. Audio-Visual Media Services	p.138
6.1 <u>Requirements and Authorisation Procedures</u>	p.138
7. Telecommunications	p.140
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.140
8. Challenges with Technology Agreements	p.143
8.1 <u>Legal Framework Challenges</u>	p.143
9. Trust Services and Digital Entities	p.147
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.147

1. Metaverse

1.1 Laws and Regulations

Metaverse Laws and Regulations

The metaverse is defined by the World Economic Forum as “a fully immersive digital reality”. Such multi-dimensional nature of the metaverse requires governance by several laws, each regulating a feature of this virtual world; but this new technology brings new uncertainties. Currently, there is no particular or unified legislation dealing with metaverse technology in Egypt. However, metaverse technology is generally dealt with under a number of legislations, which are set out below.

The Telecommunications Law

The Telecommunications Law No 10 for 2003, as amended (the “Telecommunications Law”) is the primary governing legislation overseeing the telecom sector in Egypt. It covers licensing regimes, frequency spectrum usage, powers and responsibilities of the National Telecommunications Regulatory Authority (NTRA), penalties, etc. The law establishes the NTRA as the authority for overseeing and improving communications services in Egypt.

Metaverse growth stems from combining small and large virtual worlds as a network of interconnected virtual worlds. Thus, collaborations between different service providers are inevitable; in law, certain provisions refer to interconnection and international collaboration.

The Telecommunications Law also provides a broad framework for telecommunications and technology services, on such issues as users’ data, consumer protection and competition rules between telecommunications service providers. This framework has resulted in the promulgation of numerous key legislations relating to technol-

ogy, such as the E-Signature Law, the Data Protection Law and the Cybercrimes Law.

Key Legal Challenges to the Implementation of the Metaverse in Egypt

Intellectual property rights

The metaverse promotes itself as a space for innovative collaboration, providing enterprises and individuals with new avenues to expand and improve their services. Consequently, businesses and individuals may be concerned about safeguarding their intellectual property (IP) rights or enforcing their brand in such a virtual environment.

There is no tailored legislation for the protection of IP rights in the metaverse. However, several provisions under the Intellectual Property Law No 82 for 2002 (the “IP Law”) could apply to some IP challenges that may arise in metaverse technology.

There are three main types of IP protection under the IP Law:

- copyrights;
- patents; and
- trade marks.

All of these may be protected under the IP Law where the relevant registration requirements are fulfilled. However, in a virtual space such as the metaverse, potential IP infringements and disputes may occur, especially for non-IP holders.

Questions of applicable law and jurisdiction are also fundamental when raising IP disputes in a metaverse context, and are decisive when allocating the rights of the parties in an IP dispute and for the relevant enforcement mechanism.

Data protection

The Egyptian Data Protection Law No 151 for 2020 (the “Data Protection Law”) established the necessary protections for data collected for the purpose of metaverse technology. The Data Protection Law further established the Data Protection Centre (DPC) as the regulatory authority for data protection.

However, questions remain on the applicability of privacy laws within the metaverse, and on whose jurisdiction will apply, particularly given the complicated cross-section of protections. As the metaverse should have no “owner”, no one legislation can apply, though a globally unified code is likely at this time.

Cybercrime

Due to the structure of the old regime, several cyber-activities have been criminalised but dispersed among different legislation. The Cybercrimes Law No 175 for 2018 (the “Cybercrimes Law”) encompasses all these crimes, which is particularly significant given how the metaverse enables the advancement of new cybercrimes such as crimes against children, disinformation, ransomware, online harassment, impersonation and financial crimes.

The Cybercrimes Law criminalises several cyber-activities, including:

- unauthorised use of information technology systems;
- unauthorised access to websites, private accounts and information systems;
- altering, damaging or intercepting data, software or information systems; and
- hacking or encroaching on emails, websites, private accounts and information systems.

Although the Cybercrimes Law sets out a number of obligations to be observed by technology service providers (such as data storage, security and confidentiality), it is difficult to predict the application of the Cybercrimes Law in crimes committed using metaverse technology, due to the nature of such technology (which may be far more advanced than current technology schemes). Additionally, law enforcement measures in such crimes will require more advanced forensics and trained expertise than may be available at the time.

The current penalties for these cybercrimes range from a minimum fine of EGP10,000 to a maximum fine of EGP10 million, as well as imprisonment for a minimum of three months to a maximum of five years. These strict sanctions act as a frontline in cybercrime deterrence; however, questions remain on whether new crimes committed in the metaverse could escape this.

Obtaining licences

As metaverse platforms are created by combining multiple technologies, ensuring the competence of related service providers and setting clear guidelines is imperative. Thus, licence applications to the NTRA are necessary to evaluate an applicant’s capabilities and to set the conditions on which the licensee is to conduct their business. Accordingly, the NTRA issues various licences ranging from infrastructure to service provisions with specific obligations.

However, given the diverse technologies pertaining to the metaverse, the number of required licences could prove hectic for the licensee. In this regard, there are five types of licences related to the metaverse that are granted by the NTRA:

- operational licence;

- special permit;
- frequency usage licence;
- wireless services licence; and
- international services licence.

Each of these involves its own conditions and required procedures.

Cryptocurrencies

Money would be needed even in virtual reality; therefore, there is no escape from using cryptocurrencies that allow for direct user-to-user transactions, while non-fungible tokens (NFTs) function as a deed, proving ownership of digital assets in the metaverse. For this immersive experience to function in a manner allowing trade and sale of products, a sustainable e-economy and virtual space needs functional legislation. However, the New Banking Law has prohibited the issuance, dealing or promotion of cryptocurrencies, unless a CBE requisite licence is obtained.

For now, the lack of regulation brings with it the burden of uncertainty in cases where digital assets have been stolen, and uncertainty on whether victims trading in these prohibited currencies will find protection under the law. The suggestion that NFTs can prove true ownership is in much legal contention, as users believe that owning an NFT corresponding to a digital asset gives them absolute right of ownership. The issue arises straightaway, where users accept the terms and conditions of the metaverse platforms. Many metaverse and NFT platforms reserve the right to prohibit user access to digital property or to terminate it completely, at their sole discretion under their prescribed terms and conditions.

It is ambiguous whether Egyptian law extends its scope to protecting these digital assets, par-

ticularly if such trades are prohibited. However, for the time being, contractual relationships between the concerned parties could be the key to resolving these issues.

2. Digital Economy

2.1 Key Challenges

Laws and Regulations

The Telecommunications Law

The telecommunications sector is generally regulated under the Telecommunications Law. This law applies to all telecommunications services (including telecommunications networks' installation and operation, use of telecommunications equipment, providing wired and wireless communications, connectivity, radio frequency, and broadband services) in addition to all types of information technology services.

The importance of the Telecommunications Law in the context of the digital economy can be seen in how it interjects with the regulatory framework applicable to digital services by using information technology. The Telecommunications Law also interjects, legally and practically, with other applicable laws in the digital economy field such as the E-Signature Law, the Consumer Protection Law, the Cybercrimes Law and the Media Law. Although these are regulated under special legislation, in practice the interjection between multiple laws in connection with the digital market can be unclear and complex.

The E-Signature Law

E-signatures and e-contracts are generally regulated under the E-Signature Law No 15 of 2004 (the "E-Signature Law") and its executive regulations issued by Ministerial Decree No 109 of 2005 as amended. The E-Signature Law also established the Information Technology Indus-

try Development Agency (ITIDA), which is the authority mandated to regulate and supervise e-signature activities and services in Egypt.

The E-Signature Law enables the use of technology in contract formation. It recognises e-signatures and established the evidence standard for electronic contracts by creating a means of validating e-signatures and e-writing to produce legal effects in civil, commercial and administrative dealerships. This was a major legislative step, since previously Egyptian evidence law did not recognise digital documents and signatures as legally effective.

In this respect, Article 18 of the E-Signature Law specifies the following proof criteria for e-signatures, e-documents and e-writing:

- the e-signature must be linked to the signatory only;
- the signatory has control over the electronic medium; and
- there is the possibility to detect any modification or replacement in the data provided in the e-document or e-signature.

Verification and issuance of e-signature certificates under the E-Signature Law is permitted to licensed service providers. The licence is granted by ITIDA. The e-signature licensed service providers should comply with the e-signature services requirements provided under the E-Signature Law's executive regulations, such as:

- compliance with the data security system to preserve the information;
- management of PKIs and security;
- a secure custody system to preserve the e-signature creation data and e-certificates; and

- use of a contract service template with customers in the form approved by ITIDA.

In practice, the use of e-signatures is a complex process and is only for companies that are licensed for their use.

The Consumer Protection Law

Consumer protection generally comes into play, especially when raising B2C transactions in digital market practice. Consumers are the ultimate end users of digital services and, therefore, having a strong legislative and regulatory system in place that enables building trustworthy relations between consumers and service providers is essential, especially in e-commerce.

In this respect, the new Consumer Protection Law No 181 of 2018 and its executive regulations were issued by the Cabinet of Minister's Decree No 822 of 2019 (the "Consumer Protection Law"), which extended consumer protection to online contracts.

The Consumer Protection Law incorporated novel terminologies to capture the application of consumer protection to online dealerships and digital services, such as:

- online contracting – offering, buying or selling products by using an internet platform or any other means of visual, audio or print communication, or by telephone or other means;
- advertiser – any person who advertises a commodity or service, or promotes it by themselves or by others, using any means of media or advertising, including digital means; and
- supplier – any person engaged in a commercial, industrial or professional business providing a service to the consumer, producing, manufacturing, importing, exporting, selling,

renting, displaying, circulating, distributing or marketing a commodity for the purpose of presenting it to the consumer or dealing or contracting with the consumer about it in any manner, including through electronic means and modern technology means.

The Consumer Protection Law stipulated numerous measures and protective rights for the consumer, such as the right of disclosure of pre-contractual and post-contractual information, and methods to restrict unfair impositions on a customer.

Additionally, the Consumer Protection Law provided a full chapter specifically dealing with online contracting. The chapter included a number of rights and important legal protections for the consumer, such as:

- the right to obtain all necessary information to a contract;
- the right to confirm the approval to contract within a specific period (ie, seven days);
- the obligation of the supplier to observe all duties and consumer rights provided under the Consumer Protection Law in remote contracts; and
- the right of the consumer to revoke the contract within 14 days from the date of receipt of the product.

Nevertheless, online services under the Consumer Protection Law are excluded from the following activities:

- banking and financial activities;
- capital markets trade;
- newspaper subscription;
- flight ticket reservations; and
- hotel reservations.

These activities are subject to separate legal and regulatory applications, such as the media and banking laws.

Application of the Consumer Protection Law is mandated to the Consumer Protection Authority (CPA) which supervises and undertakes action against violations of said law.

Additionally, the NTRA also supervises consumer protection in telecommunications services. For this, the NTRA has issued general rules to protect the rights of users of telecommunications services. These rules have established several important guidelines to protect the rights of telecommunications service users by setting mandatory obligations on telecommunications service providers in providing telecommunications services. These obligations include:

- the duty to use agreement templates approved by the NTRA;
- transparency;
- non-discrimination;
- preparing a database of users, and carrying out the necessary updates to this database; and
- obtaining NTRA approval on the applicable services fees, publishing these fees on the service provider website, specifying the means of collecting these fees and indemnifying users against any breaches or violations of the service agreement including the service level duty.

The Data Protection Law

Egypt recently issued a data protection law in 2020. While the executive regulations of this law are still awaited, it is a key step towards applying the international standards required for online services and digital market transformation. In this context, the Data Protection Law No 151

of 2020 (the “Data Protection Law”) upholds the data protection rights for natural persons whose data and information are processed by digital means. The Data Protection Law generally regulates personal data gathered and processed digitally, and adopts broad definitions as regards extending the protection to data gathered digitally by online service providers. The following are worth noting:

- “personal data” means “any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking such personal data and other data such as name, voice, picture, identification number, online identifier or any data which determines the psychological, medical, economic, cultural or social identity of a natural person”;
- “processing” means “any electronic or technological operation to write, collect, record, save, store, merge, display, send, receive, circulate, publish, erase, change, edit, retrieve or analyse personal data using any electronic or technological medium whether partially or wholly”;
- “data subject” means “any natural person to whom electronically processed personal data is attributed which identifies them legally or factually and enables their identification from any other person”; and
- “electronic marketing” means “sending any message, statement, or advertisement or marketing content, via any technological means, which aims, directly or indirectly, to promote goods, services or commercial, political, social or charitable petitions or requests, addressed to specific persons.”

Furthermore, the Data Protection Law sets out particular requirements for the use, collection and processing of personal data, including:

- setting out the rights of the data subject and cases where the processing of personal data is deemed lawful;
- specifying the obligations of the data processor, data controller and data receiver;
- the express consent of the data owner to allow the data gathering and processing;
- the obligation to inform the data owner of the purpose for which the data is gathered/processed;
- the measures to secure and protect the gathered personal data; and
- restrictions on direct electronic marketing communications by imposing certain requirements, such as specifying the purpose of the marketing communication, obtaining the approval of the data subject and securing the personal data.

The Data Protection Law generally prohibits any direct digital marketing without obtaining the data subject’s prior consent. The digital marketing communication should include the name of the sender and location, and specify that the communication is for marketing purposes, enabling the data subject to reject or give their approval for the marketing communication.

Furthermore, the Data Protection Law establishes the Personal Data Protection Centre (PDPC), which is the authority mandated to license and regulate data processing in Egypt. The PDPC is not yet incorporated, and it is expected that the relevant executive regulations will be issued in 2023.

It is worth noting that the Data Protection Law upheld additional protection for the collection and processing of sensitive information, such as information relating to health, biometric and financial data, and criminal records. Information relating to children is by default considered

sensitive information (sensitive data). The Data Protection Law prohibits the collection and processing of sensitive data except with prior permission from the PDPC – though this is yet to be incorporated.

The Cybercrimes Law

On 15 August 2018, the Cybercrimes Law came into force (see **1.1 Laws and Regulations**). Its executive regulations, specifically No 1699 of 2020, regulate online activities and aim to penalise, inter alia, unlicensed online activity and content violations, such as accessing a site or a private account, using an authorised right to do so, and exceeding the limits of this right in terms of time or level of entry.

Service providers under the Cybercrimes Law have a number of obligations that protect service users, such as:

- keeping and storing a record of the information system or any means of information technology, for a continuous period of 180 days;
- maintaining the confidentiality of the data that has been saved and stored;
- not disclosing the data without a justified order from one of the competent judicial authorities; and
- securing data and information in a manner that preserves its confidentiality, and not penetrating or damaging it, etc.

Thus, the Cybercrimes Law covers offences that significantly relate to the digital economy, such as offences violating confidentiality, the integrity and availability of computer data, computer-related offences, privacy infringements, and so on.

The FinTech Law

Law No 5 of 2022 regulating and developing the use of financial technology in non-banking financial activities (the “FinTech Law”) came into effect in February 2022. This law aims to reinforce the inclusion of the non-banking sector in the digital market and encourage the transition towards a cashless society. Non-banking financial activities are supervised and regulated by the Financial Markets Authority (FRA).

The FinTech Law specifically regulates the use of technology in non-banking financial activities. “Non-banking activities” are defined as “financial markets and non-banking tools supervised by the FRA, including capital markets, insurance, real estate finance, financial leasing, factoring, SMEs’ financing activities and consumer finance.”

Additionally, under the FinTech Law “financial technology” is defined as “any mechanism that utilises modern and innovative technology in the non-banking financial sector to support and facilitate financial services, financing and insurance activities using applications, software, digital platforms, artificial intelligence or electronic records.”

The FinTech Law lays out entity incorporation and activity licensing requirements. There are three main licensing requirements for companies operating in the field of non-banking financial activity using financial technology. These requirements include, in particular:

- determining the direct and indirect shareholding structure, as well as related parties of the applicant;
- that the required technological infrastructure, facilities, information technology and other

- security means must be availed by the applicant; and
- that the company's activity is limited to those specified in the licence issued by the FRA – however, the FRA shall issue further regulations addressing such additional requirements pertaining to the shareholding structure, board of directors' composition and conflict of interest regulations.

The New Banking Law

Egypt has issued the new Banking Law No 194 for 2020 (the “New Banking Law”), which replaces the old Banking Law No 88 of 2003 as a step towards integrating the banking system as part of digital economy growth. The New Banking Law recognises and introduces key innovative areas such as digital banks, cashless payments, payment service providers, payment systems operators, cryptocurrency and e-money.

The Central Bank of Egypt (CBE), in line with the New Banking Law, has permitted the use of financial technology and electronic payment services. This extends to enabling technical payment aggregators and payment facilitators, payment services using prepaid cards, and standards for the issuance and acceptance of contactless payments in the banking field.

The New Banking Law permits the use of financial technology in rendering banking services. Additionally, the New Banking Law sets out licensing conditions and outlines the main rules for operating a payment system, as well as outlining penalties for violations of payment service providers (PSPs) and payment systems operators (PSOs). The New Banking Law provides the following definitions:

- “payment systems” means “a set of means and procedures for the paying off, setting off

or settlement of funds by transferring funds between two or more parties via an electronic system”;

- “financial technology” means “a business, application or financial product based on the use of technology”; and
- “payment services” means “all services related to account information or issuing or sending orders and payment operations, receiving such or executing such, whether in local or foreign currencies, including the issuance and management of payment tools and electronic money.”

According to the New Banking Law, natural and juristic persons are prohibited from conducting any activities related to operating payment systems or providing payment services, unless they have obtained a licence from the CBE. The CBE also further extends the licensing requirement to PSPs and PSOs operating inside Egypt or who target Egyptian residents from abroad.

The New Banking Law also requires licensed service providers to preserve an electronic copy of the registry, contracts, correspondence, commercial papers and documents relating to banking and payment transactions. These copies would have the same legal value as the original documents as long as these documents were preserved, processed and retrieved in the technical manner decided by the CBE (Article 203).

Key Challenges

Although Egypt has witnessed a number of efforts to support growth of the digital market, in practice challenges remain in some areas, as discussed here.

Regulatory framework

The digital market involves numerous regulatory authorities, depending on the type of digital

activity. This perhaps stems from the fact that there is no consolidated e-commerce law and e-commerce authority that regulates all e-commerce fields or provides adequate mechanisms of enforcement. In addition, the E-Signature Law (the main law dealing with digital transactions) was issued in 2004 and is significantly outdated considering current technology markets development, especially globally.

The current legislative platform in Egypt for dealing with e-commerce is also unclear as regards the conclusion and execution of electronic transactions, parties' liabilities and rights, and the burden of proof. Egypt also remains slow in the enactment of an e-government regulatory framework to enable the digital transformation of government services, which would ease and support integration with the commercial digital market, especially on a local level.

The regulatory framework was among the key issues raised under the national e-commerce strategy with UNCTAD in 2017, which aims to underline the key strategic and legislative reforms for developing the digital economy in Egypt (the "E-Commerce Strategy"). The E-Commerce Strategy highlighted the legislative and practical improvements needed in the e-commerce field. These include addressing the issue of intermediary liability of the internet service provider, e-procurement and the provision of adequate data protection enforcement mechanisms. Despite the enactment of the Data Protection Law, in practice its application remains unclear since the relevant licensing body is not yet established, and said law's executive regulations are yet to be issued.

Tax

The tax application regime in the digital market and in e-commerce remains a complex matter.

Key challenges pertaining to tax application in e-commerce include identifying the permanent establishment (PE) subject to tax, determining tax liability, and enforcement.

Egypt has worked towards including e-commerce in the tax system. The Egyptian Minister of Finance issued Decree No 307 of 2020 incorporating an e-commerce department mandated to register e-commerce businesses for taxation purposes.

Subsequently, the Egyptian Tax Authority (ETA) issued Executive Circular No 89 of 2021, requesting commercial and non-commercial activities to register with the ETA. These activities include:

- e-commerce;
- audio-visual media content platforms; and
- publication and production of reading content.

The ETA classifies taxpayers' registration under these activities into two categories:

- sole proprietorship (individuals); and
- companies (corporate).

Currently, e-commerce activities are subject to revenue and value-added tax (VAT). Revenue tax applies to direct income generated from online services, while VAT applies indirectly to services rendered to customers. The ETA also introduced the electronic invoice, which is mandatory for all merchants and business practitioners in Egypt, including in e-commerce. Application of the electronic invoice and reporting of tax in digital activities are quite novel and remain unclear in practice.

Intellectual property

Finally, the IP Law (see **1.1 Laws and Regulations**) did not allocate specific protection of IP and copyrights in online and digital markets. It is still unclear which authority is competent and how for protecting IP rights in the digital economy. The IP Law requires the registration of a trade mark and IP rights in order to gain the legal protection prescribed under said law in Egypt. Although major initiatives have been undertaken since, there is yet much room for enhancement, such as by granting ITIDA the authority to investigate related infringements via an online complaints system, and training officers for electronic evidence procurement.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Cloud and edge computing activities were recently introduced into the Egyptian market. These activities are broadly subject to a number of legislations in Egypt, including the Telecommunications Law, the Data Protection Law and the Cybercrimes Law. The Egyptian government opted for a cloud strategy in 2014 which aimed to move the governmental sector towards cloud technology and towards enacting e-government services. To date, however, this strategy has yet to be substantially realised.

In 2021, the NTRA issued the regulatory framework for establishing and operating data centres, and for the provision of cloud and data hosting services (the “Cloud Framework”). The Cloud Framework sets out the licensing and registration requirements for:

- cloud service providers;

- co-location/multi-tenant public data centre providers; and
- private data centres.

The requirements are summarised as follows.

Cloud Service Providers (CSPs)

CSPs are defined as companies that provide various cloud computing services of all types, whether through entirely owned data centres or via data centres leased from a public data centre. Examples of CSPs include Microsoft Azure, AWS, GCP Alibaba Cloud and IBM Cloud.

CSP services provided in Egypt would require prior registration with the NTRA. The registration would be valid for 15 years.

In order to obtain the approval of the NTRA on registration, the applicant should:

- fulfil and submit the relevant identification information to the NTRA (such as the name, address, telephone number and commercial register); and
- fulfil and submit activity information, particularly on the hosting system, data centres inside Egypt, address, contact details and website.

CSP service providers are required to evaluate their cybersecurity system and obtain a system tiering accreditation certificate from the NTRA for the purposes of cybersecurity system evaluation and data protection.

Registration as a CSP service provider would enable providing cloud computing services inside Egypt (for own use or for other users inside Egypt) and connecting to submarine systems via infrastructure service providers.

Public Data Centre Providers (PDCPs)

PDCPs are data centres established in Egypt for the purpose of hosting other service providers such as regards the cloud, content, Equinix, digital reality and internet exchange point (IXP). PDCPs are required to obtain the relevant licence from the NTRA. The licence's duration is 15 years, and would enable a PDCP to:

- establish and operate data centres for providing hosting services;
- provide site rental (co-location) to customers in Egypt through the licensee's data centres;
- provide cloud computing services for the licensee's own use or for other clients inside Egypt; and
- directly connect with submarine cable systems through contracting infrastructure service providers to rent cables and relevant capacities.

Private Data Centres (PDCs)

PDCs are data centres established by a natural or juristic person for their own and sole use. PDCs do not require prior registration with or a licence from the NTRA, unless the PDC would be providing the service to other users. In this case, the PDC would transform into a PDCP, and the licensing requirements of the NTRA would apply.

Cloud and edge computing services are generally subject to the Data Protection Law in terms of licensing and processing, using and storing personal data, and ensuring application of the relevant security measures as clarified in **2.1 Key Challenges**. Data subjects generally have the right to submit a complaint against the data processor or controller to the DPC in cases where there is any violation of the rights conferred under the Data Protection Law.

Conversely, the Data Protection Law excludes personal data with the CBE and entities that are supervised/regulated by the CBE – except remittance and exchange companies. Data protection and secrecy are among those customer rights provided under the New Banking Law. In February 2019, the CBE issued instructions in connection with protecting customers' interests. These instructions included:

- maintaining secrecy and protecting customers' data;
- protecting customers in digital and electronic services; and
- payment and digital service providers' duties towards customers.

The CBE's instructions consider all customer data (whether personal or financial) confidential and prohibit its use, disclosure or sharing without the prior consent of the customer. A complaint in connection with any banking service is generally assigned and dealt with by the customer protection unit of the CBE.

The main challenge encountered with cloud and edge computing activities occurs at both the regulatory and practical level. To date, there is no clear regulatory framework dealing with cloud and edge computing services. This is particularly problematic since the Data Protection Law's executive regulations are not yet issued, and the DCP is also not incorporated. In practice, this leaves the licensing and reporting requirements for data protection violations and data collection rights enforcement uncertain and unrealised.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Laws and Regulations Relating to the Use of Artificial Intelligence

Artificial intelligence (AI), and in particular data-driven methods such as machine learning, heralds a fundamental change not only in the Egyptian economic and social systems but globally as well. The key importance of AI is that it helps people predict the future and thus enables them to make better strategic decisions.

Currently, AI is not regulated under specific Egyptian legislation. The telecommunications sector, however, has attempted to implement and enhance the use of AI technology in Egypt.

In this regard, the Cabinet of Ministers Decree No 2889 for 2019 was issued in November 2019 to establish the National Council for Artificial Intelligence (NCAI). The NCAI follows the Ministry of Telecommunications and is presided over by the Minister of Telecommunications. The NCAI is mandated to develop, implement and manage AI strategy through close collaboration with experts and stakeholders. The NCAI should co-ordinate national efforts, develop Egypt's strategy for AI, develop various applications related to AI, recommend capacity-building programmes, and enhance the skills and knowledge of national cadres. Currently, the Egyptian government has upheld an AI strategy that aims to strengthen the Egyptian technology platform and economy, and to encourage international partnerships in that field.

Elements Relevant to AI Technology

Data protection and consumer protection

AI as a mechanism requires the collection of big data and learning the patterns of such data. In other words, large sets of data are combined for a specific task or mission through an intelligent collection process, where several patterns are found in the collected data; as a result, outcomes can be easily predicted for specific outputs.

In view of this, any collected and/or processed data for the purpose of AI technology is protected under Egyptian law. The Data Protection Law states that in order to collect, process and retain personal data, the following conditions must be met:

- personal data must be collected for the legitimate, specific and declared purposes of the person concerned;
- collected data must be true, sound and secure;
- collected data must be processed in a manner that is lawful and appropriate to the purposes for which it was compiled; and
- collected data must not be kept for a period longer than the period necessary to fulfil the purpose specified for it.

Further, the Consumer Protection Law states that a supplier must preserve the consumer's information and data, and must not trade or disclose it in violation of the provisions of said law or the laws related to this matter, unless the consumer expressly agrees. A supplier must also undertake to take all necessary precautions to maintain the confidentiality and privacy of the data and information.

Intellectual property – inventor of the inventor

It is a well-known general principle that only those who hold a legal personality can be protected and regulated under the law, which means that AI inventors could certainly legally protect their patent rights where they comply with the required conditions stated under the IP Law and its executive regulations. The question arises, however, as to whether an AI machine could protect its own inventions, for it is highly expected that AI machines could reach such a high level of intelligence as to allow them to invent patents that would otherwise be protected if invented by a human being. The answer to this question is left open not only in Egypt but also worldwide, as AI technology is brutally evolving every day, while comparatively the currently applicable laws are standing still. The general approach in Egypt and worldwide is, nevertheless, to not grant patent rights to AI machines as they do not possess a legal personality “yet”.

Liability and insurance

Were an AI machine (eg, a robot) to commit a certain act that results in damage to a certain person or thing, questions arise as to who should be liable (ie, the inventor of the robot or the robot itself).

One might argue that the inventor of the AI machine should be liable for whatever damage was caused by the AI machine unless such damage was unpredictable and inevitable. However, an AI machine evolves every time it interacts with human intelligence, which enables the AI to develop its own personality and reactions to various human interactions, making it nearly impossible to predict or contain an AI.

In this regard, the Egyptian Civil Code No 131 for 1948 states that whoever takes over the guardianship of objects whose protection requires

special care, or the guardianship of mechanical machines, shall be responsible for the damage caused by those objects, unless it is proved that the occurrence of the damage was due to a foreign cause beyond their control. Therefore, an AI inventor could be held liable in the case where their invention caused damage, and such damage was predictable and could have been prevented.

In addition, the Consumer Protection Law states that a supplier shall be liable for any damage caused by the product if it is proven that the damage arose from a defect in the product due to its design, manufacture or installation. Also, the supplier shall be liable for any damage caused by the product due to using it in the wrong way, if it is proved that the damage is due to the supplier's failure to take sufficient care to prevent the occurrence of damage, or to alert to the possibility of its occurrence. The supplier shall further be responsible for any damage caused by the product if it is established that the damage arose from a defect due to the method of preparing the product for consumption, preservation, packaging, circulation or display.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Regulations Relating to the Internet of Things

In view of the recent spread and steady growth of the internet of things (IoT) all over the world, Egypt, in line with its 2030 vision adopting the establishment of many smart cities such as the New Administrative Capital, has concentrated its attention on IoT and its related services. In January 2022, the NTRA issued the first regulatory framework concerning the IoT, pursuant

to the Telecommunications Law, thus advancing the growth of IoT services in Egypt, as well as studying the obstacles facing the spread of these services and how to overcome them.

IoT is defined under this framework as a service that is based on the use of technical means to enable automatic communication between things or objects in order to exchange, analyse and process data between them and make it available to users. Things or objects are defined under this framework as any physical objects that are connected to a digital/electronic identity which enables them to make connections, such as refrigerators, cars, power stations and others.

In other words, IoT includes all devices, physical and digital components, and systems that are connected for the purpose of benefiting from the data collected by sensors and embedded systems in machines and other physical objects, and sharing that data across communication networks where it can be processed and used for various purposes.

IoT is divided under the NTRA IoT framework into five classifications, depending on the nature of use:

- consumer IoT apps – such as wearable devices and smart home systems through which users are able to monitor and manage their home;
- commercial IoT apps – such as intelligent transportation systems (ITS), surveillance systems and vehicle-to-vehicle (V2V) connections;
- industrial IoT apps – these include digital industrial control systems, smart agriculture and industrial indicator monitoring, which allows for automatic detection and control of malfunctions in industrial equipment and for

taking appropriate action in emergency situations;

- infrastructure IoT apps – these include smart city applications, in which infrastructure sensors are used to monitor temperature, humidity and pollution levels, to control irrigation and lighting, to monitor vacant parking areas and to control waste; and
- governmental IoT services – these include applications related to services provided to citizens, such as applications for healthcare services and applications for public utilities such as water, electricity, gas, transportation, education and others.

Data Protection

IoT technology mainly depends on the collection of data and its exchange, analysis and processing. Therefore, an IoT service provider is obligated to fulfil all necessary institutional and technical procedures and steps to protect the confidentiality of information and data of the service users, as per the general obligations prescribed by the NTRA IoT regulatory framework. Further, this framework is explicitly subject to the provisions of the Telecommunications Law and, in particular, the Data Protection Law.

Any collected and/or processed data for the purpose of IoT technology is therefore protected under Egyptian law. As per the Data Protection Law and its executive regulations, and the Consumer Protection Law, the conditions discussed under Data protection and consumer protection in **4.1 Liability, Data Protection, IP and Fundamental Rights** must be met.

The Cybercrimes Law

See under The Cybercrimes Law in **2.1 Key Challenges**.

The Cybercrimes Law covers offences that relate to IoT technology, such as offences violating confidentiality, the integrity and availability of computer data, computer-related offences and privacy infringements.

Machine-to-Machine Communications

Machine-to-machine (M2M) communications refer to services connecting devices with each other and transferring data between them either by wired or wireless connections, as per the above-mentioned NTRA IoT framework.

Since M2M applications and services are concerned with the process of connecting devices to each other, they are considered part of IoT applications and services.

Currently, mobile phone service providers or other companies operating in various commercial or industrial activities use M2M services according to one of the following methods:

- M2M services related to mobile phone networks; and
- M2M services related to private networks for personal use only.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Audio-visual services are generally regulated by Law No 180 of 2018 regulating press and media (the “Media Law”) and its executive regulations issued by Prime Ministerial Decree No 418 of 2020. The licensing requirements for media services are also set out in the President of the Supreme Media Council Decision No 26 of 2020 (the “Licensing Regulations”).

Regulatory application extends to all types of media, press and marketing content and broadcasting services, including content disseminated or generated via audio, video, satellite, electronic media, marketing, and internet platforms (media services). The Media Law establishes the licensing requirements for press, media, websites, online platforms and broadcasting activities. In this context, social media platforms and user-generated content would fall under the ambit of the Media Law. This inclusion aims to track content as well as income generated from these platforms for tax purposes.

The Media Law requires obtaining a prior licence from the Supreme Council for Media Regulation (SCMR). To obtain the SCMR licence, specific prerequisites for audio-visual media services should be met by an applicant.

The prerequisites and licensing requirements are as follows.

Prerequisites

Media

Media institutions are defined under the Media Law as “institutions that manage media means”. Media means are defined as “terrestrial and satellite television channels, and wired, wireless and electronic broadcasting stations”. The Media Law prohibits the incorporation or operation of any media means or websites, or advertising for these services, without a prior licence from the SCMR (Article 59). The Media Law also prohibits carrying out broadcasting services from outside accredited media locations except with the approval of the SCMR. In addition, the Media Law restricts broadcasting of any media means which include commercial materials, whether electronic, visual or audio, through smartphones or other types of equipment, except with the

approval of the SCMR and subject to the applicant being a holder of a tax card.

The licence will set out the duties of the licensee, which inter alia shall include:

- the type of service and broadcasting technology;
- duration of the licence;
- territory;
- quality of service requirements; and
- IP rights.

Participating in and owning media means and online websites is permitted for Egyptian nationals, whether individual or juristic entities. Also, the Media Law requires that the prospective owner or participant not be subjected to crimes of dishonour or deprived of practising their political rights.

Furthermore, the Media Law requires that the owner of the media means that undertakes audio, visual or electronic broadcasting through use of the internet takes the form of a company (Article 51). The minimum authorised share capital for a media company is as follows (Article 54):

- EGP50 million for TV, broadcasting and news channels;
- EGP30 million for specialised TV channels;
- EGP15 million for each radio station;
- EGP2.5 million for a TV station or digital TV channel; and
- EGP100,000 for online websites.

Foreigners, whether natural or juristic persons, may not own the majority of shares or acquire controlling rights in media institutions. Foreigners wishing to obtain a licence to provide media means should have a foreign media licence or a

legal domicile abroad (Article 22 of the Licensing Regulations).

Websites

The Media Law defines a website as a “licensed electronic page, link or application through which press, media or advertising content is presented, whether it is textual, audio, visual, static, mobile or multimedia, and is issued under a specific name and has a specific electronic address and domain, and is created, hosted or accessed through the internet.”

The Media Law prohibits establishing or operating websites, or creating branches of websites, operated from abroad in Egypt without a prior licence from the SCMR.

Application to own or operate a website is permitted for Egyptian nationals, whether natural or juristic, as long as the applicant is not subjected to crimes of dishonour or deprived of practising their political rights. Corporate entities wishing to own a website and obtain the relevant licence should have a minimum share capital of EGP100,000. Foreign websites providing news, media or marketing content in Egypt also require a prior licence from the SCMR.

Licensing

Media

Media services require a prior licence from the SCMR. To obtain this, the relevant application form should be filled in and submitted to the SCMR, supported with the requisite information, as follows:

- the signature of the applicant or the legal representative of the applicant (if the applicant is a juristic person);
- the name, nationality and address of the applicant;

- the name of the website or media means, its activity, financial resources, editorial and administrative structures;
 - the name of the broadcasting responsible, the name of the programme manager, the budget and the broadcasting location;
 - a copy of the identification card (if the applicant is a natural person), or a copy of the commercial register (if the applicant is a juristic entity);
 - the name of the newspaper's website and broadcasting location;
 - proof of payment of the EGP50,000 application fee for the website and the EGP250,000 fee for media means; and
 - compliance with the code of ethics issued by the SCMR.
- a copy of the memorandum and articles of association (if the applicant is a juristic person);
 - names of the board of directors, their nationality and IDs (if the applicant is a juristic person);
 - the budget;
 - financial statements (if the applicant is a juristic person);
 - a trade mark registration certificate for the website;
 - an undertaking to avoid transmitting content in violation of the applicable laws;
 - a copy of the lease or title deed of the location for managing the website, duly notarised by the notary public; and
 - payment of EGP50,000 in fees.

Websites

Websites, whether in the form of an application, platform or page, require a prior licence from the SCMR. The Licensing Regulations stipulate the licence requirements for websites by specifying those activities that fall within the category of “websites” as follows:

- news;
- media;
- advertisement activities; and
- marketing content, whether for business, services, products or individuals using the internet inside Egypt (Article 13).

To obtain a website licence, the applicant should submit the relevant application to the SCMR supported with the necessary documents and information. These would include:

- a copy of the commercial register and tax card;
- a copy of ID(s) of the owner(s) of the website;

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The telecommunications sector is regulated in Egypt mainly by the Telecommunications Law (see **1.1 Laws and Regulations**). Additionally, the Ministry of Telecommunications and Information Technology has issued the following:

- Ministerial Decree No 667 of 2017 by the Minister of Telecommunications and Information Technology issuing contraventions and penalties regulations on communications service providers (the “Contraventions Regulations”); and
- Ministerial Decree No 258 of 2003 issuing wireless and radio frequency equipment licensing requirements (the “Equipment Licensing Requirements”).

The Telecommunications Law defines telecommunications (telecom) as “any means of send-

ing or receiving signs, signals, messages, texts, images or sounds of whatsoever nature, whether the communication is wired or wireless”. The Telecommunications Law also defines telecommunications services as “providing or operating telecom, whatever the mean used.”

Telecommunications Services and Activities

Fixed services

These include:

- landline services (fixed telephone and fixed virtual telephone) and data services (internet connectivity Class A & VOIP services);
- internet connectivity Class B services; and
- global peering services such as IPS, data content services, and Arabic internet domain services under international top-level domains (TLD) and “.Egypt” domains.

Wireless services

These include mobile services, mobile networks, message services and VAS.

Satellite services

These include:

- providing telecommunications services through satellite (VSAT – except for media content);
- providing global mobile communications by satellite (GMPCS system operator);
- providing mobile telecommunications satellite services (GMPCS service provider);
- providing satellite broadcasting services (eg, Nile Sat);
- wireless trunk services (TETRA);
- automated vehicle location services (AVL); and
- providing telecommunications services on aircraft and ships (maritime and aviation navigation services).

International services

This concerns establishing and operating an international telecommunications gateway.

Infrastructure leasing

These services are related to:

- establishing, operating and managing telecommunications infrastructure;
- use of frequencies;
- establishing and operating telecommunications towers;
- establishing, operating and leasing maritime cables and international infrastructure; and
- access to closed urban communities.

Telecommunications equipment

These services are related to using, assembling and manufacturing telecommunications equipment. Telecommunications equipment is defined under the Telecommunications Law as “any equipment, machinery or accessories used, or that could be used, in telecommunication services”. This includes wired, wireless and radio frequency telecommunications equipment.

Data hosting and cloud computing services

These services involve the following:

- cloud computing service providers (CSPs) – companies which provide various cloud services of all types, whether through fully owned data centres or through rented data centres from a public data centre provider licensee; and
- public data centres and co-location services – this concerns data centres which are established in Egypt for the purpose of hosting other data service providers.

Licences and Permits

Launching and using telecommunications services in the Egyptian market requires the prior authorisation of the NTRA. The Telecommunications Law generally distinguishes between two types of NTRA authorisation: licences and permits. Licences are required for establishing or operating telecommunications networks, carrying out telecommunication services, using radio frequencies or passing international phone calls (Article 21 of the Telecommunications Law). Permits are required for importing, trading, manufacturing and assembling telecommunications equipment (Articles 44 and 48 of the Telecommunications Law).

Licences

A prior licence from the NTRA is required to provide telecommunication services in the Egyptian market. The Equipment Licensing Requirements further set out radio frequency licensing requirements. The licence to provide telecommunications services generally requires submitting the relevant application form to the NTRA, including but not limited to the following:

- the name and details of the applicant;
- proposed pricing;
- financial and operational plans;
- market analysis; and
- any other requirements from the NTRA.

The licence will specify the scope, duration, territory, quality of service, secrecy of information and other obligations of the applicant.

In addition to the above, the Telecommunications Law establishes the interconnection and integration obligation between licensed telecommunications service providers (Article 28 of the Telecommunications Law). Interconnection is defined as “connecting the licensed networks

of two or more providers with each other, enabling connection between users through whatsoever networks or services they use.”

In this context, the integration of telecommunications services in the Egyptian market requires obtaining the relevant licence from the NTRA and entering into an interconnection agreement with a licensed telecommunications service provider. For this, telecommunications service providers will have the duty to:

- disclose the technical specifications and data of the offered services that may be required for achieving interconnection;
- conclude agreements to achieve interconnection with reasonable terms that do not discriminate between any of the telecommunications service providers, and subject to these agreements being approved by the NTRA; and
- submit the data necessary to establish and prove the extent of harm that occurred to the telecommunications service provider as a result of an act by any subscriber of another telecommunications service provider network.

Consequently, and to ensure setting a clear framework for the provision of interconnection in Egypt, the NTRA issued the Interconnection and Wholesale Services Policy (the “Interconnection Policy”). The Interconnection Policy provides guidelines on entering into reference interconnection offers (RIOs) and service level agreements (SLAs) with Telecom Egypt (the state telecommunication operator and company controlling the telecommunications infrastructure in Egypt) and with other licensed telecommunications service providers in Egypt. The Interconnection Policy highlights the following aspects:

- regulatory – determining the agreement’s validity period, and the parties’ commitment to publishing the agreement, to not engage in monopolistic or discriminatory terms, to guaranteeing to protect the licensed telecommunications service provider network, and to abide by the IP rights of the parties;
- technical – specifying the type of services, parties’ responsibilities, location on interconnection points, network management, fault recovery method, service quality standards and protections of the licensee network; and
- economic – determining the interconnection charges, terms of payment, billing procedures and cost models (as approved by the NTRA).

Permits

The Telecommunications Law requires obtaining a permit from the NTRA to import, assemble or manufacture telecommunications equipment and peripheral communications devices. The Equipment Licensing Requirements further set out the conditions for obtaining this permit. Recently, the Telecommunications Law was amended by way of the Law No 172 of 2022 (“Amended Telecommunications Law”). By way of this amendment, the penalty of possessing, assembling, using or marketing the telecommunications equipment without requisite NTRA permit would expose to a fine ranging between EGP 2million and EGP5million in addition to imprisonment between one to five years.

In addition to the NTRA permit, the acquisition, operation and use of portable or fixed transmission devices also requires approval from the SCRM, as highlighted in **6.1 Requirements and Authorisation Procedures**.

The NTRA permit would generally apply in the case of importing telecommunications equipment and is granted to companies manufactur-

ing, assembling or trading in telecommunications equipment. To obtain this permit, an application for “type approval” from the NTRA is required. This approval is also requisite for the purposes of customs clearance in the case of importation. The “type approval” will attest to technical safety and suitability to import and use the equipment in the Egyptian market.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Technology agreements are recognised under Egyptian legislation in the context of the transfer of technology. To understand the challenges involved with transfer of technology agreements, it is important to first examine the related legal provisions. Transfer of technology agreements are dealt with under the Commerce Law No 17 of 1999 (the “Commerce Law”).

Article 73 of the Commerce Law defines a transfer of technology agreement as “a contract in which the supplier of technology undertakes to transfer, against payment, technical know-how to the importer of technology to use it in a special technical way, for the production or development of a specific commodity, the installation or operation of machines or equipment, or for the provision of services. The mere sale, purchase, lease or rental of commodities or trade marks shall not be considered a transfer of technology, unless this is set forth as part of, or is connected with, the transfer of technology agreement.”

The above definition incorporates the transfer of technology to agreements that entail the transfer of technical know-how against payment of consideration. Types of transfer of technology agreements would include:

- technical assistance;
- technical know-how;
- patents;
- utility;
- commodity; and
- grant of licence agreements.

In this context, agreements not dealing with the transfer of technical know-how (such as business know-how, marketing, and financial strategies) will not be considered a transfer of technology agreement. The term “transfer of technology” under Egyptian law is however very broad. It would extend to any agreement, whether standalone or part of another contract (Article 72-2). The Commerce Law provides that these provisions shall apply to each transfer of technology agreement used in Egypt notwithstanding the nationality of the parties, their place of residence, whether the transfer is international or national (Article 72-1), or whether the transfer is provided in an ancillary agreement.

The technology transfer agreement should be made in writing; otherwise, the agreement will be null and void. The transfer of technology agreement should also incorporate all the information in connection with the technical know-how and elements of knowledge being transferred (Article 74).

The supplier is under the obligation to disclose the following information to the importer, whether during the negotiations or in the contract:

- the risks that might occur from using the technology and in particular those connected with the environment, public health, or the safety of lives or property, and the funds and methods to avoid these risks;
- judiciary actions and other obstructions that might impede the use of technology-related rights, particularly those connected with letters patents; and
- the provisions of the local law concerning the authorisation for the export of technology.

In addition, the supplier must also submit to the importer information, data and other technical documents as required for the assimilation of the technology, as well as the necessary technical services requested by the importer for the operation of the technology, particularly expertise and training. The supplier must inform the importer of improvements to the technology during the validity period of the contract, and transfer these improvements to the importer if the latter so requests.

It should be noted that the Commerce Law upholds a protective approach towards the importer of technology. This is illustrated in its granting broad rights to such importer of technology, and grounds to annul the technology transfer agreement if these rights are breached. Article 75 of the Commerce Law prohibits provisions that would result in restricting the freedom of the importer in using, developing, acquainting with or announcing the production of the transferred technology. Such restrictions could result in invalidation of the underlying provisions.

More specifically, the Commerce Law lists a number of contractual provisions in the technology agreement that would be deemed of a binding and restrictive nature to the importer in the context of Article 75, as follows:

- the importer accepting the improvements introduced by the supplier to the technology, and paying their value;
- prohibiting the introduction of improvements or modifications to the technology to suit

the local conditions or the conditions of the importer's establishment;

- prohibiting the importer from acquiring another technology similar to or competing with the technology that is the subject of the contract;
- using specific trade marks to distinguish those commodities in whose production the technology was used;
- limiting the importer's volume of production, its price, the method of its distribution or its export;
- participation of the supplier in running the establishment of the importer, or interference in choosing the permanent workers in said establishment;
- purchase of the raw materials, equipment, machines, apparatuses or spare parts for operating the technology, from the supplier alone, or from the establishments exclusively specified by the supplier; and
- restricting the sale of the production, or the delegation for its sale, exclusively to the supplier or the persons defined thereby.

The inclusion of any of these conditions in the technology transfer agreement could ultimately result in nullifying the underlying provision.

Notably, Article 87 of the Commerce Law provides default jurisdiction of the Egyptian courts over disputes arising out of technology transfer agreements. Arbitration is permitted only if it is held in Egypt according to the provisions of Egyptian law. Any agreement to the contrary shall be null and void.

Key challenges in connection with the transfer of technology agreements essentially arise in relation to legislation. Proper observance of the restrictions and obligations imposed by the Commerce Law for transfer of technology agreements is important to avoid realisation of risks.

These challenges and elements of consideration are summarised as follows.

Default Applicable Law and Jurisdiction

Perhaps the most remarkable risk is the mandatory application of Egyptian law which may not be derogated by the agreement of the parties. Article 87 of the Commerce Law grants default jurisdiction to the Egyptian courts in disputes arising in connection with the transfer of technology agreements used in Egypt. The Egyptian legislature has set out the conflict of law rule by making Egyptian law the only applicable law, and excluding jurisdictional considerations delimiting Egyptian courts' jurisdiction in deciding on transfer of technology disputes, such as regards the nationality of the parties or their place of residency, or the type of transfer (national or international).

Although Article 87 of the Commerce Law permits resorting to arbitration to resolve disputes in transfer of technology agreements, the applicable law and seat of arbitration shall by default be those of Egypt. This position was upheld in a recent decision rendered by the Cassation Court in 2021 (case No 10305/83) where the court decided that Article 87 of the Commerce Law is a mandatory rule of law. Accordingly, if a foreign licensor insists upon a foreign governing law and seat of arbitration in a transfer of technology contract with an Egyptian counterparty, such provision is likely to be declared null and void by the Egyptian courts.

The rule set out in Article 87 of the Commerce Law has long been debated. The current position is that this rule is of public order and may not be deviated from by the agreement of the parties, and consequently restricts the parties' freedom to choose the applicable law and jurisdiction (seat) of their dispute.

Nullification

The Commerce Law provides a wide range of grounds for invalidating the technology transfer agreement prescribed under Article 73, which primarily aims to protect the importer's rights. Egyptian law considers the importer the weak party in a transfer of technology agreement. This position grants Egyptian courts broad powers to classify and weigh the provisions of the technology transfer agreement.

Guarantee and Liability

Article 85 of the Commerce Law provides for liability of both the importer and the supplier of technology towards third parties in connection with damages that occur from the use or application of the technology.

Additionally, Article 85 provides that the supplier must guarantee:

- the conformity of the technology and the documents attached to it with the conditions prescribed in the transfer of technology agreement; and
- the production of the commodity, or the performance of the services agreed upon according to the specifications prescribed in the transfer of technology agreement.

This is deemed a default guarantee unless otherwise agreed upon in writing between the parties. Accordingly, it is important that the parties agree to the specifications and guarantees in the transfer of technology agreement to avoid the default application of the guarantee prescribed by law.

The parties should also be aware of the technology services requirements, especially from the standpoint of consumers, data privacy and cybersecurity. In this sense, proper consideration should be given to consumer and data pro-

tection rights and cybersecurity requirements under Egyptian law, as this may involve liability or other implications for the parties when performing their duties under the technology transfer agreement. These requirements could also differ depending on the use of the transferred technology and activities related thereto. For instance, data secrecy and security in the banking sector are subjected to additional requirements and more stringent monitoring under applicable laws.

Secrecy

Article 83 of the Commerce Law recognises how the duty of secrecy in a transfer of technology agreement differs depending on a party's position in the agreement. For instance, the importer has the duty to preserve the secrecy of the improvements introduced by the importer to the technology, and where these improvements are transferred to the supplier as per the agreement. Breach of this duty would trigger the liability of the importer to indemnify the supplier against losses resulting from breach of that duty, whether or not this breach occurred during the negotiation phase or after the signature of the transfer of technology agreement.

Conversely, the supplier's duty of secrecy towards the importer only covers improvements introduced by the importer to the technology as per the transfer of technology agreement's provisions. Therefore, it is important for the parties to review their respective confidentiality duties and rights in the transfer of technology agreement. Parties should also take into consideration particular confidentiality and protection factors regarding IP rights.

Duration

Article 86 of the Commerce Law permits the parties to a technology agreement to request termi-

nation or amendment of the terms of the transfer of technology agreement upon the lapse of five years from the date of the agreement. It is thus important for parties to expressly agree on the duration and rights for termination or review of the terms of the transfer of technology agreement, to avoid this default application under Article 86.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Trust services, the use of e-signatures and digital identity schemes are mainly all regulated under the E-Signature Law and its executive regulations. The E-Signature Law falls under the auspices of the Telecommunications Law, which regulates the telecommunications sector.

The E-Signature Law was further issued in light of the Evidence Law No 25 for 1968, and the Protection of Intellectual Property Rights Law No 82 for 2002.

The key purpose for issuing the E-Signature Law was to regulate e-signatures (defined below) and to establish an authority (ie, ITIDA) responsible for regulating the activity of e-signature services and other activities in the field of electronic transactions and the information technology industry (see The E-Signature Law in **2.1 Key Challenges**).

On 4 March 2021, ITIDA issued a general “Certificate Policy” (CP) guideline, which is pursuant to the E-Signature Law and its executive regulations. The CP guideline established that ITIDA shall operate the Egyptian Root-CA, which issues certificates for certification service

providers (CSPs) issuing digital certificates for e-signatures and electronic seals. The Egyptian Root-CA therefore serves as a trust anchor for all e-signatures based on certificates that are issued in Egypt. There is a limited number of licensed CSPs in Egypt (currently only three).

Additionally, the New Banking Law No 194 for 2020 expressly provides that licensed banking entities and representative offices of foreign banks in Egypt must keep electronic copies of records, contracts, correspondences, commercial papers and documents related to banking transactions and payment services, for the periods legally specified for keeping their originals.

These copies shall have the same evidential powers as the original documents when their retention, circulation and retrieval have been carried out in accordance with the rules and technical standards determined by the board of directors of the Central Bank of Egypt.

Elements Relevant to the E-Signature Law

Fundamental rights

As per the E-Signature Law, e-signatures and electronic documents, within the scope of civil, commercial and administrative transactions, shall have the same evidentiary effect as given to written signatures and official and customary documents in the provisions of Egyptian evidence law in civil and commercial materials, as long as the conditions stipulated in the E-Signature Law are fulfilled (see **2.1 Key Challenges**).

Further, a copy from an official electronic document has the evidential effect of being identical to the original of the document, as long as the official electronic document and the e-signature are present on an electronic backup.

Data protection

Without prejudice to the general protections conferred under the Data Protection Law, the E-Signature Law also reinforces data protection in all data related to e-signatures. In particular, the E-Signature Law states that e-signature data and all electronic information provided to an entity authorised to issue electronic certificates (ie, a CSP) is confidential, and the person to whom it was presented or who was contacted, by virtue of their work, may not disclose it to others or use it for a purpose other than that for which it was presented.

Intellectual property

In furtherance to the IP Law, the E-Signature Law is eager to protect those entitled to IP rights, and grants ITIDA the authority to deposit and register the original copies of computer programs and databases submitted by entities or individuals who publish, print and/or produce them, in order to preserve their IP rights and any other rights.

Jurisdiction

According to the E-Signature Law, ITIDA is the authority responsible for licensing and supervising e-signatures. The E-Signature Law confers a number of powers on ITIDA, including:

- the issuing and renewing of licences necessary to engage in e-signature services, and in other activities in the field of electronic transactions and the information technology industry;
- determining the standards of the e-signature system;

- deciding on complaints relating to e-signature activities;
- providing technical advice on disputes that arise between parties in e-signature activities;
- providing technical advice to entities working in the field of information technology activities; and
- registering the original copies of computer programs and databases submitted by entities or individuals who publish, print and/or produce them, in order to preserve their IP rights and any other rights.

Moreover, the E-Signature Law authorise ITIDA to revoke or suspend a licence if the licensee (ie, CSP) violates the licensing conditions.

Liability

As regards liability, there are mutual obligations on both ITIDA and on CSPs that aim to ensure the legally binding effect of e-signatures and electronic seals.

A CSP must first obtain the relevant licence from the competent authority under the control of ITIDA, and use said licence within the scope of its issuance – that is, issuing digital certificates for e-signatures and electronic seals. The validity of a certificate issued by a CSP must not exceed that of the CSP licence.

ITIDA must comply with the E-Signature Law and its executive regulations when licensing CSPs.

Shehata & Partners was founded in 1996 and is driven by a vision to provide unique legal services that cater to the business needs of corporate entities doing business in Egypt. The firm's core mission is to provide the most trusted and effective legal advice on both dispute resolution and corporate law in Egypt. Shehata & Partners

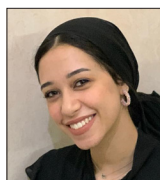
is results-driven and delivers exceptional services to clients across various practice areas and multiple industries. The firm continues to achieve the highest client satisfaction rates in the region due to the meticulous implementation of its client-centric approach.

Authors



Nevine El-Shafei joined Shehata & Partners as a partner in 2022. Nevine is a diversified lawyer with over 15 years of experience in the corporate, banking, finance and business fields. Her

practice focuses on corporate, commercial, TMT and pre-contentious matters. Previously, Nevine worked in both in-house and private practices in Egypt, Qatar and across the MENA region. She has acquired extensive experience within the banking and finance sectors, and in the telecommunications and real estate fields. Nevine obtained her Maîtrise in law from Université Paris 1 Panthéon-Sorbonne, France, and a licence in law from Cairo University, Egypt. Nevine also has a Master's in International Business Law from Paris Dauphine and Cairo University and a Diploma in International Commercial Arbitration from the Chartered Institute of Arbitrators in the UK.



Tasneem El-Naggar is an associate with over two years' experience in the corporate department. She recently joined Shehata & Partners after starting her career at Khodeir & Partners.

Tasneem has interned in several top-tier law firms in Egypt. In addition, she has assisted several Egyptian start-ups such as Seqoon, The Food Lab and Balad with conducting business smoothly and efficiently in Egypt. Tasneem has also been actively involved in the automotive sector through assisting Yazaki in developing its private free zone project in Egypt. Furthermore, Tasneem has been actively working in the fintech sector by delivering strategic advice to Balad and to other start-ups in this promising sector.

Contributed by: Nevine El-Shafei and Tasneem El-Naggar, **Shehata & Partners**

Shehata & Partners

Cairo Business Plaza
North Tower
Second Floor
Unit 204
New Cairo, Cairo
Egypt

Tel: +20 28135682
Email: info@shehatalaw.com
Web: shehatalaw.com



Law and Practice

Contributed by:

Bertrand Liard, Clara Hainsdorf,
Saam Golshani and Guillaume Vitrich
White & Case LLP see p.166



Contents

1. Metaverse	p.152
1.1 <u>Laws and Regulations</u>	p.152
2. Digital Economy	p.153
2.1 <u>Key Challenges</u>	p.153
3. Cloud and Edge Computing	p.153
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.153
4. Artificial Intelligence and Big Data	p.155
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.155
5. Internet of Things	p.157
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.157
6. Audio-Visual Media Services	p.159
6.1 <u>Requirements and Authorisation Procedures</u>	p.159
7. Telecommunications	p.161
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.161
8. Challenges with Technology Agreements	p.162
8.1 <u>Legal Framework Challenges</u>	p.162
9. Trust Services and Digital Entities	p.164
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.164

1. Metaverse

1.1 Laws and Regulations

While there is no official definition for the metaverse and this is mostly a prospective subject, the notion is used to describe real-time online virtual worlds that are deeply immersive and often include 3D technologies and avatar representations of their users. The metaverse may also rely on other Web3 technologies such as cryptocurrencies and non-fungible tokens. It is sought to be used in a wide variety of areas such as gaming, arts, education, and professional and social activities. For the moment, the metaverse mostly raises challenges regarding data protection, intermediary services regulation and intellectual property.

The French Minister of Economy recently commissioned a report on the metaverse, which was published on 24 October 2022 and addresses some of the key legal considerations related to the metaverse.

Data Protection Implications

The metaverse is likely to raise personal data protection issues, as it will involve information relating to identified or identifiable individuals. Metaverse platforms that are either established in France or target data subjects in France will therefore have to comply with the General Data Protection Regulation (GDPR) and the French Data Protection Act of 1978 as amended.

The metaverse will generate an increase in personal data collection and subsequent data processing operations due, among other things, to virtual reality headsets and other biometric sensors used to render the user experience more immersive. This possibility will however have to be articulated with the data minimisation principle and the security obligation laid by Articles

5(1)(c) and 32 of the GDPR. Part of this personal data may also qualify as special category data under Article 9 of the GDPR and health data under the French Data Protection Act, resulting in the application of a more restrictive legal regime.

Data controllers will also have to find valid technical solutions to collect data subjects' freely given, specific, informed and unambiguous consent for processing operations that rely on such consent as a lawful basis.

Intermediary Services Regulation Implications

Metaverse platforms will likely qualify as intermediary services subject to the Confidence in the Digital Economy Act of 2004 and the EU Digital Services Act of 2022. Such platforms will therefore have specific obligations as well as a particular liability regime depending on their exact qualification under such laws and their average number of users.

Intellectual Property Implications

The metaverse is expected to display many elements that may be protected by intellectual property, such as copyright or trade marks; therefore, it will have to comply with the applicable intellectual property laws governing the permitted and prohibited uses of such elements.

On 30 September 2022, the French Higher Council for Literary and Artistic Property (*Conseil Supérieur de la Propriété Littéraire et Artistique* or CSPLA), an entity responsible for advising the Minister for Culture on intellectual property matters, published a report on the intellectual property implications of virtual reality and augmented reality. The CSPLA also recently announced the creation of a committee dedicated to the metaverse. Their report on the matter is expected to be published in July 2023.

2. Digital Economy

2.1 Key Challenges

The rise of the digital economy has led to the adoption of numerous laws in France and the European Union in order to govern digital services, content regulation and digital markets.

Digital Services and Content Regulation

Digital services and content regulation are currently mostly ruled by the Confidence in the Digital Economy Act of 2004 (*Loi pour la confiance dans l'économie numérique*), which transposed the EU Directive on electronic commerce of 2000 and has been frequently amended since its coming into force. The Confidence in the Digital Economy Act provides the legal regime for hosting services, including their particular civil and criminal liability regime and their obligations regarding content regulation. The French Consumer Code lays down the obligations that are applicable to online platforms in their relations with consumers (eg, pre-contractual duty to inform).

The applicable regime is currently evolving due to the recent entry into force of the EU Digital Services Act (DSA) of 2022. The DSA establishes an EU-wide set of rules for intermediary services and online platforms, which imposes new obligations and requirements regarding the content they host, transmit and make available to the public. In this regard, the DSA empowers regulators with broad investigative and enforcement powers to deal with non-compliance at the national and EU level. The DSA will progressively enter into application until 17 February 2024.

Digital Markets Regulation

Digital markets are currently mostly regulated by general competition law (merger control and prohibition of anti-competitive practices). The

EU Regulation on platform-to-business relations (P2B Regulation) was adopted in 2019 to impose transparency and fairness obligations on online intermediation services and online search engines used by business users to provide goods and services to consumers.

More recently, the Digital Markets Act (DMA) was adopted on 14 September 2022 to regulate certain very large online platforms (gatekeepers) which are important gateways for business users to reach end users. The designated gatekeepers under the DMA will be subject to a list of ex ante obligations and prohibitions.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Cloud Computing

While there is no official definition of cloud computing, the notion usually covers the use of a remote information system, under the control of the client on a shared platform. Cloud services refer to a variety of services, such as infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS). They allow a client to switch part or all of its IT infrastructure and resources to the cloud, rather than managing it locally or internally.

Under French law, there is no particular contractual law category related to cloud computing contracts. As such, they are subject to common French contract law. Particular attention should be given to the content of the contract, notably regarding data integrity and security, service level agreements (SLAs), the clear division of the responsibilities of each party, and compliance with data protection laws and regulations. In addition, the termination of the contract should

also be anticipated with the use of precise clauses such as notice periods, chain termination of contracts, reciprocal restitution and reversibility.

In March 2022, the National Cybersecurity Agency for France (ANSSI) published version 3.2 of its certification framework for cloud service providers (SecNumCloud), to promote a protective digital environment in line with technical developments. The SecNumCloud identifies trusted cloud services and provides the service providers with a label that confirms that the service provider complies with the security and regulatory standards set out in the framework. In particular, the framework ensures that the cloud service provider and the respective data that they process must be subject to European laws in order not to undermine the level of protection by them.

Cybersecurity Implications

Cloud service providers are qualified as “digital service providers” under the EU Directive Network and Information Security (NIS Directive), which was transposed into French law, notably in Law No 2018-133 of 26 February 2018. As a result, they are subject to specific cybersecurity obligations such as carrying out risk assessments on their system, taking technical and organisational measures regarding the security of their systems, implementing processes for managing security incidents, and, if required, notifying the French National Cybersecurity Agency (ANSSI) of any such incidents.

To obtain a certification pursuant to the SecNumCloud, the service providers must comply with the security standards set out in the framework. Since 2019, France has been engaged in the creation of the European certification scheme for Cloud providers (EUCS). The new version of the SecNumCloud is designed to ensure a very

high level of certification and works in the future as a reference.

Data Protection Implications

Cloud computing services usually involve storing and sharing data that may fall within the scope of regulations on the protection of personal data. Therefore, it is essential that any cloud project be compliant with data protection laws and regulations. As such, the General Data Protection Regulation (GDPR) and the French Data Protection Act of 1978, as amended in June 2019, will be applicable to the processing of personal data within a cloud project.

Importantly, it will be necessary to assess whether the cloud service provider will act as data controller or data processor regarding the personal data processed by the cloud service. In most cases, the cloud provider will be qualified as data processor and the client as data controller, but this may vary depending on the nature of the processing and the general cloud project. In addition, transfer of data outside of the EU must be carried out only with appropriate safeguards. To ensure this, a contractual framework must be put in place between the provider and the client, which must also address the requirements provided for in Article 28 of the GDPR regarding data processing.

The new version of the SecNumCloud also provides guarantees on data protection against non-EU legislation. Of particular importance is herein the incorporation of the aftermath of the Schrems II ruling of the European Court of Justice. The design of the data protection regulations are compliant with the requirements of the Schrems II ruling. The French data protection authority, the CNIL, even recommends the use of this standard for all data controllers who want to guarantee a high level of data protection.

Regulation in Specific Industries

The banking industry is subject to specific provisions regarding cloud computing. Indeed, on 25 February 2019, the European Banking Authority (EBA) adopted new guidelines on outsourcing. These guidelines include specific provisions – for instance, regarding:

- the protection of confidentiality and personal or sensitive information; and
- the need to comply with all legal requirements relating to the protection of personal data, banking secrecy or confidentiality obligations concerning customer data.

The French supervisory authority for banks and insurance (ACPR) has published a notice to ensure that these guidelines are followed in France.

Finally, the insurance industry is also subject to similar requirements. On 6 February 2020, the European Insurance and Occupational Pensions Authority (EIOPA) published its Guidelines on Outsourcing to Cloud Service Providers, which provides guidance to insurance and reinsurance providers on how outsourcing should be carried out to cloud service providers in order to comply with their industry-specific regulations. The ACPR has also published notices relating to the modalities for the implementation in France of the EIOPA guidelines.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

As the issues and challenges of artificial intelligence (AI) and big data are similar, the following points are common to all of them.

Big Data

Big data technologies have enabled emergence of AI, which requires both high computing power and large volumes of data to train and test models. Companies are now looking to integrate AI into their business processes and information systems. On issues such as image and voice recognition, AI innovations have reached an advanced level. Consequently, two major issues have arisen related to big data:

- the protection of personal data; and
- the reuse of public data with the phenomenon of “open data”.

For instance, in order to train AI's system or machines to best fit users' or companies' needs – advertising, internet of things (IoT), etc – AI requires a huge amount of data. Nevertheless, merging and exploiting several datasets during the processes of data mining sometimes delivers information that can allow the inference of very intimate personal information with a very high degree of accuracy. As a result, the governance arrangements for the collection and processing of digital data have very profound implications for human rights and accountability. On a more practical approach, companies may have to collect, process and store personal data on databases for business purposes and for a certain amount of time. Therefore, some warranties have to be given by the companies processing such data.

Data Protection

The protection of personal data is ensured by the EU General Data Protection Regulation (GDPR), implemented in France in the law of 6 January 1978 entitled *Informatique et Libertés*. The GDPR grants rights to users whose data is processed, including the rights of rectification, deletion and access in order to give the user control

over their data. It also obliges data controllers to take effective and precise security measures to avoid endangering the personal data being processed. The obligations of the data controllers also include an obligation to minimise data, transparency and legitimacy in relation to the purpose of the processing. Individuals whose data is being collected, processed or stored must be informed of the purposes of such processing, which must rely on one of the legal bases given by the GDPR and embedded in the French law.

These rights, and especially the purpose restriction and prior information, must be considered when launching a big data project, since it is unlikely that the user would have been informed of a purpose and processing that had not even been envisaged when the data were collected.

In 2022, the French Data Protection Authority (the CNIL) issued an online guidance on “AI: ensuring GDPR compliance”. The CNIL recommends, among other things, to use data pseudonymisation or filtering/masking mechanisms when developing an AI system. In January 2023, the CNIL also announced the creation of an Artificial Intelligence Department dedicated to AI matters.

Responsibility/Liability

As AI can take decisions with a degree of autonomy, a key legal issue is responsibility/liability. As of February 2023, no legal regime is in place to deal with the liability of a robot or a machine that would act according to an autonomous AI process – autonomous cars, for example. In France, it is then necessary to look for the legal basis in the tort liability of Articles 1240 and seq of the French Civil Code, which states that any damage caused must be remedied by the person who caused it. Regarding tort liability, French law sets

out three conditions that need to be fulfilled for liability to be attributable to a party:

- fault;
- damage; and
- a causal link between the two.

The burden of proof lies with the claimant. However, this regime may not be adequate in that its application requires the presence of a legal personality.

In this context, the European Commission published a white paper on artificial intelligence in 2020 and by April 2021 it had issued a proposal for a new regulation on AI (Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence), for which the legislative process is still ongoing. The Commission bases its approach on the identification and framing of risks related to AI by creating categories (unacceptable risk, high risk and non-high risk) according to the fields of application concerned. Accordingly, AI categorised as having unacceptable risks would be prohibited. High-risk AI would be permitted subject to compliance with certain mandatory requirements and an ex-ante conformity assessment. For other non-high-risk AI systems, only limited transparency obligations would be imposed.

On 28 September 2022, the European Commission (EC) adopted two proposals to adapt the liability rules to the digital age. First, the EC published a proposal to revise the Directive 85/374/EEC on liability for defective products to include a compensation for damages caused by products like robots, drones, smart home systems made unsafe by software update, AI or digital services such as software as well as cybersecurity vulnerabilities. Second, the EC published on

the same date, a proposal for an Artificial Intelligence Liability Directive (AILD) in order to adapt non-contractual civil liability rules to AI systems. It lays down consistent rules for aspects of non-contractual (tort) civil liability in connection with damages caused by or with the involvement of AI systems. A “presumption of causality” and a “right of access to evidence” are additional measures provided to consumers in complement to the Directive on defective products.

Intellectual Property

Many elements of big data and/or AI systems may be protected by intellectual property rights (or assimilated), for example, content, algorithms under certain conditions, computer programs, models, robots, database, etc. It is necessary to take into account the type of protection appropriate for each element (ie, patent, copyright if original and specific form for content, computer programs, designs for robots, etc).

Of particular interest is the protection of creations by AI, since AI is already creating potential proprietary content, from works of art to algorithms and computer programs. It is obvious that the intellectual property protection system is based on human creativity, which will render the works of AI difficult to protect under the prevailing circumstances. No related case law is evident in France but, in the DABUS case, the European Patent Office denied patent protection of an invention by AI on the grounds that no human was named as inventor. There are workaround solutions, such as naming a physical person as inventor or author, but this does not fully solve the issue, and a legislative intervention seems necessary on this topic.

Data Economy

Big data and the internet of things (IoT) have brought on new challenges to consumers as well

to companies, but they have also brought new opportunities. The EC addressed data access, fairness in the digital environment, the stipulation of a competitive market and increasing opportunities for data-driven innovation by proposing new rules on who can use and access data generated in the EU across all economic sectors in February 2022 (Data Act). The proposal for the Data Act includes:

- measures to allow users of a connected device to gain access to data generated by their devices and the ability to share such data with third parties;
- measures to balance the power between SMEs and big companies; and
- means for public sector bodies to access and use data held by the private sector if exceptional circumstances prevail.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection Liability

The question arises as to who is responsible in the case of damage caused by a connected object. As French law stands, there is no specific legal framework applicable to liability for connected objects or connected robots. General liability rules will then apply. A distinction must be made between contractual and extra-contractual liability. In addition, several liability regimes may apply, in particular defective products or the custody of the object.

For instance, if the manufacturer/producer of the connected objects does not respect its pre-contractual information as referred to in Articles 1112-1 of the French Civil Code and Articles L

111-1 and seq of the French Consumer Code with regard to the substantial characteristics of connected objects, they could be held accountable for that omission.

However, these regimes do not fully meet the challenges related to connected objects and artificial intelligence in general. It seems necessary either to adapt the existing regimes or to create a specifically adapted regime.

In December 2021, the French National Institute for Research in Digital Science and Technology (INRIA) published a white paper on the internet of things (IoT). It defines the scope of the IoT, its genesis and its current status, and it identifies the main societal, technical and scientific challenges.

It confirms that, at the present time, no specific regime is being developed for connected objects; these are only envisaged in relation to personal data. Indeed, the white paper highlights the “permanent tension between IoT data exploitability and IoT user privacy”.

Data Protection

The French Data Protection Act of 6 January 1978, amended following the implementation of the GDPR, regulates the liability of the various actors involved in the data collection, processing and storage process. It imposes obligations of security and transparency vis-à-vis the data and the user for both the data controller and the data processor or subcontractor. It also allows individuals whose data is being collected to access their data, modify it or erase it. The difficulty lies in the identification of these different actors in IoT projects. This can be complicated due to the interoperability of the connected objects and their communication system allowing them to exchange data at any time.

Beyond the obligations imposed by GDPR and French data protection law, the *Commission Nationale Informatique et Libertés* (the French authority enforcing data protections legislations) also recommends proceeding to Data Protection Impact Assessments when implementing IoT projects before processing personal data in order to highlight the purposes of the processing and the legitimate means of achieving them. It also provides guidelines to data subjects using connected objects to better protect themselves from the risks inherent to the use of IoT.

Consent

Consent is one of the legal bases for any data processing. In IoT devices, it is not always possible to request consent directly. Therefore, in order to implement the GDPR requirements for freely given, specific, informed and unambiguous consent, IoT manufacturers must find other ways to collect consent.

Cybersecurity

In January 2019, the INRIA published a white paper on cybersecurity. This study shows that vulnerable connected objects represent a risk because a breach in their components can have an impact on thousands of people. Breaches can thus be exploited to divert objects from their main uses, such as involving them in large coordinated cyber-attack (eg, an attack using Mirai software).

INRIA has developed SCUBA, a tool which automatically evaluates the risk of a connected object in its environment. SCUBA allows to audit the security of a connected device in its global environment.

For example, SCUBA made it possible to detect a security breach between a connected doorbell and its service in the cloud. The doorbell,

with a camera, sends a picture of the person at your door to the cloud and then sends it to your phone. However, this communication between the doorbell and the cloud is not encrypted and the photo is sent in a clear message, allowing an attacker to intercept the message containing the photo and replace it with another one.

On 15 September 2022, the European Regulation on Cybersecurity Act came into force. The latter established a certification system whose evaluation methodology will differ depending on the level of insurance targeted. Therefore, entities manufacturing/producing connected objects can acquire from ANSSI a label ensuring their compliance to cybersecurity standards.

In the same context, ANSSI published its recommendations on the security of connected objects that aims on one hand to realise an assessment of the security level by listing the potential threats that could be faced in this industry and on the other hand by providing general technical recommendations to address those threats.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Audio-visual services traditionally cover TV, radio and on-demand audio-visual media services (AVMS). AVMS include services commonly include on-demand video services (VOD), catch-up television and audio podcasts.

Audio-visual services are subject to the Law 86-1067 of 30 September 1986 on the freedom of communication and regulated by an independent administrative authority, the *Autorité de régulation de la communication audiovisuelle et*

numérique (Arcom since 1 January 2022, formerly CSA).

While the requirements and associated procedure for providing an audio-visual service will depend on the nature of the service, there are general obligations to which all providers are subject. Indeed, the Arcom will make sure that providers do not undermine the dignity of the person or the rights relating to privacy and that they comply with specific provisions concerning the protection of minors. In addition, programmes must promote the use of the French language, they must not undermine the protection of public order, and they must be free from any incitement to hatred or violence.

For TV and Radio Providers

The Arcom must grant authorisation to TV and radio providers using the network of assigned frequencies before they can provide their services. Private providers have to participate in a call for applications and be selected by the Arcom in order to be provided with an assigned frequency. The applications must be presented by the provider of the services, and must notably contain the general and technical characteristics of the service, the forecasts of expenditure and income and the composition of the applicant's shares, governing bodies and assets.

The provider must also sign an agreement with the Arcom, which sets the specific rules applicable to the service, taking into account its coverage and its share of the advertising market, as well as the compliance with competition rules. The authorisation provided by the Arcom may not exceed ten years for TV services and five years for radio services, but can be renewed up to two times without going through a new call for application.

For other services provided without using the assigned frequencies, the applicable procedure will depend on the service. As a principle, such services may be broadcasted only after entering into an agreement with the Arcom, defining their specific obligations and the contractual penalties available to the regulator for non-compliance. However, services with a budget under EUR75,000 for radio and EUR150,000 for TV are only required to make a prior declaration rather than entering into an agreement.

Finally, distributors of audio-visual services not using assigned frequencies (for instance, providers offering a television “package” service) are subject to a prior declaration before distributing such services. Such declaration must notably include the corporate form, the name or business name and the address of the head office of the service distributor, the list of services and the structure of the offer of services made available to the public, as well as a letter of intent to conclude a distribution agreement from a paid television service.

For AVMS Providers

AVMS must be declared to the Arcom prior the provision of such services. The purpose of such declaration is to facilitate the identification of AVMS, better ensure their regulation and be able to verify their obligations. This declaration must notably include the description of the service and the designation of a responsible person and can be completed online.

Requirements for Companies with Online Video Channels With User-Generated Content

Video-sharing services were traditionally excluded from the scope of AVMS when the user content was provided without the editorial control of the service provider.

A major reform was conducted at the EU level via the revised Audiovisual Media Services Directive (Directive (EU) 2018/1808 of 14 November 2018). This Audiovisual Media Services Directive extends certain audio-visual rules to video-sharing services, such as YouTube. It has been transposed in France by an ordinance dated 21 December 2020 and published on 23 December 2020.

In order to be considered as a video-sharing service, the service must meet the following conditions:

- it is provided by means of an electronic communications network;
- it provides user-created programmes or videos to inform, entertain or educate as its main purpose;
- it has no editorial responsibility for the content; and
- it is related to an economic activity.

Such video-sharing services are subject to specific obligations. In addition to ensuring that the services comply with the general obligations regarding content, the Arcom will also have additional powers – for instance, being in charge of dispute resolution between users and providers of these services or making sure that these providers comply with transparency obligations.

Note that these powers are limited to video-sharing platforms which are established in France, as the principle of country of origin applies. However, video-sharing services established in other EU member states may be subject to the French system of contributions to the production of cinematographic and audio-visual content, even though they will remain regulated by their country of origin.

Specifically, regarding the possibility for online video channels with user-generated content operated by companies to be considered as an AVMS, this assessment needs to be made on a case-by-case basis.

In this respect, the ECJ qualified as an AVMS the catalogue of videos proposed by an online press website with a content independent from that of the written press articles, since these videos, produced by a local television publisher, were comparable to those of other services of the same nature (ECJ, 21 October 2015, C-347/14). On the contrary, the ECJ found that a commercial video on a YouTube channel could not be considered an AVMS as it did not inform, entertain or educate viewers (ECJ, 21 February 2018, C-132/17).

In France, the Arcom qualified as AVMS pages of radio stations' websites offering a catalogue of video programmes, which constituted an autonomous offer of other content (CSA, decision of 29 May 2013). Similarly, the Arcom considered that an online video channel – in this case, a YouTube channel, “*Les recettes pompettes by Poulpe?*” operated by a company – qualified as an AVMS and was thus subject to the obligations applicable to this category of services, notably relating to the protection of young audiences (CSA, decision of 9 November 2016). More recently, the Arcom held that the YouTube channel of a television channel operated by a company also fell under the definition of AVMS (CSA, decision of 3 July 2019).

It follows from such decisions that programmes offered on video-sharing services (eg, “channels”) may be considered AVMSs should the on-demand channel include content organised by the editor of that service, allowing the user to choose from a catalogue of content.

European Media Freedom Act

The European Commission adopted in September 2022 a proposal for the European Media Freedom Act to protect media pluralism and independence in the EU. It builds on the revised Audiovisual Media Services Directive, the Digital Services Act, and the Digital Markets Act. The European Media Freedom Act is part of the EU's project to promote participation in democracy, to address fake news and disinformation and to support media freedom and pluralism. The Act shall ensure an easy cross border operation of media in the EU internal market. Thus, the focus of this legislation lies on the independence (also in regard to stable funding) as well as on the transparency of media ownership. The Act also regulates the protection of independence of editors and the disclosure of conflicts. The Act furthermore creates a new independent European Board for Media Services to act as a watchdog for media freedom. Further measures the legislation wants to implement are safeguards against espionage software, transparent state advertising and the new user right to customise their media offer. In 2023, the European Parliament and the member states will discuss the proposal of the European Media Freedom Act. If adopted, the Act will be directly applicable across the EU.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Local telecommunications rules traditionally apply to electronic communication networks (ECNs) and electronic communication services (ECSs) (Article L 32 of the French Postal and Electronic Communications Code).

At an EU level, however, the Directive (EU) 2018/1972 of the European Parliament and of the

Council of 11 December 2018 establishing the European Electronic Communications Code (the EECC Directive) modified and updated the applicable framework. In France, the EECC Directive was transposed by Ordinance No 2021-650 of 26 May 2021 in application of Article 38 of Law No 2020-1508 of 3 December 2020.

Importantly, the EECC Directive expands the definition of ECSs by including so-called “interpersonal communications services”, defined as services normally provided for remuneration that enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipients. Accordingly, and subject to the transposition ordinance of the EECC Directive, voice-over internet protocol (VoIP) and instant messaging falls under the new scope of the telecommunications rules. This was confirmed by Recital 15 of the EECC Directive, and is in line with ECJ’s previous ruling, which considered that SkypeOut offering a VoIP service constitutes an ECS (ECJ, 5 June 2019, C-142/18).

The qualification of radio-frequency identification (RFID) as ECS remains unclear, as it is not specifically covered by the new scope of the telecommunications rules. However, the French telecommunication authority (*Autorité de Régulation des Communications Électroniques et des Postes* or ARCEP) considers RFID technology as radio-electric installations, which can be used on certain frequencies only and with defined technical settings.

Applicable Requirements

The declaratory regimes for ECSs has been abolished by Ordinance No 2021-650 of 26 May 2021. The provision and the establishment

of ECNs is now free subject to compliance with rules laid in Article L 33-1 of the French Postal and Electronic Communications Code (obligation to notify security incidents to ARCEP, net neutrality, interoperability of services, etc).

In France, every operator must pay an administrative tax under the conditions provided by the finance law. It must also pay an additional fee in case of use of a specific frequency or the provision of a specific numbering.

Providers of instant messaging are subject to stricter data protection law requirements with regard to messages under the Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the ePrivacy Directive). This Directive notably obliges member states to ensure the confidentiality of communications and the related traffic data by means of an ECN or ECS through national legislation. For example, traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when no longer needed with regard to Article 6 of the ePrivacy Directive.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges Parties’ Level of Expertise

Most issues arising from information technology (IT) service agreements relate to late or wrong performance of the parties’ respective contractual obligations. Because of the technical aspect of an IT service agreement, the allocation of

responsibilities between the parties is key. In many instances, customers are not very familiar with the technology supplied by the service provider, which is therefore subject to an obligation of advice and information during the negotiation (Article 1112-1 of the Civil Code) and the performance of the agreement (Article 1104 of the Civil Code). This obligation implies:

- an obligation to provide information (the service provider must inform itself about the customer's needs and wishes); and
- an obligation to warn (eg, in the event the service provider considers that the customer's expectations are unlawful or risky, it has a duty to inform the customer and may even refuse to contract with the customer on this basis).

As for the customer, it has a duty to collaborate with the service provider.

Furthermore, in 2016, French law extended the protection against unfair clauses to all pre-formulated standard agreements (*contrat d'adhésion*), including B2B agreements. Some IT service agreements may qualify as such pre-formulated standard agreements provided customers cannot negotiate their content. The terms of these agreements may be considered unfair if they create a significant imbalance between the rights and obligations of the parties. As a consequence, the unfair clauses may be deemed unwritten and therefore unenforceable. If the unenforceable clause is essential, then the IT service agreement as a whole may also be unenforceable.

Liability of the Service Provider

One of the main challenges in IT services agreements is to assess the existence and the extent of the provider's liability, as providers usually

tend to impose an exclusion or a limitation of liability clause. It is thus strongly recommended to clearly indicate whether providers are subject to a performance obligation (where the provider must reach a specific result) or an obligation of best efforts.

Providers may try to exclude or limit their liability by excluding indirect damages; such exclusion is authorised under French law, although providers will try to have a broad definition of "indirect damages" to include loss of data, loss of clients, breach of data privacy, etc. Unless these liability clauses deny the essential obligation of the provider – in which case they are prohibited – liability clauses (including the amount of the liability cap, if any) are often one of the key topics of the parties' service agreement negotiations.

However, because the parties may not have the same bargaining power, especially when customers are consumers or businesses with no IT expertise or when the product is complex or customised, those clauses may be more easily challenged and unenforceable. In order to better identify providers' contractual breach, customers would be advised to detail their needs as much as possible and to set out clear specifications in terms of performance (eg, through a service level agreement) or in terms of timeframe (eg, including provision for liquidated damages).

Service Level

In order to assess whether the service provider has complied with its obligations under IT service agreements, in particular its obligation to reach a specific result, the parties usually agree on service levels and a quality assurance plan. This implies the definition of key performance indicators and the payment of penalties in the event those indicators are not met.

Changes in the Economic Situation of the Parties

The COVID-19 pandemic has recently illustrated that, in some cases, the parties' economic situations may change and that IT service agreements may need to be adjusted accordingly. Article 1195 of the Civil Code allows a party to any agreement, if a change in circumstances – unforeseeable at the time of the conclusion of the agreement – makes performance excessively onerous for such party that had not agreed to assume the risk, to request a renegotiation of the agreement with the other party. Note, however, that parties may agree not to apply Article 1195.

Specific IT Service Agreements

With respect to software licence agreements, one of the main issues is whether the licensee is allowed to repair or correct any bug – in other words, whether the licensee may perform, or have performed by a third party, the maintenance of the software, or if such maintenance must/can only be carried out by the licensor. French law allows software editors to retain the right to correct bugs, which creates serious difficulties for licensees that have not entered into a maintenance agreement with the editor/licensor.

In the event a customer enters into a licence agreement and a maintenance agreement (and/or any other IT service agreements) with the same service provider, those agreements may or may not be interdependent. It is therefore highly recommended to provide contractually whether the expiration or early termination of one IT service agreement automatically puts an end to the other IT service agreements. Once IT service agreements are terminated or expired, customers will often enter into new IT service agreements with third parties, in which case it is key to ensure that a reversibility clause will allow

customers to benefit from a smooth transition from a service provider to another.

Concerning bug fixing by decompilation, the Court of Justice of the European Union recently held, concerning a licensee who had decompiled a part of a software in order to disable a defective function, that such decompilation was lawful. The Court also stated that decompilation must be subject to a certain number of conditions (necessity, absence of specific contractual provisions, decompilation for the sole purpose of error correction). It therefore seems appropriate to regulate decompilation for the purpose of error correction through the contract, as well as through the maintenance terms implemented by the editor (CJEU, 6 October 2021, C-13/20).

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Electronic Signatures

Electronic signatures are governed by the EU regulation on electronic identification and trust services for electronic transactions of 2014 (eIDAS Regulation) and the French Civil Code.

Three categories of electronic signatures exist pursuant to the eIDAS Regulation. Advanced electronic signatures are the electronic signatures that meet the requirements set out in Article 26 of the eIDAS Regulation. Qualified electronic signatures are advanced electronic signatures that are created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures. Simple electronic signatures are electronic signatures that are neither qualified nor advanced.

Article 25(1) of the eIDAS Regulation specifies that electronic signatures shall not be denied legal effect and admissibility as evidence in legal proceedings solely due to their electronic form or because they do not meet the requirements for qualified electronic signatures (non-discrimination principle). Article 25(2) of the eIDAS Regulation indicates that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature (functional equivalence principle).

Article 1367 of the French Civil Code indicates that an electronic signature must use a reliable identification process guaranteeing its link with the document to which it is attached. Article 1 of the Decree no 2017-1416 of 28 September 2017 further specifies that qualified electronic signatures under the eIDAS Regulation are presumed to be reliable.

Further guidance on electronic signatures is available on the website of the French National Cybersecurity Agency (*Agence nationale de la sécurité des systèmes d'information* or ANSSI).

Electronic Identification

Article L 102 of the French Postal and Electronic Communications Code establishes the framework for electronic identification to online services in France as well as the presumption of reliability of electronic means of identification and the procedures for their certification.

The security requirements applicable to these electronic means of identification are based on the provisions of the eIDAS Regulation and the associated Implementing Regulation no 2015/1502. Decree no 2022-1004 of 15 July 2022 sets out the conditions for the certification by ANSSI of electronic identification means as well as the specifications for establishing the presumption of reliability of these means.

Further guidance on electronic identification is available on the ANSSI website.

White & Case LLP has 44 offices across 30 countries, making it a truly global law firm, uniquely positioned to help clients achieve their ambitions in today's G20 world. Not only is White & Case a pioneering international law firm, it is also one of the oldest US/UK law firms in France (opened in 1926), with a history of excellence. The Paris office has 180 lawyers, including 47 partners, who work with some of the world's most respected banks and businesses, as well as start-up visionaries, governments

and state-owned entities. Its TMT practice is made up of a large group of dedicated lawyers across numerous practices. The practice has deep experience with a wide range of technologies in areas that include both hardware and software across a variety of applications, uses and deployment, such as data centres, analytics, communication infrastructure, on-premises and SaaS, embedded technologies, internet of things, security, privacy and data protection, semiconductors and more.

Authors



Bertrand Liard heads the intellectual property and information technology practice of White & Case in Paris, offering services in both contentious and non-

contentious domains. Bertrand advises clients on use and development of their IP (licences in and out, R&D agreements), IP enforcement (infringement and combatting piracy), IT and the internet, particularly in sourcing and outsourcing transactions and internet litigation, as well as on complex contractual arrangements, such as strategic alliances and partnerships. Bertrand is a frequent speaker, author and commentator on privacy, technology and fintech issues. He is a member of the Strategic Orientation Committee of CashWay and of the European Outsourcing Association.



Clara Hainsdorf is a partner in the intellectual property and information technology department of White & Case in Paris. She has a thorough knowledge of legal issues

related to information and communication technologies (ICT) – technology licences, e-commerce and social media – as well as in relation to complex industrial and commercial contracts. Clara has extensive experience in the field of privacy and data protection, especially in litigation and international contexts. She advises clients notably in relation to international data transfers, discovery and investigation procedures, as well as compliance with the GDPR. Clara is a frequent speaker and author on privacy and cybersecurity.



Saam Golshani is a partner in the EMEA private equity team of White & Case's global mergers and acquisitions practice. He has more than 20 years' experience representing clients

in all manner of M&A, private equity and restructuring transactions in all industries, notably in the tech sector. Saam's reputation is based on a record of accomplishment and he is distinguished as a key expert in the technology sector. Saam is a frequent speaker, author and commentator on private equity and restructuring issues. He is a member of the Iranian/French lawyers association.



Guillaume Vitrich is a partner in the EMEA private equity team of White & Case's global mergers and acquisitions practice. Well known as a leading corporate practitioner in the French

market, Guillaume's practice covers a wide range of both domestic and international private equity, corporate and M&A transactions, notably across Europe and Africa in the digital and tech sectors. An innovative lawyer with an ability to lead pioneering work on behalf of his clients, Guillaume has developed a reputation for – and a strong expertise in – venture capital-related matters, advising venture capital funds, large tech companies, and start-ups.

White & Case LLP

19, place Vendôme
75001
Paris
France

Tel: +33 1 55 04 15 15
Fax: +33 1 55 04 15 16
Email: chainsdorf@whitecase.com
Web: www.whitecase.com

WHITE & CASE

Law and Practice

Contributed by:

Christian Schröder and Tobias Lantwin

Orrick, Herrington & Sutcliffe see p.179



Contents

1. Metaverse	p.169
1.1 Laws and Regulations	p.169
2. Digital Economy	p.170
2.1 Key Challenges	p.170
3. Cloud and Edge Computing	p.171
3.1 Highly Regulated Industries and Data Protection	p.171
4. Artificial Intelligence and Big Data	p.172
4.1 Liability, Data Protection, IP and Fundamental Rights	p.172
5. Internet of Things	p.174
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection	p.174
6. Audio-Visual Media Services	p.175
6.1 Requirements and Authorisation Procedures	p.175
7. Telecommunications	p.176
7.1 Scope of Regulation and Pre-marketing Requirements	p.176
8. Challenges with Technology Agreements	p.177
8.1 Legal Framework Challenges	p.177
9. Trust Services and Digital Entities	p.178
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes	p.178

1. Metaverse

1.1 Laws and Regulations

Germany does not yet have any regulations specifically targeting the metaverse. There have been expert hearings before the parliamentary committee for digitalisation of the German Bundestag on opportunities and risks of the metaverse and other web3.0 concepts in December 2022 that have not yet resulted in any legislative initiatives. As an EU member state, Germany will be bound by any future legislation by the European Union that may specifically target the metaverse or other web3.0 applications. The legal landscape surrounding the metaverse can be expected to be constantly evolving over the coming months and years.

However, existing laws and regulations in Germany may already apply to legal challenges that the metaverse poses. In this regard, a briefing of June 2022 by the European Parliament has identified several risks and policy implications in connection with the metaverse, such as data protection, cybersecurity, competition and liability.

Data Privacy

Given the sheer amount of personal data that is processed by a variety of actors in connection with the provision of metaverse-related services, establishing and maintaining sufficient data privacy and cybersecurity will be particularly challenging. To this end, the processing of personal data in Germany is governed by the General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG).

- Depending on the specific context in which the metaverse is used, there may be specific laws that apply, such as:

- (a) Section 26 of the BDSG, which covers the processing of personal data of employees;
- (b) Article 9 of the GDPR, which provides safeguards for the processing of sensitive data; and/or
- (c) Article 22 of the GDPR, which regulates profiling and automated decision-marking.
- The safeguards in place for sensitive data are particularly relevant, as many use cases of the metaverse involve the processing of large amounts of biometric data, as well as data on the emotional and physiological responses of natural persons.
- Under the GDPR, minors enjoy special protection and can give valid consent only from the age of 16 years.
- Allocating responsibilities in certain processing operations relating to the metaverse presents another key challenge as there is often a multitude of actors (including controllers and processors) involved in the creation and provision of virtual realities. Not only does this further complicate the obtaining of valid consent, but it could also potentially impede the enforcement of data subject rights as well.

Cybersecurity

With regard to cybersecurity – apart from the requirement to implement sufficient technical and organisational measures to ensure the security of processing under the GDPR – specific rules under the NIS2 Directive of December 2022 covering critical infrastructures will have to be transposed into national law by the end of 2024. These rules target many different sectors, among them cloud computing service providers and other digital infrastructure providers, but also digital providers, such as search engines and social networking sites. These could poten-

tially encompass providers of metaverse-related services.

Intellectual Property

Finally, the metaverse also poses challenges to the protection of intellectual property. The unauthorised use of registered trade marks in the metaverse is on the rise, as are copyright violations through other web3.0 concepts, such as non-fungible tokens (NFTs). Additionally, more and more trade marks are filed that refer to the metaverse or NFTs. Therefore, the European Intellectual Property Office (EUIPO) has issued guidance on virtual goods, NFTs and the metaverse in June 2022 for classification purposes.

2. Digital Economy

2.1 Key Challenges

In Germany, the digital economy is not governed by a single law, but rather by a multitude of different provisions scattered across several national and Union laws, some of which pose risks of significant monetary sanctions in case of non-compliance.

E-Commerce

One of the legal foundations for the digital economy in Germany is formed by the e-Commerce Directive 2000/31/EC, transposed into German law in the German Telemedia Act (*Telemediengesetz*, TMG). It regulates the respective liabilities of online intermediaries (such as access and host providers, as well as other services including caching and mere conduit) and defines content moderation obligations. Most notably, it stipulates a “notice and takedown” procedure for host providers in case they are made aware of illegal content on their services.

Digital Services Act

Against the backdrop of existing regulations in the German Telemedia Act and other, sector-specific regulations on the moderation of certain kinds of contents in EU law (such as the Digital Single Market (DSM) Directive on copyright, the Audiovisual Media Services (AVMS) Directive, the Regulation on Terrorist Content Online (TCO), etc) and national law (such as the NetzDG (a law stipulating content moderation obligations) and specific youth media protection acts, etc), the Digital Services Act (DSA) was introduced by the EU in 2022. It provides for a common set of rules on the obligations of intermediaries, including transparency reporting and content moderation obligations regarding illegal contents (such as hate speech) and a ban on certain types of targeted advertising.

Very large online platforms (VLOPs) and very large only search engines (VLOSEs) are subjected to stricter rules and are required to meet additional risk management, data sharing and auditing obligations. The liability concept introduced by the e-Commerce Directive and currently in place in the TMG remains largely untouched; it is expected that the corresponding provisions in the TMG will soon be repealed. The DSA is generally directly applicable from 17 February 2024. First notification requirements have already applied since 17 February 2023.

Digital Markets Act

Another “centrepiece” of the EU’s digital strategy is the Digital Markets Act (DMA) which was introduced alongside the DSA. It aims at regulating large online platforms that act as “gatekeepers” to ensure free and fair competition across the EU. It limits large online platforms’ abilities to impose unfair terms and conditions on competitors and consumers. Companies with a strong economic position that are active in multiple

EU member states with a strong intermediation position between users and businesses will have to comply with a broad set of rules, among which are obligations to allow third parties to interoperate with the company's services and to access data generated on these platforms. Additionally, these "gatekeepers" are prohibited from treating their own services more favourably in rankings as compared to other services or preventing their customers from linking up to other businesses outside of their platform. The DMA is directly applicable in all EU member states from 2 May 2023.

Codes of Conduct

Finally, there are Codes of Conduct in Germany that have been published by the German Association for the Digital Economy (*Bundesverband Digitale Wirtschaft*) on a variety of areas, such as affiliate and content marketing, search engine advertising (SEA) or search engine optimisation (SEO).

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Cloud and edge computing are not regulated as such, but these technologies are affected by several different laws in Germany that concern data protection, cybersecurity and highly-regulated industries.

Data Privacy

As far as the processing of personal data is concerned, the General Data Protection Regulation (GDPR) applies. In this regard, the transfer of personal data to third countries regularly raises practical issues. Data transfers are governed by Chapter V of the GDPR and are subject to specific restrictions. The use of US cloud computing

services is particularly challenging, specifically since the Schrems II decision by the European Court of Justice of 16 July 2020, which introduced extensive transfer impact assessment requirements to be met when exporting data to third countries.

Additionally, the use of processors, such as cloud service providers, requires the conclusion of a data processing agreement (DPA) which must meet certain substantive requirements. This often proves difficult when large service providers are involved as these processors regularly impose their own conditions that do not necessarily align with the requirements set out in Article 28 GDPR.

NIS and NIS2 Directives

Both the NIS and NIS2 Directives (Directives (EU) 2016/1148 and (EU) 2022/2555) specifically target cloud computing services and impose on them comprehensive cybersecurity obligations, such as the implementation of appropriate technical and organisational measures to tackle risks and incident reporting obligations. The NIS Directive has been transposed into German national law in the IT Security Act (*IT-Sicherheitsgesetz*) that amended several laws in Germany. The NIS2 Directive will have to be transposed into national law by the end of 2024.

Regulated Industries and Guidance by Supervisory Authorities

In Germany, certain sector-specific restrictions are applicable for highly-regulated industries (such as insurance and banking) which limit outsourcing via cloud services. For example, the outsourcing of activities and processes are subject to restrictions in Section 32 of the Insurance Supervision Act (*Versicherungsaufsichtsgesetz*, VAG), Section 5(3) of the Stock Exchange Act (*Börsengesetz*, BörsG), Section 80(6) of the

Securities Trading Act (*Wertpapierhandelsgesetz*, WpHG) and Section 25b of the Banking Act (*Kreditwesengesetz*, KWG).

In this regard, several German supervisory authorities have issued guidance on cloud services and outsourcing, such as the independent conference of the German data protection supervisory authorities (*Datenschutzkonferenz, Orientierungshilfe – Cloud Computing*, 9 October 2014) or the Federal Financial Supervisory Authority (BaFin, *Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter*, November 2018).

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

The legal landscape surrounding artificial intelligence is constantly evolving. While Germany still does not have specific legislation regulating AI, there are legislative proposals on an EU level and discussions among legal scholars concerning certain AI-related issues.

AI Act

Aiming to provide for harmonised rules on artificial intelligence, the EU is in the late stages of enacting an AI Act, the proposal of which had been published by the Commission as early as 2021. Following a risk-based approach, the proposed AI Act envisages a gradual regulatory framework which subjects different AI systems to different requirements, depending on the specific risks associated with these systems.

While some very high-risk AI systems are outright banned (such as AI systems employing subliminal techniques beyond a person's con-

sciousness, social scoring systems for general purposes, real-time remote biometric identification systems in publicly accessible places for certain law enforcement purposes), other AI systems are generally permitted, yet placed under certain rules.

So called "high-risk AI systems" (such as AI systems intended to be used as a safety component of a product, AI systems for purposes of biometric identification of natural persons, education, employment, law enforcement, etc). Under the proposed AI Act, high-risk AI systems may only be trained with data where data quality requirements are met. In addition, specific record-keeping, transparency, human oversight, and conformity assessment requirements apply.

For certain lower than high-risk AI systems (such as emotion recognition systems, biometric categorisation systems, or deepfakes), transparency obligations apply that shall ensure that natural persons are informed that they are interacting with an AI system.

For low-risk AI systems, the AI Act encourages the development of, and voluntary adherence to, specific codes of conduct.

Data Privacy

Training artificial intelligence (for example, through machine learning algorithms) often involves the processing of large amounts of data. These sets of training data often involve both personal and non-personal data. Where personal data is concerned, the processing of such data must be based on a lawful basis and the processing must be compatible with the purposes for which the data has been collected. Moreover, the processing for training purposes will regularly require the use of anonymised data. As it constitutes a processing of personal data

as well, the anonymisation of personal data also requires a lawful basis and that the anonymisation for training purposes is compatible with the purposes for which the data was collected. In many cases, a data protection impact assessment (DPIA) will have to be conducted. As far as non-personal data is involved, Regulation (EU) 2018/1807 applies.

The independent conference of the German data protection supervisory authorities (*Datenschutzkonferenz*, DSK) has published a policy paper on artificial intelligence on 3 April 2019 (DSK, *Hambacher Erklärung zur Künstlichen Intelligenz*, 3 April 2019), outlining seven guiding principles that should govern the development and utilisation of AI:

- AI must not turn humans into objects;
- AI may only be used for purposes legitimised by the constitution and must not override the purpose limitation requirement;
- AI must be transparent, comprehensible, and explainable;
- AI must avoid discrimination;
- the principle of data minimisation applies to AI;
- AI demands responsibility by a controller; and
- AI requires technical and organisational standards.

Liability for AI Malfunctions

With regard to AI malfunctions, there are debates among German legal scholars on questions of liability. While some argue that already-existing contract or tort laws should be applied to address the infliction of damages by an AI, other voices in academia and practice propose that such damages should be covered by specific insurance solutions. Additionally, there are proposals that call for strict liability of AI manufacturers and/or operators of AI. Other solutions

involve the creation of an own legal personality in AI systems (so-called “e-persons”); however, apparently this proposal has not been able to attract broad support.

On an EU level, in September 2022 the Commission adopted two proposals to adapt and modernise liability rules to meet current technical and market developments. One of the policy proposals concerns the proposal for an AI Liability Directive which aims at fostering the enforcement of claims by individuals who have been harmed by AI products through alleviating the victims’ burden of proof and facilitating access to relevant evidence.

Intellectual Property Issues

Under German copyright law (*Urheberrechtsgesetz*, *UrhG*), big data collections are not protected as such. The creation of a big data collection merely involves the systematic and indiscriminate collecting of data points which does not constitute an “author’s own intellectual creation” as is required under Section 4(2) of the *UrhG* to warrant protection as a database work. A protection of the collection as a right of the maker of a database pursuant to Section 87a et seq of the *UrhG* can generally seem conceivable under certain circumstances, if the maker of the database has made significant investments in obtaining, verifying and/or presenting the data and if they have arranged them systematically or methodically.

Finally, big data collections can be granted a *sui generis* protection as a trade secret under the German Trade Secrets Act.

Further, the creation of new text and art by AI machines such as ChatGPT will pose significant challenges to copyrights as the AI driven machines create text and/or art based on smaller

or larger fragments of works that enjoy copyright protection. Apart from the question as to whether these fragments still enjoy copyright protection, it is entirely unclear how such copyrights could be enforced. Likely, the new AI creations will not enjoy their own copyright protection.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There is no law in Germany that specifically governs the Internet of Things (IoT). The notion of IoT usually involves devices that monitor or communicate with smart cars, smart homes, work environments or physical activities. In its Opinion 8/2014 on recent developments on the IoT of 16 September 2014, the EU's Article 29 Working Party defined the concept of the "Internet of Things" as to refer to an "infrastructure in which billions of sensors in common, everyday devices (...) are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities".

Although there is no specific legislation targeting the IoT, several laws governing the processing of personal data necessarily involved with using IoT devices apply. Among these are:

- the General Data Protection Regulation (GDPR) and the German Federal Data Protection Act (*Bundesdatenschutzgesetz*, BDSG); and
- the ePrivacy Directive 2002/58/EC, which has been implemented in German law in the Federal Telecommunications Telemedia Data Protection Act (*Telekommunikation-Telemedien-Datenschutz-Gesetz*, TTDSG).

Data Privacy

Privacy-related issues connected to the IoT are manifold. Several of these issues have been identified by the Article 29 WP in its Opinion 8/2014 on recent developments on the IoT.

- There is a general lack of control, depending on the transparency with which the IoT devices collect data. This may result in excessive self-exposure beyond a data subject's control.
- This lack of information may lead to data subjects not being aware that their IoT devices are processing data which, in turn, presents a significant burden to obtaining valid consent. It should be noted that the processing of health or other sensitive data is subject to additional protection under Article 9 GDPR.
- Due to the large amounts of data created and collected by IoT devices, there is the inherent risk that inferences are drawn from data processed for purposes other than those for which this data had originally been processed (eg, to allow conclusions as to the health or habits of users). It is thus important, as Article 29 WP notes, that personal data is only processed for purposes compatible with the purposes for which it was collected and that these purposes are known to the data subject.
- The fact that conclusions of an individual's habits, behaviours and preferences may be inferred from the data collected by IoT devices may significantly change a data subject's behaviour.
- IoT has the potential to put a severe strain on the ability to remain anonymous given that, for example, wearable devices in close proximity to data subjects can reveal a range of other identifiers, such as MAC addresses, which can be used for purposes such as location tracking, fingerprinting or analysis

of movement patterns of individuals or even crowds of people.

To address these privacy issues, developers of IoT systems must, in particular:

- inform data subjects of the specific purposes for which their data is collected;
- ensure that data subjects give valid and informed consent;
- conduct a data protection impact assessment (where sensitive categories of data is processed);
- limit a device's data collection to conform with the GDPR's privacy by design and by default principles;
- implement appropriate technical and organisational measures to address cybersecurity risks.

Cybersecurity

IoT devices can raise cybersecurity concerns, some of which had already been identified by the Article 29 WP's Opinion 8/2014. Vulnerabilities of IoT devices can be exploited and misused for purposes of surveillance and data theft or to attack critical infrastructures. Some vulnerabilities can also be linked to a lack of regular security updates or an appropriate end-to-end-encryption.

Some of these risks will be addressed by the Cyber Resilience Act (CRA) proposed in September 2022 by the European Union which seeks to close regulatory gaps with regard to IoT products. The main objectives of this initiative are:

- to foster the development of secure products with fewer security vulnerabilities;

- to ensure that manufacturers and developers are appropriately addressing a digital product's security throughout its lifecycle;
- to enhance the transparency of a product's security properties; and
- to enable consumers to make educated decisions as to their choice of digital products.

For these purposes, a coherent cybersecurity framework shall be established.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Audio-Visual Media Services

Due to Germany's federal structure, audio-visual media services are governed at both the federal and state levels in Germany by the State Media Treaty (*Medienstaatsvertrag*, MStV) and State media laws. Under these laws, broadcasting requires permission by the respective media authorities. Broadcasting is defined as any linear provision and distribution of moving images and/or sound for simultaneous reception by the general public along a broadcasting schedule using electromagnetic transmission paths (be it, for instance, via satellite, cable, terrestrial or the internet). Audio-visual media provided "on demand" (eg, on video sharing platforms) is regularly exempt from this definition.

However, livestream content on streaming platforms can often constitute "broadcasting" within the meaning of the regulations mentioned above, especially in cases that it follows along a broadcasting schedule. The fees for the authorisation procedure can cost between EUR1,000-2,500 or, in some cases, up to EUR 10,000, depending on the administrative effort necessary for the

authorities and on the economic value of the company requesting an authorisation.

Video-Sharing Platforms

Video-sharing platform services are also targeted specifically under a variety of German laws. Most importantly, the latest review to the Audio-Visual Media Services Directive (EU) 2018/1808 of 14 November 2018 has brought many changes to several media laws in Germany over the past few years. The legal situation in Germany for video-sharing platforms tends to be rather complex, as the relevant provisions are scattered across many different laws.

The obligations for video-sharing platform services are mainly laid out in:

- Section 10a, 10b of the Telemedia Act (*Telemediengesetz*, TMG);
- Section 97 et seq of the State Media Treaty (*Medienstaatsvertrag*, MStV); and
- Section 5a, 5b, 14 of the Youth Media Protection State Treaty (*Jugendmedienschutz-Staatsvertrag*, JMStV).

The obligations stipulated in the provisions stated above mainly concern content moderation obligations to protect minors and the general public from hate speech, the incitement of violence and other hateful content, as well as criminal and child pornographic content.

In addition, other legislation that does not specifically target video-sharing platform services only but more generally stipulates obligations for the moderation of harmful or illegal content for many different kinds of platform or host services may apply as well, namely:

- several content moderation obligations under the Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*, NetzDG);
- Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (TCO-Regulation);
- provisions based on the Directive (EU) 2019/790 on Copyright in the Digital Single Market (DSM Directive), transposed into German law in the Copyright Service Provider Act (*Urheberrechts-Diensteanbieter-Gesetz*, UrhDaG); and
- in the near future, several obligations under the Digital Services Act (DSA) targeting online platforms and/or very large online platforms (VLOPs).

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Telecommunications Regulation

In Germany, telecommunications are regulated in the Telecommunications Act (*Telekommunikationsgesetz*, TKG) which has transposed rules laid out in the European Electronic Communications Code (EECC – Directive (EU) 2018/1972) into German law. To promote competition in the telecommunications sector and efficient telecommunications infrastructures, the TKG follows a technology-neutral approach to ensure that adequate and sufficient services can be provided across Germany. Telecommunications services regulated under the TKG are:

- internet access services;
- interpersonal telecommunications services; and
- services which consist wholly or mainly in the transmission of signals, such as transmission

services used for machine-to-machine communications and for broadcasting.

Interpersonal telecommunications services (also called “OTT-I” services, ie, over-the-top-I services, such as instant messaging, web mail services, internet (video) phone services, etc) are services usually provided for remuneration that enable a direct interpersonal and interactive exchange of information over telecommunications networks between a finite number of persons, whereby services which enable interpersonal and interactive telecommunications merely as a subsidiary ancillary function inextricably linked to another service are not included. OTT-I services are partially governed by the TKG, whereas OTT-II services (eg, blogs, streaming, websites, etc) are not covered by the TKG.

Pre-marketing Requirements

The Telecommunications Act regulates both communications networks and communications services. Under the EECC, the provision of such networks or services is subject to a “general authorisation” (Article 12, EECC) and thus does not require a grant of a licence or specific authorisation. However, any intended commencement, change or termination of such services must be notified to the Federal Network Agency (*Bundesnetzagentur*, BNetzA) without undue delay. The same applies for any changes to an operator’s or service provider’s name/company name, legal structure or address.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Technology agreements (ie, agreements relating, inter alia, to the development, sale, transfer, provision and maintenance of software, hardware or

cloud solutions, etc) are not specifically regulated as such under German contract law. Instead, general contract law and the law of general terms and conditions (*Allgemeine Geschäftsbedingungen*, AGB) of the German Civil Code (*Bürgerliches Gesetzbuch*, BGB) apply. Depending on the subject of the technology contract, the rules of different contract types are applicable, such as sales contracts, service contracts, rental contracts or work contracts. In addition, antitrust rules may apply which are not covered by this analysis.

Exact Specification of the Services and Products

Since the different contract types entail different rights and obligations, especially with regard to the provision of the technology subject to the contract as well as with regard to warranties and liabilities for defects, a precise and detailed description of the services/products is necessary to clearly define the scope and the nature of the respective technology agreement. Under all circumstances, parties must make sure not to confuse different contractual elements or choose descriptions that refer to a type of contract that is not appropriate for the service or product provided and which establishes rights and obligations that are inappropriate or too far-reaching. This can often occur whenever pre-formulated standard clauses are used that are not specifically adapted to the concrete service or product. For example, Software-as-a-Service (SaaS) or software rental contracts involve different service descriptions that result in different rights and obligations for both parties.

Licensing and Liability

Software licensing can cause difficulties, especially when open-source software (OSS) is involved. Many OSS licences require the licensee, if they publish modifications based on the

OSS, to make the source code available and publish it under the same licence terms as the original OSS licence (so-called “Copyleft” principle). This can lead to problems where open-source software code is combined with other open-source or proprietary software code under different, and possibly conflicting, licence terms. Here, careful consideration is necessary to avoid violating any licensing conditions.

Finally, in cases where a group licence is to be granted, attention must be given to the means by which it can be granted in a legally secure manner. Notably, in general, no additional licences can be granted on the basis of a simple licence.

Wherever general terms and conditions are used, some restrictions can also stem from German laws specifically targeting general terms and conditions. Extensive exemptions and limitations of liability are often deemed invalid by German courts, as are comprehensive disclaimers of warranties.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

German law sets out specific rules on trust services in the Trust Services Act (*Vertrauensdienstegesetz*, VDG) and in the Trust Services Ordinance (*Vertrauensdiensteverordnung*). It includes various regulations on trust services, electronic signatures and seals, as well as the validation of such identification methods. These rules complement the eIDAS Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market. Formal requirements for electronic signatures are established in the German Civil Code. It regulates the cases in which a mandatory written form can be replaced by an electronic signature.

However, electronic signatures are only catching on very slowly because they require special hardware and software, an effort that many – except for individual industries – have tended to avoid up to now.

Orrick, Herrington & Sutcliffe is a modern and inclusive law firm focused on serving the Tech & Innovation, Energy & Infrastructure and Finance sectors. Based in 25+ markets globally, the firm helps its clients grow and innovate, protects them, and helps them win. Financial Times has selected Orrick as a Top 3 Most Innovative Law Firm for seven years in a row. Fortune also named the firm to the 2022 list of the 100 Best Companies to Work For for the seventh year in a row. From managing complex global compli-

ance matters and cyber incidents to responding to litigation and regulatory investigations, Orrick helps clients navigate the cybersecurity and privacy legal landscape. The firm maximises data value, addresses global privacy requirements and reduces security risk for its clients. Whether clients are managing compliance challenges, licensing their data or acquiring new companies, Orrick creates forward-thinking solutions to solve data challenges.

Authors



Christian Schröder leads Orrick's Cyber, Privacy & Data Innovation Group in Europe and closely collaborates with team members in the US, Europe, and Asia to provide support to global

clients. As a technology-focused partner, Christian advises on cybersecurity and privacy regulatory compliance, incident response, regulatory investigations and enforcement, litigation, IP licensing, and transactional matters. He helps clients consider the privacy and AI implications of new technology, supports their compliance programmes, and helps them stay ahead of enforcement trends. Christian authors the chapter on international data transfers of Germany's leading GDPR commentary Kühling/Buchner and is co-author to the Corporate Privacy Handbook Forγό/Helfrich/Schneider.



Tobias Lantwin is a scientific assistant at Orrick focusing on the intersection between IP and privacy law. Tobias is a PhD in law student at the University of Düsseldorf.

Contributed by: Christian Schröder and Tobias Lantwin, **Orrick, Herrington & Sutcliffe**

Orrick, Herrington & Sutcliffe

Heinrich-Heine-Allee 12
40213
Düsseldorf
Germany

Tel: +49 211 3678 7269
Email: cschroeder@orrick.com
Web: www.orrick.com/en/People/E/A/D/Christian-Schroeder



Trends and Developments

Contributed by:

Christian Schröder

Orrick Herrington & Sutcliffe see p.185

Data Privacy Litigation in Germany – A Growing Concern for Businesses?

While the first few years since the inception of the General Data Protection Regulation (GDPR) were marked by ever more rigid public enforcement efforts by EU member state supervisory authorities and a growing number of administrative fines of several hundred million euro, it was the last few months in particular that saw a considerable uptick in private enforcement activities across Germany. Increasingly, German courts have had to deal with claims for immaterial damages or injunctions for alleged privacy violations. Given the potential for mass enforcement of such claims by professional litigants or through representative actions, businesses in virtually all sectors thus face a growing risk of being subjected to private enforcement efforts in the field of data privacy in Germany.

Immaterial damages for GDPR violations

Claiming compensation of immaterial damages pursuant to Article 82(1) of the GDPR for privacy violations has become one of the most common private enforcement practices in Germany. Recently, these claims have begun to cover an increasingly broad variety of supposed violations and processing situations. However, given many legal uncertainties still lingering around the provision of Article 82 of the GDPR, it is still unclear as to which kinds of privacy violations are eligible for compensation and under which conditions immaterial damages may be claimed at all. Unsurprisingly, many questions surrounding Article 82 of the GDPR have already been referred to the Court of Justice of the European Union (CJEU) for a preliminary ruling.

Among the most pressing issues is the question as to whether any kind of violation can lead to a claim for compensation of immaterial damages in principle or whether there is a “de minimis” threshold that excludes minor damages or “petty” violations of GDPR provisions that do not inflict any meaningful, perceptible damage on an affected data subject. Despite numerous decisions being rendered by German courts in the interval (far more than a hundred published decisions so far), case law still does not paint a clear picture.

Referring to a “de minimis” threshold, many local, regional, higher regional and labour courts have denied claims, arguing that a merely “perceived impairment” does not amount to any immaterial damages eligible for compensation under the GDPR. However, other local, regional and labour courts have been more generous in awarding immaterial damages for a broad variety of violations. That is, in their view, since the notion of “immaterial damages” ought to be interpreted broadly so that data subjects receive “full and effective compensation”. In addition, some courts have also argued that damage amounts granted as compensation must serve a “dissuasive” effect. Notably, the German Federal Labour Court in August 2022 formed the opinion that, generally, any violation of the GDPR automatically leads to immaterial damages eligible for compensation under the GDPR.

Thus, German courts have awarded compensation for immaterial damages with damage amounts ranging from as low as EUR25 to approximately EUR5,000, for instance, for the following GDPR violations:

- delayed and incomplete data subject access request response (EUR5,000, Labour Court Düsseldorf, March 2020);
- unlawful reporting to a credit scoring agency (EUR5,000, Regional Court Mainz, November 2021);
- unlawful processing of data relating to criminal convictions (EUR5,000, Higher Regional Court Dresden, November 2021), notably, in this decision, the company director was also held personally liable;
- data breach following a cybersecurity incident (EUR2,500, Regional Court Munich I, December 2021);
- unlawful intra-group data sharing (EUR2,500, Regional Court Hamm, December 2021);
- unlawful transfer of a website visitor's personal data to a third country via the use of Google Fonts (EUR100, Regional Court Munich I, January 2022); and
- receiving of an unsolicited marketing email (EUR25, Regional Court Heidelberg, March 2022).

Given these significant differences in the severity of the privacy violations, awarding immaterial damages does not seem appropriate in each of the cases mentioned above. Indeed, there is good reason to conclude that some of these violations are so trivial that awarding any compensation does not seem warranted. Incidentally, this view is shared by Advocate General (AG) of the CJEU Campos Sánchez-Badona, who in early October 2022 provided his opinion on questions referred to the CJEU for a preliminary ruling which concerned the existence of a “de minimis” threshold and whether compensation for immaterial damages must have a dissuasive effect, among other issues.

In the opinion of October 2022, the AG concluded that not every violation of the GDPR auto-

matically leads to immaterial damages but that actual damages must have occurred. In fact, a “mere annoyance” or “upset” in connection with a privacy violation is not sufficient to constitute immaterial damages and there is no irrebuttable presumption that immaterial damages occur in every instance of a privacy violation. Finally, the compensation of immaterial damages is not intended to have a dissuasive effect as is the case for administrative fines, since the GDPR does not provide for punitive damages.

The CJEU is set to finally decide on these questions in 2023. Until then, it will remain an open question as to which direction the CJEU will steer the future of private enforcement in Germany. Should the CJEU decide in line with the AG's position, this would mean great relief for many businesses, particularly those involved in large scale data processing activities.

Current risk environment in Germany

Despite the many legal uncertainties surrounding immaterial damages, the risk environment for private enforcement in Germany has been characterised by a growing volume of claims asserted by a diverse set of actors in an ever-broader range of sectors. Areas most often in the crosshairs of privacy litigation are, notably:

- the employment context;
- data breaches and their aftermath; and, increasingly
- international transfers of personal data to third countries outside the European Union.

In many cases, privacy litigation starts with a data subject access request (DSAR). It is therefore vital to have sufficient DSAR management in place to answer requests sufficiently and in a timely manner, as even a belated or insufficient response to an access request can itself give rise

to potential claims for immaterial damages. It also makes sense to adequately identify the risk associated with each type of DSAR (eg, DSARs arising in an employment or post-breach context are often of a higher risk than are DSARs sent via a standardised template form by consumers).

Another risk for privacy litigation can stem from negative press following media reports of a data breach or of an inquiry by a supervisory authority. Such reports sometimes lead to a rising number of DSARs and, potentially, subsequent claims for immaterial damages.

Litigation risks in the employment context

As regards the employment context, companies have been witnessing a proliferation of data subject access requests during termination proceedings made with the intention to uncover and potentially threaten to litigate any GDPR violations as part of subsequent settlement negotiations. Given that some labour courts have granted immaterial damages claimed during termination proceedings, the mere threat of privacy litigation often suffices to significantly leverage the negotiation position of disgruntled former employees. This once again illustrates the importance of a co-ordinated and smooth off-boarding procedure for companies.

Litigation risks regarding international transfers

Another area that has been exposed to increased scrutiny through private enforcement activities concerns international transfers of personal data to third countries outside the European Union. Given that a general uncertainty as to the legality of international transfers is now much more the norm than the exception, since the CJEU's Schrems II decision of 16 July 2020, there is much room for error for companies – room which is readily exploited by litigious individuals and

professional litigants. Already, these claimants can rely on existing case law to support their claims since immaterial damages have been granted for unlawful transfers of personal data by German courts (for instance, Regional Court Munich I in January 2022 above).

Litigation risks regarding data breaches

Finally, a third important area giving rise to serious privacy litigation risks involves data breaches and cyber-attacks, including phishing mails, malware, DDoS, Advanced Persistent Threat (APT) and ransomware attacks. Given an ever-evolving cyber threat landscape, there is a growing risk for companies of every sector of being affected by cybercrime, service outages and data leaks, potentially affecting many data subjects at once. Not only have some courts already awarded immaterial damages to data subjects affected by data breaches (such as the Regional Court Munich I in December 2021 above), but specialised law firms have already started advertising their services specifically to individuals potentially affected by certain data breaches – most notably those that have received great media attention.

Mass litigation and representative action

Considering recent and future developments surrounding mass claims and representative actions, it is large-scale processing of personal data in particular that can increasingly prove a liability for businesses. For instance, specialised law firms have begun representing large numbers of data subjects (in the hundreds or even thousands) affected by data breaches. In addition, there are companies that provide legal assistance to affected data subjects exerting claims for immaterial damages before court.

What is more, the European Union's Representative Action Directive (EU) 2020/1828, which had to be transposed into national law by EU Member

States by December 2022, will further incentivise mass claims on behalf of consumers affected by privacy infringements. This should prove to make enforcement of damages considerably easier in cases affecting large numbers of individuals, as is often the case in employment- or consumer-related cases. Additionally, the rules provided in the Directive regarding disclosure of evidence will also facilitate private enforcement of privacy violations.

This enhanced environment for mass claims and professional litigation is also likely to make inquiries and/or imposition of fines by supervisory authorities (eg, after breaches or unlawful international transfers) increasingly dangerous starting points for follow-up litigation by entities and individuals that pursue compensation of immaterial damages. Since the Representative Action Directive also provides for actions brought by qualified entities established in other member states, this may expose businesses to even greater risk of litigation by different interest groups across the EU. In fact, there could be an increase in forum-shopping that could lead claimants to sue in jurisdictions known to award high damage amounts, should the CJEU not follow the AG and should the particularly low bar for immaterial damages set by some German courts thus finally materialise.

Warning letters and cease and desist orders

In late 2022 in particular, Germany saw a spike in abusive claims for immaterial damages exerted via warning letters against companies and individuals. Attracted by the particularly low bar for immaterial damages in Germany, lawyers have been deliberately targeting thousands of website providers using the web font service “Google Font” after a ruling by the Munich Regional Court I in early 2022 found using the service triggers data transfers to the US that the court deemed unlawful under the GDPR. Hence, a single court deci-

sion sufficed to lead lawyers to send out warning letters to a multitude of website operators with the intention of securing a settlement payment – a tactic that has already paid off given that a number of companies have already agreed to pay the proposed settlement fees for fear of litigation.

The absence of a “de minimis” threshold thus also provides for a significant incentive to file abusive claims. However, besides this, there are already new possible venues for abusive claims on the horizon: over the past few months and years, a great number of German courts have also permitted injunctions filed by data subjects against certain processing operations and practices. Perhaps not coincidentally, the Munich Regional Court I’s “Google Fonts” ruling discussed above also issued an injunction against the use of the service. It therefore seems highly likely that data subjects will increasingly assert claims for injunctive relief and, in addition, try to enforce their rights by way of interim relief. The latter, in particular, would be certain to create a whole new dynamic and speed in private enforcement developments.

Outlook

The assertion of immaterial damages claims has paved the way for ramped-up private enforcement efforts within the last two years and will likely remain one of the defining privacy topics in Germany and across Europe in 2023. With an ever-broader range of areas affected, businesses of all kinds will have to expect further increases in private enforcement activities and are well-advised to resolve any shortcomings in their privacy compliance which are particularly vulnerable to litigation. Finally, there is hope that, in the coming months, the CJEU will provide much-needed light at the end of the tunnel and put a stop to litigation practices pursuing immaterial damages in mere minor cases.

Contributed by: Christian Schröder, Orrick Herrington & Sutcliffe

Orrick Herrington & Sutcliffe is a modern and inclusive law firm focused on serving the Tech & Innovation, Energy & Infrastructure and Finance sectors. Based in 25+ markets globally, the firm helps its clients grow and innovate, protects them, and helps them win. Financial Times has selected Orrick as a Top 3 Most Innovative Law Firm for seven years in a row. Fortune also named the firm to the 2022 list of the 100 Best Companies to Work For for the seventh year in a row. From managing complex global compli-

ance matters and cyber incidents to responding to litigation and regulatory investigations, Orrick helps clients navigate the cybersecurity and privacy legal landscape. The firm maximises data value, addresses global privacy requirements and reduces security risk for its clients. Whether clients are managing compliance challenges, licensing their data or acquiring new companies, Orrick creates forward-thinking solutions to solve data challenges.

Author



Christian Schröder leads Orrick's Cyber, Privacy & Data Innovation Group in Europe and closely collaborates with team members in the US, Europe, and Asia to provide support to global

clients. As a technology-focused partner, Christian advises on cybersecurity and privacy regulatory compliance, incident response, regulatory investigations and enforcement, litigation, IP licensing, and transactional matters. He helps clients consider the privacy and AI implications of new technology, supports their compliance programmes, and helps them stay ahead of enforcement trends. Christian authors the chapter on international data transfers of Germany's leading GDPR commentary Kühling/Buchner and is co-author to the Corporate Privacy Handbook Forγό/Helfrich/Schneider.



Tobias Lantwin is a scientific assistant at Orrick focusing on the intersection between IP and privacy law. Tobias is a PhD in law student at the University of Düsseldorf.

Contributed by: Christian Schröder, **Orrick Herrington & Sutcliffe**

Orrick, Herrington & Sutcliffe LLP

Heinrich-Heine-Allee 12
40213 Düsseldorf
Germany

Tel: +49 211 3678 7269
Email: cschroeder@orrick.com
Web: www.orrick.com/en/People/E/A/D/Christian-Schroeder



Law and Practice

Contributed by:

Abhishek Malhotra, Bagmisikha Puhani, Sapna Chaurasia and Meghana Chandorkar

TMT Law Practice see p.198



Contents

1. Metaverse	p.188
1.1 <u>Laws and Regulations</u>	p.188
2. Digital Economy	p.189
2.1 <u>Key Challenges</u>	p.189
3. Cloud and Edge Computing	p.190
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.190
4. Artificial Intelligence and Big Data	p.191
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.191
5. Internet of Things	p.192
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.192
6. Audio-Visual Media Services	p.193
6.1 <u>Requirements and Authorisation Procedures</u>	p.193
7. Telecommunications	p.194
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.194
8. Challenges with Technology Agreements	p.195
8.1 <u>Legal Framework Challenges</u>	p.195
9. Trust Services and Digital Entities	p.195
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.195

1. Metaverse

1.1 Laws and Regulations

India does not have any specific law or regulation to govern any act or omission committed within the metaverse. However, any entity that extends its services across the metaverse will continue to be bound by the provisions of the Information Technology Act, 2000 (IT Act) and its rules pertaining to cybersecurity, data collection and intermediary liability. Further, the entity would be required to abide by the central bank's regulations on payment systems, know-your-customer (KYC) obligations, data localisation, and cross border financial data transfer. With the incidence of the taxation liability under the Income Tax Act, 1961, where virtual digital assets are involved in any transactions, they may be subject to appropriate taxation. Consumer protection statutes and allied guidelines, along with the penal codes, will further regulate activities in the metaverse and the host of digital services on offer. Consumer protection statutes and guidelines provide for offences related to unfair trade practices and misleading advertisements that may be implemented in the digital sphere. Further, the IT Act and the Indian Penal Code, 1860 (IPC) factor in any offences which may take place on the metaverse, owing to the immersive experience offered, in some rudimentary form. The Consumer Protection (E-Commerce) Rules, 2020, have also been notified to regulate e-commerce entities and may also extend to social media platforms.

The intellectual property regulatory framework in India does not grant software any protection in patent law, and accordingly reliance must be placed on copyright laws. Separate components of this ecosystem will have to rely upon different statutes for seeking protection of the trade marks, copyrighted works, and where there is a

hardware component, patent and design protection must also be sought, as required. Since a lot of applications will be relying upon the combination of both hardware and software solutions, it will be necessary that they are able to establish enough evidence to seek patent protection as computer-related inventions. India does not have any comprehensive legislative framework for data privacy and data protection; it relies on sectoral prescriptions from the banking, insurance, and health regulators, depending on the specific sector.

A draft data privacy and protection legislation has been issued by the appropriate Ministry for stakeholder comments, and further changes are expected to be brought in 2023. With respect to blockchain specifically, no framework has been prescribed already. However, several government agencies have issued white papers and have conveyed their intentions to rely on blockchain, decentralised ledger technology (DLT) oriented solutions for the implementation of governmental and private functions. There are telecoms regulations that have recognised DLT methods being put to use by service providers for defined purposes. It is expected that the incoming Digital India Act, which will seek to replace the IT Act, 2000, will address harms in the metaverse and provide for indicative guidance on the compliance actions to be undertaken by enterprises to offer such services in India. Considering that the metaverse may be implemented upon DLT, it is likely that future trade agreements with overseas jurisdictions may cover such instances of cross-border co-operation for grievance redressal.

2. Digital Economy

2.1 Key Challenges

The digital economy is regulated under the provisions of the IT Act and its allied rules pertaining to cybersecurity, data processing and intermediary liability. The data collection rules require entities to seek user consent before seeking sensitive personal data, and they provide for defined cybersecurity (technical and organisational standards), which must be implemented within the framework of an enterprise to ensure fair processing of information. The government has further sought to impose compliance basis the nature of intermediary function, performed by an enterprise. For instance, news publishers, social media intermediaries and gaming intermediaries (pending enforcement of the amended law) are treated differently in law, due to the difference in their outreach, objectives, and social impact, which provides for a graded approach to compliance.

Further, entities offering paid services will be required to abide by the directions issued by the banking regulator (Reserve Bank of India - RBI) on payment systems, know-your-customer obligations, data localisation, and overseas data transfer. Consumer protection statutes, and allied rules on operation of e-commerce websites, shall further regulate transactions on the internet. Entities will be required to abide by the advertising regulations prescribed under the Consumer Protection Act, 2019, and any other guidelines released by the Central Consumer Protection Authority, and the Advertising Standards Council of India. The Competition Act, 2002 and the Companies Act, 2013 will regulate the corporate structuring of entities in this space. Telecoms regulations, such as the Indian Telegraph Act, 1885 (Telegraph Act), the Wireless Telegraphy Act, 1933 (WT Act), the Telecom

Regulatory Authority of India Act, 1997 (TRAI Act) may also require compliance, depending on the mode of operation of the entity. The Telegraph Act regulates the establishment, maintenance and work of telegraphs, which enjoy a wide definition, with a scope covering every aspect of communication.

With the surge in uptake of OTT communication services, it is expected that the incoming telecommunications bill will address concerns around regulation of such services which are hitherto not under any form of regulation from a telecom perspective, akin to the European Electronic Communications Code. Additionally, there are several statutes at the pre-legislative consultation stage that relate to telecommunications services, data protection, digital services; these may be notified shortly.

The legislation pertaining to digital services, digital markets and content regulation is antiquated and in urgent need of an upgrade to bring it in line with the innovative pace of the industry, as well as the global standards for regulation. To that end, the government of India has commenced public consultations for a slew of pieces of legislation to be introduced to regulate digital services and digital markets. It is expected that the new statute will impose an array of additional compliance rules, and mandate entities to have a corporate presence in India to offer their services to Indian audience. Any business seeking to commence digital services may be required to urgently modify their front-end and backend systems, should the legislations come into force during such timeline. It is also expected that this impending legislation may also include contours around overcoming appreciable adverse effects in competition. Any such incoming statute will likely impose regulations upon gatekeeping

Contributed by: Abhishek Malhotra, Bagmisikha Puan, Sapna Chaurasia and Meghana Chandorkar,
TMT Law Practice

entities, which function as gateway to a host of services/products made available to end users.

Also, it is possible that a lot of the information which will be available in this ecosystem may qualify as trade secrets under global conventions and treaties; however, at present, there is no specific legislation in India to protect know-how, trade secrets and confidential information. In the absence of statutory protection, several judicial decisions have upheld trade secret protection on the basis of principles of equity, and often, upon a common law action of breach of confidence, which in effect amounts to a breach of contractual obligation.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

India does not have any designated laws or regulations catering to the specific regulation of cloud and edge computing, and deference is made to the existing laws governing the information technology and enabled services ecosystem. Accordingly, the industry will be regulated under the provisions of the IT Act and its allied rules. In the absence of any specific law for data privacy and protection, sectoral regulations for the protection of health information and financial information which are in furtherance of the privacy principles must be adhered to, as well as the apex court's pronouncement in the matter of Justice KS Puttaswamy (Retd) v Union of India and Ors (Puttaswamy Judgment), which held the right to privacy as a fundamental right.

Apart from this, general compliance with respect to consumer laws and compliance rules that apply to the corporate entity under the relevant business and corporate laws shall be applica-

ble. To put in other words, while there is no specific regulation of cloud computing and related services, cloud services have been specifically included as an entry under the goods and services tax regime.

The delivery of cloud services may involve a range of providers and intermediaries:

- the owner and controller of the cloud facility;
- intermediaries that connect such persons with cloud users; and
- aggregators that package and integrate several cloud services into a composite offering for cloud users.

Accordingly, enterprise must remain cognizant of any developments in the telecommunications sector, should it have a material impact on the provision of cloud services. The Telecommunications Regulatory Authority of India (TRAI) had, vide its recommendations to a published consultation paper, recommended that industry bodies for cloud services may be set up, with their specific codes of conduct and grievance redressal protocols, and be regulated under the purview of the Department of Telecommunications. TRAI has conducted several rounds of consultation to bring in a framework for the regulation of cloud computing activities.

The RBI and the insurance regulator have specific prescriptions that regulated entities must respect when they are engaging with cloud service providers. The RBI provides indicative guidance in the use of cloud computing services by regulated banking entities, and mandates that cloud service providers (CSPs) be selected on the basis of a comprehensive risk assessment exercise. The CSPs must be based in a jurisdiction where agreements executed under Indian laws are enforceable, they must have adequate

vulnerability management, and disaster recovery protocols must have been put in place by such CSP. Similar obligations have also been imposed by the insurance regulator in India to ensure that the registered entity remains accountable to the end users for any actions of the cloud service provider. The capital markets regulator, the Securities Exchange Board of India (SEBI), has proposed a cloud framework for its regulated entities, highlighting risks and control measures entities need to consider before adopting cloud-based solutions.

The proposed cloud framework has suggested nine high-level principles:

- governance, risk and compliance (GRC);
- data localisation;
- data ownership and process visibility;
- access, risk assessment and due-diligence on CSPs;
- security controls;
- legal and regulatory obligations;
- business continuity planning (BCP);
- disaster recovery and cyber-resilience; and
- vendor lock-in.

India does not have any specific regulations for processing personal information in the context of cloud computing; however, the regulations of the central bank, insurance regulator and capital markets regulator provide guidelines on cyber-security measures and disaster recovery protocols to be maintained by a regulated entity under such sectoral regulations. The sectoral regulations flow on similar lines, to ensure liability upon the entity availing such services. They provide for compliance rules to be extended to service providers by way of service level agreements.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

There are no specific pieces of legislation governing the use of artificial intelligence and big data in India; however, sectoral regulators have sought to bring in certain guidance towards the use and assessment of these items. SEBI issued a circular in Jan 2019 to Stock Brokers, Depository Participants, Recognised Stock Exchanges and Depositories and another in May 2019 to All Mutual Funds (MFs)/ Asset Management companies (AMCs)/ Trustee Companies/Board of Trustees of Mutual Funds/Association of Mutual Funds in India (AMFI) on reporting requirements for Artificial Intelligence (AI) and Machine Learning (ML) applications and systems offered and used. The reporting is aimed towards creating an inventory of AI systems in the market and establishing the basis for future policies for governance in the space.

In the digital health space, the strategy for National Digital Health Mission (NDHM), now the Ayushman Bharat Digital Mission (ABDM), identifies the need for the creation of guidance and standards to ensure the reliability of AI systems in health. The Data Empowerment and Protection Architecture (DEPA) by NITI Aayog (which is the apex public policy think tank of the government of India) presents a technical framework for people to retain control of their personal data, and the means to leverage it to avail of services and benefits. Furthermore, in anticipation of the use of AI technologies in telecommunications, the Telecommunications Engineering Centre (TEC) of India has released a draft consultation paper on the “Fairness Assessment and Rating of Artificial Intelligence Systems”, enumerating

detailed procedures for accessing and rating artificial intelligence systems for fairness.

While the aforementioned guidelines pertain to sectoral considerations, the information technology framework, the IT Act and its allied rules, shall continue to govern any activity conducted over a computer network. In order to support the research and adoption of AI technologies, the Ministry of Electronics and Information Technology (MeitY) has constituted several committees to address issues and provide recommendations for:

- the uptake of AI by big tech;
- the cybersecurity considerations; and
- leveraging such technologies to accomplish national objectives in key sectors.

The points of discussion around IP in **1.1 Laws and Regulations** remain prevalent for this purpose. Further, in line with global standards, regulators must seek to develop standards for AI assessment, based on its risk and industry applications as well as its effect on the legal rights of individuals. While the consultation paper released by the TEC is a welcome first step in this direction, there is an urgent need for a pan-Indian framework in this regard, in view of the wide application of AI in diverse sectors. Further, remediation measures for algorithmic bias violations are to be set out as well; in the absence of data privacy legislation that can regulate the manner of processing of information, AI remediation measures may be necessary to ensure that a user is not subject to an adverse impact as a result of any AI data processing in a biased manner.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There are no specific laws to regulate internet of things services in India. The Indian government had released a draft “Internet of Things Policy” in 2015, aiming to promote the creation of an IoT ecosystem and development of IoT products specific to Indian needs in areas such as agriculture, health, water quality and natural disasters. A lot of changes will also be brought in this regard by way of the incoming telecommunications legislation. The policy document is supported by provisions of the IT Act and the allied rules pertaining to cybersecurity, data collection and intermediary liability, which seek to govern activities in the digital space.

Any consumer-facing services or products will invariably fall under the consumer protection laws, and their sale over the internet will also be managed by the applicable laws for e-commerce and protection of users across the online set-up. These statutes will require compliance from most of the entities operating in this space, due to the interconnected network, which may be facilitated by internet access provided by internet service providers.

The National Telecom (NT) Cell, the government body dealing with policy and regulatory aspects related to machine-to-machine (M2M) communication, released a National Telecom M2M Roadmap in May 2015. After this release, the NT Cell formulated KYC norms for SIM-embedded M2M devices, a numbering scheme for M2M, registration of MSP (M2M service provider) and M2M pilots. The Department of Telecommunications (DoT) issued a notification on May 2018 for implementing restrictive features for SIM cards

used only for M2M communication services and related KYC instructions for issuing M2M SIM cards to organisations providing M2M communication services. The restrictive features, inter alia, include non-transferability of mobile connections, adherence to KYC norms by M2M service providers prior to SIM issuance, calls/SMS to be from a predefined set of numbers, and predefined IP addresses for data communication.

Further, the DoT released the guidelines for “Registration process of M2M service providers and WPAN/WLAN Connectivity Providers for M2M Services”, in order to address concerns regarding technology service providers (TSP), KYC, security and encryption. M2M service providers must provision resources from an authorised licensee, and details of all customers of M2M services must be made available to such authorised licensee from time to time. Further, any equipment sought to be used for M2M services must be certified by the TEC and comply with any additional instructions issued by the DoT.

In order to receive authorisation from the DoT to offer telecommunication services, entities must enter into a unified licence (UL) agreement with the DoT, which converges multiple licence terms for service providers. The licensee is also required to comply with additional standards prescribed for technology services by the TEC, under the IT Act, or by TRAI advisories. In the event that a M2M service provider engages with an authorised licensee for provision of services, obligations imposed upon the licensee flow down to the service provider contractually for their necessary adherence. The terms of the UL permit the DoT to seek details about the end users, enforce interception requests, and demand complete access to M2M equipment where necessary to counteract espionage,

subversive acts, sabotage or any other unlawful activity. The M2M service provider must further provide decryption facilities for the content on its network as and when required by the DoT or any authorised agencies. The entity that encrypts the content shall be responsible for its decryption. Similar obligations for interception may be imposed by way of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules 2009 (Decryption Rules), which permit an authorised agency of the government to intercept, monitor or decrypt information generated or transmitted in any computer resource, subject to procedural safeguards.

In addition to the foregoing, any entity that processes the personal data of end users will be required to comply with the applicable laws as discussed, and depending on the sector that the solution is aimed at, there might be additional considerations and prescriptions made under sectoral frameworks.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

The regulation of audio-visual content is dependent upon the mode of delivery of audio-visual content, whether by broadcast or internet services. Broadcasting content is regulated under:

- the Cable Television networks (Regulation) Act, 1995;
- the Cinematograph Act, 1952;
- the Sports Broadcasting Signals (Mandatory Sharing with Prasar Bharati) Act, 2007; and
- the Press Council Act, 1978, which seeks to regulate content provided by news, entertainment and sports channels.

Contributed by: Abhishek Malhotra, Bagmisikha Puhan, Sapna Chaurasia and Meghana Chandorkar,
TMT Law Practice

Further, the Cable TV Networks (Regulation) Act, 1995 and its allied rules are instrumental to the regulation of advertising content published on broadcast television as well, by way of the Advertising Code. The Ministry of Information and Broadcasting has formulated guidelines for the uplinking and downlinking of television channels, last modified in 2022. Distribution of cinematographic content is regulated under the Cinematographic Act, 1952, along with the allied rules thereunder. Advertising content must further comply with the regulations issued by the Advertising Standards Council of India (ASCI), a non-statutory body dedicated to self-regulation of the advertising industry. Apart from this, compliance with the IT Act, the Copyright Act, 1957, and provisions of the IPC is also necessary. The provision of news content is further regulated by regulations of industry bodies, such as the News Broadcasters and Digital Association, which lays down the fundamental principles to be adhered to during reporting. Content distributed over the internet must adhere to the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021), which lays down general principles for digital content made available online, and proposes a voluntary certification scheme, to examine the age-appropriateness of any content distributed over the internet. In order to provide a framework for content regulation on the internet, the IT Rules, 2021 rely upon the aforementioned statutes to devise the “dos and don’ts” for digital content. The sector is further regulated by the advisories and guidelines issued by the Ministry of Information and Broadcasting, which may pertain to advertisements made available online or via television.

Radio services are provisioned upon execution of a Grant of Permission Agreement with the Ministry, whereby compliance rules for incorporation and the content of radio channels are

provided for by the government. Radio content must further stand in compliance with any advisories issued by the Ministry of Information and Broadcasting, and they must comply with any advertising regulations in effect.

With respect to the content providers who wish to host or offer services over the internet, there is no requirement to seek a prior approval. However, they are still bound to follow the rules that may apply to them as a result of their status with respect to qualifying as an intermediary, an IT enabler/service provider, and accordingly with consumer and data protection laws.

For the purposes of starting a TV channel, the processing fee of such an application will amount to INR10,000, and the annual permission fee for the purposes of uplinking a channel will be INR200,000 per channel, and for downlinking from India the price is INR500,000 per channel. Where downlinking is for a channel based outside of India, the annual permission fees is INR1,500,000 per channel, and where there is the requirement of uplinking a foreign channel from an Indian teleport, the charge is INR200,000 per channel. A one-time registration fee for downlinking TV channels which are uplinked from other countries shall amount to INR1,000,000. There are other requirements with respect to the net-worth requirements, the amount payable as a performance bank guarantee, and security deposits, depending on the service offerings.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The telecoms laws allow for DLT solutions to be integrated into the solutions that are offered by

the approved entities under the telecom regime. However, they do not place any embargo on how and when such technology can be integrated into a solution and provide a general code of practice which is communicated to such service providers. There are prescriptions with respect to how smart contracting can be used by them for the purposes of engaging in commercial communications. The general principle that no harm must be caused to the end user on account of such technology continues to be there.

With respect to the impending telecoms legislation, there is a possibility that consideration may be made with respect to leveraging AI and big data in this sector, as per earlier consultation papers which were floated by the TRAI in this regard.

General compliance will have to be achieved with respect to how such technology will interact with conventional systems or other laws. Additionally, in case of any hardware components being required to be integrated, one has to ensure that such equipment may be brought into India without violating any trade norms or import restrictions.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

With respect to entering into a technology agreement with a local organisation, any company must ensure that in the absence of an absolute patent regime for software and data privacy legislation, there should be sufficient redressal for IP and data privacy requirements. Additionally, as technology agreements could involve flow and availability of data, an incontrovertible migration clause is in place, enabling seamless transfer of

data and information in the case of termination of services to another service provider within a defined timeline. Typically, the Service Level Agreement (SLA) contained within a contract covers uptime guarantee, remedies, warranty periods, and similar undertakings. Additionally, clauses ensuring data privacy, continued access to data, confidentiality, ownership of intellectual property, indemnity, limitation of liability, appropriate representations and warranties are few of the clauses inserted for protection of the customer's rights, as well as clearly etched out consequences of breach and termination.

Additionally, the financial sector requires that any payment and transaction information which pertains to a transaction taking place in India must be stored locally and may be accessed or processed overseas within the first 24 hours, and then that information has to cease to be available overseas. However, there is no embargo on the foreign leg of such transactions. It is in this respect that several companies who offer other services but also allow for incidental services to occur on their platform shy away from overseas transfer of data. With respect to price revision restrictions, there is no prescription in law as such, but a lot of leverage is provided to the parties to the contract in terms of their negotiating tactics.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The IT Act deals with the processes that are to be put in place for issuance of digital signature certificates (DSC), and how to deal with electronic signatures. The concept that governs this process is that any electronic signature that

Contributed by: Abhishek Malhotra, Bagmisikha Puhan, Sapna Chaurasia and Meghana Chandorkar,
TMT Law Practice

is capable of attribution and non-repudiation is valid in the eyes of law. There are certifying authorities (CAs) recognised in law by the Controller of Certifying Authorities, regulating DSCs. CAs have the authority to issue DSCs to end users and depending on the nature of services for which a DSC is sought by an end user, there are different categories of these DSCs. The CAs are to be governed by the IT (Certifying Authorities) Rules, 2000, which prescribe the framework within which they can operate. These DSCs are issued only after a rigid KYC process is undertaken by the CA, and the deployment process requires additional factor authentication and several robust measures.

In addition to this, with respect to delivery of trust services, the banking sector prescribes for certain minimum standards of compliance expected of their systems and networks. It also provides for the baseline encryption standards to be implemented by the service providers. Furthermore, the advisory that flows from the RBI and the insurance regulator goes beyond providing prescriptions for user interactions, but also require a certain level of compliance for internal systems, and the physical security controls which must be put in place for data security.

Furthermore, the banking, telecoms and health sectors also rely on the unique national identifier (AADHAAR) scheme to bring in verifiable consent schemes for the end users. As AADHAAR details can be verified by validation over a one-time password generated every time a service provider tries to access AADHAAR details, this forms one of the better trusted online resource pools for immediate authentication of a user.

Tied to this is the concept of DigiLocker, which is a service of preservation, retention of online records and delivery of such records to the end

users who are registering with this government's online repository created with the aim of ensuring that people can access, download, and validate online copies of their own official documents. DigiLocker is a platform for the issuance and verification of documents and certificates in a digital form, and these documents are legally valid documents under the IT Act and are to be treated equally to original physical documents. This account can also be linked to the AADHAAR of the individual, which is intended to become the single point of identification for an individual, mapped to their banking, telecoms, health, and other sensitive points of social and official interactions.

Similarly, the National Health Authority is also creating a framework aiming to create a unique health identifier attributable to one individual, and the users who become part of this network will be able to rely on the underlying health information exchange to access and act upon the electronic health records available within the ecosystem.

Very recently, the Ministry of Civil Aviation has also revolutionised the way paperless travel with appropriate security controls can become a reality, enabling smoother processing of passengers journey during air travel. This also allows users to validate their identity either via by AADHAAR – based e-verification, or by extracting relevant documentation from the DigiLocker account of the individual.

The apex court in the Puttaswamy judgment did eliminate the indiscriminate collection of AADHAAR details by private parties, and the court has since gone on to recognise the right to privacy of individuals as a fundamental right. The government has to be careful in processing personal information about individuals and must

Contributed by: Abhishek Malhotra, Bagmisikha Puan, Sapna Chaurasia and Meghana Chandorkar,
TMT Law Practice

always adhere to the tests of legitimacy, necessity and proportionality.

While companies are at liberty to seek cybersecurity insurance from the insurers in the country, it is not always a sine qua non for companies who are working in this dominion to seek the same from a counterpart in any IT or information technology enabled service (ITeS) commercial arrangement.

Contributed by: Abhishek Malhotra, Bagmisikha Puan, Sapna Chaurasia and Meghana Chandorkar,
TMT Law Practice

TMT Law Practice is a law firm offering a wide array of services in the technology, media and telecommunications sectors. The firm's services include practice area offerings such as IP, dispute resolution and arbitration (including white collar crime), regulatory litigation and advisory, corporate/commercial and transactional support in M&A, private equity and venture capital transactions, competition law, insolvency and bankruptcy and employment law. It also provides policy and legislative support across

industry verticals. The firm represents a broad range of clients including Fortune 500 companies, SMEs and start-ups. While the firm engages in the practice of the conventional domains of law, it is also heavily invested in the niche, emerging areas of practice including technology, space and aviation; pharma, life sciences and healthcare; data privacy and protection; sports; e-commerce and cybersecurity; IoT and AI; and fintech, healthtech and agritech.

Authors



Abhishek Malhotra is a founding partner of TMT Law Practice and member of the Bar Councils of Delhi and California. He has 25 years of experience in advising clients in the

technology, media and telecommunications sectors. His areas of expertise include intellectual property, commercial disputes resolution, and policy/regulatory advisory. As principal advisor on various policy think tanks, he is regularly invited to speak on emerging issues and regulatory changes in the TMT space, including the Telecommunications Bill, the Information Technology Rules, the Data Protection Bill, Web 3.0 policy concerns, and the Telemedicine Guidelines. He is recognised as the "go to" professional for issues across IP, broadcasting, satellite communications, online gaming and e-sports.



Bagmisikha Puan is an associate partner and has previously worked with Wipro (privacy role) to implement privacy solutions at an enterprise level. Bagmisikha

works with clients across sectors, advising them on matters related to regulatory compliance with a focus on digital health, fintech, spacetechnology, digital gaming and other new age technologies. She has worked with NITI AAYOG in creating a framework for telemedicine and the Federation of Indian Chambers of Commerce & Industry (FICCI) for at-home diagnostics, and regularly works with the Competition Commission of India (CCI), the National Association of Software and Service Companies (NASSCOM) on matters related to her practice areas.

Contributed by: Abhishek Malhotra, Bagmisikha Puan, Sapna Chaurasia and Meghana Chandorkar,
TMT Law Practice



Sapna Chaurasia is a partner at TMT Law Practice and leads the Mumbai operations of the firm. She has over 17 years of experience working with law firms and in-house. Her primary

area of expertise are IP, dispute resolution, media and entertainment, employment issues, property transactions and internal compliances by companies. Sapna works on both the litigation and non-litigation side. She regularly advises clients in the media and entertainment sector and provides end-to-end transactional support. On the litigation side, she has expertise in civil disputes including arbitration, intellectual property rights, contract laws and commercial disputes.



Meghana Chandorkar has over 13 years of experience as an IP lawyer. She has worked with the IP teams of different law firms, and as an in-house counsel, for music and media companies.

Working with law firms has helped her develop a strong legal base and working in-house has given her an insider's perspective, to understand and address business and commercial requirements and provide well-rounded advice while minimising risks. Her areas of expertise include the following: trade marks, copyright, media and entertainment, contract law, drafting, structuring, and negotiating agreements, and providing advisory pertaining to the protection and exploitation of IP rights.

TMT Law Practice

C-2/39,
Safdarjung Development Area
New Delhi
110016
India

Tel: +91 11 4168 2996; +91 22-4011 1409;
Email: varnika.malhotra@tmtlaw.co.in;
Web: www.tmtlaw.co.in



Trends and Developments

Contributed by:

Rahul Goel and Anu Monga

AnantLaw Solicitors & Advocates see p.206

Introduction

India is expected to become the fastest-growing telecoms advertisement market, with market surveys indicating an annual growth of 11% between 2020 and 2023. A recent report published by the Network Readiness Index 2022 states that India secured first rank in “AI talent concentration”, second rank in “mobile broadband internet traffic within the country” and “international internet bandwidth”, third rank in “annual investment in telecommunication services” and “domestic market size”, fourth rank in “ICT services exports”, and fifth rank in “FTTH/building internet subscriptions” and “AI scientific publications”.

In order to keep pace with the change in technology and the way business operates in present times, the government has been reviewing the laws/policies/legislation and, in certain cases, has proposed new draft bills, which eventually, if adopted, will replace the existing legislation. The government has also disbanded the Digital Communication Commission (DCC), a multi-ministry apex decision-making body overseeing all critical telecoms matters, and thereby handed over the decisions regarding budgeting to the Department of Expenditure. The aim of this move is to speed up the decision-making process and improve the ease of doing business in India.

The Ministry of Electronics and Information Technology (MeitY) (government of India) has introduced a Digital India flagship programme. The main objectives of Digital India are to:

- provide for high speed internet as a core utility for delivery of services to citizens;
- create shareable private space on a public cloud;
- create safe and secure cyberspace;
- provide for integrated services across departments or jurisdictions;
- create availability of services in real time for online and mobile platforms;
- create citizen entitlements that are portable and available on the cloud;
- digitally transform services to ease of doing business;
- promote cashless financial transactions;
- leverage geospatial information systems (GIS) for decision support systems and development;
- promote digital literacy by providing digital services in all languages; and
- create digital platforms for participative governance.

India has witnessed the 5G spectrum auction and the launch of 5G services by various telecoms operators. It is estimated that the demand of smartphones in India is likely to reach 400 million by 2026 and 80% of the devices will be connected using the 5G services.

The government also moved towards regulating the transactions relating to crypto-assets and, in the 2022 financial budget, it announced the imposition of 30% tax and 1% TDS on income derived from transactions relating to crypto-assets. The Reserve Bank of India also announced the launch of the digital rupee.

The Department of Electronics and Information Technology (DeitY) has also been tasked with developing standards for e-governance systems in India, in accordance with the policy on open standards for e-governance. This policy is followed by all e-governance programmes, including those that are government-to-government (G2G), government-to-business (G2B), and government-to-citizen (G2C).

The government has brought online gaming and e-sports under the Second Schedule of the Government of India (Allocation of Business) Rules, 1961, online gaming being under the purview of MeitY and e-sports under that of the Ministry of Youth Affairs and Sports.

In August 2022, the government also withdrew the Personal Data Protection Bill from parliament stating that a comprehensive legal framework will be introduced to regulate the online space, including separate laws on data privacy, the overall internet ecosystem, cybersecurity, telecoms regulations, and harnessing non-personal data to boost innovation in India. Subsequently, in December 2022, MeitY introduced the draft Digital Personal Data Protection Bill, 2022 (“Data Protection Bill”) and has invited feedback from the public as part of its public consultation exercise.

In addition, the Web 3.0 and the metaverse are new domains currently under discussion. The tech companies are exploring the metaverse and investors are looking to invest in it; it is believed that the new-age gaming industry will empower users as finance and gaming are two of the biggest applications in Web 3.0. The benefit is that the assets in the form of cryptos and non-fungible tokens (NFTs) earned in one game can be easily used in other games.

India is also prepared to join the global NFT revolution, while sports and entertainment NFTs will upend the Indian economy. It is only a matter of time until India sees the development of an NFT-based market for films and sports collectibles given the current trends across the world and the government’s pending legislative and regulatory framework in this area.

More industry players are becoming aware of the significance of AI, especially its capacity to foster competitive advantage and shape the future of work. The emphasis on cost savings and productivity improvements may change for India’s AI initiatives. Utilising data today plays a big role in running supply networks.

With the growing emphasis on digitisation, India will soon accept cutting-edge technology like satellite internet and data science. There is no doubt that India’s telecoms development has significantly advanced from telegraphy.

Business in India has seen several developments as a result of the tremendous growth of technology. The technology sector grew enormously in 2022 and India continued to rank second among all countries for internet subscriptions. The TMT industry as a whole, and in particular the telecoms industry, are currently experiencing managed competition, selective privatisation and slow growth.

Legal and Regulatory Developments

Technology

Online gaming made a significant leap this year. According to a survey by Statista, the market value of the gaming industry in India is nearly USD1 billion and could go up to USD3.4 billion in 2024. With Dream 11, the fantasy sports platform (OFSP), sponsoring the Indian Premier League 2020, interest in fantasy sport has sig-

nificantly grown in India. The OFSP includes not just Dream 11 but many other players, such as My 11 Circle, My Team 11 and Howzat Fantasy, that have gained prominence in recent years.

With the view to regulating the sector, the Online Gaming (Regulation) Bill, 2022 was introduced in Lok Sabha in April 2022. The aim of the Bill is to “establish an effective regime to regulate the online gaming industry, to prevent fraud and misuse, and for matters connected therewith or incidental thereto.”

Moreover, MeitY has also introduced a draft amendment to the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to online gaming and the draft proposal is open for public comment. Given the proliferation of such portals, the issue of online gaming is becoming more and more pressing. This has prompted the Indian government to take action, creating an inter-ministerial seven-member task force to study the regulation of the online gaming sector. Rummy, fantasy sports and poker have all been categorised as games of skill by several high courts in India. However, the Hon’ble Supreme Court of India’s final ruling on this complex legal issue will bring the conclusive results to the confusion.

The introduction in 2022 of the Data Protection Bill, which covers broad aspects of data protection, will give comprehensive protection to personal data. The Data Protection Bill contains provisions such as the regulation of personal data, doing away with the segregation of different types of data such as sensitive, critical and personal, along with financial penalties. The Data Protection Bill also envisages the establishment of a data protection board which will adjudicate cases relating to data breaches. Moreover, the Data Protection Bill has done away with the

provision of a data localisation requirement. In other words, the Data Protection Bill has created norms for transferring and storing data in trusted countries to ease the compliance requirements, especially for start-up companies which do not have funds to engage firms specifically for strict and complicated compliance. The Data Protection Bill is considered to be primarily based on common principles of privacy, including lawfulness, fairness and transparency, purpose limitation, data minimisation, data accuracy, storage limitation and authorised collection.

MeitY has introduced a set of directions relating to information security practices, procedure, prevention, response and reporting of cyber incidents aimed at building a safe and trusted internet, wherein organisations have to mandatorily report cyber incidents occurring within their systems or when they notice any such incident to the Computer Emergency Response Team (CERT-In).

MeitY also published the draft India Data Accessibility and Use Policy on 21 February 2022 for maximising access to and use of quality non-personal data available with the public sector, enhancing the efficiency of service delivery and other policy objectives.

India will see a rise in the utilisation of geospatial technology for digital twins as the 5G revolution begins to take shape. A more dense telecoms network with strategically and unambiguously placed towers will be necessary for 5G. As a result, better spatial analytics (driven by digital twins) will be essential for planning the deployment of 5G infrastructure. Massive amounts of data are transferred via the higher frequency bands necessary for 5G, but, because of their limited ranges, even slight obstructions might cause problems.

Furthermore, as digital twins are incorporated into IoT and metaverse technologies, narrowing the digital-human divide, India stands at the forefront of a vital technological revolution. The development of virtual towns, villages, structures and other physical infrastructure can benefit from the use of digital twin technology. In terms of technology, the combination of digital twin technology with the metaverse would be extraordinary.

As far as drone technology is concerned, in March 2022, the Chennai police arrested a man under Section 287 (negligent conduct with respect to machinery) of the Indian Penal Code and seized the drone and other equipment worth INR250,000 for illegally flying a drone near the Madras High Court. When questioned, he said that he wanted to shoot some monuments of the city for a wedding video and therefore decided to capture the Madras High Court.

Media

On the recommendation of the Ministry of Information and Broadcasting (MIB), the Telecom Regulatory Authority of India (TRAI) published a Consultation Paper on Issues Relating to Media Ownership in April 2022. In it, TRAI addressed concerns about media ownership and control, cross-media ownership, vertical integration in the industry and the current system, and solicited input from stakeholders on potential solutions.

The COVID-19 pandemic gave a massive benefit to the already-booming internet media and entertainment industry and transformed its growth trajectory from the previous year. The audience appreciated a more technologically advanced type of media that went beyond traditional media, which resulted in a widespread

use of OTT platforms and an upsurge in both viewership and watch time.

The Cable TV Networks (Amendment) Rules, 2021 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules, 2021) were challenged before the Hon'ble Supreme Court of India, which issued an order staying further proceedings before the High Courts.

Telecommunications

Following a long discussion, the government has introduced the Draft Telecommunication Bill, 2022 ("Telecom Bill"), with the aim of developing a modern and future-ready legislation, as the primary statute currently in place for telecommunications sector is the Indian Telegraph Act, 1885. The explanatory note to the Telecom Bill acknowledges this, while also setting out how the telecommunications technology has evolved over time and that the world stopped using telegraphs a decade ago. While drafting the Bill, the government examined the laws in other jurisdictions, like the UK, Japan, Singapore, Australia and European Union.

Once the sectoral watchdog, the Telecom Bill seems to limit TRAI's power to that of a mere recommendatory body as the Telecom Bill removes the current mandate that the Department of Telecommunications (DoT) has to seek TRAI's view before issuing a new licence to a service provider through an amendment in the TRAI Act.

Another policy initiative is the Production Linked Incentive (PLI), which aims to encourage domestic producers to increase their output. Such initiatives are likely going to increase operator income and, ultimately, sector revenue. The DoT has provided a list of specific telecoms

and networking products under Annexure I of the scheme, which includes the following:

- core transmission equipment;
- 4G/5G, next generation radio access network and wireless equipment;
- access and customer premises equipment (CPE), IoT access devices and other wireless equipment; and
- enterprise equipment, such as switches and routers.

The PLI provides for eligibility threshold criteria for investment in MSMEs and companies other than MSMEs. The minimum threshold of investment for an MSME is INR100 million and INR1 billion for companies other than MSMEs. Moreover, in an amendment to the guidelines dated 20 June 2022, an additional incentive of 1% over and above the applicable rates of incentive for products qualified under design-led manufacturing was provided. Incentives worth more than INR40 billion have been earmarked for the design-led manufacturing scheme of the existing PLI scheme.

The government introduced a Draft Indian Space Policy 2022 as a declaration of intent from the Indian National Space Promotion and Authorization Centre (IN-SPACe) toward non-governmental entities for increasing the involvement in the Indian space programme and for playing important roles in increasing India's market share in the global space economy. The policy will help in determining who, among many stakeholders, will be responsible for maximising the use of space assets like satellites and launch capability, and the development of new assets will be based on the verification of user entities' desires.

TRAI has also introduced a Consultation Paper on Licensing Framework and Regulatory Mech-

anism for Submarine Cable Landing in India, wherein the DoT approached TRAI to share its concern that some Indian international long-distance operators did not have any stake in the submarine cable system.

Furthermore, TRAI has introduced a consultation Paper on "Data Communication Services Between Aircraft and Ground Stations Provided by Organisations Other Than Airports Authority of India", wherein the DoT sought to consult TRAI on whether the VHF data link services to provide the Aircraft Communication Addressing and Reporting service could be beneficial to track aircraft on a real-time basis and help investigations/search and rescue operations in the unfortunate event of an aviation disaster.

Conclusion

India has witnessed massive technology advancements, innovations and an increase in focus on technologies like AI and IoT-enabled products. With the growth in 5G, AI, online gaming, Web 3.0, the metaverse and other technologies, the country is on the trail of development.

The judiciary has played a crucial role, along with policy makers, to establish the unsettled principles in law.

The government has made infrastructure sharing, automatic routes and built-in rights of way for easy access and quicker application processing available. In addition, the government plans to introduce a common entry cost under the Unified Licence.

In an era of increasing sanctions and compliance risks in supply chains, businesses are leading the charge in incorporating data analytics tools into trade compliance processes. Greater sharing of data increases cybersecurity risk exposure.

Businesses are conscious that their weakest link may be other parties with whom they do business and share data. There is a growing expectation that a technology product manufacturer will require its suppliers and logistics providers to be certified to a particular security standard, have data breach reporting obligations, and have disaster recovery and business continuity plans in place so as to lessen the impact of a cybersecurity breach.

With the proposed changes in the regulatory and policy landscape, it is expected that several issues grappling the TMT sector will be resolved and therefore help in doing business in India.

AnantLaw Solicitors & Advocates is a full-service law firm with a well-established TMT practice group that has a strong understanding of the legal and regulatory regime governing the TMT sector. It advises and represents both foreign and domestic clients, and works closely with all stakeholders on public policy issues. Members of the firm have led the TMT practices of top-tier firms in India, and have worked as

in-house counsel in some of the largest media and broadcasting companies (including online streaming companies). Members of the TMT practice group also actively practise in competition law, which provides them with a deeper understanding of the regulatory regime, especially in the rapidly evolving competition environment within the digital space.

Authors



Rahul Goel is a partner at AnantLaw whose practice focuses on competition law and TMT law. He also advises on international trade and WTO laws. Rahul has more than 20

years of professional experience in advising, assisting and representing clients in a wide variety of legal, regulatory (including licensing) and policy issues in the TMT sector. He also assists/represents clients before various authorities, including the Department of Electronics and Information Technology, the Department of Telecommunications (government of India), and the Telecom Regulatory Authority of India. Rahul regularly writes for foreign and domestic publications and is invited to speak as a guest lecturer at forums, including academic institutions.



Anu Monga is a partner at AnantLaw and has over 16 years of experience in advising clients on TMT laws competition law and international trade/WTO laws. She advises clients on

various legal regulatory issues and assists in obtaining regulatory approvals and licences from the relevant ministries/departments, such as the Department of Telecommunications (DoT) and the Ministry of Information and Broadcasting. Anu advises on privacy and data protection laws and issues relating to cloud, IoT, virtual reality and augmented reality. She works on policy-related issues with clients and government entities, and also advises on Other Service Provider (OSP) registration and related issues.

AnantLaw Solicitors & Advocates

A-2/2
Vasant Vihar
New Delhi
110057
India

Tel: +91 98 99 027 144
Fax: +98 11 26 44 74
Email: rahul.goel@anantlaw.com
Web: www.anantlaw.com



Law and Practice

Contributed by:

Carlo Impalà, Giorgia Valsecchi,
Giulia Castelli and Jun Jie Yang
Morri Rossetti e Associati see p.228



Contents

1. Metaverse	p.209
1.1 <u>Laws and Regulations</u>	p.209
2. Digital Economy	p.210
2.1 <u>Key Challenges</u>	p.210
3. Cloud and Edge Computing	p.212
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.212
4. Artificial Intelligence and Big Data	p.214
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.214
5. Internet of Things	p.217
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.217
6. Audio-Visual Media Services	p.219
6.1 <u>Requirements and Authorisation Procedures</u>	p.219
7. Telecommunications	p.221
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.221
8. Challenges with Technology Agreements	p.223
8.1 <u>Legal Framework Challenges</u>	p.223
9. Trust Services and Digital Entities	p.224
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.224

1. Metaverse

1.1 Laws and Regulations

Laws and Regulations

The metaverse can be described as an immersive and constant virtual 3D world where people interact through an avatar in order to do different activities, such as enjoy entertainment, make purchases and carry out transactions with crypto-assets.

The metaverse is not subject to specific legislation within the European and Italian legal framework.

However, in recent years the European Union (EU) has launched a regulatory revolution aimed at encouraging technological development while respecting fundamental human rights.

Key regulatory reforms that are relevant for this matter include:

- Regulation (EU) 2022/2065 (Digital Services Act – DSA);
- Regulation (EU) 2022/1925 (Digital Markets Act – DMA);
- “Proposal for a Regulation [...] laying down harmonised rules on artificial intelligence (AI) and amending certain union legislative acts”, COM (2021) 206 final (AI ACT); and
- Regulation (EU) 2016/679 (GDPR).

The expansion of the metaverse challenges the legislator with new and complex legal issues, as described below.

Data Protection

The gathering and processing of large sets of personal data in the metaverse is one of the main reasons users/avatars can have an increasingly realistic digital experience. However, it also cre-

ates considerable risks for the freedoms and rights of data subjects from a data protection point of view. In fact, the technologies driving the metaverse (eg, virtual and augmented realities, blockchains, 5G, AI, IoT, Cloud) enable the granular, real-time collection of personal data, including highly sensitive data, such as users’ physical attributes (eg, movements, including eye movements, heartbeat or brain waves) and psychological attributes (eg, behavioural reactions and emotional states of individuals triggered by different experiences therein).

From the processing of such information and of the information that the user (or their avatar) disseminates in the metaverse (such as activities performed, interests, consumption habits, and political, religious and sexual opinions eventually expressed), a hyper-individual profile of a user is drawn based on their own individual characteristics and habits. This scenario could lead to various risks, including the following.

- Deeper profiling – the collection, storage and processing of an amount of personal data bigger than ever before to allow metaverse providers to classify people in precise profiles.
- Constant monitoring – the technologies used in the metaverse (eg, wearable devices, motion sensors, microphones, heart and respiratory monitors) may lead to constant observation of every aspect of the physical lives of users, implying a constant privacy invasion and creating risks of mass surveillance, discrimination, loss of autonomy, fraud or identity theft.
- Interference of special categories of data – the functioning of metaverse platforms is based on the monitoring of special categories of personal data such as biometric data, facial expressions, eye movements and vocal

inflections. Considering the direct interaction of the users with the platforms (such as visiting a specific place or participating in a particular event), other special categories of data can also be easily gathered, such as political beliefs and sexual orientation, increasing risks for the fundamental rights and freedoms of data subjects.

Cybersecurity

Given the amount of personal data circulating in the metaverse, companies and users may face several risks related to cybersecurity. Examples of risks that could affect both companies and users include information theft (users could unknowingly share their data with hackers, thus losing control of it) and identity theft (hackers could steal and illegally use the avatar to carry out illegal activities).

On the contrary, risks related only to companies include the fear of missing out (companies might feel obliged to provide services in the metaverse in order to be considered competitive in the technological market) and the compromise of integrity, as a company might expose its data in the metaverse without considering that such data could be processed in the same way as any other public data, and thus be exposed to the risk of possible data theft.

In any case, one of the main challenges from a cybersecurity perspective is certainly the proper protection of users' biometric data processed in the metaverse. Therefore, companies should prevent any possible cyber-attack by making their security systems safe, secure and free of vulnerabilities in order to prevent damages to the companies' economy and reputation, and also to users.

Intellectual Property

The metaverse creates several issues in connection to IP rights.

One of the first issues concerns the rights to software and information technology connected to the metaverse that can be protected by copyright or by an industrial patent.

Another aspect is related to the opportunity to file an application in order to obtain IP rights in relation to classes of goods related to software, such as in the field of trade marks, with the registration under Class 9 of the Nice Classification (software).

A further issue is the infringement of IP rights in the metaverse, particularly trade marks and other distinctive signs, which include domain names and designs. Since the metaverse does not have territorial boundaries, jurisdiction can also be considered an issue here.

2. Digital Economy

2.1 Key Challenges

Laws and Regulations

The e-Commerce Directive 2000/31/EC was implemented at the national level by Italian Legislative Decree No 70/2003 and constitutes the main legal framework for the provision of digital services in the EU.

However, technologies and digital services have changed, necessitating an update of the applicable legal framework. To this end, in a document entitled "A European strategy for data", the European Commission (EC) expressed its intention to develop a legal framework aimed at regulating the data economy, in order to ensure respect for free market principles and competi-

tion in digital sectors, and to fight unfair business practices and limit the dominant position of Big Tech.

The data economy legal framework is as follows:

- the DSA, entered into force on 16 November 2022 and applicable from 17 February 2024;
- the DMA, entered into force on 1 November 2022 and applicable from 2 May 2023;
- Regulation (EU) 2022/868 (Data Governance Act – DGA), entered into force on 23 June 2022 and applicable from September 2023; and
- “Proposal for a Regulation [...] on harmonised rules on fair access to and use of data” (Data Act).

Considering that the Regulations are directly applicable to all member states, such rules will constitute the legal framework applicable at the national level as soon as they come into effect.

The DSA

The DSA applies to various online intermediaries and platforms, and complements sectoral regulations such as the Audiovisual Media Services Directive and the Copyright Directive.

It contains due diligence obligations that will apply (depending on the role, size and impact of the intermediaries and platforms on the online ecosystem) to all digital services that connect consumers to goods, services or content, and provides new procedures for the faster removal of illegal content and a comprehensive protection for users’ fundamental rights online. Concretely, the DSA provides for (inter alia):

- measures to counter illegal goods, services or content online, such as a mechanism for

users to flag such content and for platforms to co-operate with “trusted flaggers”;

- new obligations concerning the traceability of business users in online marketplaces, to help identify sellers of illegal goods;
- effective safeguards for users, including the possibility to challenge platforms’ content moderation decisions;
- a ban on certain types of targeted adverts on online platforms (when they target children or when they use special categories of personal data);
- transparency measures for online platforms; and
- obligations for very large platforms and very large online search engines to prevent the misuse of their systems by taking risk-based action and by undertaking independent audits of their risk management systems.

It is worth noting that the DSA does not define “illegal content” online, but it is based upon the concept of “what is illegal offline should also be illegal online”. In order to classify illegal content, reference should be made to other European or national legislation, such as that which considers illegal terrorist content, child pornography or illegal forms of online hate speech. However, in the absence of a common understanding of “illegal content”, the term’s vagueness and broadness may trigger over-removals of content and affect the right to users’ freedom of expression, and may also involve a cautious approach by platforms that could compromise the scope of the DSA.

The DMA

Considering that some large online platforms act as “gatekeepers” in the digital market, the DMA aims to ensure that such platforms behave online in a fair way, and to provide benefits to innovators and technology start-ups so that they

can compete in the online platform environment without having to comply with unfair terms and conditions imposed by the gatekeeper itself.

Moreover, consumers shall have more and better services to choose from, more opportunities to switch their provider, direct access to services, and fairer prices.

The DMA qualifies the “gatekeepers” by defining objective criteria that the online platform shall meet, such as the fact that a platform must have a strong economic position in the internal market and be active in multiple EU countries. Furthermore, the DMA provides “dos” and “don’ts” with which the gatekeeper must comply, as follows.

- Do:
 - (a) allow third parties to inter-operate with the gatekeeper’s own services in certain specific situations; or
 - (b) allow their business users to access the data that they generate in their use of the gatekeeper’s platform.
- Don’t:
 - (a) treat services and products offered by the gatekeeper itself more favourably in ranking than similar services or products offered by third parties on the gatekeeper’s platform; or
 - (b) track end users outside of the gatekeepers’ core platform service for the purpose of targeted advertising, without effective consent having been granted.

In the event of non-compliance with the DMA rules, the EC may issue fines or periodic penalty payments. Additional remedies may be imposed for systematic infringements of the DMA obligations by gatekeepers.

On a final note, the DGA provides procedures and structures to facilitate data sharing between companies, individuals and the public sector, while the Data Act clarifies who can create value from data and under what conditions. The DGA and the Data Act seem to represent an attempt to identify the first rules regarding the monetisation of data, which, however, should always be consistent with the principles of the GDPR, such as free and specific consent, purpose limitation and data minimisation.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Regulations

Cloud and edge computing services are not subject to specific legislation within the Italian legal framework, but rather are regulated by various different laws and regulations, based upon, inter alia, the sector involved and the legal issues considered.

Cloud-based services

In this context, cloud-based services must be provided in compliance with various European and national laws, including the following.

- GDPR and Italian Legislative Decree No 101/2018, which amended Italian Legislative Decree No 196/2003 (Privacy Code), applicable when the services entail personal data processing.
- Directive (EU) 2016/1148 on the security of networks and information systems (NIS Directive), transposed at the national level by Italian Legislative Decree No 65/2018, pursuant to which cloud services have been expressly included within the relevant scope of application and classified as “Digital Service Provid-

ers”, thereby becoming subject to the obligations set out therein. The NIS Directive was replaced by the NIS 2 Directive, which came into force on 16 January 2023.

- Italian Legislative Decree No 82/2005, which sets forth, inter alia, specific provisions and technical rules regarding the creation, reproduction, storage and transmission of digital documents that apply to public administrations, public service providers, public control companies and private individuals.

The DSA and the DMA, which are key regulations recently adopted by the EU, also provide relevant provisions concerning cloud-based services.

In addition, suppliers of cloud-based services can voluntarily adopt control measures and therefore comply with ISO certification standards (eg, ISO/IEC 17788:2014, ISO/IEC 27017:2015, ISO/IEC 27001/2017 and ISO/IEC 27001/2022).

Edge computing

There is no official definition of edge computing, but it is generally considered a subsection of cloud computing, as it is the deployment of cloud computing capabilities at the edge of the network. Edge computing is a distributed, decentralised IT architecture where computation and data storage are closer to the data source, reducing the need to process data in a remote data centre. In this case, therefore, data is processed and computed in connected objects closer to the data source and to the users, allowing for much faster operations and giving users more control over their data. Such data can be sent to a central data centre or cloud storage repository.

A hybrid infrastructure that includes edge computing could be a solution in several fields, such as big data analytics and IoT.

Cloud and Edge Computing in Specific Industries

A number of industries are also regulated by specific laws – eg, banking and insurance.

Indeed, cloud and edge computing constitute two important technology infrastructures applied and used within many sectors, and are frequently provided through outsourcing agreements.

On this point, the applicable legal framework sets forth general provisions concerning the regulation of the outsourcing of functions and outsourcing agreements, including:

- Directive (EU) 2014/65 on markets in financial instruments;
- Directive (EU) 2009/138, known as the Solvency II Directive; and
- Delegated Regulation (EU) 2015/35, known as the Solvency II Delegated Regulation.

Specific provisions are also set forth in guidelines and circulars issued by the competent authorities.

In the banking industry, reference shall be made to the “Guidelines on outsourcing arrangements” (EBA’s Guidelines) issued by the European Banking Authority (EBA) in February 2019. The EBA’s Guidelines establish measures for financial institutions’ governance frameworks and require such institutions to:

- ensure that personal data is adequately protected and kept confidential;
- execute business continuity and contingency arrangements;

- guarantee greater certainty about the conditions under which subcontracting can take place; and
- provide specific documentation concerning outsourcing arrangements (eg, an updated register of information that shall include the cloud service, the deployment models, the type of data to be processed and the locations where such data will be stored).

EBA's Guidelines were implemented by the Bank of Italy through Circular No 285/2013, which was updated in November 2022. This Circular imposes specific requirements that banks must satisfy when using a cloud service, such as the implementation of a risk-based approach with reference to the location where data is stored and processed and the security of the information.

For the insurance industry, reference shall be made to:

- “Guidelines on outsourcing to cloud service providers” issued by the European Insurance and Occupational Pensions Authority, which provide guidance to market players on the measures to be implemented whenever insurance activities are outsourced to cloud service providers and on the requirements regarding documentation and notification to the supervisory authorities; and
- the final report supplementing the provisions of the “Guidelines on outsourcing to cloud service providers”, published by the European Securities and Markets Authority (ESMA), applicable to a wide range of entities supervised by ESMA, which contain indications concerning the governance principles, documentation and mechanisms of the supervision and monitoring of cloud providers; the assessment and due diligence procedures to be followed by cloud providers;

and the minimum content of outsourcing and sub-outsourcing agreements.

Data Protection

When cloud and edge services entail the processing of personal data, the GDPR and the Privacy Code shall apply, as well as guidelines and measures adopted by the relevant authorities.

Regarding cloud computing, one of the main challenges concerns the transfer, storage and processing of data in multiple locations, and the compliance with specific security obligations. Similar arguments could be extended to edge computing where data protections issues still arise, despite the data being transferred in a safer way.

With specific regard to data transfer, the GDPR prohibits any transfer of personal data outside the EU unless appropriate safeguards are put in place, as provided in Chapter V of the GDPR, which are applicable according to a layered approach. In this context, the location of servers is important in order to comply with the rules provided by the GDPR, and controllers are required to ascertain said location.

Moreover, cloud providers may voluntarily comply with Codes of Conduct enacted by the SWIPO (Switching Cloud Providers and Porting Data). Such Codes of Conduct are considered by certain associations (eg, Gaia-X) to be the standards to follow for data portability.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Laws and Regulations

To date, there is no specific national legal framework applicable to AI and Big Data (BD) projects. However, with specific reference to AI, the EU is working on a package of measures (to date, still not applicable) to support the roll-out of AI by fostering trust, composed of:

- the AI ACT, aimed at establishing harmonised rules for the development, marketing and use of AI systems, with a risk-based approach;
- the “Proposal for a directive [...] on liability for defective products” (Product Liability Directive); and
- the “Proposal for a Directive [...] on adapting non-contractual civil liability rules to artificial intelligence” (AI Liability Directive).

The Directives complement each other and the AI ACT. More particularly, the Product Liability Directive modernises the existing EU-level strict product liability regime and will apply to claims against the manufacturer for damage caused by defective products, material losses due to loss of life, damage to health or property and data loss. It is limited to claims made by private individuals. The AI Liability Directive makes a reform of national fault-based liability regimes and will apply to claims against any person for fault that influenced the AI system which caused the damage (any type of damage covered under national law, including resulting from discrimination or breach of fundamental rights like privacy). Claims can be made by any natural or legal person.

Although the aim of the EU is to create a clear legal framework, AI and BD entail various different potential risks for individuals and, therefore, various different legal challenges are to be evaluated.

Data Protection

The successful performance of AI software depends mainly on the amount and type of BD (personal and non-personal data) collected and processed. When personal data is processed, the GDPR shall apply; when the processing involves “non-personal data”, Regulation (EU) 2018/1807 shall apply.

Although the main goal of the GDPR is to grant data subjects full control over their personal data, some activities behind AI systems (ie, BD analytics) may be in conflict with such goal. However, the increasing availability of personal data raises the possibility of carrying out different types of processing activities, some of which are not even foreseeable. This approach violates the principle of data minimisation set forth in Article 5 of the GDPR, which requires controllers to process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

The use of AI software introduces additional risks. The processing of inaccurate data may lead to a wrong decision, which could lead to social discrimination or intrusion into people’s personal lives.

Moreover, a systematic analysis of BD, through sophisticated AI software, could also lead to a profiling of data subjects that is (in most cases) not grounded on the appropriate legal basis (ie, their consent) and to discrimination against such individuals based solely on automated (and often opaque) decision-making processes,

which are – in any case – forbidden by Article 22 of the GDPR.

Although the GDPR does not directly deal with BD and AI, it sets forth general provisions aimed at addressing the potential risks arising from the unlawful processing of personal data, profiling and automated decision-making, by referring to the controller's accountability with respect to all the necessary assessments in order to consider such processing operations "privacy compliant".

AI and Liability

Existing national liability provisions are not well suited for handling claims for damages caused by AI-enabled products and services. In fault-based liability claims, the damaged party is required to identify who to sue and explain the fault, the damage and the causal link between the two in detail. When AI is involved, this might not be easy due to the specific characteristics of AI, including complexity, autonomy and opacity, which may make it difficult or prohibitively expensive for victims to meet their burden of proof.

In order to enable victims to claim compensation for damages, the AI Liability Directive – which applies to damages caused by any type of AI system (both high-risk and non-high-risk) – introduces (inter alia) the presumption of causality measure (Article 4 of the AI Liability Directive).

Considering that it can be challenging for claimants to establish a causal link between non-compliance and the output produced by the AI system or the failure of the AI system to produce an output that gave rise to the relevant damage, Article 4 provides for a targeted rebuttable presumption of causality that can be considered "the least burdensome measure" to address the need for fair compensation of the victim.

However, notwithstanding the presumption of causality (which may find application when it can be considered likely that the given fault has influenced the relevant AI system output or lack thereof, to be assessed on the basis of the overall circumstances of the case), the claimant still has to prove that the AI system (ie, its output or failure to produce one) gave rise to the damage.

Articles 4 (2) and (3) of the AI Liability Directive distinguish between:

- claims brought against the provider of a high-risk AI system or against a person subject to the provider's obligations under the AI Act – in this case, the defendants' compliance with the obligations set forth therein have to also be assessed in light of the risk management system and its results under the AI Act; and
- claims brought against the user of such systems.

Article 4(4) of the AI Liability Directive establishes an exemption from the presumption of causality in the case of high-risk AI systems if the defendant proves that the damaged party has sufficient evidence, expertise or information to prove a causal link between the non-compliance and the harm suffered.

Conversely, in the case of non-high-risk AI systems, Article 4(5) of the AI Liability Directive establishes a condition for the applicability of the presumption of causality, whereby the latter is subject to the court determining that it is excessively difficult for the claimant to prove the causal link.

BD and IP

Under the Italian legal system, BD and the results obtained from the processing thereof are not specifically regulated and protected, even

under the legislation on copyrights (Italian Law 633/1941 – the Copyright Law) for the following reasons.

Database as an intellectual creation of the author

Articles 1, 2(9) and 64-quinquies of the Italian Copyright Law provide for legal protection of the expressive form of databases (and not their content), provided that such database meets the requirement of creativity, which can be inferred from the choice or the systematic and methodical arrangement of the material within the database.

Considering that the BD collection process is characterised by an indiscriminate and systematic collection of data originating from many different sources, such datasets can hardly be considered “creative” since the author, in such process, lacks the possibility of choosing which data to collect and determining its arrangement within the database.

“Non-creative” databases

Articles 102-bis and -ter of the Italian Copyright Law provide for the protection of “non-creative databases” through a sui generis right: the person who has made significant investments in the establishment of the database has the right to prohibit the extraction from the database and its re-utilisation.

Given that the activity of collecting BD is the product of an automatic collection from diversified sources such as sensors or machines, it may not be the object of a significant economic investment or the result of a “significant investment”. Therefore, it seems difficult to consider BD datasets as non-creative databases.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

The concept of the Internet of Things (IoT), as clarified by Working Party 29 in its Opinion 8/2014, refers to an infrastructure in which billions of sensors embedded in common everyday devices – “things” as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.

There is no specific regulatory framework applicable to such technologies, at neither the European level nor the national level.

However, considering that the IoT is based on the collection of data and the interconnection of objects, which necessarily involves the transmission of signals between the objects themselves, the legislation applicable to the IoT includes:

- the GDPR and the Privacy Code, since the data processed may identify, directly or indirectly, the data subjects;
- Directive 2002/58/EC (e-Privacy Directive), implemented at the national level by Italian Legislative Decree No 259/2003 and recently amended by Italian Legislative Decree No 207/2021; and
- Directive (EU) 2018/1972 establishing the European Communications Code, implemented by Italian Legislative Decree No 207/2021, since the latter establishes an authorisation regime for the use of frequencies used by IoT technologies that, in compliance with the principle of proportionality, aims to ensure

“the development of innovative business projects”.

Moreover, reference shall be made to the Data Act, which is a key pillar of the EU strategy for data and will ensure fairness by setting up rules regarding the use of data generated by IoT devices.

IoT and Data Protection Challenges

In the context of the development of IoT-based projects, attention shall be paid to the potential legal issues associated with the unlawful processing of data deriving from such use.

The interconnection of objects and systems involves the collection, recording and processing of personal data from users who are often unaware of it. In particular, such interaction between IoT objects generates data flows that can hardly be managed with the traditional tools used to ensure the adequate protection of data subjects' interests and rights. Therefore, in the absence of the possibility to effectively control how objects interact with one another, it may become extremely difficult for data subjects to control the generated data flow, to express valid consent for their processing and to control its subsequent use.

To this end, to protect the rights and freedoms of data subjects with regard to the processing of their personal data, companies wishing to develop IoT systems must, in general terms, comply with the provisions of the GDPR and the Privacy Code and, in particular:

- fulfil the necessary obligations provided for by the GDPR and guarantee an “informational self-determination” to data subjects, ensuring that they:

- (a) are aware of the risks that may arise from the direct or indirect use of smart objects, in order to assess their impact on their privacy;
 - (b) have the ability to control and monitor the collection and processing of their personal data; and
 - (c) are aware of possible uses/abuses of their personal data by third parties, outside their sphere of action;
- ensure that data subjects do not give consent based on a lack of information and not for all the purposes actually pursued, therefore being aware of all the purposes;
 - ensure that data is only used for such purposes and not for other purposes that are unknown by data subjects;
 - ensure compliance with the GDPR's obligations (eg, carrying out a data protection impact assessment, when necessary; ensuring that devices are secure by design and default; appointing a data protection officer);
 - make an assessment of the privacy roles of the parties involved in the processing, considering that the IoT context relies on the co-ordinated intervention of a significant number of stakeholders (ie, device manufacturers; data aggregators; application developers; social platforms; device lenders or renters); and
 - implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, considering that the greatest risks that may arise are related to the theft or unlawful use of data.

In this regard, extensive safeguards are requested in the IoT sector, from the physical security of the device and the interconnected device, to the granting of confidentiality, integrity and availability of the information acquired, stored, processed or transmitted by the devices.

To this end, during 2022, the International Organization for Standardization (ISO) together with the International Electrotechnical Commission (IEC) published ISO/IEC 27400:2022, which will be followed by other ISO standards applicable to the IoT sector during 2023.

The new ISO provides guidelines on risks, principles and controls for the security and privacy of IoT solutions.

Security System

Considering the security risks that IoT products and software may present, the EU Commission adopted the “Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020” (Cyber Resilience Act – CRA), which aims to safeguard consumers and businesses buying or using products or software with a digital component by introducing mandatory cybersecurity requirements for manufacturers and retailers of such products.

The CRA would complement existing legislation, specifically the NIS2 Framework, and apply to all products connected directly or indirectly to another device or network, except for specified exclusions such as open-source software or services that are already covered by existing rules, which is the case for medical devices, aviation and cars.

The CRA will guarantee:

- harmonised rules for products or software with a digital component that is intended to be placed on the market;
- a framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, with obli-

gations to be met at every stage of the value chain; and

- an obligation to meet a duty of care for the entire lifecycle of such products.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Pursuant to the current applicable legal framework, audio-visual media services are intended to be all mass media – ie, media intended for reception by a substantial proportion of the public, placed under the editorial responsibility of a media service provider, the main purpose of which is the provision of programmes aimed at informing, entertaining or educating the general public, via electronic communications networks, encompassing activities that are primarily economic. The provision of such services is subject to the obtainment of an authorisation, granted following a defined procedure and provided that certain requirements are met, which vary depending upon the services provided.

The Italian legal framework was updated in December 2021 with Italian Legislative Decree No 208/2021, which transposed Directive (EU) 2018/1808 and amended Italian Legislative Decree No 177/2005 (the Consolidated Law on Radio and Audio-Visual Media Services – AVMS Code). Specific provisions are also provided for by various Resolutions of the Authority for Communications Guarantees (*Autorità per le Garanzie nelle Comunicazioni* – AGCOM), which establish the relevant framework for different types of services.

The AVMS Code includes the general principles for the provision of audio-visual and radio digital media services and video sharing plat-

form services, regulating different audio-visual services, such as the transmission of television programmes (linear and on-demand), radio programmes and data programmes, as well as regulating the provision of associated interactive services and conditional access services on any broadcasting platform, including audio-visual commercial communications and video-sharing platform services.

Article 2 of the AVMS Code defines the scope of application of the Italian framework for audio-visual and radio media services by providing a series of requirements (such as having the principal office in Italy, taking the main editorial decisions in Italy and having a significant presence of operators in the Italian territory) that entail being subject to the Italian provisions.

Authorisation Procedure

For the provision of linear services, the legal framework requires different authorisations, depending on the broadcasting method: the Ministry of Economic Development (MISE) is responsible for the provision of cable services and for digital broadcasting on terrestrial frequencies, while AGCOM is responsible for those services provided via satellite and other electronic means of communication (as indicated in Articles 18 and 19 of the AVMS Code). The competent authority may deny the authorisation through its own reasoned decisions, based on reasoned grounds.

In detail:

- linear audio-visual media services transmitted by cable require the operator to hold a general authorisation issued by MISE that follows the submitting of a specific form to AGCOM; and

- pursuant to AGCOM Resolution No 127/00/CONS, linear audio-visual media services transmitted by satellite require the operator to hold a general authorisation from AGCOM. Satellite authorisations issued within 60 days of application are valid for a period of six years, and are renewable. For the purposes of granting and/or renewing authorisations, Article 6 of the Resolution establishes the payment of a financial contribution by way of reimbursement of the costs of the preliminary review for the decision on the application for authorisation.

The broadcasting of audio-visual and radio media services through platforms consisting of the internet network, including broadband and mobile networks (ie, on other electronic means of communication) is permitted in both linear and on-demand services.

These services are subject to different legal disciplines: in one case it is necessary to obtain a specific authorisation title, while in the other a general authorisation is required. For both of them, annual revenues “deriving from advertising, teleshopping, sponsorships, contracts and agreements with public and private entities, public subsidies and pay television offers” are limited, and must exceed EUR100,000.

In detail:

- pursuant to AGCOM Resolution No 606/10/CONS, linear or radio audio-visual media services transmitted by other electronic means of communication (ie, web-TV, IPTV and mobile TV) require the operator to hold a general authorisation from AGCOM. The activity covered by the authorisation request may be started following the 60-day period in which it is due to receive silent consent; and

- pursuant to AGCOM Resolution No 607/10/CONS, for on-demand audio-visual services, the operator is required to submit a Certified Notification of Initiation of Activities (SCIA) to AGCOM, as provided by AGCOM's application form. The activity covered by the authorisation request may be commenced from the date of submission of the certified report to commence activity.

With regard to these two latter points, authorisations are valid for a period of 12 years and are renewable. Article 6 of both the abovementioned Resolutions prescribes that the person applying for the issue/renewal of the authorisation is required to make a payment to AGCOM, by way of reimbursing the costs of reviewing the application for authorisation.

Video-sharing Platform Services

Video-sharing platform services are regulated by Chapter II of the Title IV of the AVMS Code and have the same obligations as audio-visual service providers in respect of advertising and other content restrictions, considering the limited control they can exercise over advertising on their platforms that is not marketed, sold or arranged by them. In this regard, AGCOM is entrusted with the power, through its regulations, of defining and adopting measures by which the free circulation of programmes, user-generated videos and audio-visual commercial communications conveyed by a video-sharing platform may be limited for the purpose of combating incitement to racial, sexual, religious or ethnic hatred, and the violation of human dignity.

Furthermore, providers of video-sharing platforms established in Italy pursuant to Article 41(1-5) of the AVMS Code shall be governed by Articles 3, 4, 5 and 14 to 17 of Italian Legislative Decree No 70/2003 on certain legal aspects of

information society services in the internal market, in particular electronic commerce.

On a final note, online content sharing platforms are also regulated by Directive (EU) 2019/790 (Copyright Directive) which is transposed at the national level by Italian Legislative Decree No 181/2021 and aims to regulate and standardise the legislation of member states with regard to:

- exceptions to/limitations on copyright, the digital environment and the cross-border environment;
- the improvement of licensing procedures to ensure broader access to content; and
- the inclusion of guarantees of proper functioning of the market for copyright.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The Italian legal framework regarding telecommunications rules was updated in December 2021 with Italian Legislative Decree No 207/2021 (EECC Decree), which transposed Directive (EU) 2018/1972 at the national level and established the European Electronic Communications Code, combining the previous rules on electronic communications into a single regulatory text.

The new features introduced by the EECC Decree include new definitions of electronic communication services, which take into account the technological and market developments and allow over-the-top (OTT) services to be brought within the scope of the EECC Decree.

Technologies and Services Falling Within the Scope of the EECC Decree

Article 1 of the EECC Decree entirely replaced Articles 1–98 of Italian Legislative Decree No 259/2003 and subsequent amendments (the Electronic Communications Code, or Italian ECC). Pursuant to Article 1 of the EECC Decree, which amended the former Article 2, the following technologies fall within the scope of the Italian telecommunications rules:

- electronic communications networks and services for public use, such as phone centres, internet points, internet service providers' products, telephone traffic resale, Voice over Internet Protocol, fax services, public telephone services, public network supplies, satellite services, networks used for the broadcasting of sound and television programmes, and cable television networks;
- closed user groups, defined as a plurality of subjects linked by a stable professional or common user interest so as to justify the internal requirements of confined communication, satisfied by means of exclusive, closed electronic communications networks and services;
- electronic communications activities for private use, such as radio amateurs and low-power equipment to support companies (eg, radio stations used for taxis, security services, civil protection associations);
- submarine electronic communications installations; and
- radio-electric services.

With particular regard to the technologies falling within the scope, the EECC Decree extends the definition of “electronic communication service” to include:

- internet access services;

- interpersonal communications services; and
- services consisting wholly or mainly of the conveyance of signals, such as transmission services used for broadcasting and the provision of machine-to-machine services.

The EECC Decree defines an “interpersonal communications service” as a service, normally concerning payments, that enables the direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine their recipient(s), including services such as traditional voice calls between two persons, email messages, messaging services and group chats. In this way, most of the so-called OTT companies are covered by the definition, which does not include services enabling interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

Requirements

Pursuant to Article 11 of the EECC Decree, which replaced the former Article 25, the provision of electronic communication networks or services (other than number-independent interpersonal communications services number), without prejudice to the specific obligations referred to in Article 13 of the EECC Decree, shall be subject to a general authorisation issued by MISE following the submission of a specific SCIA that shall include:

- the applicant's declaration of its intention to start supplying specific services;
- general information about the operator's organisation (nationality, registered office, VAT number, contact information, details of the legal representative); and

- technical information such as a description of the network or service to be provided.

Once the declaration has been filed, the applicant may immediately start providing the service indicated in the SCIA.

Within 60 days, MISE will issue a reasoned resolution prohibiting the company from continuing its activity and revoke the authorisation if it finds out that the necessary requirements are not satisfied.

The applicant is also required to be registered in the Register of Communications Operators kept by AGCOM, and to pay the relevant administrative costs.

The general authorisation has a duration of 20 years and is renewable for no more than 15 years by submitting a new SCIA to MISE.

After consulting with AGCOM on matters falling under its competence, MISE may define – by publishing specific regulations in accordance with the requirements of the EECC Decree – detailed schemes for specific regimes for the general authorisation for particular categories of networks or services, with which the company intending to offer these networks or services must comply.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

“Technology agreement” is a broad term that can cover several kinds of services (eg, licensing, maintenance, outsourcing or even the development of software; selling and purchasing of hardware; providing cloud computing services;

engineering). Moreover, with the advancement and rapid development of technology and services provided via the internet, such definition does not cover homogeneous categories of services and agreements, and has become increasingly dynamic. New developed technologies include machine learning, 5G, AI, IoT, cloud and cognitive systems designed to predict and detect errors in software.

Considering the above, one of the main challenges is often the impossibility/difficulty to include these agreements within the categories and institutions of the Italian civil law system.

Indeed, since the technology agreements, *latu sensu* intended, do not have a precise definition, it cannot be possible to refer to a specific regulation under Italian civil law: they are not typical/standard contracts – in the technical legal sense provided under the Italian civil law system – and, therefore, are not subject to a specific legal framework.

For this reason, when negotiating and drafting a technology agreement, it is important to appropriately qualify the characteristics of the services or technologies to be provided in order to identify the applicable legal framework, which may include the joint application of different types of contracts and their specific provisions; with a complete and well-drafted technology agreement, some legal issues can be prevented.

As a general rule, the provisions of the Italian Civil Code regarding purchase agreements (*vendita*), service contracts (*appalto di servizi*) and supply contracts (*somministrazione*) shall apply, even though a specific assessment on a case-by-case basis shall always be made.

Moreover, it is necessary to consider further issues that are relevant to the regulation of technology agreements, such as:

- intellectual and industrial property matters;
- personal data protection;
- representations and warranties of the parties;
- tax matters (eg, connected to the e-commerce sector);
- consumer protection matters (eg, the Italian Consumer Code, recently reformed by Italian Legislative Decree No 173/2021, which implemented Directive (EU) 2019/770, which regulates certain aspects about the supply of digital content and digital services between consumers and sellers); and
- the application of mandatory provisions related to health and safety in the workplace (to be deemed applicable when the services to be rendered may entail on-site activities) and to employment, accident prevention, wage and social insurance regulations.

IP

In Italy, software and computer programs are protected primarily by the Italian Copyright Law, since they are considered works of intellect, pursuant to Article 2575 of the Italian Civil Code. Considering this, it shall be necessary to guarantee the protection of the software and the relevant IP rights, whether pre-existing or specifically created as a result of commissioning the development.

Data Protection

When the technology solutions entail the processing of personal data, the parties shall comply with the data protection legislation that is applicable in Italy, in particular the GDPR and the Privacy Code, such as by:

- appointing the contractor as processor pursuant to Article 28 of the GDPR;
- specifying the security obligations of the parties;
- defining the liability regime of the parties; and
- limiting the transfer of personal data outside the EU, unless adequate safeguards are put in place.

Therefore, in order to provide requested technology solutions, the service provider may be required to satisfy specific requirements under Italian law (eg, declarations and certificates aimed at affirming and demonstrating compliance with anti-bribery, anti-money laundering and anti-corruption provisions). Further requirements may be imposed when the client is an Italian public entity.

Technology Agreements Related to Specific Industries

The technological evolution has an impact in various industries that are also regulated by dedicated provisions, such as banking, insurance and public administration.

In the banking sector, new technologies (such as AI, machine learning, cloud, robotics, Application Programming Interfaces and cybersecurity) are going to be frequently used, with a wide variety of agreements (eg, outsourcing and complex services agreements, development and licensing agreements, collaboration agreements, cloud services agreements, reseller agreements and marketing agreements). Therefore, in various specific industries, such as the banking sector, the national and European regulators prescribe strict standards, requirements and indications that companies must meet (eg, cybersecurity, regulatory compliance and service continuity). Greater restrictions could be identified on the

basis of the sector involved and the legal issues considered.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The Italian legal framework in relation to the delivery of trust services, the use of electronic signatures and digital identity schemes is set forth at the European and national level with particular reference to Regulation (EU) 910/2014 (eIDAS Regulation) and Italian Legislative Decree No 82/2005 (as subsequently amended – CAD).

The eIDAS Regulation aims to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the EU.

In Italy, the regulation is set forth by the CAD, the provisions and related technical rules of which apply to public administrations, public service operators and public control companies. Moreover, pursuant to Article 2(3) of the CAD, its provisions concerning, inter alia, electronic documents, electronic signatures, the reproduction and storage of electronic documents, digital domicile and electronic communications also apply to private individuals.

The Agency for Digital Italy (*Agenzia per l'Italia Digitale* – AgID) plays a key role in the implementation and enforcement of the CAD rules.

Trust Services

In the eIDAS Regulation, a trust service is defined as an electronic service (normally provided for remuneration) consisting of:

- the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services;
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.

A qualified trust service is a trust service that meets the requirements laid down in the eIDAS Regulation and provides the relevant guarantees in terms of security and quality; therefore, the qualified services provided are characterised through the use of the EU trust mark for qualified trust services. In Italy, such providers are permitted to provide qualified trust services pursuant to Article 29 of the CAD and are supervised by the AgID, which publishes the list of trust service providers established in Italy, together with information on the relevant services.

Electronic Signatures

The legal framework regulates different types of electronic signatures (simple, advanced, qualified and, in Italy, the digital signature defined by Article 1(1)(s) of the CAD), which have linked different legal effects and add consequent different value to the electronic documents to which they are affixed.

In this regard, the “simple” electronic signature provides a lower level of legal certainty, since, in any legal proceedings, the suitability of the document to which it is affixed to satisfy the requirement of written form and its evidentiary

value are freely assessable in court, in relation to the characteristics of security, integrity and unchangeability. However, pursuant to Article 25(1) of the eIDAS Regulation, an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

Different and greater legal effects of advanced and qualified electronic signatures, on the other hand, can be attributed to the following, in particular.

- As provided for by Article 20(1-bis) of the CAD, their ability to enable the electronic document to satisfy the requirement of written form as well as the particular effectiveness of such document envisaged by Article 2702 of the Italian Civil Code. Their legal effectiveness is guaranteed, since these signatures are considered reliable as to the identity of the signatory, and the private contract is full evidence (until an action of fraud) of the declaration's provenance from the person who signed it, if the person against whom the private contract is produced recognises the signature, or if it is legally considered as recognised.
- Their probative value and the regime of burden of proof, to be understood as the identification of the person who, in the event of a dispute, must provide evidence to prove the validity or invalidity of the disputed signature.

In this regard, there is a difference between advanced electronic signatures and qualified (and digital) electronic signatures:

- when an advanced electronic signature is used, the party to whom the signature relates

may disown it, and it is the party wishing to avail itself of the legal effects of that signature which has to prove compliance with the legal requirements; and

- when a qualified electronic signature is used, pursuant to Article 20(1-ter) of the CAD, the signature is presumed to be attributable to the holder of the electronic signature, unless said holder proves otherwise, and thus the burden of proof is reversed.

Furthermore, in light of the greater security they can guarantee with regard to the integrity and provenance of the document, qualified and digital signatures produce broader legal effects:

- Article 25(2) of the eIDAS Regulation states that “A qualified electronic signature shall have the equivalent legal effect of a handwritten signature”;
- they can be further used for the signing of the categories of acts referred to in Article 1350 of the Italian Civil Code (so-called contracts with written form *ad substantiam*), which must be stipulated in the form of a public deed or private deed, under penalty of nullity; and
- pursuant to Article 25(3) of the eIDAS Regulation, there is a principle of mutual recognition of qualified electronic signatures in that, if “based on a qualified certificate issued in one Member State, it shall be recognised as a qualified electronic signature in all other Member States”.

Digital Identity

The Public Digital Identity System (SPID) has been implemented in Italy since 2019, allowing citizens to access the online services of public administrations and private entities with a single digital identity, in a unique, safe and secure manner. The service is provided by a list of authorised

identity providers, which are entities accredited by AgID that, in compliance with the rules issued by AgID, provide digital identities and manage user authentication.

With Determination No 157/2020, AgID published the “Guidelines for the electronic signing of documents” pursuant to Article 20 of the CAD, recognising the possibility for citizens (ie, natural persons) to sign deeds and contracts with SPID and, therefore, regulating a fifth type of electronic signature: the electronic signature with SPID, which is recognised as having the same legal value as a handwritten signature. The SPID Guidelines allow SPID to be used in accordance with Article 20(1-bis) of the CAD, pursuant to which an electronic document satisfies the requirement of written form and produces the effects referred to in Article 2702 of the Italian Civil Code.

Furthermore, with Determination No 318/2019, AgID has published the “Guidelines for the issuance of digital identity for professional use”, which identify the procedures to be followed by

identity providers when issuing identities for professional use, allowing the data of the organisation for which one is acting on a service made available by a service provider to be conveyed through SPID in addition to the data of the individual. SPID credentials for legal persons must mandatorily be requested by the company’s legal representative who, once in possession of such credentials, may request the issue of additional credentials for professional use for persons authorised to operate on behalf of the company.

Morri Rossetti e Associati provides integrated consultancy to Italian and international clients in a variety of legal and tax matters. The TMT and data protection department operates through a multidisciplinary team of professionals specialising in multiple areas of law (corporate and commercial, IT, media, data protection, cybersecurity, tax advisory and tax compliance), providing assistance in the telecommunications, media and technology, digital innovation, e-commerce and online advertising sectors, with

a particular focus on national, EU and international regulatory developments. The team is able to offer highly innovative and tailor-made solutions, together with a strong sensitivity and ability to understand the opportunities and the business models of such sectors, as well as the legal and tax-critical features of the technological evolution. Recent clients include leaders in the data centre market, clients operating in the programmatic advertising market, and a number of start-ups operating in different sectors.

Authors



Carlo Impalà is a partner at Morri Rossetti and head of the TMT and data protection department. He is a member of the Italian Bar and a certified Data Protection Officer. His

practice focuses on corporate and commercial law, extraordinary corporate transactions, and the preparation and implementation of corporate governance and compliance models (in particular with reference to data protection law). He has particular expertise in drafting and negotiating national and international commercial agreements, with a specialisation in antitrust and regulatory profiles, mainly in the automotive, ICT, insurance, fashion, organised large-scale distribution and advertising sectors. Carlo is a member of national and international professional associations and working groups, and has written several publications on corporate law and corporate compliance.



Giorgia Valsecchi is an associate at Morri Rossetti and works within the TMT and data protection department on law and regulation applicable to privacy and data protection,

internet, online publishing and advertising, e-commerce and information technology. She also focuses on the negotiation and drafting of commercial contracts in different sectors. Giorgia qualified as a lawyer in 2020, and is a member of the Italian Bar Association in Milan.



Giulia Castelli is an associate at Morri Rossetti and works within the TMT and data protection department, with a focus on the regulation applicable to privacy and data protection, the

telecommunications sector and information technology. Before joining the firm, she did an internship in the business department of a multinational television broadcasting company, dealing with contractual compliance. Giulia qualified as a lawyer in October 2022, and is a member of the Italian Bar Association in Milan.



Jun Jie Yang is a junior associate at Morri Rossetti and works within the TMT and data protection department, providing legal assistance to Italian and foreign companies in

corporate and commercial law, the regulation applicable to internet, telecommunications, ICT, media and online advertising and data protection law. Before joining the firm, Jun Jie started her professional experience in a Beijing-based business advisory firm.

Morri Rossetti

Piazza Eleonora Duse, 2
20122
Milan
Italy

Tel: +39 02 7607 971
Fax: +39 02 7607 97206
Email: Carlo.Impala@morrirossetti.it
Web: www.morrirossetti.it

MORRI
ROSSETTI

A vertical red line graphic located to the right of the Morri Rossetti logo.

Law and Practice

Contributed by:

Hiromi Hayashi, Masaki Yukawa and Daisuke Tsuta
Mori Hamada & Matsumoto see p.242



Contents

1. Metaverse	p.231
1.1 <u>Laws and Regulations</u>	p.231
2. Digital Economy	p.232
2.1 <u>Key Challenges</u>	p.232
3. Cloud and Edge Computing	p.233
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.233
4. Artificial Intelligence and Big Data	p.234
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.234
5. Internet of Things	p.236
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.236
6. Audio-Visual Media Services	p.237
6.1 <u>Requirements and Authorisation Procedures</u>	p.237
7. Telecommunications	p.238
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.238
8. Challenges with Technology Agreements	p.239
8.1 <u>Legal Framework Challenges</u>	p.239
9. Trust Services and Digital Entities	p.239
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.239

1. Metaverse

1.1 Laws and Regulations

Metaverse is currently attracting attention from businesses and government, and accordingly discussions on legal issues related to the metaverse have been going on. In November 2022, the government set up a council consisting of businesses, legal experts and government officials to discuss legal issues regarding the metaverse. The council is expected to publish a report in 2023.

Intellectual Property Rights

Copyright

Reproducing the real world in the metaverse will not infringe copyright in most cases. While architectural works with copyrightable properties are often used as landmarks in the metaverse, that use is permitted by Article 46 of the Copyright Act. Article 46 permits the use of architectural works or works of art that are publicly available (like a statue in a park), but does not apply to signboards or other works that are copyrightable. However, Article 30-2 of the Copyright Act allows a third party copyrightable work to be incidentally included in another copyrightable work as long as the inclusion is minor and incidental to the principal copyrightable work (eg, where a third party's copyrighted work was included in a photo). Based on this provision, when a vast space in the real world is reproduced in the metaverse, a signboard with copyrightable material that is also reproduced in the metaverse will be considered to be only a minor inclusion compared to the entire reproduced space so that the inclusion will be allowed under Article 30-2 of the Copyright Act.

An avatar that is generated using a user's creativity may be copyright-protected. However, if the avatar lacks creativity (eg, it resembles a

real person), it is not copyright-protected. Thus, determining creativity for purposes of copyright protection would be an issue. A further issue is determining what rules would be fair or appropriate for user generated contents.

Trade mark

Virtual goods may be produced with trade marks as in real-world goods. Since the goods and service classifications between the real world and the metaverse are different, trade marks for real-world goods would not be protected in the metaverse unless they are registered for virtual goods and services. Having said that, since an increasing number of brand-owning companies apply for virtual goods and services, metaverse providers would need to be more careful about using a third party's trade marks. In light of the market growth of metaverse, more brand-owning companies are expected to register their trade marks for virtual goods and services.

Publicity rights

An avatar may be generated from an image of a public figure. There is a judicial precedent ruling that a publicity right is granted if the name or image of the public figure has the power to promote the sale of goods and that publicity right is infringed if the name or image is used solely for the purpose of promoting sales (Supreme Court, 2 Feb 2012). Thus, such an avatar cannot be used to promote sales, but a publicity right would not be infringed if the user generates the avatar only for personal satisfaction or use.

Privacy Law

Users' actions in the metaverse are collected and recorded by metaverse service providers, which can also collect and use users' data, such as the users' profiles, behaviour, interests, and preferences.

Not all users' information in the metaverse is considered "personal information" under the Act on the Protection of Personal Information (APPI). The APPI defines "personal information" as information relating to a living individual which contains a name, date of birth, or other descriptions through which a specific individual can be identified. Therefore, if, for example, an individual registers only a nickname to use a metaverse service, the information collected by the provider of the metaverse service would not be considered "personal information". However, if in using the metaverse, an individual's real name or email address that could identify that individual is registered, then that information is considered personal information under the APPI.

Separately from the APPI, Japanese courts recognise a person's right to privacy, which is the right for that person's private life not to be disclosed except for legitimate reasons. Certain information collected in the metaverse can be protected as part of a person's private life. Therefore, even if a piece of information is not considered personal information under the APPI, it is necessary to examine whether certain users' data are protected as part of the users' private lives.

Telecommunications Business Act

The Telecommunication Business Act (TBA), which was amended in 2022, requires large-scale social networking services (SNS) (ie, SNS with at least 10 million users if the service is provided without consideration, and with at least 5 million users if the service is provided with consideration) to file a notification with the Ministry of Internal Affairs and Communications (MIC). Metaverse service providers may also be subject to the TBA if they are large-scale as previously described. See 7. **Telecommunications** for details on TBA.

2. Digital Economy

2.1 Key Challenges

In Japan, trading practices and consumer protection in the context of digital platforms recently attracted public attention and two pieces of legislation were promulgated in 2020 and 2021.

Transparency and Fairness of Digital Platforms

The Act on Improving Transparency and Fairness of Digital Platforms was enacted in June 2020 and took effect in February 2021. Under the Act, the Ministry of Economy, Trade and Industry (METI) designates providers of regulated digital platforms with a certain size in sales according to the category of the platform:

- e-commerce marketplace with annual sales of JPY30 billion or more;
- app store with annual sales of JPY20 billion or more;
- advertisement media with annual sales of JPY10 billion or more; and
- digital advertising platforms with annual sales of JPY5 billion or more.

If so designated, such digital platform providers are required to disclose the conditions of accepting business operators, reasons for requesting purchasing services, factors affecting rankings, and other information. Such designated providers are also required to annually report their complaints handling, disputes resolution, disclosure and self assessment to METI.

Consumer Protection of Digital Platforms

The Digital Platform Consumer Protection Act was enacted in May 2021 and took effect in May 2022. The Act applies to platforms on which consumers may purchase goods, services or rights for consideration, without regard to the

size of sales. The Act requires platform providers to proactively protect consumers from sellers, which are not platform providers but just merchants in digital platforms. Digital platform providers are required to take measures to enable smooth communication between sellers and consumers, investigate sellers in response to consumer complaints about transactional conditions, and require sellers to provide information on their identity as necessary. Digital platform providers may be requested by the Consumer Affairs Agency to remove certain goods, services or rights if there are any false or misleading descriptions that are not voluntarily remedied. Consumers may require digital platform providers to disclose the names, addresses, phone and facsimile numbers, email addresses, and corporate registration numbers of sellers if they need the information to exercise their rights against sellers.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

In Japan, there are no laws or regulations which are generally applicable to cloud computing. However, certain services using cloud computing, such as voice communication services and email services, may constitute a telecommunications business under the Telecommunications Business Act (TBA). Please see **7. Telecommunications**.

Where personal information is stored in a cloud, the APPI will apply. The Personal Information Protection Commission (PPC), the principal regulatory authority regarding the APPI, has clarified that businesses using cloud services must take security measures to protect personal information stored in a cloud service provided by a

third party, but they do not need to supervise the providers of the cloud service or obtain consent from data subjects if the cloud service providers cannot access the stored personal information, regardless of whether the relevant data centre is located in or outside Japan.

Industry-Specific Guidelines on Cloud Computing

Government cloud procurement

The Japanese government operates the Information System Security Management and Assessment Programme (ISMAP), pursuant to which Japanese government organisations may procure cloud services from cloud service providers registered with the ISMAP steering committee. The registration process requires applicants to submit an assessment report prepared by a third-party auditor registered with the committee, as well as other required information, including information regarding the risk of compulsory data access due to the applicability of foreign laws to enable the committee to review those foreign laws.

Financial service operators

Financial service operators – such as banks, insurance companies and financial instrument business operators – are required by the supervisory guidelines issued by the Financial Services Agency (FSA) to take outsourcing management measures. Since the use of cloud services provided by a third-party service provider is a form of outsourcing, financial service operators must implement outsourcing management measures such as conducting a due diligence check of the service provider, entering into a service agreement that satisfies the supervisory guidelines and auditing the service provider. More specifically to cloud, the financial service sector often refers to the guide to cloud implementation and operation of financial institutions published by

the Centre for Financial Industry Information Systems (FISC).

Healthcare information

The healthcare industry (eg, hospitals, clinics, dentists and pharmacies) is subject to the Security Guidelines for Medical Information issued by the Ministry of Health, Labour and Welfare. Providers of cloud service to the healthcare industry are subject to the Security Guidelines for Information Service Providers for Medical Information issued by METI and MIC. These guidelines include both mandatory requirements as well as government recommended actions.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Product Liability and General Tort Liability

Under the Product Liability Act (the PL Act), a producer of a manufactured or processed movable good is liable for damages to human life or body, or property caused by a defect in the good, regardless of whether or not the producer is negligent.

Since big data, machine learning and artificial intelligence (AI) are not movable goods, producers of big data, machine learning or artificial intelligence themselves will not be subject to the PL Act. Rather, it is the producers of movable goods into which big data, machine learning or artificial intelligence is installed which will be liable for the damages caused by a defect in those movable goods, including a defect in the installed big data, machine learning or artificial intelligence.

Producers of big data, machine learning or artificial intelligence may be subject to general tort liability under the Civil Code. General tort liability is not a strict liability, unlike liability under the PL Act, and the plaintiff must prove intentional act or negligence (including simple negligence) on the part of the defendant to successfully claim for damages.

Autonomous Vehicle Accident Liability

Under the Act on Securing Compensation for Automobile Accidents, any person who has control over or operates an automobile for their own benefit (eg, an owner or a driver) – the “responsible person” – is liable for damages for the death or bodily injury of another person arising from the operation of the automobile. The foregoing liability, however, does not apply if the responsible person proves that they and the driver exercised due care in controlling and operating the automobile, that the injured party or a third party other than the driver acted intentionally or negligently (including through simple negligence), and that there was no defect in the structure or functions of the automobile.

One issue is whether this special liability under the present automobile accident compensation framework should be modified to properly address car accidents caused by cars operated by artificial intelligence, such as holding the car manufacturers liable for damages. The Research Report on Damage Liability regarding Autonomous Vehicles, which the Ministry of Land, Infrastructure and Tourism published in March 2018, concluded that it is appropriate not to modify the existing special liability for automobile accidents during the transition period until 2025 when autonomous vehicles are expected to be widely used. The report recommended that insurance companies that have compensated for damages caused by a defect in any autonomous driving

equipment installed in a vehicle should be able to recover the compensation they paid from the car manufacturers that installed the defective artificial intelligence-driving equipment.

Based on the recommendation, the Japanese Road Transport Vehicle Act was amended in May 2019 so that any autonomous driving equipment is required to have recording equipment to provide insurance companies with evidence as to the cause of an automobile accident.

Data Protection Consideration

The APPI has not imposed strict conditions focused only on processing personal information by AI. The APPI requires business operators using a personal information database in their business (“handling operators”) to use personal information only within the scope of the purpose of use notified to data subjects or publicly announced when collecting personal information. Therefore, as a general rule, it is required to notify or publicly announce the purpose of machine learning in order to use personal information for machine learning.

In this regard, the purpose of generating statistical data by aggregating or analysing a large amount of personal information does not have to be notified to data subjects or publicly announced. However, the purpose of profiling, such as user journey analysis for targeted advertisement and credit scoring, must be notified to data subjects or publicly announced.

Further, if handling operators pseudonymously process personal data, they will be allowed to internally use the pseudonymously processed information beyond the original purpose of use that was notified to data subjects or publicly announced when collecting the original data. Thus, handling operators may use personal data

for machine learning even where the machine learning is not included in the purpose of use notified to the data subjects when the personal data was collected.

Copyrights Consideration

In the process of machine learning, copyrighted works may be copied or adapted, which may cause an infringement of copyrights. To promote AI developments, the Copyright Act grants an exemption allowing the use of copyrighted works to the necessary extent without permission from the copyright owner where the use (i) does not aim to let the user or others enjoy thoughts or sentiments expressed in the work, and (ii) does not unjustifiably harm the copyright owner’s interests, taking into consideration the type and purpose of the work and the manner in which the work is used.

This exemption covers the use of copyrighted works for extracting informative elements from a large amount of copyrighted or other works and analysis. The Copyright Act was amended in 2019 to clarify that this exemption covers not only statistical analysis but also deep learning, and not only copying but also transmission for grid computing.

Protection of “Shared Data with Limited Access”

To promote data sharing between businesses so that big data will be more widely used, the amendment to the Unfair Competition Prevention Act introduced the protection of “shared data with limited access” which is defined as any technical or business information:

- that is accumulated in a reasonable amount by electronic means;
- that is provided to specified persons as a business; and

- the access of which is controlled by electronic means.

Information controlled as a secret, which would be protected as a trade secret, is excluded from the concept of shared data with limited access. Most typically, where data such as location of smartphones or cars is collected by a business operator (the “data holder”) and sold to third-party business operators for a fee (or shared among business operators in a consortium without charge) under the condition that the data can be used only for a certain purpose such as internal marketing analysis and cannot be redistributed or used for unauthorised purposes, the data would be protected as shared data with limited access. If shared data with limited access is wrongfully acquired, redistributed to third parties or used for unauthorised purposes, the data holder may seek an injunction and damage compensation under the Unfair Competition Prevention Act.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Under the Radio Waves Act (the RWA), in principle, users of radio equipment – including Internet of Things (IoT) devices using radio waves such as Bluetooth or Wi-Fi – must obtain a radio station licence from MIC. However, certain smaller-scale radio stations, including Wi-Fi and Bluetooth devices, are exempted from such licence requirement if the device conforms to the technical requirements established by MIC and bears a certification mark indicating such conformity (an R-mark). For users to comply with the foregoing requirements, manufacturers, importers or sellers of those devices apply for the certificate

of conformity and put the certification mark on their products.

Radio equipment that has undergone technical conformity certifications conducted by foreign certification bodies based on mutual recognition agreements between Japan and certain foreign countries (currently, the USA, the EU and Singapore) is deemed to conform to the technical standards established by MIC in Japan and may bear an R-mark without a separate certification in Japan.

Please note that, due to Brexit, the mutual recognition agreement between the EU and Japan no longer applies to certification bodies in the UK and there is no mutual recognition agreement between the UK and Japan. However, the Minister for Foreign Affairs of Japan has issued a letter stating that the Japanese government will accept the certification by certification bodies in the UK in accordance with Article 38-31 of the RWA, which is similar to a mutual recognition agreement framework except that only non-Japanese manufacturers can rely on this Article 38-31 and Japanese manufacturers cannot use the certification bodies in the UK unlike under mutual recognition agreements.

There is an exemption to the certification requirement that is available for devices which conform to technical specifications designated by MIC such as IEEE802.11b/11a/11g/11n/11ac/11ad and Bluetooth Core Specification Version 2.1 or later, if solely used for testing purposes. To rely on this exemption, a notification must be filed with MIC stating the start and close of the testing period. The testing period must be 180 days or shorter. Before filing the start notification, one must ensure that the device complies with at least one of the technical specifications designated by MIC.

Internet Connection

Under the TBA, any telecommunications device which is connected to a telecommunications circuit facility, such as an internet connection provided by a telecommunications business operator, must satisfy certain technical requirements, be certified by a registered certification body, and bear a “T-mark”. However, the guidelines issued by MIC on 22 April 2019 clarified that a Bluetooth device is exempt from the TBA certification requirement if it:

- can be used by connecting to a smartphone;
- does not have other functions that directly connect to telecommunications circuit facilities; and
- is certified as complying with the Bluetooth specifications.

A similar exemption applies to a Wi-Fi device if:

- the Wi-Fi device cannot be directly connected to the internet provided by a telecommunications business operator and is connected to the internet only through a certified router which bears a T-mark; and
- there is a statement in the manual that the device cannot be directly connected to the internet.

Data Protection Consideration

If an IoT device collects personal information, such as a person’s appearance recorded by a camera or a voice recording enabling the specification of a certain person, the service provider which collects the personal information through that IoT device would generally need to comply with the requirements under the APPI.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Licence for Broadcasting Business

As described in 7. **Telecommunications**, a telecommunications business under the TBA does not include broadcasting businesses, which are separately regulated under the Broadcasting Act. Note that the key regulator of both the telecommunications business and the broadcasting business is MIC.

The Broadcasting Act requires a licence prior to offering broadcasting services in Japan, which include:

- terrestrial-based television broadcasting;
- satellite-based television broadcasting; and
- cable television broadcasting.

The Broadcasting Act does not apply to companies with video-sharing platform services. In fact, there is no specific law which regulates video-sharing platform services.

The Broadcast Act restricts foreign investments in the broadcasting business. The following entities or parties are not eligible to hold a broadcasting licence:

- a person who is not a Japanese national;
- a foreign government or its representative;
- a foreign entity; and
- a company or entity in which any of the aforementioned entities or persons is the executive director, or holds 20% or more of the voting rights.

Licence for Radio Station

As described in 7. **Telecommunications**, users of radio equipment must obtain a radio station

licence pursuant to the RWA, with certain exceptions. Thus, if a provider of broadcasting services uses radio equipment for the services, it must obtain a licence not only under the Broadcast Act but under the RWA as well.

As described in 7. Telecommunications, the RWA restricts foreign investments regarding licences to use radio equipment. While there are exceptions to such restriction, those exceptions are not available for the use of radio equipment for a broadcasting business.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Licence for Telecommunications Business

Under the TBA, “telecommunications” means sending, delivering or receiving codes, sounds or pictures by wire, wireless means, or any other electromagnetic means which includes the internet. A broadcasting business is excluded from the definition of telecommunications business.

The TBA requires a licence prior to offering telecommunications services in Japan. There are basically two types of such licences under the TBA, namely:

- a registration (*toroku*); and
- a notification (*todokede*).

If a provider of a telecommunications business installs or owns (including in the form of an “indefeasible right of use” or IRU) telecom circuits (eg, optic fibres or coaxial cables) at certain levels, it must be a registration carrier. Other providers who do not install such circuits (eg, ISPs) are basically required to only notify MIC prior to offering telecommunications services.

A party seeking to provide a telecommunications service must submit application documents to MIC. In the case of a registration, it must also appoint a general manager for the telecommunication facilities (*denki tsushin setsubi toukatsu kanri sha*) or a chief telecommunications engineer (*denki tsushin shunin gijutsu sha*). A notification is a relatively straightforward procedure which would take only several days if all the necessary documents are complete. The filing fee for registration is JPY150,000, but no fee is necessary for filing a notification. There is no licence term or annual fee for either registration or notification. It is advisable to unofficially consult with MIC before filing an official application.

Licence for Radio Station

As described in 5.1 Machine-to-Machine Communications, Communications Secrecy and Data, a user of a radio equipment must obtain a radio station licence pursuant to the RWA, with certain exceptions. Thus, if a provider of telecommunications services uses radio equipment for the services, it must obtain a licence not only under the TBA but also under the RWA.

The RWA restricts foreign investments in relation to obtaining a licence to use radio equipment. The following entities or parties are not eligible to hold the licence:

- a person who is not a Japanese national;
- a foreign government or its representative;
- a foreign entity; and
- a company or entity in which any of the aforementioned entities or persons is the executive director, or holds ⅓ or more of the voting rights.

However, there are exceptions to the foregoing restriction. For instance, if the purpose of the radio equipment is to operate a telecommuni-

cations business, the foregoing restriction does not apply.

The term of the licence is five years. There is also an annual fee for the use of radio frequencies. The amount of the licence application fee and the annual fee to use radio frequencies varies depending on the type of radio frequencies and the power of the antenna of the radio equipment.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges IT Service Agreements

There are no specific laws or regulations that apply to IT service agreements. In addition, there are no laws that strictly regulate the location of data storage or a data centre, data-localisation, or price revision. However, the general contract law based on the will of the contracting parties applies to IT service agreements.

Parties should remember the following when incorporating a liability limitation clause into a contract:

- in a contract between a company and a consumer, a liability limitation clause may be invalidated under the Consumer Contract Act (CCA); and
- while the CCA does not apply to contracts between companies, a provision that exempts one contracting party from liability in the case of intentional or gross negligence may be invalidated under case law.

Data Localisation

There are no data localisation regulations. However, for some sectors, such as the medical sector, there are guidelines recommending storing

data in locations where Japanese law applies, that is, Japan. These guidelines are not strictly required to be observed, but are usually complied with by the relevant sectors as a matter of practice.

Economic Security

In 2022, the Act on the Promotion of National Security through Integrated Economic Measures was legislated. Under the Act, essential infrastructure businesses such as electric power, telecommunication and financial service providers must file a plan with the government before introducing or entrusting management of certain important equipment. The government will review the plan and may issue a recommendation or order entities to modify or discontinue the plan if the government finds security issues. The provisions of this Act regarding the designation of essential infrastructure business operators will take effect within 18 months of 18 May 2022 and those regarding the requirement to submit the plan will take effect within 21 months of 18 May 2022. If contracting with designated critical infrastructure business operators in Japan, this Act should be taken into consideration.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Electronic Signatures

Japan does not have an equivalent to electronic identification and trust services (eIDAS) regulations to regulate trust services comprehensively, but the Act on Electronic Signatures and Certification Business (the Electronic Signatures Act) grants an “electronic signature” the same legal status as wet-ink signatures. An “electronic signature” refers to a measure taken with respect

to information recorded electronically and which meets both of the following requirements (Article 2):

- a measure to indicate that the relevant electronic information was created by the person who has taken that measure; and
- a measure to confirm that the relevant information has not been altered.

Although government authorisation is not mandatory, 12 electronic signature service providers received confirmation that they satisfy the requirements of enabling “electronic signatures” from the Minister of Justice in accordance with Article 7, Paragraph 2 of the Act on Strengthening Industrial Competitiveness.

Please note that the Legal Affairs Bureau, which operates the real property and the company registration systems, does not accept all electronic signatures. Although electronic filing is permitted under laws and regulations, only electronic signatures designated by the Minister of Justice are accepted. Thus, there are still many applicants who apply for registration using physical documents, in which case, the originally signed documents may need to be submitted, depending on the type of registration they are applying for.

Time Stamp

There are no laws that require time stamps on documents, except when documents on national tax are electronically stored. The Electronic Book Preservation Act requires scanned data of paper-based documents on national tax and originally electronically produced documents on national tax to be accompanied by time stamps before they are electronically stored. Providers of the time stamps must enable proof of non-tampering for the term of the statutorily required storage period and a batch verification for a certain

taxable period. Although an authorisation is not required to issue time stamps, the Japan Data Communications Association, a private association, established a voluntary accreditation programme for time stamp service providers.

Japanese Public Key Infrastructure (JPKI)

For the purposes of tax and social welfare, a unique identification number is assigned to each individual residing in Japan, regardless of nationality. That unique identification number can be used only for the purposes of tax, social welfare or other statutorily defined purposes and the collection and use of such unique number is strictly restricted in the private sector. However, each unique identification number card issued by the government is installed with a digital certificate, which the private sector can use to establish the identity of users online (called the Japanese Public Key Infrastructure or JPKI). A business may verify that digital certificate through the use of the revocation list or Online Certificate Status Protocol (OCSP) service provided by the Japan Agency for Local Authority Information Systems (J-LIS), provided that it obtains authorisation from the Minister of MIC or outsources the verification to an authorised service provider.

A considerable number of financial service providers recently started to rely on the JPKI for the purpose of complying with the Know Your Customer (KYC) requirement. Compared to traditional KYC measures, reliance on JPKI is efficient in time and cost. Driver’s licenses are also installed with an IC chip which can also be used for KYC purposes.

eKYC in the Financial Sector (other than JPKI)

In the context of KYC, separately from relying on the digital data stored in ID cards, another measure used by financial institutions to establish

users' identity online is to require a user to take a selfie (with a random pose) and a digital image of a government-issued ID cards by installing and using a smartphone application provided by the financial institution and to send both the selfie and the ID card image to the financial institution. The financial institution will compare the photo printed on the government-issued ID card and the selfie photo sent by the user. The comparison can be automatically processed provided that the false acceptance rate (FAR) is lower than a certain level determined by the government (note that the number is not publicly disclosed). This KYC measure is used by an increasing number of financial service providers.

Future Trust Services in Japan

According to the Comprehensive Strategy regarding Data issued by the Digital Agency in June 2021, Japan aims to establish a basis to introduce trust services within the early 2020s, such as by introducing standards for trust services and accreditation of trust services by a certification body.

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo, with offices in Fukuoka, Nagoya, Osaka, Takamatsu, Beijing, Shanghai, Singapore, Yangon, Bangkok, Ho Chi Minh City and Hanoi. The firm has over 700 attorneys and a support staff of approximately 600, including legal assistants, translators and secretaries. The firm is one of the largest law firms in Japan and is particularly well known in the areas of mergers and acquisitions, finance, telecommunications, broadcasting, and intellectual property, as well as domestic

litigation, bankruptcy, restructuring, and multi-jurisdictional litigation and arbitration. The firm regularly advises on some of the largest and most prominent cross-border transactions, representing both Japanese and foreign clients. In particular, the firm has extensive practice in, exposure to and expertise on telecommunications, broadcasting, the internet, information technology, and related areas, and provides legal advice and other legal services regarding the corporate, regulatory, financing and transactional requirements of clients in these areas.

Authors



Hiromi Hayashi is a partner at Mori Hamada & Matsumoto. Hiromi specialises in communications laws and regulations and authored the Japanese section of The Preston

Gates Guide to Telecommunications in Asia in 2005. Hiromi's other areas of practice are international and domestic transactions, takeover bids, and corporate restructuring. Hiromi was admitted to the Bar in Japan in 2001 and in New York in 2007. Hiromi worked at Mizuho Corporate Bank from 1989–94 and was with Davis Polk & Wardwell in New York from 2006–07.



Masaki Yukawa is a counsel at Mori Hamada & Matsumoto. Masaki advises on regulatory, data protection and cybersecurity issues for financial institutions, payment service

providers, blockchain projects, telecommunications businesses and technology companies in and outside Japan. Masaki was admitted to the Bar in Japan in 2009 and in California in 2016. He was with the Bank of Japan from 2003–08 and the Financial Services Agency from 2014–15.

Contributed by: Hiromi Hayashi, Masaki Yukawa and Daisuke Tsuta, **Mori Hamada & Matsumoto**



Daisuke Tsuta is a counsel at Mori Hamada & Matsumoto. Daisuke specialises in cybersecurity and privacy law. He was admitted to the Bar in Japan in 2010. Daisuke worked

at the Kinki Local Finance Bureau of the Ministry of Finance from 2014–15, at the Ministry of Internal Affairs and Communications from 2015–17, and at the National Centre of Incident Readiness and Strategy for Cybersecurity (NISC) from 2017–20.

Mori Hamada & Matsumoto

16th Floor,
Marunouchi Park Building
2-6-1 Marunouchi
Chiyoda-ku
Tokyo 100-8222
Japan

Tel: +81 3 6212 8330
Fax: +81 3 6212 8230
Email: mhm_info@mhm-global.com
Web: www.mhmjapan.com

MORI HAMADA & MATSUMOTO

Trends and Developments

Contributed by:

Keiji Tonomura, Minh Thi Cao Koike,
Akira Komatsu and Hiroya Nadamoto
Nagashima Ohno & Tsunematsu see p.250

Initiatives for Developing Web3 and Metaverse

Background

The Japanese government is currently looking to “web3” and “start-ups” as engines of growth of the Japanese economy and it promoted various relevant government policies in 2022.

Among these, the key trends in 2022 were the intensive discussions at the government and private levels regarding the promotion of web3 and the blockchain-based ecosystem in Japan, including non-fungible tokens (NFT) and decentralised autonomous organisations (DAO), as well as the metaverse, which is also evolving rapidly and has a close relationship with web3 (albeit web3 and metaverse are different concepts).

Web3 (including NFTs and DAOs)

In March 2022, the Project Team regarding NFT Policies within the Headquarters for the Promotion of a Digital Society of the Liberal Democratic Party, the ruling party in Japan, announced the “NFT White Paper: Japan’s NFT Strategy for the Web3.0 Era” (NFT White Paper). The NFT White Paper illustrates the challenges and proposals regarding the following six topics:

- establishment and advancement of a national strategy for the Web3.0 era;
- measures necessary for NFT business development;
- measures necessary to protect the rights of content IP holders;
- measures necessary for user protection;

- measures necessary to foster a healthy blockchain ecosystem; and
- measures necessary to protect social and legal interests.

In response to the NFT White Paper and governmental policies, the Web3.0 Study Group was established under the Digital Agency. That group conducted hearings and held discussions regarding establishing the environment for the promotion of web3, and a report was published by the group in December 2022. The report presents basic guidelines for the healthy development of web3 and introduces discussions on:

- digital assets;
- DAO;
- Decentralised Identity (DID);
- relationship with the metaverse; and
- user protection and legal enforcement.

The report is a useful tool to understand the future course of efforts in Japan to promote web3.

In addition to discussions at the government level, private-level discussions are also moving forward. Industry associations related to cryptocurrency/NFT businesses in Japan are discussing issues and working on designing rules through the development of self-regulatory guidelines. For example, the Japan Cryptoasset Business Association, an industry association related to crypto-assets, published in March 2022 an update to the Guidelines for NFT Businesses. The update added explanations regarding cop-

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Hiroya Nadamoto,
Nagashima Ohno & Tsunematsu

wright and amended explanations regarding designing NFT gaming services from the perspective of whether these services constitute gambling. In September 2022, the Council for Sports Ecosystem Promotion, an industry association for sports, published the NFT Guideline (guideline on NFT package sales using sports content and establishment of secondary markets). The NFT Guideline explains the possibility that NFT package sales together with the establishment of secondary markets may not fall under gambling under Japanese law and can be legally developed while considering consumer protection, and the legal framework for returning a part of the sales from the secondary market to a content holder who minted an NFT. Although these are non-binding soft law, they should be referred to when considering conducting NFT package sales.

Metaverse

The metaverse is also expected to have considerable potential for new markets where Japanese IP can be utilised and monetised. The metaverse is a field that deserves attention and it has begun to be utilised for various industries such as shopping, tourism, and education, in addition to gaming and entertainment. In 2022, several initiatives were implemented at both the government and private levels.

In July 2022, the Ministry of Economy, Trade and Industry (METI) launched the “Research Project on Constructing Web-3.0-Era Creator Economies”. This research project will:

- investigate and review the legal issues in question;
- investigate overseas cases; and
- hold study group discussions regarding web3 and the metaverse, primarily from the creator’s perspective.

In order to review each issue, METI will establish the Metaverse Trial Space. In August 2022, the Ministry of Internal Affairs and Communications (MIC) also established the “Study Group on the Utilization of Metaverse Towards Web3 Era”. This study group will look into:

- matters relating to increasing convenience for users in the use of the metaverse;
- matters relating to the clarification of issues with the use of the metaverse, categorised by use cases;
- the impact of the development of use of the metaverse on digital infrastructure, socioeconomic activities, users; and
- other matters with respect to the use of the metaverse in the forthcoming era.

In November 2022, the “Public-Private Cooperative Council for New Legal Issues Concerning Contents in the Metaverse” was established in the Intellectual Property Strategy Headquarters of the Japanese government. Its activities include:

- understanding and discussing new legal issues;
- examining the establishment of rules through public-private co-operation (including soft law); and
- responding to international rule-making trends.

Close attention should be paid to the issues identified and rules implemented by the Council.

At the private sector level, as in the case of web3, efforts to improve the environment by establishing self-regulatory guidelines by industry associations have been developed. In April 2022, the VIRTUALCITY CONSORTIUM formed mainly by companies operating “Virtual Shibuya”, a

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Hiroya Nadamoto,
Nagashima Ohno & Tsunematsu

metaverse based on a real city, published the “Virtual City Guideline ver1.0”, which provided guidelines for examining issues in developing and operating the metaverse (ver1.5 was published in November 2022). The Guideline refers to the protection of legal rights related to digital objects in the metaverse, as well as various applicable regulations, including data protection/privacy issues. In November 2022, the Japan Digital Space Economy Federation, an industry association regarding the metaverse, published the “Report on the Economic Development of Digital Space”. From the perspective of the three themes (intellectual property, digital finance, and platforms), the report provides:

- an overview of issues;
- explanation of issues;
- direction of discussions; and
- future policies.

The report discusses broadly, for example, the protection of avatars, crypto-assets and NFTs, personal information, security, labour law, gambling and antitrust laws.

Increased Scrutiny on Online Advertising and Social Media

The year 2022 also saw the enhancement of regulations in the fields of online advertising and social media.

Affiliate advertising

On 29 June 2022, the Consumer Affairs Agency revised its guidelines on measures for managing the display of advertisements under the Act against Unjustifiable Premiums and Misleading Representations (the “Premiums and Representations Act”), and the guidelines stipulated the necessary measures for businesses to implement affiliate advertisements (affiliate marketing) through affiliate programmes. In the past, there

was discussion about whether advertisers would be responsible for the representations made by affiliate advertisers in affiliate programmes. However, the revised guidelines clarified that, to the extent that advertisers are involved in the determination of the content of the representation (including cases where the determination is delegated to the affiliate advertiser), the advertisers, not affiliate advertisers, should be viewed as having made the representation themselves. Thus, the advertisers should be responsible for the representations made by affiliate advertisers and must take measures to prevent misleading representations in affiliate advertisements.

Stealth marketing

Currently, Japanese law does not regulate the advertising method of stealth marketing (the act of displaying an advertisement while concealing the fact that it is an advertisement) per se. However, a report published in December 2022 by the research group on stealth marketing established by the Consumer Affairs Agency proposed that the method of stealth marketing itself be generally and comprehensively prohibited, and it is highly likely that such regulations will be introduced in the near future.

Regulation of large digital advertising platforms

The Act on Improving Transparency and Fairness of Digital Platforms (Transparency Act), which came into effect on 1 February 2021, regulates individual platform providers designated by the Minister of METI among digital platforms that meet the requirements for business classification and business scale specified by the relevant cabinet order. In addition to online shopping malls and app stores, digital advertisements were also made subject to the Transparency Act on 1 August 2022. Under the amended cabinet order, integrated media adver-

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Hiroya Nadamoto, Nagashima Ohno & Tsunematsu

tising digital platforms (including search engines, social media, video sharing services) (domestic sales of which are at least JPY100 billion) and advertising intermediary digital platforms (including digital platforms that are intermediaries between publishers with advertising space and advertisers) (domestic sales of which are at least JPY50 billion) were included as regulated platforms. Among advertising platforms that meet the above requirements, those designated by the Minister of METI (currently, Google LLC, Meta Platforms, Inc. and Yahoo Japan Corporation) will be subject to the regulations, including obligations regarding disclosure of information and establishment of relevant systems for various issues in the digital advertising field (eg, issues related to the quality of digital advertising such as ad fraud and the lack of transparency regarding prices and transaction details).

Amendment of Telecommunications Business Act

The amended Telecommunications Business Act, which was enacted on 13 June 2022 and will go into effect on 16 June 2023, included the following amendments.

Under the current law, there is no registration or filing requirement for the provision of internet search services and social media services. Under the amended Act, large-scale internet search service and/or social media service providers that are designated by the Minister of MIC must make a telecommunications business filing and comply with certain regulations under the Act.

Also, the Minister of MIC may designate telecommunications carriers among those providing telecommunications services that have a significant impact on users' benefit. If so designated, such telecommunication carriers should

properly handle specified user information ((i) information that constitutes the secrecy of communications and (ii) information that can identify users), prepare and file its information handling regulations, and prepare and publish its information handling policy.

Further, when certain telecommunications carriers stipulated in the ordinance of the MIC send information about users (such as third-party cookies, tags, and advertising IDs) externally, they must give prior notification to the users of the content of the user information that is to be sent externally and the destination of such information, or place such information in a location so that the users can become aware of the above.

Measures against illegal and harmful information circulating on platforms

Under current law, illegal and harmful information, including defamatory and false information, is regulated under certain general laws such as the Civil Code and the Penal Code. In recent years, however, there has been an increase in the spread of defamatory and false information on social media. In August 2022, MIC issued a research group report discussing measures to address this issue. In this report, it was recommended that a certain level of government involvement should be promptly implemented in measures against illegal and harmful information, such as establishing and requiring compliance with a code of conduct to ensure transparency and accountability of efforts by platform operators and the introduction of a legal framework.

Mobility

Background

In the field of mobility, the government is working with private entities to promote the development of technology, transport infrastructure, and

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Hiroya Nadamoto,
Nagashima Ohno & Tsunematsu

relevant systems. In 2014, the “Public-Private ITS Initiative/Roadmap” was formulated. This is a government-wide strategy for road transport systems using ICT (known as intelligent transport systems – ITS), and automated driving, formulated with the purpose of developing and implementing a strategy through public-private partnership. The Initiative/Roadmap has since been revised each year, and in August 2022 it was succeeded by the policy, “Future of Transportation in Society Utilizing Digital Technology 2022”. In this policy, the scope was extended to the whole mobility field, including not only ITS and automated driving, but also driving assistance, use of road-space, Mobility as a Service (MaaS), drones, and Advanced Air Mobilities (AAM).

Automated driving and MaaS

In recent years, laws and guidelines have been frequently revised in the area of mobility. Regarding automated driving, the Road Traffic Act was amended in April 2022 (scheduled to come into effect in April 2023) and a permit system for Level 4 automated driving was established. The establishment of this permit system enables a high level of automated driving. While in Level 3, people drive in an emergency, in Level 4, automated driving is implemented without human intervention, and the system also safely stops the vehicle in an emergency. Under the “Future of Transportation in Society Utilizing Digital Technology 2022”, the stated goal is to achieve the commercialisation of Level 4 automated driving on expressways and the utilisation of Level 4 automated driving in the provision of logistics services and transportation services to citizens, around 2025. It is expected that legislation will continue to be developed toward these goals.

Rules for new mobility services are also being developed. Based on the recent increasing pop-

ularity of electric kickboards and the development of automated delivery robots for practical use, the amendment of the Road Traffic Act in 2022 stipulates rules for electric kickboards and automated delivery robots.

Drones and AAM

In 2022, important legislative amendments were also made to unmanned aircrafts (UAs) such as drones. First, the amendment to the Civil Aeronautics Act in 2020, which came into effect in June 2022, provides a registration system for UAs. Furthermore, another amendment to the Civil Aeronautics Act in 2021 made it possible (from December 2022) to fly UAs in inhabited districts, such as residential areas, even when the UA is not visible to the operator. This is categorised as Level 4 flight, which allows flight outside the operator’s sight in uninhabited districts. The 2021 amendment:

- established a certification system for UAs;
- established a licensing system for operators to enable this Level 4 flight; and
- reorganised regulations on prohibited air-spaces and operational limitations.

Level 4 drones are expected to be used in a wide range of applications, including the delivery of goods, disaster relief support, and inspection of infrastructure facilities.

Further, discussions regarding aircraft with people on board such as AAM are also being carried out. For example, the discussions involve electric vertical take-off and land aircrafts (eVTOLs), which are electrically powered and are capable of automated operation and vertical takeoff and landing. The goal is to launch commercial services by AAM at the 2025 Osaka Expo. Test flights are being conducted in various locations for this purpose. In March 2022, guidelines for

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Hiroya Nadamoto,
Nagashima Ohno & Tsunematsu

application of the Civil Aeronautics Act for AAM tests were formulated (revised in December 2022). The guidelines clarified permit standards for test flights and published procedures and recommendations for obtaining permits. AAM is expected to be used for services such as logistics, passenger transport and emergency transport in the future.

Legal Tech and Contract Review by AI

Legal tech is gaining popularity as a tool to digitise legal work and make it more efficient. A typical example is services that use AI technology to review contracts and identify any missing provisions. As many as several thousand companies use these kinds of services.

However, in June and October 2022, two companies planning AI contract review services separately made inquiries about the legality of their legal-tech services. In response, the Ministry of Justice (MOJ) expressed the view for each of the above inquiries that the services planned to be provided by the companies may be illegal. Specifically, MOJ stated that the services may violate Article 72 of the Attorneys Act, which prohibits persons other than attorneys from engaging in legal services for the purpose of earning compensation.

The responses from the MOJ only cover the specific inquiries that were made and do not imply that AI contract review services in general or existing services are illegal. However, there were growing concerns that companies may hesitate to introduce such services, which may impede the growth of the market for AI contract review services.

To address these concerns, in December 2022, the Council for Promotion of Regulatory Reform in the Cabinet Office decided that the MOJ would consider formulating guidelines that introduce specific cases in which AI contract review services are considered legal. Most of the existing services are expected to be treated as legal.

After the responses from the MOJ to the inquiries, the private sector launched a self-regulatory organisation in September 2022 made up of companies providing AI contract review services. This organisation is also working to create voluntary rules to ensure the legality of the services.

JAPAN TRENDS AND DEVELOPMENTS

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Hiroya Nadamoto,
Nagashima Ohno & Tsunematsu

Nagashima Ohno & Tsunematsu is the first integrated full-service law firm in Japan and one of the foremost providers of international and commercial legal services based in Tokyo. The firm's overseas network includes offices in New York, Singapore, Bangkok, Ho Chi Minh City, Hanoi and Shanghai, and collaborative relationships with prominent local law firms throughout Asia and other regions. The firm's TMT practice group is comprised of around 50 lawyers and

legal professionals and represents Japanese major telecom carriers, key TV networks, and many domestic and international internet, social media and gaming companies, not only in transactions but also in disputes, regulatory matters and general corporate matters. Its TMT practice group is well positioned to consistently meet requests from clients to provide advice on business strategies, daily compliance and corporate matters.

Authors



Keiji Tonomura is a partner at Nagashima Ohno & Tsunematsu. His practice focuses on M&A, IP/IT-related transactions, and data security/privacy matters. He has extensive experience

representing global and local clients on complex business transactions as well as regulatory matters, with a particular focus on the TMT sectors, including new business fields such as AI, fintech, healthtech, MaaS, and blockchain/crypto. He served as a member of the Web3.0 Study Group, established by Digital Agency of Japan in 2022. He is a member of Tokyo Dai-ichi Bar Association (from 2007).



Minh Thi Cao Koike is an associate at Nagashima Ohno & Tsunematsu. He advises domestic and foreign tech companies, internet service companies, and

telecommunications companies on technology-related law and privacy regulations, and also has extensive experience in domestic and international M&A transactions involving tech companies. He was admitted to the bar in Japan (Tokyo Dai-ichi Bar Association) in 2010 and in New York in 2017. He co-authored a book on legal tech in 2020.

JAPAN TRENDS AND DEVELOPMENTS

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Hiroya Nadamoto,
Nagashima Ohno & Tsunematsu



Akira Komatsu is an associate at Nagashima Ohno & Tsunematsu. His practice focuses on TMT, especially new business fields such as web3, metaverse and AI. He also has extensive

experience on real estate, sports/entertainment and dispute resolution (including international arbitration). He worked at Mitsui Fudosan Co, Ltd from 2019-21 and Preferred Networks, Inc in 2022. He is a member of Tokyo Dai-ichi Bar Association.



Hiroya Nadamoto is an associate at Nagashima Ohno & Tsunematsu. His practice focuses on M&A and general corporate matters including technology-related matters in the TMT sectors. He is a member of Tokyo Dai-ichi Bar Association.

Nagashima Ohno & Tsunematsu

JP Tower
2-7-2 Marunouchi
Chiyoda-ku
Tokyo 100-7036
Japan

Tel: +81 3 6889 7000
Fax: +81 3 6889 8000
Email: info@noandt.com
Web: www.noandt.com/en/

NAGASHIMA
OHNO &
TSUNEMATSU

MACAU SAR, CHINA

Law and Practice

Contributed by:

Pedro Cortés, Luís Rôlo and Lúcia Sio

Rato, Ling, Lei & Cortés – Advogados (Lektou) see p.265

Contents

1. Metaverse	p.253
1.1 <u>Laws and Regulations</u>	p.253
2. Digital Economy	p.253
2.1 <u>Key Challenges</u>	p.253
3. Cloud and Edge Computing	p.254
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.254
4. Artificial Intelligence and Big Data	p.255
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.255
5. Internet of Things	p.256
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.256
6. Audio-Visual Media Services	p.256
6.1 <u>Requirements and Authorisation Procedures</u>	p.256
7. Telecommunications	p.259
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.259
8. Challenges with Technology Agreements	p.261
8.1 <u>Legal Framework Challenges</u>	p.261
9. Trust Services and Digital Entities	p.263
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.263

1. Metaverse

1.1 Laws and Regulations

There are currently no specific regulations in relation to the metaverse in Macau. However, two of the key legal challenges regarding the metaverse in Macau are the issues of applicable law and personality right of the avatar as virtual identity used in the metaverse.

When a private legal relationship involves more than one legal system, the applicable law can be determined in accordance with the conflict rules stipulated in the Macau Civil Code. The Macau Penal Code also contains provisions that help specify what laws apply when multiple legal systems are involved.

However, the metaverse is not bound by geographical borders, allowing users from different parts of the world to participate simultaneously in a virtual location. In this regard, the laws that govern the actions of the avatars may be questionable if Macau courts are called to interfere. Furthermore, in order to cope with the character of the avatar, legal consequences such as suspending the account of the avatar may need to be regulated.

In addition, uncertainty remains over whether an independent legal personality should be granted to avatars. According to the Macau Civil Code, personality begins when the person is fully born and alive. Thus, the idea of granting legal personality to avatars challenges the concept of legal personality stipulated in the Macau Civil Code.

2. Digital Economy

2.1 Key Challenges

The “distance contract”, one of the common figures in the digital economy, is framed by the Consumer Rights and Interests Protection Law (Law No 9/2021). In accordance with this Law, “distance contract” is defined as the contract concluded between the consumer and the commercial operator, without the simultaneous physical presence of the two, through the exclusive means of distance communication, from the negotiation to the conclusion of the contract, within the remote mode prepared by the trader for the supply of goods or provision of services.

Under the Consumer Rights and Interests Protection Law, special obligations are set out for the commercial operator, for instance, before concluding the distance contract, trade-related information, such as the commercial operator’s identification information, the characteristics of the goods or services, and the way in which consumer complaints are handled by the commercial operator, should be provided to the consumer in a timely, clear, accurate, and understandable manner. The distance contract must contain all the information required by the Consumer Rights and Interests Protection Law, and the contract cannot be altered.

However, there is lack of specific legislation on different aspects of the digital market. One of the key legal challenges is the legislation of the third-party electronic payment platform. Electronic payment is already a very commonly used payment method in Macau; however, there is currently a lack in regulations that specifically address issues like the establishment of third-party electronic payment platforms, oversight of cross-border transactions and cybersecurity in the digital market.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Regulations

The processing of personal data in the Macau Special Administrative Region (MSAR or Macau) is subject to the legal regime of the Personal Data Protection Act (Law No 8/2005, dated 22 August 2005 – PDPA), which defines personal data as “any information of any kind and regardless of the respective format, pertaining to an identified or identifiable natural person”. Sensitive personal data is further defined as “data related to philosophical or political beliefs, membership of a political or trade union association, religious belief, private life and racial or ethnic origin, health and sex life, including genetic data”. With regard to cloud and edge computing, there is currently no specific regulation on this matter in Macau.

The Personal Data Protection Act (PDPA)

The processing of personal data under the PDPA is subject to key mandatory principles, such as transparency, lawful basis for processing (including the strict observance of privacy rights and of the rights, freedoms and guarantees set out by the Macau Basic Law and applicable legislation), collection limited to specified, explicit and legitimate purposes, and proportionality, and may only be carried out if the data subject has given their unequivocal consent or if the processing is necessary for the purposes set out in the law.

The Macau Office for Personal Data Protection (OPDP) must be notified in writing within eight days of the start of any processing of personal data under the PDPA (either wholly or partly executed by automatic means), without prejudice to the cases where prior authorisation must be sought.

Whenever data is retrieved directly from the data subject, the person responsible for processing the data, or their representative, must provide the data subject with the information set out in the PDPA (eg, the identity of the controller and their representative, the purpose of the processing, and other ancillary information), and the documents used to retrieve the personal data must contain such information. Also, in the case of data collection in open networks, the data subject must be informed that their personal data may circulate in the network without security, at the risk of being seen and used by unauthorised third parties.

The Office for Personal Data Protection (OPDP)

In the case of cloud computing, the data is likely to be stored in servers abroad – in the case of the transfer of personal data to a destination outside Macau, the PDPA determines that such transfer can only take place if the provisions of said law are respected and if the legal system of the destination ensures an adequate level of protection. Analysis is made on a case-by-case basis by the OPDP.

The transfer to a legal system which does not ensure an adequate level of protection can be made by notification to the OPDP if the data subject has given their unequivocal consent for the transfer or if the transfer is necessary for the purposes set out in the law. It should be noted, however, that regarding sensitive data as well as credit and solvency, the need for authorisation by the OPDP overrides the simple notification procedure, and the transfer cannot take place without such previous authorisation being obtained.

Regarding specific industries such as banking and finance, the Macau Financial System Legal

Regime (Decree Law No 32/93/M, dated 5 July 1993 – RJSF) stipulates that the members of the governing bodies of credit institutions, their workers, auditors, experts, agents and other persons who provide services to them, whether on a permanent or accidental basis, may not reveal or use, for their own or someone else's benefit, information or knowledge that has come to them from the exercise of their functions, and includes in the information subject to secrecy the names and other data relating to customers, deposit accounts and their movements, investment of funds and other banking transactions. Such duty of secrecy shall survive even after the functions referred to above have ended.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

There is currently no specific legislation on big data and artificial intelligence (AI) in the MSAR. However, the challenges presented by big data (ie, large amounts of data which include traditional enterprise/company data, machine-generated/sensor data and social data) may concern, on the one hand, the type of data being transferred and generally processed in several networks and, on the other, the need to ensure that these networks are secure and compliant with personal data protection and cybersecurity legislation.

Compliance With the PDPA

One of the biggest challenges for entrepreneurs is compliance with the PDPA with regard to the processing of personal data under its mandatory principles, such as transparency, lawful basis for processing (including the strict observance of privacy rights and of the rights, freedoms and

guarantees set out by the Macau Basic Law and applicable legislation), collection limited to specific purposes, and proportionality, and the need to obtain the unequivocal consent of the data subject for the processing (or, alternatively, the need for processing for the purposes set out in the PDPA).

As big data necessarily includes large data sets which are often unorganised and may come from several jurisdictions with different personal data protection requirements, such challenge will force large corporations to have dedicated structures (such as chief data officers and ancillary teams or departments) to ensure that, in the processing of data, there is differentiation between general data and personal data, and that such processing is done in accordance with applicable legislation and the security measures provided therein.

Macau Cybersecurity Law

In relation to the Macau Cybersecurity Law (Law No 13/2019, dated 24 June 2019), which seeks to bolster the protection of computer systems regarding cybercrimes and cybersecurity threats against public and private operators of critical infrastructures (as defined in the law), the dedicated structures referred to in the previous paragraph will also need to comply with the general responsibilities and cybersecurity duties provided therein (namely, organisational duties; procedural, preventive and reactive duties; self-evaluation duties; and co-operation duties).

The list of operators of critical infrastructures is defined by Dispatch of the Chief Executive. Currently, under Dispatch 166/2021, there are 136 such operators, 70 of which belong to the financial sector. As previously indicated, there is currently no specific legislation regarding big data and AI. Although the PDPA includes the

right of the data subject not to be exposed to individual automated decisions, no further stipulations regulate the issue of automated decision-making. In this regard, and without prejudice to the principles and provisos of the law regarding personal data processing, it is incumbent on the local legislature to update the law so as to ensure that AI-driven decision-making is compatible with core legal principles such as transparency, accountability, legality, and protection of fundamental rights.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Restrictions on a Project's Scope

With regard to the internet of things (IoT) projects and the data circulating therein, the main piece of legislation which would restrict the scope of a project in such an area would be the PDPA and its stipulations regarding personal data. The processing of personal data through any such device would necessarily have to comply with the applicable stipulations of the law:

- it must be performed in a transparent manner and in strict observance of privacy rights and of the rights, freedoms and guarantees enshrined in the Macau Basic Law and in applicable legislation; and
- it may only be carried out if the data subject has given their unequivocal consent, or if the processing is necessary for the purposes set out in the law.

Personal v Sensitive Data

As previously indicated (and without prejudice to the cases where prior authorisation must be sought), the processing of personal data is gen-

erally subject to notification to the OPDP, which must be made in writing and within eight days of the start of processing. The processing of sensitive data, on the other hand, is generally forbidden, and can only take place if guarantees of non-discrimination and sufficient security measures (which include the general implementation by the data controller of appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction; accidental loss; unauthorised alteration, dissemination or access; as well as special safety procedures set out in the law) are provided, and in the cases indicated in the law, where the data subject's explicit consent has been obtained. It is also dependent on prior authorisation by the OPDP.

The IoT may also involve the transfer of personal data abroad; in this regard, the PDPA stipulates that the transfer of personal data to a destination outside Macau can only take place if the provisions of the PDPA are respected and if the destination's legal system ensures an adequate level of protection. Said analysis is made on a case-by-case basis by the OPDP. However, the transfer to a legal system which does not ensure an adequate level of protection can be made by notification to the OPDP if the data subject has given their unequivocal consent for the transfer or if the transfer is necessary for the purposes set out in the law.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Broadcasting in the MSAR is framed by Law No 8/89/M, of 4 September 1989, which establishes the legal regime for radio and television broadcasting, with the purposes set out therein. Televi-

sion broadcasting is defined as a public service and is exercised under a concession contract, whereas the activity of sound broadcasting is subject to the licensing regime, the exercise of which depends on the attribution of a licence. Both awards are normally preceded by a public tender.

Radio Broadcasting Concessions

In accordance with Law No 8/89/M, the broadcast of sound/radio is subject to the granting of a licence to operate in the radio-electric public domain spectrum of the MSAR. Sound broadcast radios may be held in the following bands:

- hectometric waves (medium), modulated amplitude – band between 526.5 kHz and 1606.5 kHz; and
- metric waves (very short), modulated frequency – band between 87 MHz and 108 MHz.

In accordance with Law No 8/89/M, the chief executive may also allocate other frequency bands of the broadcasting service which are already available or which, as a consequence of technological development, have been added to the International Frequency Allocation Plan. It appears that, to date, no such other frequencies have been included in regulation.

Regarding the administrative procedures related to radio communication services, Decree-Law No 48/86/M, of 3 November 1986, establishes the rules by which said administrative procedures shall be governed, in particular with regard to:

- the concession, installation and operation of radio communications networks or stations;
- radio operators;
- the approval of radio communications equipment; and

- the commercialisation of radio communications equipment.

The granting of permits for the activity of radio broadcasting under Law No 8/89/M is preceded by a public tender, except when ponderous and duly justified reasons advise a direct award. The radio broadcasting activity can be carried out by any legal person that has its headquarters in Macau and offers guarantees of suitability, technical qualification and financial capacity. The Social Communication Office (*Gabinete de Comunicação Social*) is the competent entity that organises the processes related to the granting of permits, and an application for a permit must be accompanied by the following elements:

- justification note of the request;
- demonstration of the economic and financial viability of the project;
- detailed description of the activity to be carried out, with emphasis on the broadcasting time and the schedule map;
- design of the facilities, including equipment, antennas and studios; and
- statutes of the applicant.

The permit is valid for five years and can be renewed, for equal periods of time, at the request of the respective holder. The attribution and transmission of permits, as well as the respective alterations, renewals or substitutions, in case of loss or unusability, are subject to the payment of fees, determined in the General Table of Fees and Fines Applicable to Radio Services approved by Administrative Regulation No 16/2010, dated 12 July 2010.

Television Broadcasting Concessions

As with radio broadcasting, the granting of television broadcasting concessions under Law No 8/89/M is also preceded by a competitive

bidding process, except when weighted and duly justified reasons advise direct concession. Television broadcasting activity can be granted to any legal person that is incorporated in corporate form and has its headquarters in Macau, for the purpose of exercising the activity to be granted, and offers guarantees of suitability, technical qualification and financial capacity.

The television broadcasting concession contract may authorise the concessionaires to carry out other complementary activities related to the main activity, by themselves or in association with other entities. These activities are those indicated by law, and in exceptional cases, concessionaires may be legal persons of public law or public utility.

Television broadcasting concessions must have a fixed term, to be determined according to the business plan to be developed and the time necessary for the amortisation of the capital invested by the concessionaires, and sub-concession is not allowed. Concessionaires are obliged to fulfil the duties indicated in the law, namely, they are obliged to make the necessary investments to guarantee full coverage, in good technical conditions, of the areas of Macau that are defined in the concession contract, which must establish the amount of investment to be made, the plan and the overall timetable for its implementation.

For the concession, a fee is due, to be determined in the respective contract, without prejudice to any initial grace period established in the contract. Concession contracts may also establish forms of remuneration other than payment in cash, namely, the use of issuance time by grantor.

Furthermore, the licensing regime for satellite television broadcasting activity is regulated by

Decree-Law No 3/98/M, dated 19 January 1998, with regard to:

- installation and operation of satellite television broadcasting telecommunications systems; and
- provision of satellite television broadcasting telecommunications services.

A licence for the installation and operation of the system or for the provision of telecommunications services for satellite television broadcasting may be requested by telecommunications companies with headquarters and a place of effective management in Macau, and which demonstrate technical suitability and adequate economic and financial capacity. The licence is requested through the Macau Post Office, which is the competent entity to organise and instruct the licensing process and analyse the request, and it is assigned by order of the chief executive, who sets out, on a case-by-case basis, the terms and conditions for exercising the activity.

The holder of a licence to exercise the activity of satellite television broadcasting is required to pay the following fees to the Macau Post Office:

- installation and operation of the system – from MOP100,000–1,000,000, depending on the complexity and purpose of the system;
- provision of the service – MOP100,000 for each broadcast programme; and
- an annual operating fee, corresponding to 3% of the respective gross operating revenues from licensed systems or services and subsidiary activities.

Online Video Channels

Online video channels such as YouTube would fall under the scope of Administrative Regulation No 24/2002, of 4 November 2002, which sub-

jects the provision of internet services to prior licensing; however, as previously indicated, the use of such technologies through internet connection by existing duly licensed telecommunications entities should not require any further licensing, without prejudice to the applicable telecoms rules.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The telecommunications sector in Macau is framed by Law No 14/2001, of 20 August 2001 (the “Telecommunications Act”), which defines the basis of the telecommunications policy of the MSAR, as well as the general framework for the establishment, management and operation of telecommunications networks and the provision of telecommunications services. The provisions of said law do not, however, apply to television and sound broadcasting services, terrestrial or satellite, which are subject to specific legislation. Telecommunications under the law is defined as the transmission, emission or reception of symbols, signs, writing, images, sounds or information of any nature by wire, radio, electricity or other electromagnetic systems. The law further determines that the establishment, management and operation of telecommunications networks and the provision of telecommunications services are in the public interest, and can only be pursued by public or private entities duly authorised to that effect under the terms of the applicable regulations.

The Telecommunications Act also stipulates the objectives of such policy, which include:

- to gradually liberalise the installation of public telecommunications networks and the provision of public-use telecommunications services;
- to ensure access to telecommunications by the whole population, at reasonable tariffs and prices, in a non-discriminatory manner and at a level of quality and efficiency that meets their needs, and also their economic and social activities;
- to ensure the existence and availability of the universal telecommunications service;
- to ensure equality and transparency of conditions of competition by promoting the diversification of services in order to increase supply and achieve quality standards compatible with the requirements of users; and
- to ensure the interoperability of public telecommunications networks, as well as the portability of the customer’s number, among others.

It is incumbent upon the government to oversee and supervise telecommunications and the activities of telecommunications operators, without prejudice to the specific competencies of the Macau Post Office.

Licensing of Telecommunications Services

On the licensing of telecommunications services, Administrative Regulation No 32/2000, of 11 September 2000, defines the legal regime for provisional licensing of the activities of public network operators and the provision of telecommunications services for public land mobile use, up to a maximum of three licences, operating in certain frequency bands, and with the adoption of the concepts established by the International Telecommunication Union (ITU). The operation of public telecommunications networks and the provision of telecommunications services for public land mobile use are further defined by the

Administrative Regulation No 7/2002, of 15 April 2002, which establishes that said activities are subject to licensing.

The allocation of licences is subject to a public tender, which can be limited with prior qualification, under the terms of the specific regulation of each tender, to be approved by executive order. The bidding regulation defines the terms of the respective procedure, including any prior qualification, as well as the information set out in the law (which includes the amount and method of providing the provisional bond to guarantee the link assumed with the submission of applications and the obligations inherent to the tender, as well as the final bond). The licensed entities are further subject to the payment of:

- fees for issuing and renewing the licence; and
- annual operating fees, corresponding to a percentage of gross operating revenue from services provided under licensed activities, to be determined by order of the chief executive, to be published in the Official Bulletin.

The fees related to the use of the radio spectrum, on the other hand, are set out in Administrative Regulation No 8/2006, dated 12 June 2006.

Voice-Over-IP and Instant Messaging

On specific technologies such as voice-over-IP and instant messaging, the applicable legislation would be the Administrative Regulation No 24/2002, of 4 November 2002, which subjects the provision of internet services to prior licensing, to be requested from the chief executive by filing an application with the Macau Post Office, signed by a person with the power to bind the applicant, and whose respective signature and the quality thereof must be certified by a notary. The application must contain the following documents:

- proof that the applicant is a commercial company duly incorporated in the MSAR, whose scope of business includes the provision of internet services;
- proof that the applicant has the necessary technical capacity and experience adequate to fulfil the obligations and further specifications of the licence the applicant proposes to obtain, having, namely, a body of qualified personnel for the development of the activity;
- proof that the applicant has adequate financial and economic capacity;
- proof that the applicant has up-to-date and adequate accounting of the analysis required for the project they wish to develop;
- a detailed proposal relating to the operation of the services, presented as a technical plan to be developed, that must contain, namely, the configuration of the technological systems to be used, with reference to access methods and the necessary equipment, as well as planning of the development of the systems and services;
- an economical and financial plan that includes the price system to be adopted;
- the applicant's organisational structure, including the identities and CVs of its main responsible personnel, as well as, where possible, financial statements and audit reports in relation to the accounts of the three prior fiscal years; and
- any other elements that the applicant deems relevant for a decision on its request.

The licence shall specify the applicable fees and their respective payment period. Namely, the provider is subject to licence issuance and renewal rates of MOP2,000, and to an annual operating fee of MOP1,000 from the year after the licence is issued, to be paid during the month of January each year. These fees do not exempt

the service provider from the payment of other fees and taxes that are legally owed.

It should be noted, however, that the use of such technologies through internet connection by existing, duly licensed telecommunications entities should not require any further licensing, without prejudice to the applicable telecoms rules.

RFID Tags

Regarding RFID tags, the Decree-Law No 18/83/M, dated 12 March, subjects the possession of radio equipment that can transmit, receive or transmit/receive, as well as the establishment or use of a radio station or network, to prior government authorisation. However, exceptions to this rule are reduced radio equipment power and short range, included in categories set out in Chief Executive Order No 198/2014, dated 14 July 2014, as well as the receivers of the radio and television broadcasting service. Therefore, RFID tags in the 13.553–13.567 MHz and 920–925 MHz frequency bands, with a maximum equivalent isotropically radiated power (PIRE) of 1 W, are exempt from prior government authorisation.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Legal Framework Features

There are currently no specific stipulations on IT service agreements in Macau, without prejudice to the general stipulations regarding data in general (regulated and protected under the general civil and commercial regime, as indicated here) and the stipulations on personal data protection (set out in the PDPA).

In accordance with the Cybersecurity Law, which established the general structure of the cybersecurity system of the MSAR (as indicated in 5. **Internet of Things**), public and private operators of critical infrastructures defined in the law are subject to the general responsibilities and cybersecurity duties (organisational duties; procedural, preventive and reactive duties; self-evaluation duties; and co-operation duties) set out therein.

The organisational duties of private operators of critical infrastructures, within the scope of their organisation, are to:

- create cybersecurity management units capable of implementing the respective internal protection measures;
- provide cybersecurity management units with the appropriate human, financial, material and patrimonial means;
- designate the main person responsible for cybersecurity and the respective substitute, from among individuals with the proper suitability and professional experience, and with habitual residence in the MSAR;
- make sure that the principal responsible for cybersecurity and their replacement are permanently reachable by the Cybersecurity Incident Alert and Response Centre (CARIC); and
- establish complaints and denunciation mechanisms related to cybersecurity.

The duties of private operators of critical infrastructures, in terms of procedures and prevention and response to cybersecurity incidents, are to:

- establish a cybersecurity management regime and respective internal operating procedures;
- adopt, in accordance with the cybersecurity management regime and applicable technical

standards, internal measures for protection, monitoring, alert and response to cybersecurity incidents;

- inform CARIC of the occurrence of cybersecurity incidents and inform the respective supervisory entity of the fact, as well as immediately initiate actions to respond to serious incidents; and
- monitor and record the health of the network.

The duties of private operators of critical infrastructures, regarding self-assessment and reporting, are to:

- assess, by themselves or through specialised entities, the security and risks existing in their networks and systems; and
- submit an annual cybersecurity report to the respective supervisory entity, mentioning, inter alia, any recorded incidents, the results of the assessment referred to in the previous bullet point and the improvement measures taken.

The duties of private operators of critical infrastructures, as well as their administrators, managers or representatives, with regard to collaboration with CARIC and supervisory entities, are to:

- allow the representatives of those services to enter their premises, provide them with access to their networks and provide them with the information they request, to the extent necessary to verify compliance with the procedural, preventive and reactive duties referred to above; and
- provide the support and collaboration necessary to ensure the good management of cybersecurity.

Therefore, any IT service agreement entered into with a local organisation defined as a private operator of critical infrastructures under the Cybersecurity Law must encompass (and comply with) the duties and responsibilities set out above.

Furthermore, and should the IT service agreement touch upon personal data, it is likely that the local entity shall be either the data controller (understood as the natural or legal person, the public entity, the service or any other body that, individually or together with others, determines the purposes and means of processing of personal data under the PDPA) or a subcontractor/processor (classified in the PDPA as the natural or legal person, the public entity, the service or any other body that processes personal data on behalf of the controller). Processing of personal data is defined by the PDPA as “any operation or set of operations performed upon personal data, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”.

A Local Entity as Data Controller

Should the local entity be the data controller, then it is bound by the obligations set out in the PDPA as indicated above, inter alia, with regard to the need to obtain the unequivocal consent of the data subject and to provide all the necessary information, as well as to ensure that the subcontractor implements the appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular, where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. Such measures must ensure a level

of security appropriate to the risks represented by the processing and the nature of the data to be protected, having regard to the state of the art and the cost of implementation.

A Subcontractor as Data Processor

Where processing of data is carried out on behalf of the data controller (eg, by a local entity), the data controller must choose a subcontractor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing of the data, and must further ensure compliance with those measures. The processing by a subcontractor must be governed by a contract or legal act, binding the subcontractor to the data controller and stipulating in particular that the subcontractor shall act only on instructions from the data controller, and that the obligations set out in the PDPA regarding data security measures shall also be incumbent on the subcontractor. For the purposes of keeping proof, the parties to the contract or the legal act relating to data protection and the requirements relating to the data security measures must be in writing in a document with legally recognised probative value.

In terms of the “electronic signatures”, three types of electronic signatures are distinguished in the Electronic Documents and Signatures Law.

- “Electronic signature” – simply a set of data in electronic form that, linked or logically associated with an electronic document, can be used as a method to make its authorship known.
- “Advanced electronic signature” – electronic signature that is unequivocally linked to the signatory and can be used to verify the signatory’s identity, is created using means that are solely under the signatory’s control, and is so linked to the document to which it is affixed that any changes made after it has been applied are detectable.
- “Qualified electronic signature” – advanced electronic signature based on a qualified certificate, the signature is created through secure signature creation device, and can effectively prevent the signature from being fraudulently used in accordance with internationally recognised standards. Affixing a qualified electronic signature is legally equivalent to an autograph signature.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The Electronic Documents and Signatures Law (Law No 5/2005) establishes the legal framework for electronic documents and signatures, in which “electronic document” is defined as the result of electronic data processing for the purpose of reproducing or representing a person, thing, or fact.

A qualified certificate should be issued by an accredited certification entity. If the certification entities based abroad or the certificates issued by the former are recognised in Macau by virtue of an instrument of international law or regional agreement, or if the certificates satisfy the other requirements specified by the Electronic Documents and Signatures Law, these certificates are equivalent to the qualified certificates issued by the certification entity established in Macau. The information related to these certificates should be disclosed by the means deemed appropriate by the accredited authority of Macau, as well as made available to the interested parties.

Last but not least, the use of electronic signatures may not be feasible when the laws, regulations or conventions regarding the mandatory use of paper or other special forms of submitting, composing, transmitting, or storing documents, in particular with respect to:

- notarial and registration acts;
- procedural acts;
- acts concerning personal legal relationships;
- acts relating to tender procedures; and
- situations in which the physical presence of the signatory or in-person signature recognition is required.

Rato, Ling, Lei & Cortés – Advogados (Lektou) is a Macau SAR-based law firm with more than 35 years' experience of legal practice. Services regularly provided by the firm include advising on Macau law, helping international companies start their businesses in Macau, and assisting in the reorganisation of economic groups with connections to Macau. In 2016, Lektou partnered with Zhong Yin Law Firm (People's Republic of China – PRC) and Fongs (Hong Kong) to open a new office in Hengqin Island, Zhuhai,

PRC – ZLF Law Firm. This was the first law office to unite firms from the two Special Administrative Regions and Mainland China. Since then, it has extended and opened an office in Shenzhen. In 2017, Lektou extended its operations to Lisbon, Portugal, through a locally based law firm, Rato & Cortés, as part of its internationalisation strategy to position itself as a legal player in the platform between the PRC and Portuguese-speaking countries.

Authors



Pedro Cortés is managing partner of Lektou, where he initiated his career as a lawyer in 2003, with experience in gaming, corporate and M&A, capital markets, and banking

and finance. He is admitted to practise law in Macau, Portugal, Brazil (São Paulo), China (as a cross-border Macau lawyer) and in East Timor. He is a member of the International Association of Gaming Advisors (IAGA), the Hong Kong Institute of Directors (HKIoD), International Masters of Gaming Law (IMGL), the International Bar Association (IBA), the Chartered Institute of Arbitrators (CIArb) and the Hong Kong Institute of Arbitrators (HKIA). Pedro is a guest lecturer at the Portuguese Catholic University – Lisbon School of Law, and of the Autónoma Academy in Lisbon.



Luís Rôlo is currently a trainee lawyer with Lektou, having joined the firm in 2020. He graduated from the University of Macau in 2008 and is registered with the Macau Lawyers

Association. His professional background includes being a senior officer at the Macau Pension Fund (1988–99), a senior officer at the Financial Services Bureau (1999–2010), a jurist at the Cabinet of the Commissioner Against Corruption (2010–14) and a jurist at the Office for Personal Data Protection (2014–18).



Lúcia Sio is currently trainee lawyer with Lektou, having joined the firm as a jurist in 2021. She holds a law degree from the University of Macau.

Rato, Ling, Lei & Cortés – Advogados e Notários (Lektou)

Avenida da Amizade, 555
Landmark Office Tower
23rd Floor
Macau SAR

Tel: +853 2856 2322
Fax: +853 2858 0991
Email: mail@lektou.com
Web: www.lektou.com



Law and Practice

Contributed by:

Jessie Tan, Liew Sue Yin and Joel Prashant
Shin Associates see p.287



Contents

1. Metaverse	p.268
1.1 Laws and Regulations	p.268
2. Digital Economy	p.271
2.1 Key Challenges	p.271
3. Cloud and Edge Computing	p.273
3.1 Highly Regulated Industries and Data Protection	p.273
4. Artificial Intelligence and Big Data	p.275
4.1 Liability, Data Protection, IP and Fundamental Rights	p.275
5. Internet of Things	p.277
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection	p.277
6. Audio-Visual Media Services	p.279
6.1 Requirements and Authorisation Procedures	p.279
7. Telecommunications	p.280
7.1 Scope of Regulation and Pre-marketing Requirements	p.280
8. Challenges with Technology Agreements	p.282
8.1 Legal Framework Challenges	p.282
9. Trust Services and Digital Entities	p.284
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes	p.284

1. Metaverse

1.1 Laws and Regulations

Applicable Laws/Regulations/Industry Codes of Conduct

Given the nascent stage of the metaverse, there is no specific regulatory framework that addresses the metaverse at this juncture. Applicable legislation governing certain activities carried out via the metaverse would depend on the technologies employed for operation and the various functionalities arising therefrom.

Applicable key legislation and codes are as follows.

Contracts Act 1950 (CA)

The CA provides that all agreements are contracts if they are entered into with the free consent of contracting parties, for a lawful consideration, with a lawful object, and are not expressly declared void.

A contract is formed under the CA when the traditional essential elements (ie, offer, acceptance, consideration, and intention to create legal relations) are met. No documentary formalities are required thereunder.

With the advent of blockchain and the adoption of smart contracts for transactions within the metaverse, smart contracts and other metaverse-based contracts may potentially be enforceable under the CA if said elements are satisfied and there are no vitiating factors (eg, coercion, misrepresentation, undue influence, illegality, fraud) rendering the contracts void/voidable.

Electronic Commerce Act 2006 (ECA)

The ECA recognises the formation of contracts by way of information exchanged in the form of

“electronic messages”, which is broadly defined under the ECA and could extend to information exchanged via the metaverse.

Such contracts are legally valid, binding, and enforceable against the contracting parties (see **9.1 Trust Services and Electronic Signatures** (Electronic signatures)), subject to formalities required under other written laws.

Personal Data Protection Act 2010 (PDPA)

The PDPA and its subsidiary legislation regulate the processing of personal data (PD) and apply to anyone who processes and controls or authorises the processing of PD in commercial transactions.

The PDPA establishes seven principles (PDP Principles) that a data user (DU) (distinguished from data processors (DP) under the PDPA) must comply with when processing PD.

- General Principle – consent for processing a data subject’s (DS) PD must be obtained unless exempted under the PDPA. Such processing must be for lawful purposes directly related to or necessary for the DU’s intended activity and adequate and not excessive for the relevant processing purpose. DUs must obtain the explicit consent of DSs to process their sensitive PD.
- Notice and Choice Principle – written privacy notices incorporating relevant information required by the PDPA must be made available to DSs by DUs. In January 2022, the Personal Data Protection Commissioner (PDPC) issued a Guide to Prepare Personal Data Protection Notices to aid DUs in the preparation of privacy notices.
- Disclosure Principle – disclosure of PD without the DS’s consent is prohibited, except for such purposes and to such parties identified

in the DU's privacy notice or as exempted by the PDPA.

- Security Principle – DUs must take practical steps to protect PD from loss, misuse, modification, unauthorised/accidental access or disclosure, alteration or destruction.
- Retention Principle – DUs may only retain PD for as long as is necessary to fulfil the purpose of processing and must thereafter destroy the PD.
- Data Integrity Principle – DUs must take reasonable steps to ensure that the PD is accurate, complete, not misleading and up to date.
- Access Principle – DSs have the right to request access to their PD and to correct any inaccurate, incomplete, misleading, or outdated PD.

DUs are prohibited from transferring PD extra-territorially unless sent to a permitted place (although such permitted places are yet to be confirmed, a proposed list has been issued) or if other exceptions apply.

DUs must have adequate security and indemnity measures to inhibit theft, loss, misuse, unauthorised/accidental access or disclosure, alteration, or destruction of PD under their care and must ensure that any DPs they use also take reasonable steps to employ such measures and provide sufficient guarantees.

Where a person is established locally and processes PD (directly or indirectly) or is not established locally but uses locally-based equipment to process PD (other than for transit purposes), compliance with the PDPA is necessary. Vis-à-vis the metaverse's global coverage, potential challenges may arise in applying the PDPA to global DUs due to the "establishment" and "transit" criteria above.

Content Code 2022 (Content Code)

The Communications and Multimedia Content Forum, established by the Malaysian Communications and Multimedia Commission (MCMC), introduced the Content Code as an industry self-regulatory guideline to identify objectionable content and provide for content requirements based on local social, cultural, and religious values. The MCMC can direct anyone to comply with the Content Code. Failure to comply with this directive may result in a fine of up to MYR200,000. Users who publish content in the metaverse may draw the applicability of the Content Code towards such publishing activities.

The Content Code focuses on regulating advertisements to increase consumer protection. The Content Code regulates advertisement claims, testimonials, and pricing information. Material information must not be omitted or presented in a misleading way and content that could offend any group is prohibited. The Content Code also addresses advertising content on religion, the rights of children and disabled persons, advertisements by gambling/betting companies, and reports on sensitive issues such as suicide.

"Virtual influencers" are recognised in the Content Code and defined as computer-generated characters or avatars with realistic characteristics, features, and personalities that behave similarly to human influencers. Users acting as "virtual influencers" would also need to disclose paid advertisements to avoid misleading customers.

While the MCMC has jurisdiction over locally-based individuals and entities, prosecution and enforcement against extraterritorial offenders are significantly limited, with the MCMC only being able to block offensive content from extra-

territorial offenders from being accessed within Malaysia.

Other legislation

The legislation in **2.1 Digital Economy** (Applicable Laws/Regulations/Industry Codes of Conduct) could apply to transactions within the metaverse, subject to jurisdictional considerations and relevant coverage elements therein.

Key Legal Challenges

Jurisdiction

Presently, no legislative provisions address cross-border jurisdictional issues concerning the metaverse.

Access to the metaverse would generally be governed by terms of use and/or end-user licence agreements (collectively EULAs) between end users and the platform operators who provide access thereto. In such instances, the governing law of the EULAs could ascertain applicable jurisdiction vis-à-vis end-users' conduct in relation to the EULAs.

In-metaverse jurisdiction is a grey area. Arguably, if there are contractual terms and conditions within the metaverse which stipulate the governing law of a particular real-world territory, then the applicable courts may apply relevant real-world laws in relation to contractual issues pertaining to the same.

Where cybercrimes are concerned, it remains to be seen whether any real-world prosecution and enforcement may be commenced and sustained. The legislative framework for cybercrimes is mainly governed by the Computer Crimes Act 1997 (CCA) and supplemented by other legislation. The CCA has effect within and outside the country, regardless of the nationality or citizenship of the offenders. However, the CCA has yet

to be revised to consider the rapid development of the metaverse and ancillary legal issues.

Anti-money laundering

In-metaverse transactions typically involve the usage of cryptocurrencies and Non-Fungible Tokens (NFTs) as the form of consideration. NFTs are digital assets with unique identifiers that can be traded and sold.

Following the issuance of the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (Prescription Order) and the Guidelines on Recognised Markets 2019 (GRM) by the Securities Commission (SC), NFTs could potentially fall within the purview of the SC and be subject to anti-money laundering/counter-financing of terrorism (AMLCFT) controls. However, there are significant challenges in enforcing AMLCFT oversight over transactions within the metaverse due to the layers of identity protection and anonymity afforded to users, which hinders the ability of institutions with AMLCFT reporting obligations to effectively police transactions within the metaverse.

Intellectual property (IP)

There are several potential IP risks in the metaverse, including copyright infringement, trade mark infringement, and patent infringement. These may be difficult to ascertain and prosecute due to the anonymity of individuals within the metaverse.

Additionally, there may be issues with counterfeit NFTs, patent infringement in technology development, and trade secret misappropriation.

Risks of trade mark infringement may also arise in virtual transactions, and proactive trade mark registration may help to guard against such risks.

The metaverse comprises interconnected online networks and services, which may have host servers outside the jurisdiction where infringement occurs, making enforcement difficult. This may be further complicated by the disparities in legislation and practices in different jurisdictions. For instance, IP enforcement may need to be done via administrative procedures in some jurisdictions, whereas in others, such as Malaysia, court injunctions are more commonly used.

Data protection

Data protection is another primary concern. Organisations that operate the metaverse can use augmented reality/virtual reality technologies and devices that collect an immense amount of information, including a wide range of PD. This could lead to novel data privacy issues for users due to the collected information's scope, scale, and sensitivity. DUs or third parties could misuse these various categories of data.

A significant gap in enforcement arises where PD is processed extraterritorially via the metaverse due to the limited applicability of the PDPA, see **1.1 Laws and Regulation** (Personal Data Protection Act 2010 (PDPA)).

2. Digital Economy

2.1 Key Challenges

Applicable Laws/Regulations/Industry Codes of Conduct

No single piece of legislation explicitly governs the digital economy. There are, however, laws, regulations, and industry codes of conduct of general application to the digital economy, including the following.

- The Communications and Multimedia Act 1998 (CMA) regulates the communications

and multimedia industry, including applications service providers (ie, providers of applications services that deliver specific functions such as voice services, data services, internet access, and electronic commerce to end-users) (ASPs) and content applications service providers (ie, a subset of ASPs that provide content, such as television and radio broadcast services, and the provisioning of information services) (CASPs).

- The CCA, see **1.1 Laws and Regulation** (Jurisdiction).
- The Consumer Protection Act 1999 (CPA) applies to all goods and services offered to consumers in trade (including via electronic trade transactions) which are primarily purchased, used, or consumed for personal, domestic or household purposes.
- The Digital Signature Act 1997 (DSA), see **9.1 Trust Services and Electronic Signatures** (Digital signatures).
- The ECA, see **9.1 Trust Services and Electronic Signatures** (Electronic signatures).
- The Electronic Government Activities Act 2007 imposes analogous regulations to the public sector as the ECA.
- The Financial Services Act 2013 (FSA) and Islamic Financial Services Act 2013 recognise electronic money as a payment instrument.
- The PDPA, see **1.1 Laws and Regulation** (Personal Data Protection Act 2010 (PDPA)).
- The Price Control and Anti-Profiteering Act 2011 generally addresses price display and product labelling.
- The Sale of Goods Act 1957 (SGA) governs contracts for the sale of goods.
- The Trade Descriptions Act 2011 outlaws fraudulent trade descriptions and false or misleading statements, conduct, and practices concerning the supply of goods or services (including through electronic means).

- The Capital Markets and Services Act 2007 governs the adoption and use of digital currencies and digital tokens which satisfy elements to be deemed as “securities” by virtue of the Prescription Order, and regulates Digital Asset Exchange (DAX) operators.
- The Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 governs reporting obligations for entities carrying out prescribed activities which could broadly cover various digital economy elements, particularly where the use of digital currencies is concerned.
- The Interoperable Credit Transfer Framework (ICTF) is a policy document issued by the Central Bank of Malaysia (BNM) under the FSA which requires registered merchant acquirers (RMAs) to ensure that any inter-bank credit transfer transactions are processed locally through an operator of shared payment infrastructure. The ICTF also prescribes steps to be taken by RMAs concerning credit transfer services offered to its customers.
- The Content Code, see **1.1 Laws and Regulation** (Content Code 2022 (Content Code)).
- The General Consumer Code of Practice for the Communications and Multimedia Industry (Consumer Code), see **7.1 Scope of Regulation and Pre-marketing Requirements** (Local Regulatory Coverage of Technologies and Services).
- The Digital Economy Blueprint, launched in 2021, has identified the need to review and amend laws on IP, competition, and internet infrastructure, among other areas.

Key Legal Challenges

Regulatory requirements to conduct business can be challenging for digital businesses operating within the digital economy. Entities engaging in commerce that intend to establish a local

corporate presence must apply for licences and registrations with various authorities to conduct business. Licensing and registration conditions or restrictions may also be imposed. These often come with lengthy application processes and, where applicable, strict compliance with directorship and equity stipulations by the relevant authorities.

The slowness of regulatory clock speeds may hinder novel digital economy developments where no governing regulatory frameworks are in place.

While cryptocurrencies are unregulated and not considered legal tender, cryptocurrency exchanges are regulated under the Guidelines on Prevention of Money Laundering and Terrorism Financing for Capital Market Intermediaries 2014 and the GRM. To operate, these exchanges must register with the SC. Once registered, cryptocurrency exchanges must abide by a set of AMLCFT obligations, which include implementing suitable customer due diligence measures and reporting suspicious customer transactions to the SC. The SC has also warned investors about the potential risks involved in initial coin offerings (ICOs), including limited legal protection and high exposure to fraud, money laundering, and terrorism financing. The recent scandal involving the FTX cryptocurrency exchange (FTX Scandal) has revealed various risks of hacking and fraud associated with such exchanges. In the wake of the FTX Scandal and with neighbouring country Singapore in the midst of tightening rules around retail investment in cryptocurrencies, it is expected that Malaysia will likely also follow suit with additional regulatory oversight to prevent similar incidents from happening in the future.

While cybercrimes have seen an uptick in recent years due to increased digital economy participation and technological developments, enforcement of the same remains challenging due to the speed at which cybercrimes have been developing and the lack of regulatory updates to keep pace.

Electronic transactions are often subject to the threat of fraud as credit card and payment account details and other pieces of information are typically required for online transactions. Ensuring secure networks and systems and developing security solutions to prevent exposure of customers' PD to malicious third parties in compliance with the PDPA and other applicable legislation, such as the European General Data Protection Regulation (GDPR), can be challenging. The PDPA is currently more limited in scope than data protection laws of other jurisdictions, such as the GDPR, and has gaps in data protection coverage.

The Malaysia Digital Economy Corporation (MDEC), an agency under the Ministry of Communications and Digital, is expected to launch its ESG framework for the digital economy ecosystem by the second quarter of 2023, in view of their aspirations to achieve a target of MYR49 billion worth of digital investments in the country by 2025. The MDEC has indicated that the framework will be based on the United Nations Global Compact (UNGC) standard.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Applicable Laws/Regulations/Industry Codes of Conduct

CMA

Cloud service providers (CSPs) are subject to the CMA. Effective 1 January 2022, CSPs must obtain an ASP Class (ASP(C)) licence with annual renewal requirements. The provision of cloud services without a licence is an offence and is punishable upon conviction with a fine not exceeding MYR100,000 and/or imprisonment for a term not exceeding two years.

Organisations or parties using cloud services (CSSs) may be subject to technical codes and guidelines, such as the Technical Code on Information and Network Security – Cloud Service Provider Selection, which specifies requirements for selecting a CSP. The CSS must conduct a risk assessment and select a CSP based on risk tolerance, industry standards, and the CSP's ability to provide certification and a third-party audit report. It also requires CSSs to collaborate with CSPs to ensure the safety and security of cloud services and to enter into formal agreements outlining responsibilities in the event of security incidents. These agreements must be comprehensible, harmless to the organisation, and include specific provisions for service delivery, availability, indemnification, and protection of IP rights. The CSS should also confirm that the CSP is certified or adheres to industry best practices.

PDPA

The PDPA contains obligations that must be adhered to where PD is processed through cloud services. See **1.1 Laws and Regulations (Per-**

sonal Data Protection Act 2010 (PDPA)) for an overview of obligations under the PDPA.

The Personal Data Protection Standard 2015 (PDP Standard) requires DUs to ensure that transfers of PD through cloud computing services are recorded and that written consent from an officer authorised by the DU organisation's top management is obtained before any transfer is made.

PD transferred through a cloud computing service must comply with the PDPA and PD protection laws of other countries.

The PDPA does not contain direct obligations on DPs, and there is no requirement for data localisation, but there have been discussions by way of a public consultation paper suggesting implementation in future.

Regulated Industry Restrictions

Financial institutions (FIs) face the highest level of regulatory oversight vis-à-vis the use of cloud services by virtue of policy documents issued by BNM requiring mandatory compliance. Additionally, various industry-specific codes of practice have been issued under the PDPA, which prescribe bespoke requirements for applicable industries. Below is a brief outline of said industry-specific regulatory requirements for the use of cloud services.

FIs

The BNM has issued several policy documents that contain specific requirements related to the use of cloud services by FIs. These policies require FIs to consult with the BNM before using a public cloud for critical systems and to notify the BNM before using cloud services for non-critical systems.

The Policy Document on Outsourcing also requires FIs to obtain the BNM's approval before entering into an outsourcing arrangement, including arrangements with CSPs, and to maintain a register containing details of the data held and the locations in which it is stored.

The Policy Document on Management of Customer Information and Permitted Disclosures also includes requirements for FIs in handling customer information throughout the information lifecycle, covering collection, storage, use, transmission, sharing, disclosure, and disposal.

FIs must also ensure that the service-level agreement with the CSP adequately reflects the FI's obligation to safeguard customer information.

Private hospitals

If PD is stored via cloud storage, then secure encrypted communications protocols must be implemented when transmitting and retrieving PD from such locations. The choice of the CSP and communication protocols must also be secure.

Where a DP processes PD on behalf of a DU, the DU shall ensure that:

- sufficient guarantees are provided by the DP for technical and organisational security measures; and
- the DP complies with such measures by taking reasonable steps.

DUs should take several steps before engaging a DP, such as conducting a pre-agreement vetting of the DP to ensure that it has adequate policies and procedures in place to keep PD secure, stringent access controls, secure premises, back-up protocols, and technical and electronic safeguards to protect PD.

The DU should also enter into a formal agreement with the DP that covers non-disclosure provisions, current anti-virus and firewall software, the right to audit security systems, inspect policies, encryption in all transmissions, back-up and restoration functions, the right to claim compensation for loss of PD, and an obligation to report data breaches within an hour of becoming aware of a breach.

Aviation sector

DUs should ensure that they have obtained the written consent of their top management to transfer PD via cloud computing services.

In December 2022, the PDPC issued the General Code of Practice of Personal Data Protection, applicable to classes of DUs who do not have existing PD codes of practice. It places the same obligations in this section.

Personal Data Processing Issues (Cloud Computing Context)

Presently, the PDPA only places PD protection obligations on DUs, as opposed to DPs who are not subject to similar requirements. See **1.1 Laws and Regulations** (Personal Data Protection Act 2010 (PDPA)) for an overview of obligations under the PDPA.

As there is a gap in legislative oversight on DPs at this juncture, PDPA breaches by DPs are not strictly actionable against the DPs themselves, which brings about difficulties in enforcement efforts.

The government is considering amendments to the PDPA to extend its applicability to DPs, to better align with international data protection legislation. However, these proposed amendments have yet to be legislated at the time of writing and regulatory initiatives to pursue cohe-

sive reforms to the PDPA are exceedingly slow, notwithstanding that numerous instances of data breaches have taken place since its inception in 2010. It has been reported, which took place in that from 2017. to date, 25 companies have been imposed with fines or penalties under the PDPA. Malaysian courts have, however, also decided on various aspects of the PDPA. Notably, in the landmark case of *Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors* (2022) 11 MLJ 898, the Court determined that the provisions of the Income Tax Act 1967 cannot be used to override protections offered under the PDPA to undertake a fishing expedition for the PD of a business's customers.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Applicable Laws/Regulations/Industry Codes of Conduct

Although no statute directly addresses the use of artificial intelligence systems/technologies (AI) and big data, legislation and industry codes of conduct of general application may apply to various facets of AI and big data usage. These include but are not limited to the law of torts, the CPA, the PDPA, the SGA, and the CA, as further described in **4.1 Liability, Data Protection, IP and Fundamental Rights** (Relevant Elements).

The government is attempting to enhance existing legislation and formulate a national framework to regulate such technologies, which includes the following initiatives.

The National Artificial Intelligence Roadmap was created through collaboration between the government and various stakeholders and covers

the period from 2021-25. It includes initiatives such as developing an AI Governance Framework, implementing a cybersecurity policy, collaborating with industries to establish privacy, security, and ethics guidelines, and creating an AI Code of Ethics.

The MDEC is tasked with spearheading the National Big Data Analytics Framework, which aims to establish a national big data analytics ecosystem for economic growth across all industries. The MDEC is also developing a national AI framework. The MCMC has previously stated that the government is considering adopting a national data-sharing and AI policy.

Relevant Elements

Liability

AI-enabled software would be treated similarly to other consumer products. AI malfunctions would be addressed under the SGA, the CPA and tort law, which address product safety and consumer protection. The SGA and CPA contain implied terms such as guarantees and conditions regarding title, quality, fitness for purpose, price, and repairs that cannot be contractually excluded. The manufacturer or supplier of AI software would be liable for malfunctions arising from breaches of these implied terms, depending on the extent of non-compliance with representations and guarantees made to the supplier and consumer regarding the software.

The CA, which addresses the rights and liabilities of contracting parties, would be relevant in evaluating liability for AI malfunctions. Contractual provisions for AI usage may be incorporated to apportion liability for AI malfunctions.

Data protection

Big data analytics and AI collect and analyse vast volumes of data, which may raise concerns

about the consent of DSs. Larger data sets are susceptible to significant breaches, which can lead to unauthorised access and disclosure of significant amounts of PD. Adequate security measures, such as those outlined in the PDPA and the PDP Standard, would be essential.

Data protection issues relating to big data analytics and AI can also be extended to other PDP Principles, such as PD being kept for longer than necessary or disclosed to parties unknown to the DS and without the DS's consent, see **1.1 Laws and Regulations** (Personal Data Protection Act 2010 (PDPA)).

The machine learning (ML) subset of AI requires large amounts of data for AI training and operation and triggers the applicability of the PDPA where PD is involved. With the growing use of data analytics, big data and the IoT, adherence to the PDPA is critical when individuals can be identified from the data exchanged or processed. This can be challenging as a DS's written consent is required for processing PD and automated ML systems could fail to consider such consent requirements before processing the data.

IP

Whether the current IP regulatory regime extends protection to AI-generated IP is questionable.

For example, while the term "inventor" is not defined in patent legislation, the language adopted in the Patents Regulations 1986 (Patents Regulations) and the Patents Act 1983 (PA) indicates that AI may be excluded from coverage thereunder. According to the Patents Regulations, patent applications must include personal identification of the inventors, or signed written declarations where anonymity is sought. The implication here is that the inventors must be

natural persons. Various jurisdictions such as the United Kingdom, the European Union, Australia, and Germany have refrained from allowing patent applications where humans are not listed as inventors. The United States case of *Thaler v Vidal*, No 21-2347 (Fed Cir 2022) elucidated that inventors in patent applications must be limited to natural persons. It is anticipated that a similar position may be adopted locally due to similarities in such formalities.

There is also uncertainty as to whether the Copyright Act 1987 (Copyright Act) affords protection to AI-created works. Potential issues on copyright ownership, potential perpetual subsistence of copyright in AI-created works, the accordance of moral rights towards AI, and whether enforcement of copyright protection is available for AI-created works is a grey area considering that the nomenclature adopted in the Copyright Act appears only to encompass rights of natural and legal persons. Local courts have yet to take a stance on whether AI-created works are eligible for copyright protection. However, case law from other jurisdictions may be persuasive. For example, in Australia, the case of *Acohs Pty Ltd v Ucorp Pty Ltd* (2012) FCAFC 16 determined that works created with the aid of a computer are not protected under copyright laws as they are not considered to have been created by a human. The Court of Justice of the European Union has consistently stated that copyright applies only to original works that are the product of the author's own intellectual creation and reflect the author's personality, implying that a human author is necessary for a work to be eligible for copyright protection, as seen in the case of *C-5/08 Infopaq International A/S v Danske Dagbaldes Forening*.

Presently, if an AI is tasked with creating content and incorporates third-party works protected by

copyright in such content without authorisation, the creator of the AI would appear to be liable for such infringement under the SGA, CPA, CA, and tort law, subject to any contractual provisions addressing liability between the creator and the user of the AI for such infringement caused by the AI.

Fundamental rights

With the rapid advancement of AI, AI may no longer be a mere product but one capable of human mimicry, consciousness, personhood, authorship, and autonomy. Myriad issues regarding whether AI should be granted rights in connection with these types of capacity and the potential resulting ramifications are bound to arise and have not yet been legislatively addressed.

The European Data Protection Supervisor recently published an opinion on 13 October 2022 about the need for a Council of Europe convention on AI, human rights, democracy and the rule of law. The opinion includes recommendations such as prohibiting AI that poses unacceptable risks to individuals, monitoring the usage of AI and implementing compliance and control mechanisms from a cross-border co-operative perspective. Similar proposals have yet to be proposed or implemented in the local context.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Applicable Laws/Regulations/Industry Codes of Conduct

Existing sector-specific guidelines address the IoT and additional laws may have general appli-

cation towards IoT projects notwithstanding the lack of specific legislation. Examples of such laws, regulations and guidelines are as follows.

CMA

The licensing and regulatory framework under the CMA, including spectrum usage requirements, must be adhered to by parties implementing IoT projects in the telecommunications sector.

A licence would be required if the IoT project involves licensable activities under the CMA, see **6.1 Requirements and Authorisation Procedure** (Applicable Procedures) and **7.1 Scope of Regulation and Pre-marketing Requirements**.

If an IoT project involves spectrum usage, it would be subject to authorisation by the MCMC and would need to conform with the Spectrum Plan, and any related Standard Radio System Plans issued by the MCMC. Communications equipment used for IoT would need appropriate product certification from the relevant certifying organisation appointed by the MCMC and SIRIM QAS International Sdn Bhd, which certifies equipment for safety and compliance with set technical standards.

Various technical codes related to the IoT have been established to provide guidelines and requirements for the secure and efficient use of IoT technology, including codes on IoT application security requirements, high-level functional architecture, security management, and short-range device specifications. Additionally, other relevant technical codes are pending registration, such as codes on industrial IoT connectivity and communication framework and the IoT interoperability framework.

Where an IoT project involves the processing of PD, compliance with the PDPA is required.

In 2020, CyberSecurity Malaysia, an MCMC-affiliated agency, issued the Guidelines for Secure Internet of Things (IoT Guidelines). The IoT Guidelines detail security requirements and controls that manufacturers, providers, and consumers must implement to have a secure IoT system. These guidelines are non-binding but aim to assist stakeholders by establishing an IoT security framework and outlining existing IoT threats and vulnerabilities.

Relevant Elements

Data protection

Cross-border data flows between IoT devices engaged in machine-to-machine communications are particularly relevant. The PDPA generally prohibits extraterritorial PD transfers subject to certain exceptions, see **1.1 Laws and Regulations** (Personal Data Protection Act 2010 (PDPA)). Of particular relevance would be considerations as to whether the relevant compliance requirements vis-à-vis consent of DSs are obtained for the cross-border transfer of PD via IoT devices.

Communications secrecy

The IoT Guidelines provide security controls for adoption in developing secure IoT systems, including risk mitigation measures pertaining to communications encryption, cloud, authentication, access control, data protection and privacy, operation and maintenance, amongst others.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Main Requirements

A variety of laws govern content. The MCMC is primarily responsible for regulating online and networked content. The Film Censorship Board (FCB) regulates traditional media outlets and content on television and in cinemas. The National Film Development Corporation Malaysia (FINAS) is responsible for regulating film production, distribution, and exhibition activities.

Licensing requirements under the CMA

CASPs are required to obtain a CASP licence unless specifically exempt. Exemptions include providers of “closed” content application services, which are not accessible to the public, and “incidental” content application services, which provide content as an incidental part of the service. Internet content application services such as over-the-top and online video-sharing platforms are also exempt.

CASP licences are issued as individual licences or class licences, see **7.1 Scope of Regulation and Pre-marketing Requirements** (Local Regulatory Coverage of Technologies and Services). CASPs that provide publicly available content of broad appeal, and which can be received by commonly used consumer equipment or have a significant impact on shaping community views, will likely require an individual licence.

Entities involved in traditional broadcasting, such as terrestrial radio broadcasting, satellite broadcasting, terrestrial free-to-air television, and subscription broadcasting, generally require a CASP individual licence. Entities that provide limited content application services are not required to hold individual licences unless

they fall under a class licence. A CASP will be regulated by a class licence if the service is limited to a specific interest group, restricted to a particular geographic area, for distance-learning purposes, or specifically linked or associated with sporting, cultural, or other one-off events.

CASP licences are subject to similar fees and eligibility criteria as telecommunications services under the CMA. Applicable fees and eligibility requirements vary between individual and class licences, see **6.1 Requirements and Authorisation Procedures** (Applicable Procedures) and **7.1 Scope of Regulation and Pre-marketing Requirements** (Market Entry Requirements).

Other licences/approvals

Depending on the facts and circumstances of each particular licence application, additional licensing requirements may apply. For instance, the production, distribution or exhibition of films may necessitate a licence from FINAS. These films may also require the FCB’s approval.

Content requirements and restrictions

Content is subject to various laws depending on its nature. These are mainly:

- the CMA;
- the Content Code;
- the Printing Presses and Publications Act 1984;
- the Sedition Act 1948;
- the Penal Code;
- Shariah law; and
- advertisement laws, codes and guidelines.

The CMA prohibits the publication of content that is indecent, obscene, false, menacing, or offensive in nature, with the intent to annoy, abuse, threaten or harass any person via a content application service. Content that is deemed

sedition will also violate the Sedition Act 1948. Other laws may also apply depending on the specific circumstances, such as the Copyright Act for copyright-infringing content.

The Content Code also applies to audio-visual media services and content platforms, see **1.1 Laws and Regulations** (Content Code 2022 (Content Code)).

Applicable Procedures

Individual licences

Applicants must submit completed forms and an application fee of MYR10,000, along with documents from a checklist provided on the MCMC website. The MCMC may also request additional information or documents. The CMA requires the MCMC to process the application and provide a recommendation to the Minister of Communications and Digital (Minister) within 60 working days. If the Minister agrees with the recommendation, the licence will be granted upon payment of an approval fee of MYR50,000. If the application is rejected or refused, the Minister must inform the applicant in writing and provide the reason for the rejection within 30 working days.

Class licences

Applicants must submit completed forms, a registration fee of MYR2,500, and documents from a checklist provided on the MCMC website. The MCMC may also request additional information or documents. The MCMC will process and register the licence within 14 working days of the applicant providing all relevant and complete information.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Local Regulatory Coverage of Technologies and Services

The CMA and its subsidiary legislation regulate communications networks and services. The regulatory and licensing framework thereunder broadly covers most technological applications, even if there are no specific references to individual applications. Service-specific issues may be addressed through regulations, guidelines, technical codes, and other voluntary codes issued by the MCMC and/or other industry forums.

There are four categories of providers that are required to be licensed under the CMA.

- Network Facilities Providers (NFPs) – Owners or operators of network facilities such as broadband fibre optic cables, satellite earth stations, telecommunications lines and exchanges, radio-communications transmission equipment, mobile communications base stations, and broadcasting transmission towers and equipment.
- Network Services Providers (NSPs) – Providers supplying basic connectivity and bandwidth to support a wide range of applications. Network services enable connectivity or transmission between networks. Typically, an NSP also owns the network facilities. These services, however, may also be provided by a person utilising network facilities owned by another.
- ASPs – See 2.1 Key Challenges (Applicable Laws/Regulations/Industry Codes of Conduct).
- CASPs – See 2.1 Key Challenges (Applicable Laws/Regulations/Industry Codes of Conduct).

CMA licences for licensable activities can be issued as “individual” or “class” licences, except for ASP licences, which are only issued as class licences. An individual licence imposes a high degree of regulatory control, is specific to a person conducting a particular activity, and may include special application conditions. A class licence, on the other hand, is a less restrictive form of regulation designed for easy market access and only requires registration.

The CMA requires all NFPs, NSPs, ASPs and CASPs (save for those who are exempted from licence requirements) to deal with consumers reasonably and adequately address their complaints, or face upon conviction, a fine not exceeding RM20,000 and/or six months imprisonment.

All CMA licensees are bound by the Consumer Code, which provides model procedures for reasonably meeting consumer requirements, handling customer complaints and disputes, using alternative dispute resolution, compensating customers if the Consumer Code is violated, and protecting consumer information, among others.

Consumers of telecommunications services would also be protected under the CPA and the Consumer Protection (Electronic Trade Transactions) Regulations 2012, which impose disclosure requirements on the goods and services offered by a business and the identification details of that business and prohibits businesses from engaging in misleading practices and representations to consumers.

Voice over Internet Protocol (VoIP) and instant messaging may be considered licensable applications services, specifically under the IP telephony and messaging services categories, necessitating an ASP licence. However, this is

still dependent on the specific facts and whether applicable exceptions apply. Presently, VoIP services that operate solely on the internet and messaging services that send and receive communications entirely over the internet do not usually require a licence.

The Communications and Multimedia (Licensing) Regulations 2000 (Licensing Regulations) and the MCMC’s Guideline on the Provisioning of VoIP Services indicates that “the provision of PC to PC based internet telephony is not subject to licensing”.

Spectrum assignment

The usage of spectrum is restricted unless the following are obtained.

- Spectrum assignment (SA) grants the authority to use one or more specified frequency bands for any purpose consistent with the MCMC’s assignment requirements.
- Apparatus assignment (AA) grants the right to utilise the spectrum to operate a network facility of a specified type at a specific frequency and frequency band or bands.
- Class assignment grants the permission to utilise the frequencies for a list of devices, and is valid until cancellation. The use of devices under class assignments are subject to the conditions set forth therein.

If the technology or device falls under any of the schedules in Class Assignment No 1 of 2021, and its use complies with the assignment conditions and requirements therein, no fees or applications will be necessary.

It should be noted that, according to the MCMC’s Licensing Guidebook (Licensing Guidebook), certain types of activities, such as online pub-

lishing and other internet content applications services, are exempt from licence requirements.

The Licensing Regulations provides that an individual or a class licence holder must adhere to certain standard requirements. This includes taking proper and adequate safety measures to protect life and property in relation to all equipment and installations used under the licence, including exposure to electrical emissions or radiation. Additionally, the licence holder must take reasonable precautions to ensure that the charging mechanism used in conjunction with any network facilities and/or services is accurate and reliable.

The CMA and the Licensing Regulations provide for standard conditions that all licence holders must comply with, regardless of whether they have individual or class licences. Compliance with numbering and electronic addressing plans, spectrum plans, consumer codes and content codes are among these conditions.

Market Entry Requirements

Companies that are locally incorporated are eligible to hold an individual licence, while a locally incorporated company, local partnership, local sole proprietorship, or Malaysian resident can hold a class licence.

See **6.1 Requirements and Authorisation Procedures** (Application Procedures) in respect of fees payable for individual and class licences. For spectrum, an SA application may only be submitted to the MCMC after an Applicant Information Package (AIP) is issued. The fees for an AA application include both fixed fees, which are determined by the type of equipment, and variable fees, which are based on the amount of bandwidth used. The application fee is MYR60 per application and the process and associated

fees can be found on MCMC's website and in the Guidelines for Apparatus Assignment.

The Licensing Guidebook provides that certain organisations or persons are not eligible for a class or individual licence. For individual licences, these include foreign companies, individuals or sole proprietorships, partnerships, and other persons as decided by the Minister. For class licences, foreign individuals who are not permanent residents, and foreign companies are not eligible.

The government liberalised the telecommunications services sector in 2012 by permitting up to 100% foreign equity participation for ASPs. However, NSPs and NFPs are restricted to 70% foreign equity participation.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Main Challenges

Some of the main challenges and areas of risk when contracting with local organisations in technology agreements include the following.

Data security

In order to comply with the data security requirements under the PDPA, organisations that engage third-party technology service providers as DPs must include certain security measures in their technology agreements. This may include contractually binding the third party to operate and carry out data processing activities, and addressing relevant warranty and indemnity provisions. The PDP Standard also sets out specific security measures that organisations must comply with when engaging DPs.

Organisations that are not based locally but are considered to be DUs and which use locally-based equipment for processing PD, other than for transit purposes, must also comply with the PDPA, see **1.1 Laws and Regulations** (Personal Data Protection Act 2010 (PDPA)).

Data localisation

There is currently no mandatory rule for data to be stored locally under the PDPA, but specific industries or types of data may have their own localisation requirements.

There are restrictions concerning the cross-border transfer of data, see **1.1 Laws and Regulations** (Personal Data Protection Act 2010 (PDPA)). Organisations must comply with the requirements of the PDPA when transferring PD extraterritorially in technology agreements. The technology service providers should also ensure that the data transfer by the organisation is PDPA-compliant.

IP rights

Patents

Patents protect products or processes resulting from an idea, not the idea itself. Certain types of inventions, such as discoveries, scientific theories, mathematical methods, and methods of doing business, are not eligible for patent protection. Obtaining a software patent is also difficult because it is considered as a set of instructions or method of data processing, which resembles mathematical methods. The PA rules out the patentability of computer software, but the Intellectual Property Corporation of Malaysia (MYIPO) has provided guidance that the product or process of the practical application of software may be patentable if it makes a technical contribution to art.

Copyright

The Copyright Act recognises computer programs as literary works and they are therefore entitled to copyright protection. Copyright is the main form of protection for the rights of the owner of computer programs and software. For a computer program or software to be protected by copyright, it must be original, created by a qualified person, and made or first published in Malaysia. Copyright is automatically conferred on computer programs once the work is created and all statutory requirements are met. No registration is required for copyright protection, but ownership can be difficult to establish in cases of infringement by third parties.

Trade marks

Brands are used by companies to distinguish their software or computer programs from others and as a marketing tool for customers to recognise the products. It is important for technology companies to protect their brands by registering their trade marks, as consumers perceive trade marks as an indicator of a product's source. While registration of trade marks is not mandatory, it provides proprietors with the right to sue for trade mark infringement and for passing off under common law. The proprietor can apply to the Registrar to register the trade mark in the manner prescribed by the trade marks Act 2019. Once the Registrar approves the application and there is no opposition, the trade mark will be registered. Registration is considered prima facie evidence of trade mark ownership. The period of protection is ten years, which is renewable for another ten years. Foreign applicants will have to file through registered trade mark agents, while local applicants can file on their own.

Layout design of an integrated circuit

The Layout-Designs of Integrated Circuits Act 2000 (LDICA) ensures comprehensive protec-

tion for layout-designs. To be eligible for protection, the layout-design must be an original work resulting from the creator's own intellectual effort and not commonly used among creators and manufacturers of integrated circuits, the right-holder must be a qualifying person at the time of creation, and the layout-design must be fixed in a material form or incorporated into an integrated circuit. Protection is automatically granted to the creator once the layout-design is created and all statutory requirements are met. Owners can submit an affidavit to assert ownership and enforce rights under the LDICA. The duration of protection is ten years from the date of commercial exploitation or 15 years from the date of creation if not commercially used.

Specific Local Legal Framework Features

Data storage

There are no restrictions on specific data storage locations under the PDPA. However, the PDPA generally prohibits the transfer of data extraterritorially unless the exceptions thereunder apply, see **1.1 Laws and Regulations** (Personal Data Protection Act 2010 (PDPA)).

Price revision restrictions

Price revision restrictions for technology agreements vary depending on the specific agreement and industry. Generally, the government may place restrictions on price revisions to protect consumers and prevent monopolies.

Excluded rules

No legislation excludes applicability to technology agreements specifically.

Mandatory laws

While there are no mandatory laws for technology agreements specifically, such agreements would need to comply with legislation of broad application, eg, the legislation outlined in **2.1**

Key Challenges (Applicable Laws/Regulations/Industry Codes of Conduct), where applicable.

Regulated Industry Restrictions

There may be other requirements or considerations depending on the particular facts. When entering into a technology service agreement with an organisation in a regulated industry, additional regulations or guidelines may apply to the organisation, such as those set out by the BNM for FIs, which include specific requirements for engaging third-party service providers.

When an external service provider handles a FI's information technology system, the FI must ensure (including via contractual arrangements) that the service provider will notify the FI in advance of any changes that could affect the system.

FIs must have a service-level agreement in place and may be required to include specific provisions in their contracts with a service provider. Additionally, some contracts may need to be approved by the BNM based on the guidelines set out in the BNM's Outsourcing and Management of Customer Information and Permitted Disclosures Guidelines.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes **Applicable Laws/Regulations/Industry Codes of Conduct**

Trust services

The government launched the Government Public Key Infrastructure Services (GPKI) project to centralise digital certificate management across all government institutions and to secure and

expedite online transactions for e-government services. The GPKI is a security service that uses digital certificates that comply with the DSA and the Digital Signature Regulations 1998 (DSR).

The GPKI consists of hardware, software, people, policies, and processes to maintain security and usually requires enabling at the user's end via Public Key Infrastructure (PKI) services, which can be delivered through various methods, such as Application Programming Interface (API). PKI services have three essential security criteria:

- identity verification (authentication);
- data encryption; and
- digital signature.

The e-filing system of the Malaysian Courts (*ekahakiman*) is an example of an application that uses GPKI for the authentication and filing of court documents for legal proceedings.

The GPKI is a mandatory ICT security service that enhances the data and information security for government ICT applications in accordance with the DSA and DSR. Government personnel who use GPKI services can use the GPKI Portal for centralised digital certificate application and maintenance.

Electronic signatures

The ECA applies to any commercial transaction concluded through electronic means, and states that information in electronic form, wholly or in part, will not be deprived of legal effect, validity, or enforceability solely because it is in electronic form.

Traditional “wet-ink” signatures are not required for contracts to be valid and enforceable. The ECA acknowledges that the communication of

proposals, acceptance of proposals, and revocation of proposals may be conveyed in an electronic message.

The ECA also recognises that electronic signatures may be used to form a legally binding contract and defines an “electronic signature” as “any letter, character, number, sound or any other symbol or any combination thereof created in an electronic form adopted by a person as a signature”.

A document in electronic form will be validly executed if it bears an electronic signature that adequately identifies and demonstrates the signer's approval and is “as reliable as is appropriate” for the purpose for which it is required. The signature will be considered “as reliable as is appropriate” if the mechanism of establishing the signature is linked to and controlled by that person alone and any alteration made to the signature or document after the time of signing is discernible.

The ECA does not apply to:

- powers of attorney;
- creation of wills and codicils; and
- creation of trusts and negotiable instruments.

For such documents to be legal and enforceable, additional formal criteria such as notarisation or attestation may apply.

Digital signatures

Digital signatures may also be used as electronic signatures. This is expressly provided for in the ECA and regulated by the DSA.

A digital signature is formed by procuring a digital certificate from a licensed certification authority (LCA) and is created by matching/pair-

ing two keys (commonly referred to as a “public” key and a “private” key). Before obtaining such a certificate, the LCA will verify the applicant’s identity and is responsible for certifying the identity of the signer who holds the digital certificate.

Under the DSA, a digital signature is legitimate if it is verified by a public key listed in a valid certificate, the signatory intended to attach the digital signature, and the recipient has no knowledge or notice that the signer has breached their obligation as a certificate holder or is not the proper person to attach the digital signature.

Where the recipient has reservations about the legitimacy of the signer, the recipient must promptly notify the signer of their decision not to rely on the signature and the reasonings for doing so.

Provided that the requirements above are fulfilled, a document will be considered valid and effective as if it were written on paper if:

- it bears in its entirety a digital signature; and
- the digital signature is verified by the public key listed in a certificate issued by an LCA and valid at the time of creation.

Relevant Elements

Differences between electronic signatures and digital signatures

While both an electronic signature and a digital signature allow for the electronic execution of documents, they differ in several respects. Digital signatures are based on a cryptosystem with two keys, public and private keys, and digital signature certificates are issued by the respec-

tive LCAs. The digital certificates will allow the signer to validate their identity or right to access information or services online, as the LCAs will carry out identity verification before issuing the certificate. Accordingly, using a digital signature would be more secure and would also assure customers that the businesses they are dealing with are authentic.

Electronic signatures are less strictly regulated and may be less secure than digital signatures. It should be emphasised that electronic signatures are versatile in that they apply to the signing of documents (where electronic signing is applicable) and to e-commerce transactions. In contrast, digital signatures are employed in transactions based on the needs of the parties involved.

Acceptance requirements of relevant authorities

Although electronic signatures and digital signatures are recognised, certain types of legal documents must be notarised or attested, see **9.1 Trust Services and Electronic Signatures** (Electronic signatures).

Instruments effecting dealings with real property, for example, must be signed using the traditional wet-ink method under the National Land Code. Agreements governed by the Housing Development (Control And Licensing) Act 1966 also require wet-ink signatures unless specifically permitted.

In practice, certain government departments, such as the stamp and land offices, typically only accept documents with wet-ink signatures.

Shin Associates is a full-service boutique law firm providing comprehensive legal advisory services across various practice areas. With a strong focus on Technology, Media, and Telecommunications (TMT), the firm specialises in representing clients on regulatory matters, from the provision of regulatory advice to assisting with compliance protocols and the obtaining of approvals and licences, to advising on data protection issues. The firm is also especially well-versed in all aspects of the media and en-

tertainment industry. Bringing together strong local market expertise and a global perspective through the firm's membership of the Cicero League of International Lawyers, an established network of international independent law firms, the firm has brought valuable insight and foresight to numerous clients across the globe. The firm has also been consistently ranked by Chambers and Partners as a recognised practitioner of the TMT practice sector in Malaysia.

Authors



Jessie Tan heads the firm's TMT practice. Jessie has been involved in Malaysia's creative industry through her involvement in the development of the Film in Malaysia Incentive, provision of

advice on TMT matters, as production attorney to international film and television productions and provision of legal and advisory services to various animation, games, music, and production houses. Jessie also manages the registration of general advisory and drafting work relating to trade mark and copyright matters. Jessie has been recognised as a ranked lawyer by Chambers and Partners in the TMT practice area.



Liew Sue Yin has significant experience in corporate, commercial, litigation, banking and finance, and real estate transactions. She has advised clients in various industry

sectors, including TMT, and has experience drafting contracts and advising on policies, procedures, best practices, and regulatory matters. Her client profile includes publicly listed companies, foreign companies, small and medium-sized enterprises, family-owned businesses, and high-net-worth individuals. She is a founding member of the Malaysia Network of the International Women's Insolvency & Restructuring Confederation (IWIRC) and currently serves as a board member.



Joel Prashant has significant experience in civil litigation, corporate, commercial, TMT, employment, intellectual property, and data protection law. Joel has advised clients on

TMT regulations, implementation of data protection measures, exploitation and licensing of intellectual property, and employment practices. Joel has also taken on advisory roles for various associations and carried out pro-bono work for the arts industry, in furtherance of local development and promotion of the arts.

Shin Associates

Suite B-11-6, Level 11
Wisma Pantai, Plaza Pantai
No.5, Jalan 4/83A
Off Jalan Pantai Baru
59200 Kuala Lumpur
Malaysia

Tel: +603 2201 5584
Fax: +603 2201 9686
Email: general@shinassociates.com.my
Web: shinassociates.com.my



Law and Practice

Contributed by:

Andrew J. Zammit, Jackie Mallia,
Ilona Vella and Jessica Camilleri

GVZH Advocates see p.303



Contents

1. Metaverse	p.290
1.1 Laws and Regulations	p.290
2. Digital Economy	p.290
2.1 Key Challenges	p.290
3. Cloud and Edge Computing	p.291
3.1 Highly Regulated Industries and Data Protection	p.291
4. Artificial Intelligence and Big Data	p.293
4.1 Liability, Data Protection, IP and Fundamental Rights	p.293
5. Internet of Things	p.294
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection	p.294
6. Audio-Visual Media Services	p.295
6.1 Requirements and Authorisation Procedures	p.295
7. Telecommunications	p.297
7.1 Scope of Regulation and Pre-marketing Requirements	p.297
8. Challenges with Technology Agreements	p.299
8.1 Legal Framework Challenges	p.299
9. Trust Services and Digital Entities	p.300
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes	p.300

1. Metaverse

1.1 Laws and Regulations

Research recently conducted by an online and telephone comparison service, [Uswitch](#), has ranked Malta as the fourth most metaverse-ready nation out of 34 countries analysed, with a total score of 7.31 out of ten. Various aspects were considered in arriving at the ranking, including the median fixed broadband speed and its cost, the number of blockchain financial services start-ups, hi-tech exports per capita and the number of searches per million on the metaverse. With this technology being still relatively young, the legal issues surrounding the metaverse and its use have not been specifically analysed or addressed in Malta, and thus there is no specific legal framework nor explicit laws that deal with the matter. Nonetheless, the technology is already regulated to some extent by existing laws, such as consumer law, data protection, product liability and general civil and criminal law. This being said, more widespread use of the metaverse will certainly result in new legal and regulatory challenges. One area that will certainly become relevant is the sale and use of digital assets and services; questions relating to the verification of ownership, authenticity of the virtual items purchased and claims of infringement will need to be navigated. This is in addition to problems of jurisdiction, territoriality, and conflicts of laws.

As a member state of the EU, Malta will be required to implement any legislation in this respect that may be enacted by the European Union. The European Parliament has issued a [briefing](#) analysing the opportunities, risks and policy implications that the metaverse may introduce, and which makes reference to a number of potential legal challenges. An example is that, from a data protection point of view, it may

become more difficult to define who is acting as a data processor or a data controller in a given scenario due to the fact that it may be difficult to ascertain which party is acting on behalf of the other. A practical example of this as laid out by the European Parliament could be in the provision of a privacy notice to users and whether this should be done by each metaverse in its entirety or by each metaverse separately, since the GDPR stipulates that users must give explicit consent for each specific purpose.

2. Digital Economy

2.1 Key Challenges Strategy

Between 2014-20, Malta implemented a general national strategy “Digital Malta” with the aim of positioning Malta to become a “digitally enabled nation”. The national strategy underpinned various sectorial digital policies currently in place in Malta relating to digital public services, cybersecurity, e-commerce and data. In accordance with the European Commission’s Digital Economy and Society Index (DESI) report 2021, Malta ranks sixth out of 27 EU member states. The DESI report also states that since 2019, all Maltese households are reached by Very High Capacity Networks offering speeds of up to 1Gbps. Malta also records good scores on human capital, especially because of the high shares of ICT graduates (6% of graduates in Malta, versus 3.9% in the EU) and performs slightly higher than the EU average in terms of ICT specialists (4.4% versus 4.3% in the EU). The large majority (71%) of Maltese SMEs in Malta have at least a basic level of digital intensity and perform particularly well in the use of technologies such as big data and cloud solutions, which are used by 31% and 38% of enterprises in the country respectively. Malta has also focused on

technologies such as blockchain and artificial intelligence. An improvement in the uptake of e-government services was also reported, with the share of e-government users reaching 63% in 2020.

Legislation

On a legislative level, Malta has enacted and continues to review the legislative framework necessary to enhance Malta's position in the digital arena. Legislative efforts in this field have focused generally on implementing various EU legislative instruments such as the General Data Protection Regulation and the Electronic Identification and Trust Services Regulation, as well as regulatory frameworks to ensure sufficient radio spectrum for mobile data communication while safeguarding the availability of spectrum for public security, to safeguard intellectual property rights, to address cloud computing and data ownership issues, to regulate contentious content, net neutrality, online contracts and licence agreements. Many of these issues are discussed in other parts of this chapter. In terms of digital services and digital markets, Malta is working to transpose the Digital Services Package, adopted by the Commission on 5 July, which comprises the Digital Services Act and the Digital Markets Act. Both these instruments are being implemented with the aim of creating an enhanced sense of uniformity with regard to the regulation of a safe digital space where the fundamental rights of users are protected, as well as to establishing a level playing field for businesses in the ever-growing tech industry.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Cloud computing is not yet expressly or specifically regulated in Malta; however, rules governing a standard level of network security and many industries, especially the banking and gaming sectors, address cloud computing. These sectors are discussed below.

Financial Services

The financial services sector is a wide sector, with different sub-sectors such as banking, insurance and investment services, all of which are subject to broadly similar rules in relation to the outsourcing of a material service or activity. Such rules are issued by the Malta Financial Services Authority (MFSA), the competent authority to regulate all matters relating to banking and finance in Malta. Generally, the use of a cloud service would be considered as material, and notification is required to be given to the MFSA prior to engaging in the use of that service. A risk assessment of the arrangement, as well as the necessary due diligence, would normally also be required to ensure that the service provider is suitable. The MFSA has also released the "Guidance on Technology Arrangements, ICT and Security Risk Management and Outsourcing Arrangements" which would more generally apply to the financial services sector as a whole. These guidelines take cloud computing into account and provide a practical framework for licence holders and requirements for different cloud computing service models – such as software as a service (SaaS) or platform as a service (PaaS) – requiring communication and information systems to protect the data they handle in transit and at rest; this data must only be accessible to authorised parties as and when needed. They further provide that confidentiality, integrity,

availability, authentication and non-repudiation should form the five pillars in the design of any technology arrangement implemented by a licensed institution. Cloud computing systems must also take into consideration the ISACA's Guiding Principles for Cloud Computing Adoption and Use.

Gaming Law

The use by a Malta-licensed gaming provider of managed information technology services is regulated in accordance with the Gaming Authorisations Regulations (Chapter 583.05, Laws of Malta) as well as the "Policy on Outsourcing by Authorised Persons", issued by the Malta Gaming Authority (MGA), the authority which regulates the gaming sector in Malta. These legal instruments state that cloud computing services would be considered a material gaming supply, which carry a number of risks to the operation of a Malta-based gaming licensee. Thus, the MGA recommends that such service providers be assessed and approved by it as part of the pre-licensing assessment or at the post-licensing stage. Where the licensee receives material gaming supplies from a third party not approved by the MGA, the licensee must assume full regulatory responsibility for such supplies. A licensee must also have a regularly updated outsourcing policy and a written agreement with the service provider containing a number of required provisions.

Security of Network and Information Systems

The Measures for High Common Level of Security of Network and Information Systems Order (Chapter 460.35, Laws of Malta) transposes Directive (EU) 2016/1148 (the "NIS Directive") into Maltese law and addresses cloud computing. The NIS Directive aims to implement measures for the achievement of a high common level of network and information system

security across the EU's critical infrastructure. The Order establishes a Critical Information Infrastructure Protection Unit (the "CIIP Unit"), which is responsible for matters relating to the identification and designation of operators of essential services and digital service providers, as well as the adoption of a national strategy on the security of network and information systems. Malta has also implemented a cybersecurity strategy which had six main goals, including the establishment of a governance framework, the strengthening of the fight against cybercrime and national cyberdefence, improving cybersecurity awareness and education, encouraging initiatives by the private sector, awareness and education, and building upon national and international co-operation.

Data Protection

Malta is subject to the GDPR; the general rules in this respect apply also to the issues brought about by cloud computing. The most common issues here relate to the fact that most service providers in this field provide standard terms which are not easily negotiable and thus any data protection-related provisions may not always reflect the required GDPR standards if the cloud service provider is based outside the EEA. Additionally, transfers of personal data need to comply with specific safeguards, the most common being the use of the Commission's Standard Contractual Clauses (SCCs). The SCCs have been amended in June 2021 following the Schrems II judgment which invalidated the EU-US Privacy Shield. As a result, international transfers have become significantly more complex. A provider of cloud computing services established outside the EU would need to show compliance with the new standards in order to be considered GDPR-compliant.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Projects involving big data, machine learning (ML) and artificial intelligence (AI) have one common factor in that they need to make use of vast amounts of data, which may be of a personal nature. This brings about challenges in relation to the management of such personal data in compliance with the GDPR and Maltese data protection law. ML and AI also raise various other legal issues, as outline below, together with potential solutions.

Data Protection

An AI system needs extensive data to train and develop the algorithmic models on which it operates in order to provide an accurate output. Much of this data may be personal in nature, thus compliance with the GDPR and Maltese data protection law is necessary; however, the volume of personal data processed makes compliance more complex to achieve. An overview of the obligations imposed on controllers and processors by Maltese and European data protection law can be found in **1. Metaverse** and **2. Digital Economy**.

These obligations become particularly problematic in the case of ML and AI since access to and collection of personal data is generally restricted by law. Furthermore, personal data can only be processed for its original intended purpose and the reuse of data for additional purposes is not generally possible. This legal requirement could limit the possibility of extracting new value from the combination of datasets. It should also be noted that, under the GDPR, decisions that were taken solely in an automated manner must allow for human review of that decision if it significant-

ly affects the data subject. Additionally, the data subject has a right to an explanation as to how a decision was reached. Whilst these principles can stifle the development of ML and AI technology to some extent, they also ensure that such technology is developed in an ethical manner that respects human rights and the right to privacy of each individual. ML and AI companies and applications that involve the use of personal data can achieve trust by ensuring that they are compliant with the requirements of the GDPR, by implementing the necessary safeguards and ensuring that data protection is present at the design stage and by default.

Ethics

Closely related to the discussion of data protection is the matter of ethical development of ML and AI technologies. In October 2018, the Malta AI Taskforce was set up by the Maltese government to advise on strategies, ethics and legal issues relating to the development of such technologies. One of the documents published by the Taskforce is the Ethical AI Framework which, though it does not have the binding force of law, lays down a set of guiding principles for trustworthy AI governance. The Framework builds upon the Ethics Guidelines for Trustworthy AI, published in April 2019 by the European Commission's High-Level Expert Group on Artificial Intelligence (AI HLEG), and adds a number of control practices which aim to guide developers and users of ML and AI technologies in terms of how the principles set out therein should be translated in practice. The Framework sets out four ethical principles for trustworthy AI, namely:

- human autonomy – humans interacting with AI systems must be able to keep full and effective self-determination over themselves;
- preventing harm – AI systems must not cause harm at any stage of their life cycle to

humans, the natural environment, or other living beings;

- fairness – the development, deployment, use and operation of AI systems must be fair; and
- explicability – end users and other members of the public should be able to understand and challenge the operation of AI systems as required for the particular use case.

Malta has set up a national AI Certification Programme, based on the Framework. Certification would provide applicants with acknowledgement that their AI system has been developed in an ethically aligned, transparent and socially responsible manner, in line with the principles and control practices established by the Framework.

Liability

Liability is often an issue when it comes to ML and AI technologies. It is not easy to establish who or what is legally responsible for the non-human decision-making of a machine. The matter becomes more complicated if the hardware and software performed precisely as they were intended and without a perceptible defect or malfunction of any kind. Malta does not have a dedicated legal framework to govern liability issues relating to ML and AI per se; however, a patchwork of legal provisions addresses the matter to a significant extent. Under the Maltese law of obligations, specifically the Maltese Civil Code (Chapter 16, Laws of Malta), one finds the general concept that a person should always show reasonable care in all their actions, and the standard of reasonable care which is required is that of a reasonable man (*bonus paterfamilias*). The corollary is that a person who causes harm by acting in a manner which falls below this standard would be liable to compensate for such harm.

Another relevant provision under the Civil Code provides that the owner of an animal, or any person using an animal during the time that such person is using it, is liable for any damage caused by it, whether the animal was under their charge or had strayed or escaped. With regard to this latter provision, academic writers have drawn a parallel with this situation and one where an AI system behaves disruptively or uncontrollably, stating that such provisions should be used in such a case.

On a final note, the Product Liability Directive (Directive 85/374/EEC) was transposed into Maltese law through part of the Consumer Affairs Act (Chapter 378 of the Laws of Malta), which brings into effect the concept of strict (no fault) liability into the product liability regime, subject to the limitations of the Product Liability Directive itself. Under the Product Safety Act, a product is safe if it meets all statutory safety requirements under European or national law (or in default thereof, Commission recommendations and codes of practice), and any distributor who supplies products which they should know to be unsafe (even having actual knowledge of this) would be liable.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection Restrictions on a Project's Scope

The term “internet of things” (IoT) describes physical objects that have technology built into them allowing them to connect to the internet or other communication networks to exchange, process, store, and transport data. The IoT includes a wide range of interconnected products and systems, including connected appli-

ances, smart home security systems, biometric cybersecurity scanners, activity trackers, and smart agricultural equipment.

Data Protection and Privacy Considerations

Since it is not always possible to obtain consent from the data subject directly in IoT technology, IoT manufacturers must look into alternative methods of obtaining consent or find another legal basis for processing the data in order to comply with the GDPR's criteria. Furthermore, processing of special categories of data, such as health and biometric data, is subject to stricter regulation and is only permitted under certain conditions and can only be processed in specific circumstances. Data subjects also have the right not to be subject to decisions based solely on automated decision-making processes, to access data held about them, to request erasure or rectification of the personal data, and to receive the personal data concerning themselves, which they have provided to a controller, in a structured, commonly used and machine-readable format. When contemplating a project with connected devices, one needs to consider how these data subjects rights will be addressed.

Data controllers behind IoT projects are also required to conduct a Data Protection Impact Assessment (DPIA) before launching a new IoT technology or device. Companies and organisations working on IoT technologies must put in place technical and organisational protections from the beginning of the design of the processing activities to preserve privacy and ensure that data protection rules are followed (ie, data protection by design). These organisations should also make sure that if personal data is processed using IoT technology, the highest requirements of data privacy are in effect by default (ie, data protection by default).

Cybersecurity Considerations

Many connected devices still seem to be at risk of hacking, virus assaults, processing mistakes and risks, and other comparable dangers. Because any connected device missing security safeguards could endanger the entire IoT network, the matter is very significant. While there are a number of laws in Malta that deal with product safety and cybercrime, these laws do not expressly cover IoT devices or the certification of such devices. Although Malta has a cybersecurity plan, which was briefly covered under the previous heading, no particular standards of behaviour for the development, manufacture, or usage of IoT devices have yet been created.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Audio-Visual Service Requirements and Applicability - Broadcasting Licences

According to the Broadcasting Act (Chapter 350, Laws of Malta), no one may broadcast audio or video content in Malta for the entire country or any part of it without a written permit from the Malta Broadcasting Authority (MBA), nor may anyone broadcast audio or video content from Malta to any foreign country without a written permit from the MBA. The MBA may grant a broadcasting licence subject to the terms, restrictions, and restrictions it sees fit. These licenses are likewise governed by the First Schedule of the Broadcasting Act. There are various classifications and types of licences, including:

- licences for nationwide television services;
- nationwide radio services;
- community radio services;
- satellite radio services;

- satellite television services; and
- other services which may be broadcast or provided on or by an electronic communications network.

The MBA may grant a general interest broadcast content licence or a commercial broadcast content licence in relation to national television services. A general interest goal service is a television broadcasting service that commits to airing a predetermined number of general interest programmes that are under the purview of a public service broadcasting service as defined by the National Broadcasting Policy.

A general interest objective service may be either a generalist service or a niche service. A “niche service” refers to a television broadcasting service which predominantly transmits programmes of a limited number of genres of a specialist subject matter, whilst a “generalist service” means a television broadcasting service which transmits a wide range of programme genres. On the other hand, a “commercial television broadcasting service” means a television broadcasting service that is either a generalist service or a niche service that is not subject to the obligations of a general interest objective service.

An application for a broadcasting licence must be made to the MBA through the relevant licence application, some of which are discussed below:

- in the case of a new nationwide TV station, arrangements have to be made in the first place with the service providers Melita Limited and GO plc, the two TV distribution networks on the island, prior to applying for a licence from the MBA;
- in the case of digital radio broadcasting (which is further regulated by Digital Radio Broadcasting Regulations (Chapter 350.29,

Laws of Malta)), arrangements have to be made in the first place with the licensed digital radio broadcasting service provider DigiB Network, prior to applying for a licence from the MBA; and

- satellite uplink services are licensed by the Malta Communications Authority (MCA), and the initial step in this case is to complete and return an application for a satellite earth station licence.

Audiovisual Media Services

A television broadcast or an on-demand audiovisual media service both qualify as audiovisual media services. A provider of an on-demand media service generally does not need a broadcasting licence as stated under the previous heading but they must notify the MBA in writing by sending a letter to the Chairman of the MCA before offering the service. This written notification must include the following information:

- in the case of a natural person, the name, surname and address, identity card number, passport number or any other identification document as may be accepted by the MCA; and
- in the case of a legal person, the name and address of the company and of the registered office.

An audiovisual media service transmitted by a media service provider falling under the jurisdiction of Malta must comply with specific provisions of the Broadcasting Act as to the content of its transmissions, as well as other provisions which may be relevant under consumer and press laws.

Requirements for Video-Sharing Platform Providers

A supplier of a video-sharing website based in Malta is subject to Maltese law. A provider of a video-sharing platform does not need a broadcasting licence as defined under the first heading in this section but they must nevertheless notify the MCA in writing by sending a letter to the Chairperson of the MCA that includes the following information:

- in the case of a natural person, the name, surname and address, identity card number, passport number or any other identification document as may be accepted by the MCA; and
- in the case of a legal person, the name and address of the company and of the registered office.

Video-sharing platform providers falling under the jurisdiction of Malta must also comply with specific provisions of the Broadcasting Act as to the content of its transmissions, as well as other provisions that may be relevant under consumer and press laws.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Authorisation of Commercial Services

The Electronic Communications (Regulation) Act (Chapter 399 of the Laws of Malta) stipulates that an entity that wants to provide some form of commercial electronic communications (electronic communications networks and services) must notify the MCA, the regulator for the telecommunications sector, in order to obtain a “general authorisation” to provide the type of service desired. This is usually done through a

notification form, which should contain the following:

- the name of the provider;
- the legal status of the provider, its form and registration number;
- the official address for service of notice in Malta, and the geographical address of the main establishment of the provider in Malta or any other member state, as the case may be;
- the website address of the provider, where applicable, associated with the provision of electronic communications networks and/or services;
- a contact person and contact details;
- a short description of the networks and/or services intended to be provided;
- the member state or member states where the networks and/or services are being provided; and
- an estimated date for starting the activity.

Upon notification to the MCA, an entity may start the activity so notified, subject to the provisions on the rights of use under the law. The entity will still be required to obtain and/or notify and comply with, any permit, licence, right of use, or other general authorisation in respect of numbering resources, equipment, or radio spectrum, and any other permit that may be necessary at law.

Voice-over internet protocol (VoIP) services using a carrier selection facility are regulated in Malta as a publicly available telephony service if they are number-dependent – that is, if the service requires numbers from the national numbering plan. A VoIP service which is not number-dependent would not be regulated. Likewise, instant messaging services that are not number-dependent (such as Facebook Messenger) would be unregulated. The internet network and

service over which such services are provided would be regulated as discussed elsewhere in this section.

Radiocommunications Equipment Licensing

The European Authorisation Directive (Directive 2002/20/EC), and rules issued by the International Telecommunications unit (the “Radio Regulations”) stipulate that a form of authorisation is required for radio transmissions. The Electronic Communications (Regulation) Act (Chapter 399, Laws of Malta) accordingly also requires that the use of radio frequencies and the installation or use of radiocommunications equipment need to be authorised.

There are various types of authorisations for radiocommunications equipment, which can be categorised under three high-level categories: individual licensing, light-licensing and licensing-exempt. These types of licences are generally managed by the MCA under its spectrum management responsibilities. The same laws require that the installation or use of radiocommunications equipment must be subject to an individual licence unless the equipment is licence-exempt or covered by a general authorisation.

The light licensing framework is laid down by the General Authorisations (Radiocommunications Apparatus) Regulation (Chapter 399.40, Laws of Malta). This framework is a general authorisation framework which applies to various types of radio equipment:

- which, when used, do not require co-ordination between users;
- for which user individualisation is not necessary;
- when the use of a frequency or of a frequency band is possible by a number of users within a particular area;

- when spectrum is available on a long-term basis; and
- when the radio applications are not subject to frequency planning, co-ordination and individual frequency assignment.

Radio Frequency Identification Devices (RFIDs) fall within this category, as do cordless telephones, radio local area networks such as Wi-Fi equipment, remote controls, PMR446 radios, certain satellite terminals, short-range devices (SRDs), and Bluetooth devices are some categories of radiocommunication equipment that are regulated by the above-mentioned general authorisation regulation. Anyone making use of such equipment must comply with its purpose of use and comply with the technical and other operating requirements as stated in the General Authorisations (Radiocommunications Apparatus) Regulations. In accordance with the Fees Leviable by Government Departments Regulations (Chapter 35.01, Laws of Malta). RFIDs are exempt from the payment of fees.

Spectrum Licensing

In accordance with the Electronic Communications Act, an authorisation is required for the right to use radio frequencies. This regulatory requirement is in place so as to ensure that harmful interference is avoided, and to safeguard the efficient use of radio spectrum. Anyone who desires to apply for the right to use radio frequencies must complete the Generic Spectrum Application Form.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Legal Framework Features

An entity that intends to enter into IT service agreements with another entity in Malta will be bound by the general concepts of Maltese contract law, unless the agreement stipulates that a different law should apply. As a general rule, the Civil Code (Chapter 16, Laws of Malta), provides that contracts legally entered into have the force of law for the contracting parties. Parties may go against what is stated in the general law by virtue of their agreement, unless there is a prohibition by the law itself by way of mandatory rules or because of a prohibition of public policy. IT service agreements would generally cover:

- a detailed description of the service;
- whether only services are being provided, or whether materials are also being supplied;
- the payable fees;
- term of contract and termination methods;
- ownership over any intellectual or other property produced during the term of the agreement;
- liability for the service provided and limitations thereon (usually governed by a Service Level Agreement);
- insurance;
- how changes to the agreement/services can be made;
- notifications to the other party;
- confidentiality, non-compete and non-solicitation;
- dispute resolution;
- data processing (where personal data is accessible by the IT service provider);
- independent relationship of the parties;
- whether the contract can be transferred.

The above-mentioned provisions are relatively standard and provided that they have been agreed to by both parties, and that valid consent can be proved, a court would follow the terms of agreement between the parties when interpreting the contract, especially where the wording is unambiguous. However, lack of clarity and proper description of the expectations of the parties are the most common legal problems that have been encountered in relation to IT service agreements.

An IT service agreement will be valid even if not done in writing, but verbal contracts of this nature are most certainly not recommended.

Limitation of Liability

It is quite common for limitation of liability clauses to be included in service contracts. In this respect, it should be noted that in certain circumstances liability cannot be limited. One example is that where fraud is involved, this would invalidate the entire contract, including any limitation of liability clauses. Furthermore, Maltese jurisprudence has also held in various situations that liability cannot be limited in cases of gross negligence.

Maltese courts have on occasion also used reasoning similar to the “doctrine of fundamental breach” to invalidate limitation of liability clauses where the party commits a breach of the contract that is so fundamental that it deprives the other party of essentially the whole of the contract’s benefits. The Maltese courts have also invalidated limitation clauses on occasion simply because they were not brought to the attention of the weaker party, even though the clause itself was technically valid, although this would probably apply more readily in the case where the recipient of the IT service is a consumer. Where the IT service contract includes the provision

of materials, one needs to consider that warranties against latent defects cannot always be excluded. Product liability issues may also need to be considered.

Penalty Clauses

IT services agreements frequently involve fines for non-performance or contract violations (for example, a breach of confidentiality or breach of the non-solicitation clause). Frequently, penalty clauses are pre-liquidated, so the sum due in the event of a certain violation would be specified in the contract itself. The Maltese courts would generally tend to uphold the penalty clause stipulated between the parties, unless the amount is grossly unfair to one of them. In this respect, it should be noted that the Civil Code provides that a court cannot abate or mitigate a penalty agreed between the parties except:

- if the service provider has performed the obligation in part, and the recipient of the service has expressly accepted the part so performed; or
- if the service provider has performed the obligation in part, and the part so performed is clearly useful to the recipient of the service.

In any such case, an abatement cannot be made if the recipient of the service, in undertaking to pay the penalty, has expressly waived their right to any abatement or if the penalty has been stipulated in consideration of mere delay. Therefore, it is important to consider the inclusion or otherwise of such wording in the contract.

Regulatory Matters

Under the GDPR and local data protection law, specific measures need to be put into place if personal data is to be transferred outside of the European Economic Area (EEA). Thus, should the IT service provider be based outside the

EEA, and wish to access personal data held by the recipient of the service, a data processing agreement will need to be concluded in accordance with the European Commission's Standard Contractual Clauses, unless other safeguards are in place.

Additionally, several companies that are subject to regulation demand that particular regulatory data be stored on EEA-based servers so that the appropriate regulatory authority can easily access it. The Malta Gaming Authority (MGA), which mandates that regulatory data be accessible, available, and traceable, is one example. For this purpose, the MGA demands access to real time information, which could present problems if such data is in a different jurisdiction or on the cloud. The matter can be solved by real-time replication of the data, on a live replication server in Malta, although this is not the only solution. Discussions with the MGA can serve to address these issues.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The eIDAS Regulation (Regulation (EC) 910/2014) permits citizens, enterprises, and public authorities to use electronic identification and trust services to access online services or handle electronic transactions. Through openness, security, technical neutrality, co-operation, and interoperability, eIDAS seeks to promote the efficient flow of trade throughout the EU. To uphold these ideals, eIDAS ensures that individuals and organisations can access public services offered online in other EU nations using their own national electronic identification schemes (eIDs) and establishes a European internal market for trust

services by guaranteeing that these services will function internationally and have the same legal standing as their conventional paper-based counterparts.

The eIDAS Regulation was transposed into the Maltese eCommerce Act and the Electronic Trust Services Notification and Fees Regulations SL 426.03 by virtue of Act XXXV of 2016, which also repealed or amended all local provisions that were previously in force but were inconsistent with the eIDAS Regulation. The Regulation deals with three types of electronic signatures: standard, advanced or qualified, as detailed below.

- An advanced electronic signature (AdES) is one that meets the following requirements:
 - (a) it is uniquely linked to the signatory;
 - (b) it is capable of identifying the signatory;
 - (c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control; and
 - (d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.
- A qualified electronic signature (QES) is an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures. In other words, a QES is an advanced electronic signature with a digital certificate that has been encrypted by a secure signature creation device through a qualified trust service provider (requirements for these are also in the law).

The Regulation states that an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or

that it does not meet the requirements for qualified electronic signatures (for example, with a scanned signature, one would need to prove its validity with additional evidence). On the other hand, a qualified electronic signature has the equivalent legal effect of a handwritten signature. If a qualified electronic signature is based on a qualified certificate issued in one member state, it must be recognised as a qualified electronic signature in all other member states.

Under Schedule 5 of the Maltese eCommerce Act, unless specifically provided in the law, the above does not apply to the following activities/areas.

- The field of taxation.
- Matters in relation to information society services covered by any laws relating to data protection.
- Questions in relation to agreements or practices governed by competition law.
- The following activities of information society services:
 - (a) the activities of notaries or equivalent professions to the extent that they involve a direct and specific connection with the exercise of public authority;
 - (b) the representation of a client and defence of their interests before the courts; and
 - (c) gambling activities which involve wagering a stake with monetary value in games of chance, including lotteries and betting transactions.
- Contracts that create or transfer rights over immovable property other than leasing rights.
- Contracts of suretyship granted and on collateral security furnished by persons acting for purposes outside their trade, business or profession.
- The law governing the creation, execution, amendment, variation or revocation of:

- (a) a will or any other testamentary instrument;
- (b) a trust; or
- (c) a power of attorney.
- Any law governing the making of an affidavit or a solemn declaration, or requiring or permitting the use of one for any purpose.
- The rules, practices or procedures of a court or tribunal however so described.
- Any law relating to the giving of evidence in criminal proceedings.
- Any contracts governed by family law.

In relation to trust services, the European Union Trusted Lists (EUTL) is a public list of trust service providers (TSPs) that are specifically accredited to offer certificate-based digital IDs for individuals, digital seals for businesses, and time stamping services for Qualified Electronic Signatures in compliance with the eIDAS. Each

EU member state generally supervises trust service providers established in that state; however, once approved in one member state, the service provider can be provided in other EU countries and accepted as having the same level of compliance. In Malta, trust service providers are supervised by the Malta Communications Authority.

Malta has also put into place the “eIDAS Node”, which complies with the EU Interoperability Framework and allows Maltese citizens to use the digital public services of other EU member states and conversely allows European citizens access to the digital services of the Maltese government.

GVZH Advocates is a modern and sophisticated legal practice composed of top-tier professionals, firmly rooted in decades of experience in the Maltese legal landscape. Built on the values of acumen, integrity and clarity, the firm is dedicated to providing the highest levels of customer satisfaction, making sure that legal solutions are not only soundly rooted and rigorously tested, but also meticulously implemented. GVZH Advocates understands that today's business environment requires legal advisors that have both skills and expertise geared

towards effectively addressing specific and technical issues in the context of complex projects, transactions and disputes. It is through the contribution of these skills and expertise in an accurate and timely manner that GVZH Advocates, as a forward-looking firm, looks to cement long-term and meaningful relationships with clients and partners. The firm is regularly involved in cross-border transactions, tapping into a wide network of international consultants, all experts in their respective field, ensuring seamless, timely and quality advice.

Authors



Andrew J. Zammit is the firm's managing partner and heads the firm's corporate, M&A, banking and finance, and gaming practices. He is actively involved in M&A, corporate finance, the

licensing of financial services businesses with the Malta Financial Services Authority (MFSA) and asset-financing transactions. Andrew is particularly active in advising businesses within the TMT space, pioneering the licensing of various fintech operators in Malta, and has led various corporate acquisitions, notably including the sale of Malta's largest quad telecoms player and a number of significant online gaming operators. Andrew is a contributor to various fintech and gaming publications, and to various online legal portal services.



Jackie Mallia specialises in gaming, information technology, intellectual property and data protection. She has extensive experience in advising the private and public sector, having

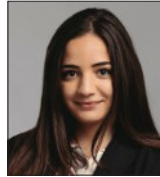
assisted private clients in numerous corporate matters, as well as helping various governments and authorities within and outside the European Union to formulate and draft legislative frameworks. She also focuses on artificial intelligence (AI) and other disruptive technologies, and she was one of the experts appointed to the Malta.AI Task Force, heading the Legal and Ethics Working Group. She regularly provides support services to investors and entities within the sectors of various emerging and innovative technologies, including AI, blockchain and esports.

Contributed by: Andrew J. Zammit, Jackie Mallia, Ilona Vella and Jessica Camilleri, **GVZH Advocates**



Ilona Vella is an advocate focusing on gaming and data protection, and has great interest in the field of medical law. She graduated from the University of Malta with a

Bachelor of Laws (Honours) in 2020. She qualified as a lawyer with a Master's in advocacy in 2021.



Jessica Camilleri is a legal trainee focusing on data protection, intellectual property, and technology media and telecommunications (TMT) Law. Jessica is also interested in

European Union law and European funding, as well as the law surrounding cryptocurrencies.

GVZH Advocates

192 Old Bakery Street
Valletta
Malta
VLT 1455

Tel: +356 2122 8888
Email: info@gvzh.mt
Web: gvzh.mt



Law and Practice

Contributed by:

Iván Ruiz Moreno, Rubén Gutiérrez Díaz,
Eli Manuel Ramírez and Erika Estrever

Ruiz Moreno & Asociados see p.318



Contents

1. Metaverse	p.306
1.1 <u>Laws and Regulations</u>	p.306
2. Digital Economy	p.306
2.1 <u>Key Challenges</u>	p.306
3. Cloud and Edge Computing	p.308
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.308
4. Artificial Intelligence and Big Data	p.311
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.311
5. Internet of Things	p.312
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.312
6. Audio-Visual Media Services	p.314
6.1 <u>Requirements and Authorisation Procedures</u>	p.314
7. Telecommunications	p.314
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.314
8. Challenges with Technology Agreements	p.315
8.1 <u>Legal Framework Challenges</u>	p.315
9. Trust Services and Digital Entities	p.316
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.316

1. Metaverse

1.1 Laws and Regulations

Laws or Regulations in Relation to the Metaverse

New technologies and applications, such as the metaverse, are quickly becoming a reality. Nonetheless, Mexico currently has no regulations in relation to the metaverse. Mexico's Telecommunications and Broadcast Law (the Telecom Law) is technology-neutral, so there is no regulation that applies to a specific type of technology. The Telecom Law and its subsidiary regulations govern public telecommunications and broadcast services and the use of spectrum and licensing, but not technologies.

Key Legal Challenges in Relation to the Metaverse

The biggest legal challenge relating to the metaverse is that there is no specific legal/regulatory framework that easily allows the implementation of the metaverse and new technologies. Mexico's telecommunications regulator (the Federal Telecommunications Institute – IFT) has promoted the discussion of the metaverse and topics for new technologies over the last year, but no law/regulation exists as of February 2023. Therefore, any projects relating to the metaverse would be subject to the same laws and regulations as ordinary intellectual property, data protection and cybersecurity matters.

2. Digital Economy

2.1 Key Challenges

Laws and Regulations Regulating the Digital Economy

In general terms, the laws or regulations applicable to electronic commerce or e-commerce are the Federal Consumer Protection Law, the Code

of Ethics for Electronic Commerce, Mexico's Commerce Code, the Federal Civil Code, the Federal Copyright Law, the Federal Law for the Protection of Industrial Property, the Federal Law for the Protection of Personal Data in the Possession of Private Parties, the Income Tax Law, the Value Added Tax Law, the Federal Tax Code and Mexican Norm NMX-COE-001-SCFI-2018.

The Federal Consumer Protection Law

The Federal Consumer Protection Law governs the contents, promotions and offers made through electronic means. Specifically, Article 76 bis of the Federal Consumer Protection Law mandates that providers of goods and services through electronic means, optic channels or any other technology, shall:

- use in a confidential manner the information provided by consumers and not disclose or share such information with third parties not related to a transaction;
- use available technical elements to provide security and confidentiality to the information provided by consumers and inform the consumer of such security and confidentiality elements prior to the conclusion of a transaction;
- provide to consumers, prior to them entering into a transaction, the seller's physical address, contact telephone numbers and means to file claims or clarifications;
- avoid using misleading commercial practices when advertising or selling a product;
- disclose all information on the terms, conditions, costs, additional charges, if applicable, and forms of payment for the goods and services offered;
- respect the consumers' choice concerning the quantity and quality of the products it wishes to acquire, as well consumers' deci-

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

sion not to receive any commercial advertisements; and

- avoid using sales or advertising strategies that do not provide consumers with clear and sufficient information about the products and/or services offered, especially in the case of marketing practices aimed at the vulnerable population.

In addition, providers of goods or services through electronic means must observe the Code of Ethics in Electronic Commerce published by Mexico's Consumer Protection Agency (*Procuraduría Federal del Consumidor* – PRO-FECO) and register themselves before PRO-FECO as responsible e-commerce providers.

Mexico's Commerce and Federal Civil Codes

Mexico's Commerce and Federal Civil Codes govern commercial operations and the exchange of data and information carried out through electronic means, as well as the methods to express consent, acceptance and validity within contracts when they are executed through the use of electronic means, optical channels or any other technology pursuant to Articles 1803, 1805, 1811 and 1834 bis of the Mexican Federal Civil Code and Articles 80, 89, 90, 90 bis, 91, 91 bis, 92, 93, 93 bis, 94 and 95 of the Commerce Code.

The Federal Law for the Protection of Personal Data in the Possession of Private Parties

The Federal Law for the Protection of Personal Data in the Possession of Private Parties regulates the way in which personal data must be treated by providers of goods and/or services, including the obligation to display a privacy notice and request a person's explicit consent to the gathering and sharing of its data.

Mexico's Federal Tax Code

Mexico's Federal Tax Code governs e-commerce as it relates to the issuance of digital tax receipts, the issuance of electronic invoices and the use of the advanced electronic signature. This relates to tax matters only.

Mexico's Value Added Tax Law

Mexico's Value Added Tax Law establishes the following digital services as services subject to value-added tax, as long as there is a payment involved:

- services provided through applications or content in digital format, via the internet or some other network; and
- these services may or may not require any human intervention.

The Federal Income Tax Law

The Federal Income Tax Law establishes that all taxpayers must pay income tax over payments they receive for the sale of goods or services through the internet, technological platforms, computer applications and any similar digital services, including payments they receive for any ancillary concepts.

The Federal Copyright Law and the Federal Law for the Protection of Industrial Property

The Federal Copyright Law and the Federal Law for the Protection of Industrial Property apply in a general sense, since:

- the Federal Copyright Law protects and regulates the distribution of content or works under different platforms, including the internet; and
- the Federal Law for the Protection of Industrial Property protects and regulates the use of trade marks, distinctive signs and domain

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

names through different means, including the internet.

Mexican Norm NMX-COE-001-SCFI-2018

Mexican Norm NMX-COE-001-SCFI-2018 regulates electronic commerce services in detail and establishes the terms and conditions that all e-commerce merchants must comply with, whether they sell their goods and/or services directly, through internet web pages or through an intermediary.

Key Legal Challenges in the Digital Economy

One of the biggest challenges in relation to the digital economy in Mexico lies with the regulation of social media, whether for commercial, expression, information or entertainment purposes. Although there is a bill in the Mexican Senate that seeks to govern the operation of social media by means of amending the Telecom Law and giving additional powers to the IFT, the fact is that such bill has been opposed by civil society, NGOs, social media groups and suppliers and it is likely that neither this bill nor similar bills will be passed prior to the coming Presidential election in 2024.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Regulations in Relation to Cloud and Edge Computing

Mexico is the second largest cloud and edge data centre market in Latin America after Brazil, and several domestic and foreign companies offer cloud computing services through a combination of domestic and international data centres that offer low latency and redundancy.

Unlike other jurisdictions in Latin America, Mexico has no general laws that impose limitations on the entrusting of certain processes or data to the cloud or edge computing, although certain regulations – like the IFT’s Collaboration with Justice Guidelines – which require telecommunications licensees to store in Mexico the information necessary to respond to information warrants from Mexican courts or crime prosecution agencies.

Nonetheless, Article 19.12 of the United States-Mexico-Canada Agreement (the USMCA) prohibits the parties from requiring members of the other parties to locate computing facilities in their own country as a condition for conducting business. Since the USMCA, like other international treaties entered into by Mexico, has a legal hierarchy right below the Mexican Constitution, Mexico’s Congress cannot pass any laws that would set such a requirement.

In addition, Article 52 of Mexico’s Data Protection Regulations defines “cloud computing” as the external supply of on-demand computer services that implicate the provision of infrastructure, platforms or software distributed through a flexible mode and virtualisation processes with dynamically shared resources; it further states that Mexican regulatory agencies shall issue governing criteria for the processing of personal data through cloud computing, within the scope of their jurisdiction and with the collaboration of Mexico’s National Institute for Information Access (INAI).

In July 2019, INAI issued its Minimum Standards for the Contracting of Cloud Computing Services that Involve the Processing of Personal Data (the Standards). The Standards are not mandatory and offer general recommendations to users who seek the safeguarding of their personal data.

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

The Standards' main recommendations to cloud service users include the following.

Prior considerations

Before executing a cloud services contract, users should carry out the following.

- Identify the data, processes or functions that will be involved in the cloud computing service.
- Identify the data provisioning model to guarantee the processing of personal data in the cloud computing service.
- Verify security policies and measures for the use of cloud computing services.
- Evaluate all aspects of the service, as well as the terms and conditions of the cloud computing service to be contracted.
- Users should verify the supplier's level of compliance and the quality of its services and safety measures, and whether the supplier has been subject to complaints or investigations from personal data authorities around the world.
- Users should check the supplier's name or business name and means of contact for customer services (email, phone, automated systems, etc), depending on the geographical area (regional offices, local offices, etc).
- Users should check the governing law and location for the processing and storage of personal data, identifying certifications that are enforceable on the supplier and the governing law of the contract, as well as the location of systems for the processing and storage of personal databases and, where appropriate, the corresponding service's regional office.
- Clients should verify that the contract includes clauses that prevent the supplier and its subcontractors from claiming ownership of the information provided by the client, at

any time, and clauses, policies or automated systems that:

- (a) guarantee that the supplier uses the information only for the purposes set forth in the terms and conditions of the cloud computing service;
- (b) restrict and limit the supplier from disclosing or modifying the processing of personal data or the information generated by the client;
- (c) keep the client informed as to who shall have access to its personal data and for what purpose;
- (d) guarantee that the client may access, amend or remove its personal data at any time;
- (e) notify the client of any changes or updates in the provision of the cloud computing service, as well as of any incident that causes a service interruption;
- (f) inform the client of any violation of safety measures for the processing of their personal data; and
- (g) provide compensation for failure or service interruption, or due to a violation of safety measures in the processing of the client's personal data.

Transparency

As regards transparency, the Standards recommend that suppliers provide the following:

- transparency regarding the people or companies subcontracted by suppliers for cloud computing services;
- mechanisms to guarantee the legal processing of personal data by outsourced third parties;
- mechanisms for clients to access, rectify or cancel their personal data or to oppose the use of it (ARCO Rights); and

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

- mechanisms for the removal of personal data through safe deletion from the cloud, which mechanisms shall prevent the recovery of personal data by an unauthorised third party.

Safety measures

As regards safety measures, the Standards recommend users to select suppliers who have clauses, policies or automated systems that:

- guarantee the processing of personal data in safe systems, whether they belong to the supplier and/or outsourced third parties;
- guarantee the availability, integrity and isolation of the client's personal data from the information of other clients;
- guarantee the client's administration, control and access over the processing of its personal data in cloud computing services;
- make suppliers subject to audits by third certified parties, regarding their compliance with applicable regulations; and
- make suppliers subject to certification.

Risk evaluation

As regards risk evaluation, the Standards recommend that clients be aware of the following risks when suppliers process their personal data:

- lack of control over the personal data lifecycle in the cloud;
- absence of transparency with outsourced third parties;
- lack of automated systems or support mechanisms when processing personal data in the cloud;
- inappropriate use of shared resources, and the absence of isolation of the client's personal data in the cloud;
- lack of portability or interoperability of the client's personal data; and

- misunderstandings in the processing of personal data when the information is used by unauthorised third parties or multi-stakeholders, or for advertising purposes, without the client's authorisation.

Other considerations

The Standards recommend that clients avoid contracting with suppliers that do not offer clauses, policies or mechanisms that offer and guarantee the retrieval of personal data when the service ends. The Standards recommend clients to verify the supplier's terms and conditions for the interoperability and portability of their personal data. The Standards advise clients to prefer suppliers that allow contract negotiation, in order to tailor the contract to the client's service requirements.

Highly Regulated Industries

The financial industry is subject to additional regulation regarding cloud services and financial institutions must therefore obtain authorisation from the National Banking and Securities Commission (CNBV) for any type of service or commission abroad. Moreover, Mexican finance laws and regulations establish that Technology Financial Institutions (ITFs) in which cloud services are provided by third parties, must adopt special measures in their respective continuity plans in order to protect the interests of their customers and to maintain their own security, operational integrity and finances, as well as the security and operational integrity of the payment system as a whole, without prejudice to any other measures imposed on the ITFs by any applicable law or its provisions.

Some regulated industries, like health, insurance and telecommunications, may be subject to additional data regulations, but these do not extend to cloud services specifically.

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

Issues Processing Personal Data in the Context of Cloud Computing

There are certain specific issues affecting the processing of personal data in the context of cloud computing, which include:

- low coverage and penetration of broadband services;
- distrust over information processing by private and governmental entities, either because of third party hacks and/or possible invasion of privacy (big brother syndrome);
- lack of exemplary punishment against data privacy violations by private or public entities;
- absence of local representatives and professional customer care; and
- a shortage of trained personnel who know how to administer cloud services.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Laws and Regulations in Relation to the Use of AI and Big Data

There are no laws or regulations that govern the use of artificial intelligence and big data in Mexico, nor are there any specific industry codes of conduct.

To date, Mexican authorities like the IFT have only conducted seminars or research studies in order to evaluate the adoption of artificial intelligence tools among Mexican users and identify areas of opportunity to provide recommendations and information to the general public.

Relevant Elements

Except for Article 52 of Mexico's Data Protection Regulations and certain industry-specific regula-

tions, any projects relating to big data and artificial intelligence would be subject to the same conditions of liability, insurance, data protection, intellectual property, jurisdiction and fundamental rights as any regular project.

Regarding data protection, Mexico has an "opt in" regime regarding the treatment of personal data, under which owners of personal data must consent to the treatment of their data through different available means, which may include a signature or a "click".

Responsible parties that process (treat) personal data are obliged to safeguard and protect a person's information, such as their name, address, email, telephone number and any other data that serves to identify an individual.

Responsible parties must also publish a data privacy notice, which must be made available to those persons whose information is collected, along with any changes to such data privacy notice. Unless expressly authorised, a responsible party or a third party cannot use personal data to contact the user to offer or promote products or services. Regarding the treatment of personal data, INAI outlines a general process for individuals to ensure the exercise of their ARCO rights (ie, access, rectification, cancellation or opposition).

This process is based on the following principles:

- lawfulness and fairness – individuals must act in compliance with the laws and regulations for the protection of personal data;
- consent – the data controller shall have the consent of the individual for the processing of their personal data;

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

- information – individuals must be informed about the main characteristics of the processing to which their personal data will be subject;
- proportionality – the controller is obliged to process personal data only if such information is necessary, adequate and relevant to the purposes for which said personal data was collected;
- purpose – personal data may only be processed in order to comply with the purpose, motive or reason for which the owner has been notified;
- quality – this principle states that processed personal data shall be accurate, correct, complete, up to date and relevant; and
- liability – this condition is based on the principle of “accountability”, which establishes the obligation to take all necessary measures to ensure the protection of personal data, even when the data is being processed by machines or AI.

These principles are mandatory under Mexico’s Data Protection Regulations for the protection of personal data held by private parties. In case of conflict, individuals may file a complaint before the INAI, which will review whether the data controller has complied with all of these principles during its processing of personal data.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Laws and Regulations in Relation to the IoT

There are currently no laws or regulations in relation to the internet of things.

As mentioned in **1.1 Laws and Regulations**, Mexico’s regulatory environment is technology neutral and the IFT only seeks compliance of regulations that apply to all electronic communications regarding hardware homologation, interconnection, no spamming, no phishing, consumer protection, collaboration with justice, numbering, net neutrality, spectrum use and signalling.

In addition, the IFT published in 2021 its Network and Traffic Management Guidelines (the Guidelines), which apply to internet service providers (ISPs).

The Guidelines are intended to ensure net neutrality and that ISPs establish general network traffic policies that comply with the following principles:

- to guarantee the quality and speed of the internet access services contracted by the end user;
- to preserve the integrity and security of internet access networks, as well as end users’ private communications;
- to guarantee users’ freedom of choice to access any content, application or internet service, without the ISP limiting, degrading, restricting or discriminating access to them; and
- to guarantee non-discriminatory treatment of end users, applications, content and/or service providers, similar types of traffic as well as own and third-party traffic on the network.

On the other hand, the Guidelines allow ISPs to supply services in which ISPs give special treatment to content, apps or services accessed by end users.

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

In this case, the cost of data for access to a specific content, application or service is sponsored by a third interested party, provided that the end user has an active data balance in either its prepaid or post-paid services.

The IFT's Guidelines also allow the provision of "free" services when the end user does not have an active data balance provided that such services:

- have the purpose of reducing the digital divide;
- promote digital financial inclusion; and
- allow end users to make top-ups, payments and contract telecommunications services.

The Guidelines also allow ISPs to provide specific or superior network resources to transmit and improve upload and download speeds or the user's experience, as long as these services in no way affect the quality or speed of other traffic transmitted through the same public telecommunications network.

It is important to highlight that ISPs that distribute content, applications or services of their own through the use of specific resources of their networks shall make these resources available to providers of applications, content or any other internet-based service, and in no circumstance shall such services require the providers of applications, content or any internet-based service to pay for the transmission of the traffic generated by their content, applications or services, under standard conditions.

Relevant Elements

Machine-to-machine communications will likely make the most use of sponsored or free ISP services under the Guidelines.

This will especially be the case for financial, gaming, security, healthcare, transportation or emergency apps and services; it is therefore reasonable to assume that banks, gaming platforms, child or elderly care companies or institutions will seek to contract these services from ISPs.

The Guidelines further require ISPs to:

- file before the IFT every six months a report that includes the name of the companies or individuals that sponsor the provision of services (data consumption sponsorship), the service rate registered before the IFT and the term of such offer, within the ten business days following the closing of each semester; and
- publish in their web portals their policy code for traffic management (the Policy Code), which shall incorporate the principles under which the ISP shall carry out its traffic and network management.

The Policy Code shall also include:

- a clear description of the ISP's network monitoring techniques that will serve as a basis for the administration of traffic and the ISP's network;
- recommendations to end users on how to reduce risks to the privacy of their communications and their network's security;
- updated references to the current legal and regulatory framework and, in its case, to international standards that support traffic and network management; and
- the last date on which the Policy Code was updated.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Main Requirements for Providing Audio-Visual Media Services

The Telecom Law regulates the issuance of universal service licences or single concessions for telecommunications and broadcast services which do not include over-the-top services (OTTS).

Therefore, the single concession licence to provide an audio-visual media service such as pay TV would be the same as the single concession licence for a fixed broadband or telephony service; however, online audio-visual platforms such as Netflix, AppleTV, Disney Plus and Amazon, as well as video-sharing platforms, are not subject to licensing or content regulation.

In the case of over-the-air TV and radio broadcast services, the Telecom Law establishes that the granting of a spectrum licence – in the case of commercial services – must be awarded through a public auction.

Procedure

Single concessions have to be filed before the IFT along with legal documents and technical and financial plans, and the IFT has 120 business days to rule over an application; this time period is usually extended by 60 days due to additional information requests from the IFT.

The government fee for the processing of a single concession application is approximately USD1,500.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements Scope of Requirements for Local Telecommunications Rules

The Telecom Law and its subsidiary regulations govern traditional telecommunications services such as pay TV, broadband, SMS, over the air TV and radio broadcast as well as ordinary telephone calls; however, modern services such as audio-visual streaming, instant messaging or video/audio calls are not regulated or subject to licensing.

The only precedent that exists as to regulation of OTT or digital services is the antitrust authorisations issued by the IFT and/or Mexico's Economic Competition Commission (COFECI).

As it refers to those non-spectrum-based services that fall within the scope of local telecommunications rules and the requirements prior to bringing them on to the market, Mexico's Telecom Law foresees two types of licensing:

- a single concession that is facilities based; and
- reseller authorisations that allow for the resale of services provided by single concession holders.

Both licences allow for the provision of telecommunications services without limiting their scope to a specific technology.

As mentioned in **6.1 Requirements and Authorisation Procedures**, all spectrum concessions for commercial purposes are licensed through a public auction. For single concessions, the IFT has 120 business days to rule over an applica-

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

tion and the government fee for the processing of such application is of approximately USD1,500.

The government fee for the processing of a reseller license is approximately USD500 and the IFT has 30 business days to rule over an application, after which term the reseller authorisation is deemed granted if there is no reply from the IFT; however, this rule does not apply to single concession applications.

In addition to licensing, services that use national numbers like regular phone calls or SMS are subject to specific regulation for matters such as the assignment of number blocks, domestic or international interconnection, signalling and numbering.

On the other hand, terminal equipment that transmits signals through the airwaves and/or connects to a public telecommunications network has to be homologated before the IFT, it must not cause harmful interferences to other telecommunications systems and, when applicable, it must comply with the applicable National Norm Certification.

Homologation is carried out before the IFT, which has from 12-30 business days to rule over a homologation application. Homologation certificates can be of three different types, which are the following.

- Type A homologation certificates apply to equipment considered as inherently compliant according to one or more of the IFT's Technical Regulations. This type of homologation certificate applies to scientific, medical or industrial equipment. The IFT has 12 business days to issue a Type A homologation certificate, and the applicable government fees is of approximately USD45.

- Type B homologation certificates apply to equipment that the interested party intends to operate during the organisation and celebration of a specific event, considering that its use is temporary and that same shall operate as secondary use. The IFT has 30 business days to issue a Type B homologation certificate, and the applicable government fees is of approximately USD150.
- Type C homologation certificates apply to equipment for telecommunications or broadcasting infrastructure that need to comply with the IFT's Technical Regulations through a verification unit. The IFT has 30 business days to issue a Type C homologation certificate, and the applicable government fees is of approximately USD170.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges Technology Agreements - Challenges

The main challenges encountered by organisations entering into technology agreements with Mexican organisations relate to the setting up of business in Mexico, since agreements may require the incorporation/organisation of a local company, the registration of the new company's by-laws before the Public Registry of Commerce, the registration of the new company before Mexican tax and social security authorities, opening a bank account and registering the new company before Mexico's National Immigration Institute as an employer. All of these requirements can take several months to complete.

Specific Features of Mexican Laws

Mexico has no provisions on technology agreements such as price revisions or restrictions on the importation of equipment, other than compli-

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

ance with general technical norms and homologation, international data transfers or storage location. No licence is required for the provision of IT services.

Heavily Regulated Industries

As in other countries, banking and insurance are subject to greater restrictions than other industries and must obtain licensing from finance regulators, which in this case are Mexico's National Banking and Securities Commission or Mexico's National Insurance and Bonds commission.

In addition, banks and insurers have to comply with applicable laws as well as regulation approved by finance authorities, including Mexico's Central Bank, Mexico's Ministry of Finance, etc.

That said, Mexico also has a law for the Regulation of Financial Technology companies which seeks to promote and organise the operation of fintech entities and protect consumers. This new law is intended to reorganise a sector that was previously mostly unregulated, and several companies that operated prior to the enactment of this new law have not been able to meet licensing and operation requirements; nonetheless, the general public has benefitted from having more transparent and reliable fintech service providers that are also overseen by the CNBV.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Laws and Regulations in Relation to the Delivery of Trust Services, the Use of

Electronic Signatures and Digital Identity Schemes

The exponential increase in electronic transactions in Mexico is rapidly moving suppliers and consumers towards a complete digital model that requires guarantees of data integrity, confidentiality and authenticity of exchanged and archived payments, information and documents through the use of trust services, electronic signatures and digital identity schemes.

Mexico's Commerce Code recognises the validity of electronic transactions and contracts. Nonetheless, Mexico also has regulation that governs the use of trust services or e-signatures, such as the Commercial Code's Guidelines for Trust Services Providers (PSC), Mexican Norm NOM-151-SCFI-216 and Mexico's Advanced Electronic Signature Law.

The purpose of the foregoing regulation is to establish standards for information security, electronic commerce and advanced electronic signature, as well as to certify trust services providers for the issuance of digital certificates and other advanced electronic signatures.

Nonetheless, the problem with many of these certifications and standards is that many of them are not the trust services or software that most people use on a daily basis, and in such case, many users may prefer to continue using common commercial trust services and e-signatures, even if they are not endorsed or certified by Mexican authorities.

The exception to the above would be Mexico's advanced e-signature, which is absolutely necessary in order to file tax returns or exchange communications with tax authorities.

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

Relevant Elements

Due to the high volume of remote or electronic transactions in which a supplier may not have a presence in Mexico and a user or consumer may therefore not have the opportunity to file complaints at a business address or representative in Mexico, concepts like liability, insurance, data protection, jurisdiction and fundamental rights have become more important than ever.

Strong regulation is necessary in order to protect consumers and users against fraud, identity theft or misuse of their personal data, which are practices that in many cases are impossible to revert, even if they get to be sanctioned. This has happened in recent cases in which Mexico's justice system prosecuted, fined or even imprisoned individuals who committed online violations like the unauthorised distribution of private content, including pictures or videos of an intimate nature.

In these cases, jurisdiction becomes a key factor, since a person may or may not be able to file a complaint or lawsuit in their country of residence against a person or supplier they consider to have violated their rights or even their fundamental rights. In this respect, Mexican and international law have a long way to go.

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever, Ruiz Moreno & Asociados

Ruiz Moreno & Asociados specialises in the telecommunications, media and technology sectors, working with external engineers, economists and financiers to provide a truly specialised and thorough service. The team provides services and solutions to a wide variety of domestic and multinational service providers, including some of the most relevant domestic and international telecommunication operators. Lawyers often work with foreign law firms on TMT matters in Mexico and abroad. Their expertise covers wireless telecommunications, broadcast, satellites, licensing, interconnec-

tion, compliance, international co-ordination and concurrence proceedings, spectrum matters, representation before the ITU, peering and online services, the internet and IoT, infrastructure deployment, fintech, big data, privacy, blockchain, intelligent networks, spectrum and services auctions, numbering and internet resources. RM&A has represented domestic and international clients in their entry into the Mexican TMT market, including in matters such as licensing, access to services and infrastructure, interconnection, infrastructure deployment and complex regulatory matters.

Authors



Iván Ruiz Moreno is the founding partner at Ruiz Moreno y Asociados and has more than 20 years' experience in TMT, regulated industries, infrastructure, corporate and

commercial law. Throughout his career, he has worked as a public officer of the former Mexican Federal Telecommunications Commission, a member of the Federal Commission of Telecommunications' (COFETEL) Consultation Council, a parliamentary counsel and outside legal counsel/board member for domestic and international companies from three different continents, including start-ups, consolidated carriers and CFE Generación II, which is an affiliate of the incumbent state-owned power company CFE. Iván has represented clients in areas such as telecommunications, broadcast, corporate law, contracts, antitrust and the electric sector.



Rubén Gutiérrez Díaz is a senior associate who works in the areas of corporate law, trade marks, real estate, contracts and fintech. Prior to joining Ruiz Moreno y Asociados, he worked

on corporate and commercial law matters at a law firm in Madrid, Spain, as in-house counsel at international real estate firm Jones Lang Lasalle, and as in-house counsel for a publicly traded lumber company with real estate in Mexico and Latin America.

Contributed by: Iván Ruiz Moreno, Rubén Gutiérrez Díaz, Eli Manuel Ramírez and Erika Estrever,
Ruiz Moreno & Asociados



Eli Manuel Ramírez is a senior associate at Ruiz Moreno y Asociados, specialising in regulatory, privacy and commercial law in general, attending to clients in the TMT

sector. Prior to joining the firm, Eli worked as an in-house lawyer and compliance officer for the Mexican subsidiary of an international wireless carrier, and as an in-house lawyer for a fixed service provider. He has participated in technology and regulatory projects for TMT clients as part of their launch of operations in the Mexican market.



Erika Estrever is a senior associate with more than ten years' experience in the TMT sector. She attends to clients in the areas of regulation, compliance, privacy, real estate,

administrative and consumer procurement law. Prior to joining Ruiz Moreno y Asociados, she worked as in-house regulatory counsel for a major TV broadcaster in Mexico, as a legal adviser to several domestic and international companies in the TMT sector, including in broadcast spectrum auctions, and as a litigation associate at a major law firm in Mexico City.

Ruiz Moreno & Asociados

Campos Elíseos N° 223
6th floor
Col. Polanco
11560 Mexico City
Mexico

Tel: +52 55 1209 6611
Email: contacto@rmlaw.com.mx
Web: www.rmlaw.com.mx

RM&A
Ruíz Moreno y Asociados

Trends and Developments

Contributed by:

Paola Morales V. and Daniel Legaspi J.
Santamarina y Steta SC see p.324

Overview

The relevance of every aspect of TMT services in a post-pandemic world is undeniable, and this increasing trend will continue to be seen in Mexico in the forthcoming years. The most recent official data available shows that 60.6% of homes in Mexico have internet access, representing 84.1 million users, and 91.6% of the population have access to a television, of which 42.8% have paid television (71.5 million people).

With respect to users of mobile phones, a total of 88.2 million people have at least one mobile phone. Telecom operators reported an annual revenue of MXN428,686 million (approximately USD21 billion). By segmenting the revenue information between the main operators that offer fixed services and those that offer mobile services, it is evident that the former had an accumulated real revenue of MXN181,346 million, a number possibly related to the increased use of fixed broadband in household activities during the pandemic. Mobile operators had annual revenues of MXN224,724 million.

Regarding social media, surveys reveal that Facebook is the social network with the highest percentage of users in Mexico (97% of social network users said they have access to Facebook). WhatsApp was the second most-used platform by Mexicans, accounting for 95% of those surveyed. In third place was Instagram, with 73%.

The data shows that the users require more efficient and faster connections to interact with basically everything in their ecosystems. From a

company's perspective, Mexico is a fertile environment to continue offering more "anything as a service" (XaaS) or Xtech services, which has led not only to the operation of those services or businesses being analysed, but also protection from an IP standpoint to allow companies to have IP rights that are enforceable against any violator.

The increase in revenue resulting from new technologies, the continued success of recently implemented technology and innovative business models will be worth following in Mexico in the coming years.

Deployment of 5G Networks and Related Services

Undoubtedly, the deployment of 5G networks by the two major telecommunications service providers has raised great expectations amongst users and service providers and has encouraged the users to start migrating to service plans that run on these networks (although still noded with 4G).

Currently, AT&T has coverage in 25 cities and Telcel has coverage in 40; Telcel forecasts reaching 120 cities with approximately 58 million clients by the end of 2023. The current challenge is to adapt these plans to make them accessible to the majority of Mexicans, who currently pay, on average, MXN145 (approximately USD8).

The issue of data consumption is also something to bear in mind, as well as the availability of devices that can operate with this technology. One of the confirmed benefits of 5G networks is

the faster download speeds; for example, if the current available plans offer between 10 and 15 gigabytes, the user will consume the capacity contracted in the plan by downloading a couple of movies.

The cost structure must also be lightened for the operators so that they can invest more and at a faster pace to make this deployment a reality. Considering this challenge, the main element currently being discussed amongst policymakers is the overpricing of the radio-electric spectrum, which in Mexico is 85% more than in other countries. Therefore, the reduction of this cost by the tax authorities is currently under discussion before the next public bid is launched.

Also, in January 2023, the regulator began the public consultation to obtain the bases and information necessary to launch the IFT-12 public bid, corresponding to the allocation of a radio-electric spectrum for the development of 5G technology. The consultation, which is expected to end in February, is intended to gather data, opinions, and specific and substantiated proposals from all those interested in the matter to prepare the draft for the next public bidding process. With this allocation, the regulator seeks to launch into the market frequencies suitable for mobile telephone and broadband services. With this, 330 national megahertz (MHz) could be made available to the market, of which 90 MHz are in low bands (below 1 GHz) and at least 240 MHz more are in medium bands.

The definition of the cost and the preparation of the coming bidding process would be key for the completion of the full deployment of these networks, allowing the latency to reduce to a minimum and the number of connected devices to multiply exponentially.

The trend services that are aimed to be rendered with the availability of this technology are gaming with augmented reality, IoT, telemedicine with the management of automated medical devices (operating robots), security systems, and autonomous cars. Service providers in these industries are already exploring business alliances and investment opportunities to be right there from the start.

E-commerce Everywhere and for Everything

Among the most popular trends in the Mexican market have been platforms, web pages, apps, and all other forms of commerce carried out by electronic or optic means or by any other technology. Now, these are the first option for all types of services.

Certain guidelines and specifications need to be met mainly for the protection of consumers. Depending on the type of services, other technical standards, like security regulations, encryption, or data privacy provisions, must also be considered. However, in general terms, investing and making available e-commerce businesses in Mexico is fairly simple. Non-regulated educational services, the sale and purchase of all types of goods, financial services, information services and insurance services were the most requested services. The increase in internet access available to the population has made this feasible. The basic premise of net neutrality in Mexico is associated with the principle of ensuring that all users can freely access all content, applications and services of their choice.

Also, internet access service providers must treat the traffic generated by their users under the same conditions regardless of content, origin or destination, and this has allowed this new manner of doing business to take shape. Accordingly, the applicable law establishes an obliga-

tion for concessionaires and authorised resellers to provide internet access services that respect users' free choice to access any content, application, or service without discrimination and with privacy, transparency and information.

Likewise, Mexican net neutrality is specific in stating that service providers must take the measures or actions necessary for traffic management and network administration to guarantee the capacity, speed and quality contracted by the user, regardless of the content, origin, destination, terminal or application, including services provided through the internet. Therefore, players intending to invest and diversify in Mexico should continue to consider this manner of doing business.

The Transformation of the Media Sector

Content in traditional broadcasting and distribution platforms requires express authorisation and classification, which must also be highlighted to the audience.

Advertisements in television broadcasting need to be appropriate for all members of the public, and there are express limitations in relation to alcohol, tobacco, bars and advertising that could be deemed offensive or not moral.

Advertising on traditional broadcasting systems must keep a balance with the time assigned to the programming. On TV stations, advertising time cannot exceed 18% of programming time. Furthermore, during electoral periods there are specific obligations for broadcasters, such as assigning broadcasting time to the National Electoral Institute and avoiding selling and transmitting advertising space for political campaigns during the period established by the Institute.

The aforementioned restrictions are not established for content delivered over the internet or any other platform. These platforms offer a catalogue of content and do not offer a limited amount of linear programming. They do not require a concession to offer the service, and they do not have guaranteed quality since they depend on the user's internet connection. They can be viewed at a time and in a sequence decided by the user. Although they require the user to have a device with internet access (ie, the user must have an additional service), they are the first form of entertainment to reach users. Accordingly, over-the-top media services for audio-visual content have found an extraordinary niche within the Mexican market, offering a near-term opportunity for business.

Additionally, in September 2021, a new law came into effect that changed how the publicity sector interacts with media, agencies, and advertisers. Certain specific requirements and restrictions were imposed to oblige these actors to reinvent and adapt their customary manner of doing business. A year and a half after this drastic change, the players have adapted, and internet advertising (mainly through digital platforms and social media) is the place to go, considering entertainment trends aimed at internet-offered content.

Metaverse Development

The metaverse is the next step to be achieved when speaking about new technologies. Although it is not yet fully-developed, businesses have started to become interested in accessing the metaverse, placing their trade marks in it, operating virtual offices, having a presence in this new parallel reality, and analysing how to comply with the current applicable laws.

There is a high probability of losing control of privacy in the metaverse due to the technological developments that allow personal data to be used and marketed without users even knowing (ie, without consent). On the other hand, companies, organisations, and even governments are aiming toward protective approaches as they have become aware of the dangers of losing privacy in this new reality. As a result, new manners of carrying out data privacy compliance and analysis are beginning to be implemented.

Algorithms, AI, and whatever comes next in shaping the metaverse are the future handlers of personal data. Therefore, having proper technical standards, software, data repositories and technology has occupied the efforts of software developers and data privacy and intellectual property lawyers.

From an IP standpoint, it is pertinent to highlight the way multiple pieces of software interact and change the way trade marks and content, such as NFTs, can be offered and protected. This challenge brings evolution to IP, which will derive new interpretations as to what can or cannot be protected or used without authorisation.

Also, from the beginning of their product development, metaverse handlers are considering populating the individual's data features using k-anonymity standards and de-identification techniques to "manage" those unwanted traits that may damage the acceptance of these new desired anonymous or parallel interactions.

Accordingly, all matters related to the metaverse are among the most important new business trends to be explored in Mexico.

Protecting Intellectual Property Associated with Technology

The use of technology is part of our daily activities; this has led consumers and companies to provide a more efficient and secure environment, specifically when it comes to personal data. However, the development of these new technologies has placed companies in a position where they have to determine the type of information that may be seen by the user (ie, source code).

Information on the method of protecting a source code is becoming more frequently requested by companies, which has required them to provide tailor-made strategies that may include secret industrial policies, work-for-hire agreements, amendments to individual labour contracts, non-disclosure agreements or other collateral analyses.

Furthermore, trade marks in digital environments such as the metaverse have influenced the Nice Classification to incorporate terms such as non-fungible tokens to bring more certainty to their holders.

IP receiving increased attention from companies is a positive result, bringing "win-win" situations to holders. On one side, having different strategies to protect technology brings confidence to the holders and developers. On the other hand, the consumer is also benefiting from the tools provided by technology in its day-to-day operations.

Therefore, it is likely that the interest from companies in protecting other intangible assets besides trade marks will continue growing and challenging IP specialists to create tailor-made strategies focusing on such protection without affecting the operation of the technology.

Santamarina y Steta SC stands out for its highly valued expertise. With more than 80 lawyers in its Mexico City, Monterrey, and Querétaro offices, Santamarina y Steta's clients rely on a specialised multidisciplinary team for TMT, IP, data privacy, e-commerce, and consumer protection. Santamarina y Steta's team has assisted Honeywell in its aerospace and telecommunications services; Paramount Pictures and Grupo CIE in their media requirements; Tesla, Walmart, and New Balance in their e-commerce and data privacy needs; Walmart Con-

nect in some advertising services; and Solera, Kolonus, and Teleperformance in registering the IP side of their apps. It has also assisted other start-ups that have required assistance in applying the best strategy to protect their IP. The firm is known and regarded for its proficiency in the design of structures for foreign investments to participate in telecommunications, broadcasting, IT services, and new tech industries. In addition, the firm's resourcefulness consistently allows it to meet the demands of clients in developing disruptive business models.

Authors



Paola Morales V. has over 22 years of experience and is the leading partner of the TMT, e-commerce, privacy and data protection practices at Santamarina y Steta SC. She

has advised international and local clients in the TMT sector implementing their businesses and investments in Mexico from a transactional and regulatory standpoint. Likewise, she reviews, negotiates and prepares legal instruments for e-commerce operations in Mexico and data privacy compliance. Paola is a member of ITECH Law and Abogadas MX, and she recently served as a jury member in the "Innovation and Best Practices in the Protection of Data Privacy Contest" organised by the National Institute for Transparency, Access to Information and Personal Data Protection.



Daniel Legaspi J. has over 15 years of experience and is the partner leading the IP, franchising, licensing, and IP technology practices at Santamarina y Steta SC. His

practice specialises in assisting national and international clients in maximising the profitability of their intangible assets by developing and executing customised strategies in and out of Mexico through the assistance of the firms' other practices. He has been a panelist, speaker, and professor in intellectual property, entrepreneurship, and technology through the International Trademark Association (INTA), the Inter-American Association of Intellectual Property (ASIPI), and other associations and universities. He is part of the Executive Committee of the National Chamber of Commerce (CANACO), where he leads the IP practice.

Contributed by: Paola Morales V. and Daniel Legaspi J, **Santamarina y Steta SC**

Santamarina y Steta, S.C.

Campos Elíseos 345
floors 2 & 3
Polanco Chapultepec
Miguel Hidalgo
11560, CDMX
Mexico

Tel: +52 55 5279 5400
Email: comunicacionsys@s-s.mx
Web: www.santamarinasteta.mx

Santamarina
+ Steta

Trends and Developments

Contributed by:

Herald Jongen, Radboud Ribbert,
Dr Robert Hardy and Eduard Stein
Greenberg Traurig, LLP see p.332



Introduction

In 2023, the Netherlands will continue to be governed by a centrist but overall progressive and generally pro-business coalition and will remain a top jurisdiction for tech, media and telecommunications in Europe. Its infrastructure and connectivity are top of the bill, hosting not only the AMS-IX internet exchange but also a multitude of data centres including Google and Microsoft. Its workforce is highly skilled in information technologies and media production, and its government, regulatory authorities and courts are competent, professional and generally pro-business.

In 2022, the Netherlands reached a high degree of pushback against the dominance of big tech platforms, seeing, for example, multiple class action suits, the scuttling of Meta's plans for a hyperscale data centre, high-profile regulatory cases against Apple (among others), and significant political posturing. This discussion has recently died down with other issues taking centre stage in the public's attention, especially the war in Ukraine, and as a result the government and politicians will have the space to take a more nuanced view going forward. However, Dutch regulators, in particular the competition authority and the data protection authority, are seeing their regulatory scope and powers expanded due to new EU regulations and other factors; therefore, it seems likely that there will more enforcement action in the near future, even in a context that is friendlier overall.

The main topics for concern for the government at this time seem to be the following:

- AI, after a number of high-profile cases where the government itself overstepped its boundaries; and
- cybersecurity, with the war in Ukraine raising threat awareness.

There have also been interesting developments arising out of social media platforms and the new media environment, including new policy rules in respect of influencer marketing and increasing discussion on synchronisation copyrights. From a media infrastructure perspective, 2023 also looks to be an interesting year, with spectrum auctions for commercial FM radio stations upending an established market, and auctions for faster 5G frequencies having the potential to alter competitive dynamics in telecommunications.

Below, discussion will cover a number of relevant developments in the Netherlands in more detail.

5G and FM Frequency Auctions to be Held

2023 will be a busy year for media companies and telecommunications companies, with auctions of both 5G and FM frequencies taking place.

In June 2020, the Netherlands auctioned off its first sections of 5G spectrum, for 700 MHz frequencies. The second auction of 5G spectrum, for 3.5 GHz frequencies, is now set for 2023. The

ultra-high speed, low coverage 26 GHz bands will follow, but the exact timing is not yet clear.

The Dutch government must also reallocate the nine FM frequencies for commercial radio stations, the Trade and Industry Appeals Tribunal (*College van Beroep voor het Bedrijfsleven*) ruled in December 2022. The Tribunal thus drew a line under the government's intention to extend the existing licensees' licences for the use of these FM frequencies from 31 August 2022 onwards.

The nine FM frequencies were first allocated by auction in 2003. At the time, five FM frequencies were subject to programme content requirements, such as broadcasting news and current affairs or broadcasting dance music. The remaining four FM-frequencies had a free format. The highest bid was made by John de Mol's Radio Noordzee, with a bid of over EUR80 million for a FM frequency with a free format.

The FM frequencies were distributed in 2003 for a period of eight years and three months, and the licences ended on 31 August 2011. Since then, the licences have been extended several times, and current licence holders retained their FM frequencies. This precluded new parties from entering the market. In 2022, the Dutch government again decided to extend the existing licences for a period of three years to allow the licence holders to recover from the damage they allegedly suffered as a result of the COVID-19 pandemic. However, the Trade and Industry Appeals Tribunal ruled in December 2022 that this extension was a disproportionate measure, and that it was unlawful towards newcomers to the commercial radio station market. The FM frequencies must therefore be reallocated.

Once again, nine FM frequencies are at stake in 2023. The licence term will be 12 years. Only two

FM frequencies are subject to content requirements, namely a radio station for broadcasting Dutch-language music and a radio station for broadcasting news and current affairs. The Dutch government limits the number of FM-frequencies a commercial radio provider can have to three. This means that John de Mol's Talpa, now holder of licenses to use four separate FM-frequencies, will lose at least one FM frequency. The allocation must be completed by 1 September 2023, the Trade and Industry Appeals Tribunal ruled.

Contours for Algorithm Oversight Released, High-Profile Cases in Government Use of Algorithms for Decision Making

From 2023, the Dutch Data Protection Authority (DPA) will start acting as the Dutch regulator for algorithms. An extensive policy document on the intended approach to these tasks was issued in December 2022. Based on the policy document, the DPA will, at first, play an important role in co-ordinating the effective regulation of algorithms as many other sectoral regulators have their own independent responsibility in this respect. It will focus on creating platforms for co-operation between regulators, creating risk-based assessments of where to act in particular, and developing tools and methods to improve regulation. It will also continue to take direct regulatory action based on the power granted to it under the GDPR and its budget to do so has been expanded. It is as such fair to expect that from 2023 onward, scrutiny of the use of algorithms and AI will continue to increase.

In this respect, it is worth noting that 2022, and the end of 2021, saw a number of high-profile cases in respect of the use of algorithms by governments. The two most egregious breaches were by the Dutch tax authority. Both related to the use of extensive racial, ethnic and other

forms of discriminatory profiling by the Dutch tax authority, and resulted in the two highest fines ever issued by the DPA, EUR2.75 million and EUR3.7 million.

Increasing Protection for Gig Workers

The re-classification of gig workers from independent contractors to employees is still a hot topic in the Netherlands. On 17 June 2022, Advocate General (AG) De Bock issued an advisory opinion in a landmark court case between FNV, a Dutch trade union, and online meal delivery company Deliveroo. The main question in her view should be whether the work is “organisationally embedded” in the company. When the work carried out forms part of the company’s core activities, the work is organisationally embedded, which would immediately mean that there is employer authority or “control” over the work, implying the individual conducting such work activities qualifies as an employee. The Supreme Court’s decision was expected on 23 December 2022 but has been postponed. As it stands, digital platforms that rely on a large force of workers to perform a key activity for their business should assume there is a significant probability those workers may qualify as employees (regardless of the content of the contract into which parties have entered).

Active Competition Regulator Gearing-Up for DMA and DSA Oversight

The Dutch Competition Authority (ACM) has taken an active stance on monitoring and regulating major tech companies, developing its own views and approaches complementary to the EU competition regulators. Exemplary for this is its August 2021 decision establishing that Apple was abusing its economic dominance by forcing dating app providers to accept terms by which they must either utilise Apple’s payment service or use less customer-friendly alternatives,

rather than other third-party payment providers. Apple complied with the ACM’s decisions in June 2022, after having fought the decision in court and forfeiting EUR50 million in penalties for delayed compliance.

In 2022, the digital economy was also one of the ACM’s key focus areas, with a specific focus on combating unfair terms for online services, undue influencing of minors, misleading or fake reviews and likes, and a study into the market for cloud services, among other things. Though not formally stated, it can be seen that the ACM is anticipating new EU regulations, in particular the Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Governance Act, and the Data Act.

The DMA will represent a shift in competition enforcement in the EU – for example, while in the past enforcement was largely done *ex post*, the DMA sets out *ex ante* rules. The objective of the DSA is to ensure transparency, user safety, and accountability for online platforms. Both the DMA and DSA will have a considerable impact on business in the Netherlands in 2023, as market players gear up to comply. The DMA will become applicable in May 2023. The so-called designated “gatekeepers” will have a maximum of six months after their designation decision by the European Commission – which is expected at the latest in September 2023 – to ensure compliance with the obligations set out in the DMA; thus, ultimately, compliance should be ensured in March 2024. The DSA will apply from February 2024. As regards the obligations for so-called “very large online platforms” and “very large online search engines”, the DSA will apply from an earlier date – four months after their designation.

The ACM has also proposed amendments to the Data Act, based on its study into the market for cloud service providers. The key risks it has identified in the market for cloud service providers are its extreme concentration and the switching costs, due to both actual financial costs imposed for switching (such as data migration fees) and the high level of technical integration of services, which hobbles customers in using services from multiple sources. Though the DMA will resolve some of these issues, in particular high financial impact of migration and data portability, interoperability is not covered fully as a separate topic, and the ACM has therefore proposed that the Data Act contain specific and more extensive provisions on interoperability, as a separate topic from data portability, to address these risks more fully.

Increasing Merger Control

The complexity for transactions in the tech space in 2023 will increase. Key drivers are:

- future notifications under the EU Foreign Subsidies Regulation regime (adopted on 28 November 2022 and due to apply by mid-2023), intended to limit the ability of entities subsidised by foreign states to acquire EU companies;
- pre-closing submissions pursuant to the forthcoming Dutch National Security Investment Act (*Wet veiligheidstoets investeringen, fusies en overnames*), intended to keep vital infrastructure and services under national control, which is expected to enter into force in the first quarter of 2023; and
- increasing EU merger control for transactions with effects only in one member state as a result of Case T-227/21, *Illumina, Inc v European Commission*, which will require EU merger control analyses to be applied even

for transactions that only impact the market in the Netherlands.

Cybersecurity Strategy and New Opportunities

Cybersecurity is a matter of increasing concern in the Netherlands and has become a clear government priority in the coalition agreement. The Netherlands issued its cybersecurity strategy for 2022-29 on 10 October 2022 along with a plan of action with high level timelines. Most relevant for participants in the Dutch market is that the plan has a heavy focus on public/private shared action and responsibility, development and implementation of security technology, and skills and capability building – ie, it is likely that the market for these services will expand significantly over this period, as will the Dutch talent pool (which is already excellent).

Regulations for “Influencer” Marketing Being Tested

The rise of social media platforms, such as Instagram, YouTube and Snapchat, has provided a stage to those with purported expert-level knowledge and/or social influence in their field (“influencers”). These influencers have a (seemingly) unlimited scope for sharing their vision, ideas, and other messages with their followers. However, their content is also often of a commercial nature (eg, advertisement of products or services, offers of advice, and promoting political opinions). Given their large audience, influencers can be very effective in creating online engagement for the companies that employ their services, but also in manipulating the opinions and purchases of their followers, at least in part because followers are not always able to distinguish between genuine and sponsored advice.

On 1 July 2022, Dutch Media Authority (DMA) set policy rules with respect to influencers,

determining which influencers would fall within the regulatory scope of the Dutch Media Act as a commercial media service on demand. If so classified, the influencer is required to register with Stichting Reclame Code and the Netherlands Institute for the Classification of Audio-visual Media. Moreover, influencers must now meet extensive requirements for fair advertising, including making clear in the broadcast that the programme is sponsored or that it contains advertisements or product placement. In the policy rules, the DMA determined that influencers active on YouTube, Instagram or TikTok with over 500,000 followers or subscribers who regularly upload videos, obtain compensation in cash or in kind for their videos and are registered with the Dutch Chamber of Commerce will be considered commercial media services on demand.

The DMA is now undergoing a transition and trial period, wherein it is testing the effectiveness of the rules and providing influencers with time and guidance to become compliant.

Sync Rights are Increasing in Popularity

There has been a significant spike in the use of popular songs in combination with short videos on major video platforms, such as TikTok, YouTube, and Instagram. Typically, this is referred to as synchronisation, ie, the simultaneous integration of music used as a soundtrack with visual images. Prominent examples of such use are the Oscar-winning movie “Bohemian Rhapsody” and the use of Kate Bush’s “Running Up That Hill” in the Netflix series Stranger Things, both resulting in substantial royalties.

Synchronisation rights involve to the right to authorise the inclusion of musical works in audio-visual works. However, this right is not recognised at the international level by any of the copyright agreements and treaties, nor is it

embedded in the Dutch Copyright Act (*Auteurswet*) or the EU Copyright Directive (Directive 2001/29).

The Dutch courts have generally been evasive with regard to carving out a definition for synchronisation rights, with one exception where the District Court (*rechtbank*) of Amsterdam ruled on a case wherein music was synced to a theme park attraction in Efteling, a Dutch theme park. The District Court of Amsterdam held that the use of a musical work at an attraction was exclusively a form of publication within the meaning of Article 12 of the Dutch Copyright Act. Publication is the exclusive right of the copyright holder to communicate the work (eg, a musical work) to the public.

The Court of Justice European Union (CJEU) has only decided on synchronisation rights in relation to neighbouring rights (eg, the rights to a sound recording). In *Atresmedia v AGEDI and AIE*, the CJEU confirmed that fusion of a sound recording into an audio-visual work does not constitute a reproduction of that sound recording. Therefore, the synchronisation does not fall under the umbrella of the (exclusive) neighbouring right.

In reality, synchronisation rights receive more recognition in business practice, where collective rights organisations (eg, Buma/Stemra in the Netherlands) play a distinct role in enforcing the synchronisation rights of artists and record labels. However, the enforcement actions available are only those following the breach of contract wherein the synchronisation right defined and granted.

Article 17 of Directive 2019/790 on Copyright in the Digital Single Market creates a system in which the content service provider such as Tik-

Tok, YouTube and Instagram must obtain permission from the rights-holders for the use of copyrighted work. This directive is expected to ensure an increase in the amount of synchronisations on the internet, and consequently an increase in revenue for rights-holders.

Government Cloud Policy

There is a continued and accelerating move towards the cloud happening across the private and public sector, providing a strong market opportunity. In this context, the Dutch government issued its government-wide cloud policy in August 2022, under which it sets the guidelines for using cloud service providers. These guidelines are practical and implementable, including for US service providers, and thus enable the Dutch public sector, the semi-public sector and concerned companies in the private sector to access the benefits of cloud services going forward, thus opening up significant new markets.

New Reporting Obligations for Platform Companies in Respect of Tax

In March 2021, the Council of the European Union adopted Directive 2021/514 (also known as DAC-7), with the aim of improving administrative tax co-operation, countering tax fraud/tax evasion and addressing the challenges posed by the digital platform economy. They include new rules extending EU tax transparency requirements to digital “platforms” and introducing an obligation for “platform operators” to provide

information on income derived by sellers through those platforms. The rules affect platform operators offering sellers access to:

- the rental of immovable property, including both residential and commercial property, as well as any other immovable property and parking spaces;
- a personal service;
- the sale of goods; and
- the rental of any mode of transport.

The Netherlands implemented the DAC-7 directive into its local laws as per 1 January 2023.

Delayed Introduction of Digital Services Tax

In their December 2021 coalition agreement, the Dutch parliamentary parties that agreed to form a new government set out their new government’s plans and ambitions for 2021–25. These plans included the introduction of a digital services tax in the Netherlands. However, unlike several other EU member states, the Netherlands has not yet introduced such tax. Instead, it seems likely for now that the Netherlands will await global acceptance of the OECD’s initiative to adapt the multilaterally agreed international tax system currently in place in such a way that some of the world’s largest multinational e-commerce businesses would need to start paying income taxes not based on where they are located or are otherwise active, but based on where their consumers are located (also known as “Pillar 1”).

Greenberg Traurig, LLP is an international law firm with approximately 2,650 attorneys serving clients from 44 offices in the United States, Latin America, Europe, Asia, and the Middle East. The firm's dedicated TMT team consists of more than 100 lawyers, seven of whom are located in Amsterdam. The Amsterdam team is well-versed in representing clients around the

world in domestic, national, and international policy and legislative initiatives, as well as guiding them through the business growth cycle for a variety of technologies. As a result, the firm provides forward-thinking and innovative legal services to companies producing or using leading technologies to transform and grow their businesses.

Authors



Herald Jongen is co-managing shareholder at Greenberg Traurig. He focuses his practice on outsourcing, technology transactions, data protection, strategic relationships and M&A.

He has led many complex multi-jurisdictional matters in the technology and financial industries. His forte is deal-making and he goes where the deal is, which has taken him to New York, Silicon Valley, London, Paris, Brussels, Stockholm, Berlin and Frankfurt, among other places. Jongen is known for his efficient pressure-cooker negotiations. In recent years, he assisted the Dutch government on landmark negotiations with large US tech.



Radboud Ribbert has over 25 years of extensive experience and is an experienced entertainment and media lawyer. He is a well-known expert on media law, copyright law and

neighbouring rights law. Ribbert advises clients on the creation of television and radio stations, and on the distribution of the signals of these stations. He has litigated copyright issues with respect to the satellite transmission of music in television signals with copyright societies, and was involved with the auction of the FM radio frequencies for commercial radio broadcasters.

NETHERLANDS TRENDS AND DEVELOPMENTS

Contributed by: Herald Jongen, Radboud Ribbert, Dr Robert Hardy and Eduard Stein, **Greenberg Traurig, LLP**



Dr Robert Hardy has over 14 years of experience in antitrust litigation and competition regulation. He represents clients before the European Commission, the Dutch

Competition Authority, Dutch administrative law courts, and the EU courts in matters relating to cartels, dominance, merger control, and state aid proceedings. In addition, he represents clients before the Dutch civil law courts on issues relating to standard-essential patents and fair, reasonable and non-discriminatory licensing disputes. Robert's sector focus includes technology and telecommunications.

Eduard Stein is a senior technology lawyer. He has broad and deep knowledge of IT, IP, privacy and contract law. Eduard combines his legal experience with strong commercial acumen and technical knowledge, having worked as a strategy consultant at the Boston Consulting Group and as a digital and IT strategy consultant at Royal Dutch Shell. He constantly keeps his technical skills up to date, for example, by building simple AI models, training in ethical hacking and creating low-code applications and data visualisations.

Greenberg Traurig, LLP

Beethovenstraat 545
1083 HK
Amsterdam
The Netherlands

Tel: +31 651 289 224
Email: Herald.Jongen@gtlaw.com
Web: www.gtlaw.com



Law and Practice

Contributed by:

Ijeoma Uju, Oghomwen Akpaibor,
Tomisin Olanrewaju and Victoria Oloni

Templars see p.354



Contents

1. Metaverse	p.335
1.1 Laws and Regulations	p.335
2. Digital Economy	p.336
2.1 Key Challenges	p.336
3. Cloud and Edge Computing	p.341
3.1 Highly Regulated Industries and Data Protection	p.341
4. Artificial Intelligence and Big Data	p.343
4.1 Liability, Data Protection, IP and Fundamental Rights	p.343
5. Internet of Things	p.345
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection	p.345
6. Audio-Visual Media Services	p.346
6.1 Requirements and Authorisation Procedures	p.346
7. Telecommunications	p.349
7.1 Scope of Regulation and Pre-marketing Requirements	p.349
8. Challenges with Technology Agreements	p.349
8.1 Legal Framework Challenges	p.349
9. Trust Services and Digital Entities	p.352
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes	p.352

1. Metaverse

1.1 Laws and Regulations

Regulating the Metaverse

Nigeria currently does not have any specific laws or regulations on the metaverse. However, as technology advances and the practical uses of the metaverse expand, it is highly probable that new legal and regulatory issues will arise and trigger some legislative response to address those nuanced features of the metaverse. Businesses will need to navigate questions around jurisdiction and conflicts of law, which as of today are yet to be satisfactorily resolved even for the current internet.

Over the past 30 years, nations with significant internet usage (including Nigeria) have developed or are in the process of developing new regulations in emerging sectors such as e-commerce, technologically based crimes, consumer rights for digital content, and the liability framework for internet service providers, among others. Despite this, Nigeria is yet to develop a specialised set of rules or guiding principles for the metaverse. Certain provisions under extant legislation, however, could be interpreted to extend their application to the metaverse.

Key Legal Considerations

Intellectual property

The metaverse creates new opportunities for intellectual property (IP) rights holders to exploit and monetise their works. While the legal jurisprudence around IP of the metaverse is still at a nascent stage, the current legal framework for intellectual property protection could be expanded to cover certain components of the metaverse.

Under the Nigerian Copyright Act, computer programs are protected as literary works, and

this may be broadly construed to accommodate copyright protection in the metaverse. Separately, Nigeria is a signatory to various international treaties on IP and to the WIPO Copyright Treaty, which updates the Berne Convention for the digital age and makes clear that the storage or reproduction of a protected work in digital form on an electronic medium (such as an NFT or a file whose content is visible in the metaverse) constitutes a reproduction that requires the prior consent of the owner of the protected work. It should be noted that although Nigeria is a signatory to and has ratified a number of IP conventions/treaties, most of these are yet to be domesticated into laws in line with the Nigerian Constitution.

Trade mark protection is tied to registration under Nigerian law. Nigeria currently uses the ninth edition of the NICE Classification for its trade mark registrations. Although the NICE Classification does not expressly recognise trade mark protection in the metaverse, such protection may be classified under Class 9 specifically as “recorded and downloadable material”. This is attributable to the 3D component of the metaverse, which may be used to create renderings in the metaverse. Trade marks in the metaverse can also be protected under the following classes:

- Class 35 – provision of advertising services via the internet;
- Class 36 – provision of financial services via the internet;
- Class 38 – telecommunications services, chat room services, portal services, email services, providing user access to the internet, radio and television broadcasting; and
- Class 42 – protection for marks involving scientific and technological services and the creation, maintenance and hosting of web-sites.

Another important aspect of IP protection in the metaverse is patents. To the extent that the component features of the metaverse meet the eligibility requirements under the Patents and Designs Act, they should be eligible for patent protection. To be eligible for patent protection under the Patents and Designs Act, the invention for which an application is filed must be new, result from inventive activity and be capable of industrial application.

Data protection and cybersecurity

Along with its tremendous growth potential, the metaverse raises serious privacy and data protection concerns, particularly regarding jurisdiction, consent, sensitive personal data, etc.

The Nigerian Data Protection Regulation (NDPR) is the primary law regulating data protection in Nigeria. The NDPR provides strict guidelines that regulate the use, processing and transfer of personal data of persons resident in Nigeria and Nigerian citizens resident abroad.

The NDPR could arguably apply to the metaverse, as could the Draft Data Protection Bill 2022. However, given the novel nature of the metaverse, to ensure that users' rights are protected, the provisions of these laws may need to be revisited. In the interim, companies that operate metaverse platforms and other parties must adhere to various standards before handling personal data belonging to users. These standards include identifying and documenting the lawful basis for processing data (in the case of sensitive data, explicit consent), disclosing the reason for data collection, the type of data collected and the intended use of the data. These companies are also required to report data breaches and file audit reports where applicable.

The metaverse also raises cybersecurity concerns, including in regard to financial fraud, identity theft, security breaches, virtual/augmented/mixed/extended reality threats, and social engineering. In this respect, metaverse platforms will be required to comply with the Cybercrimes (Prohibition and Prevention) Act (CPPA) 2015. Under the CPPA, metaverse platforms are required to keep all traffic data and subscriber information as may be prescribed by the relevant authority for a period of two years. In addition, any person or institution who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team (CERT) Co-ordination Centre of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT may take the necessary measures to tackle such issues.

2. Digital Economy

2.1 Key Challenges

The Nigerian Communications Act 2003

The Nigerian Communications Act 2003 (NCA) is the principal law for the regulation of telecommunications services in Nigeria. The Act establishes the Nigerian Communications Commission (NCC) which is the primary telecommunications regulator in Nigeria. Under the Act, the NCC has the authority to make subsidiary legislation by way of regulations, guidelines, etc, to regulate the provision of communications services (including communication of things) in Nigeria.

The NCA provides that anyone who intends to operate a communications system or facility or to provide a communications service must have been authorised and licensed by the NCC or have been exempted from such requirements.

A separate licence is usually required for each type of telecommunications activity, although it is also possible for several activities to be undertaken under a single licence.

The NCC provides two general categories of licence – individual licences and class licences. Individual licences are typically bespoke licences where the terms and conditions upon which the licence is granted are specific to the activity undertaken by the licence holder; whereas for class licences, the terms and conditions upon which the licence is granted are common across all licensees.

The Nigerian Data Protection Regulation 2019

The Nigerian Data Protection Regulation 2019 (NDPR) is the principal data privacy law in Nigeria, with the core objective of safeguarding the privacy rights of natural persons residing in Nigeria or citizens of Nigeria residing outside the country in tune with international best practices.

As an improvement to the provisions of the NDPR, the Data Protection Bill 2022 (DPB) is being considered by the national legislature. The DPB designates the data freedom and data rights of data subjects as fundamental human rights, and seeks to protect these rights through technological and organisational measures.

The National Digital Economy Policy and Strategy

The National Digital Economy Policy and Strategy (NDEPS) is a national strategy plan developed by the Federal Ministry of Communications and Digital Economy. The policy document sets out a ten-year plan within which digital technologies would be adopted for the stimulation of growth in all sectors of the economy. A core objective of the NDEPS is that Nigeria achieve 95% digital literacy within the next ten years.

The Advertising Regulatory Council of Nigeria Act 2022

The Advertising Regulatory Council of Nigeria (ARCON) Act 2022 establishes a regulatory framework for the Nigerian advertising and marketing communications industry for the purpose of ensuring that Nigerians are only exposed to pre-approved content. The ARCON Act establishes the Advertising Regulatory Council of Nigeria (ARCON), which is empowered to formulate policies on all activities relating to advertising, advertisements and marketing communications in Nigeria. From this, the ARCON has set out the following policies:

- from December 2022, brand owners, digital agencies, secondary digital media space owners (such as bloggers and influencers) and other advertising stakeholders in the digital and online media space in Nigeria are required to obtain pre-exposure approval from the ARCON in respect of all advertisements, advertising and marketing communications; and
- from January 2023, all advertising, advertisement and marketing communications materials directed at the Nigerian market are required to achieve a minimum of 75% cumulative local content.

The National Information Technology Development Agency Act 2007

The National Information Technology Development Agency Act 2007 establishes the National Information Technology Development Agency (NITDA), an agency which operates under the supervision of the Federal Ministry of Communications and Digital Economy. The NITDA is at the forefront of efforts for the promotion and facilitation of the digital economy in Nigeria, as it has demonstrated through the proposal of guide-

lines, frameworks and regulations to enhance this economy.

The Cybercrimes (Prohibition and Prevention) Act 2015

The Cybercrimes (Prohibition and Prevention) Act 2015 (CPPA) creates an effective and comprehensive regulatory framework in Nigeria for the promotion of cybersecurity and the protection of Nigerians in the cyberspace. In line with global best practices, the CPPA criminalises a plethora of activities such as identity theft, hacking, cyberstalking, bullying and pornography, among others, being acts which are peculiar to the cyberspace and which have the capacity to fetter the thriving digital economy in Nigeria.

Importantly, the Act declares the offences it creates as extraditable. In view of the borderless nature of cybercrimes, the CPPA sets up a regulatory regime within which the Attorney General of the Federation may request or receive assistance from any agency or authority of a foreign state in the investigation or prosecution of offences created under the Act. Alternatively, the Attorney General of the Federation may authorise or participate in any joint investigation or co-operation carried out for the purpose of detecting, preventing, responding to or prosecuting any offence created by the Act.

The Nigerian Copyright Act

The digital economy has introduced unprecedented ease in the creation and publication of digital and creative works. This continuous digitalisation of the Nigerian economy has brought to fore the inadequacy of the Nigerian Copyright Act, which does not anticipate most of the recent technological innovations.

In view of this, a Copyright Bill with more expansive provisions was proposed in 2021, and is

expected to cater more appropriately to the demands of the digital economy. Among other provisions, the Bill provides that the owner of copyright in online content may issue a notice of infringement to the relevant service provider with a request that the service provider take down or disable access to any infringing content hosted on its system. In this regard, the service provider has an obligation to take down or disable access to the infringing content where the alleged infringer or subscriber fails to provide any justification for the continued hosting of the content complained of.

The Securities and Exchange Commission's Rules on Issuance, Offering Platforms and Custody of Digital Assets

Digital and/or virtual assets, which include cryptocurrencies such as Bitcoin, form an intrinsic part of the digital economy.

While there is still uncertainty as to the manner in which virtual assets should be regulated, many advanced countries have adopted a progressive and liberal approach while the specifics of the relevant laws are thought through and firmed up. The Nigerian Securities and Exchange Commission (SEC) has adopted a similar approach by assuming regulatory authority over virtual assets which it classifies as securities. In the same vein, the SEC has rolled out a body of rules on the issuance, offering and custody of digital assets in Nigeria (the "Rules").

The Rules contain more specific rules on:

- the issuance of digital assets as securities, targeted at all issuers of digital assets seeking to raise capital through digital assets offerings;

- the registration requirements and procedures for digital assets offering platforms and digital assets custodians; and
- specific rules targeted at virtual assets service providers.

Guidelines for Nigerian Content Development in Information and Communication

Technology

Local content development guidelines were issued by the NITDA for the purpose of boosting local participation in the information and communication technology (ICT) industry in Nigeria and, consequently, gearing up the ICT industry to compete globally. In view of its core objectives, the guidelines contain provisions which support the transfer of technology into Nigeria in efforts to build local capacity within the industry.

Companies Income Tax (Significant Economic Presence) Order 2020

The digital economy is here to stay, and companies rendering digital services have established their presence in Nigeria now more than ever. Accordingly, the Finance Act 2019 and subsequently the Finance Act 2021 provide for the taxation of companies rendering digital services in Nigeria where they are established as having significant economic presence in Nigeria. In determining taxable businesses in Nigeria, the Companies Income Tax (Significant Economic Presence) Order 2020 focuses on economic substance as opposed to traditional establishment.

A foreign company is said to have significant economic presence in Nigeria in any accounting year where it earns any income or receives any payment from a person resident in Nigeria or a fixed base or agent of a company, other than a Nigerian company, in Nigeria, and such foreign company is taxable in the case of the following.

- It derives NGN25 million (annual gross turnover or its equivalent in other currencies from any of, or a combination of, the following:
 - (a) streaming or downloading services of digital content, including but not limited to movies, videos, music, applications, games and e-books to any person in Nigeria;
 - (b) transmission of data collected about Nigerian users which has been generated from such users' activities on a digital interface including websites or mobile applications;
 - (c) provision of goods or services directly or indirectly through a digital platform to Nigeria – in this regard, the activities carried out by connected persons in the relevant accounting year shall be aggregated; or
 - (d) the provision of intermediation services through a digital platform, website or other online application that links suppliers and customers in Nigeria.
- It uses a Nigerian domain name (ie, “.ng”) or registers a website address in Nigeria.
- It has a purposeful and sustained interaction with persons in Nigeria by customising its digital page or platform to target persons in Nigeria, including reflecting the prices of its products or services in Nigerian currency or providing options for billing or payment in Nigerian currency.

The Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries

The Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries (the “Code”) sets out best practices and expectations required of certain digital platforms to combat online harm such as disinformation/misinformation and to make the digital ecosystem safer for Nigerians. Platforms are classified

as either interactive computer service platforms (ICSPs) or internet intermediaries (IIs) (collectively referred to as “Platform Providers”) both of which are subject to the same compliance obligations. The Code defines ICSPs as electronic mediums or sites where services are provided by means of a computer resource for remuneration and on demand, and where users create, upload, share, disseminate, modify or access information, including websites that provide reviews and gaming platforms. The definition of IIs includes social media operators, websites, blogs, media sharing websites, online discussion forums, streaming platforms, and other similarly oriented intermediaries where services are provided, transactions are conducted and where users can create, read, engage, upload, share, disseminate, modify or access information.

The Code further prescribes obligatory provisions that Platform Providers are required to comply with, including:

- takedown requirements (within 48 hours) for unlawful content even without a court order (upon receiving substantiated notice from an authorised government agency);
- takedown requirements (as soon as is reasonably practicable) for unlawful content (upon receiving substantiated notice from a user to remove, disable or block access to non-consensual content that exposes a person’s private information);
- disclosing the identity of individuals that are the source of certain unlawful or harmful content further to a court order; and
- filing annual compliance reports with the NITDA.

The NITDA Bill

As previously mentioned, the NITDA is at the forefront of efforts for the promotion and facilitation

of the digital economy in Nigeria. To improve the efficiency of the NITDA in the regulation of the digital economy, a bill has been introduced to “repeal the National Information Technology Development Agency Act No 28, 2007 and enact the NITDA Act to provide for the administration, implementation and regulation of information technology systems and practices, as well as digital economy, in Nigeria and for related matters (2022)”. This legislative process is an attempt to keep the NITDA Act up-to-date with the current realities in the Nigerian digital economy space.

Key Legal Challenges in Nigeria in Relation to the Digital Economy

Although the digital economy in Nigeria has experienced significant growth in the last few years, it is still beleaguered by certain challenges, such as the following.

Archaic laws and systems

Despite the efforts of the NITDA in facilitating and improving the digital economy in Nigeria, subsistent laws are still catching up and are unable to adequately cater to the unique legal problems that characterise the digital economy.

The digital economy relies very heavily on IP protection. However, Nigerian IP laws are not comprehensive enough and do not provide adequate protection that reflects current global realities. In addition, the systems and mechanisms for the registration and enforcement of IP in Nigeria are not progressive. Filings for IP registrations are mostly manual and protracted. The process for the enforcement of infringed IP rights is also challenging due to the slow pace of the judicial process in Nigeria.

Lack of regulatory co-ordination

The approach of the SEC to the regulation of digital assets is progressive and liberal. As previously discussed, the SEC has set out a regulatory regime for the regulation of digital assets and the registration of all digital asset exchanges, offering platforms and custodians. The Central Bank of Nigeria (CBN) has, however, taken a stricter approach by restricting the access of digital assets exchanges to the Nigerian banking system, an effect which renders SEC rules impracticable.

Digital skills knowledge gap

In Nigeria, the skills and capabilities required to explore various digital products and innovations are significantly limited and only concentrated in a small segment of the populace. This, among other factors, is a result of lack of good-quality education and of inadequate digital skills training programmes, which are essential for building such skills and capabilities.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Regulatory Landscape for Cloud and Edge Computing

Governmental and regulatory bodies in Nigeria have increased their attention on the TMT industry over the past few years in the hope of creating legal precedents that might aid in the development of a strong regulatory framework for governance. In furtherance of this objective, the Nigeria Cloud Computing Policy (the “Cloud Policy”) was issued. The goal of the Cloud Policy is to ensure a 30% increase in adoption of cloud computing by 2024 among FPIs and SMEs that provide cloud services to the government. The Cloud Policy also targets a 35% growth in cloud

computing investments by 2024, and recognises three basic kinds of cloud computing service offerings or cloud-based service models:

- Software as a Service (SaaS);
- Platform as a Service (PaaS); and
- Infrastructure as a Service (IaaS).

The Cloud Policy is applicable to all public institutions, at the federal, state and local government levels. It also applies to all corporations fully or partially owned by the federal government in Nigeria, as data generated by these institutions is regarded as “government data”. By extension, the Cloud Policy also encourages the adoption of cloud services by SMEs to ensure they are able to provide quality, reliable and secure services to the public sector.

The Cloud Policy was developed by the NITDA, to promote a “Cloud First Policy” to federal public institutions (FPIs) and SMEs as an efficient way of acquiring and deploying computing resources for better and improved quality of digital services. The Cloud First Policy refers to the Nigerian government’s strong commitment and support for cloud computing service adoption, especially from local cloud service providers, as a first-choice consideration while deploying and accessing computing resources in the public sector and by the SMEs that provide computing services to the public sector.

Developments in the Regulated Sector – Financial Services

The CBN regulates the banking sector and has explored the impact and power of cloud computing on the financial services sector. In 2010, the IT Standards Council of the Central Bank of Nigeria developed the Nigerian Financial Services Industry IT Standards Blueprint (the “Blueprint”) to provide a framework and point of

reference for the utilisation of information technology in the Nigerian financial services sector. The Blueprint was issued in 2014 and revised in 2019. It recognises cloud computing as one of the emerging trends in digital technology, highlights the positive implications and the risks of adopting cloud computing, and provides for minimum standards for deploying cloud computing in the financial services sector.

Data Protection and Cloud Computing

One of the key issues of cloud computing is data protection and privacy. Cloud computing poses risks to personal data in a number of ways, including through unauthorised disclosure or access, malicious activities targeting the cloud service provider (eg, hacking or viruses) and poor security practices.

A key data protection concern in cloud computing is the territorial nature of data protection laws vis-à-vis the global nature of cloud services. Data protection laws are typically applied based on the physical location of personal data – ie, where personal data is collected, processed, stored, used, etc. In a distributed system, this can be difficult to determine and control. To cure this mischief, the Cloud Policy provides that although cloud information may be processed or stored in jurisdictions with privacy and information protection laws different from those in Nigeria, government agencies must do so in line with requirements of the NDPR and any other content regulation. Under the Cloud Policy, routine government business data (data of moderate sensitivity) and secret, sensitive government and citizen data are required to reside primarily in a cloud framework within the Nigerian territorial boundary, while classified or national security information must reside only on the premises of public institutions or collocated in a cloud within the Nigerian territorial boundary.

However, as highlighted above, the Cloud Policy has a limited scope of application and does not bind all persons. The NDPR, on the other hand, has general application and can be broadly interpreted and applied. Under the NDPR, the user of cloud services will most likely be classified as a data controller if they determine the purposes for which, and the manner in which, the personal data is being processed. The cloud service provider will be classified as the data processor. Therefore, persons who store or process personal data in the cloud and cloud service providers are required to comply with the NDPR.

To the extent that data controllers choose to store personal data with cloud services located outside Nigeria, they will be required to comply with the transfer of personal data provisions of the NDPR, among other numerous compliance obligations. Under the NDPR, transfer of personal data to a foreign country can only take place:

- after a decision by the NITDA or Attorney General as to the adequacy of safeguards in the foreign country;
- where as regards the transfer of data within a group of companies or an affiliate company, standard contractual clauses (SCCs) or binding corporate rules (BCRs) adopted by the NITDA or the specific industry are in place; or
- where there is verifiable documentation of one of the exceptions under the NDPR.

Another point of convergence between cloud computing and data protection is the requirement under both the Cloud Policy and the NDPR to ensure timely reporting of data breaches to the NITDA. The Cloud Policy mandates cloud service providers to report breaches immediately as they become aware of them. A similar requirement under the NDPR mandates con-

trollers and processors to report data breaches within 72 hours of knowledge of the breach.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Regulatory Landscape for Artificial Intelligence and Big Data

There is currently no legal/regulatory framework specifically dedicated to artificial intelligence (AI) in Nigeria. In 2022, the NITDA made a call for contributions to the National Artificial Intelligence Policy (NAIP). According to the call for applications, the policy is being developed to create a framework for the planning, research, development, standardisation, application, co-ordination, monitoring, evaluation and regulation of IT practices, activities and systems in Nigeria.

As part of its digital technology drive, the federal government developed the National Digital Economy Policy and Strategy (NDEPS) (2020–2030) to reposition the Nigerian economy to take advantage of the numerous opportunities that digital technologies provide. The NDEPS document is based on the Federal Ministry of Communications and Digital Economy (FMoCDE) eight pillars for the acceleration of the national digital economy for a digital Nigeria. The seventh pillar is digital society and technologies, which focuses on the introduction of an emerging technologies programme that will deal with AI and other emerging technologies.

Notwithstanding the absence of an AI strategy, Nigeria leads the African continent in the area of AI research and development, being the first country on the continent to establish a dedicated government institution to promote the research

and development of AI systems in Nigeria. In November 2020, the Honourable Minister of the FMoCDE commissioned the National Centre for AI and Robotics (NCAIR), a state-of-the-art facility, along with its modern digital fabrication laboratory (FabLab). In accordance with the NDEPS, the NCAIR was established as a digital innovation and research facility that focuses on AI, robotics and drones, the internet of things, and other new technologies.

The building of a thriving ecosystem for innovation-driven entrepreneurship (IDE), job creation, and national development is another goal of the NCAIR. Since its establishment, the NCAIR has introduced various programmes including SB4Kids (a programme aimed at enabling young children to be conversant with emerging technologies like 3D design, coding, VR and digital communication around the world), NCAIR Project Drive and digital skills training.

Another AI initiative of the federal government was the partnership between the FMoCDE and IBM in January 2020 to provide Nigerians with over 280 hours of free learning and over 85 courses on key emerging technologies such as AI and Blockchain.

In the financial services sector, the Blueprint also recognises big data and AI as emerging trends in digital technology. The Blueprint also highlights the positive implications and the risks of adopting these emerging technologies, and provides for minimum standards for their deployment in the financial services sector.

Key Challenges

The absence of a formal legal or regulatory framework means that the creation and application of AI, machine learning and big data have mainly been left to industry practices.

Intellectual property

Nigerian IP laws do not consider instances in which an AI creation such as AI-generated computer codes would be protected, or in which AI could be granted any IP rights. The Copyright Act attaches the idea of authorship to individuals (natural persons), and eligibility for copyright protection to both individuals who are citizens of or are domiciled in Nigeria and to body corporates established by or under the laws of Nigeria. Under the Patents and Designs Act, the right to a patent in respect of an invention is vested in the statutory inventor, the person (individual or corporate body) who, whether or not they are the true inventor, is the first to file.

Data protection

In the area of data protection, machine learning (which is a subset of AI) involves the collection of increasing amounts of data and large-scale monitoring of human behaviour, which presents privacy and data protection challenges. Under the NDPR, data controllers and data administrators are required to conduct data protection impact assessments (DPIAs) where they intend to embark on a project that would involve the intense use of personal data. The Nigerian data protection regulator, the Nigerian Data Protection Bureau (NDPB), is empowered to request the submission of a DPIA where the processing activities are deemed to involve high impact on data subjects, including activities involving evaluation or scoring (profiling) and systematic monitoring, which are all important elements of AI.

Another important area of intersection between data protection and AI is automated decision-making. Under the NDPR, in addition to the

requirement to conduct a DPIA, data controllers are also required to obtain the consent of data subjects prior to deploying automated decision-making algorithms of this nature. Data subjects also have a right to data portability (the right to receive and request the transfer of personal data concerning them from data controllers, to obtain their personal data from the data controller in a structured medium, and to have this data transmitted across data controllers and platforms).

Human rights

In relation to human rights, AI has the potential to negatively affect a wide range of human rights, including the right to privacy (eg, large-scale monitoring of human behaviour) and the right to freedom of expression (eg, deployment of AI in content moderation). In the absence of AI-related strategies, regulations or case law, it is difficult to determine how AI-related human rights infringements will be determined in Nigeria.

Liability

The deployment of AI also raises questions around legal liability for AI computer systems. Nigerian law does not recognise AI as a legal person, which means that AI may not be held personally liable for damage it causes. The question of who is liable for the harm that results from the actions of AI logically emerges. It is safe to conclude that Nigerian liability laws will need to change to ensure that AI and big data are not utilised as a loophole by organisations to avoid liability. To mitigate this risk, parties to an AI service agreement must carefully consider how to allocate liability for the AI's functionality ahead of entering such agreement.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection Regulatory Landscape for the Internet of Things (IoT)

Presently, there is no law in Nigeria that specifically relates to or regulates the IoT. However, there are laws and regulations that are broad enough to apply to IoT projects as well as sector-specific guidelines that govern the IoT. Examples of these laws, rules and regulations are listed below.

Telecommunications

Under the NCA, a “communication” is defined as any communication, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of these forms. This brings IoT technology under the regulatory scope of the NCC. The NCA sets out a broad licensing and regulatory framework for telecommunications and, in the absence of explicitly stated exemptions, the jurisdiction of the NCC extends to the licensing of IoT projects. Therefore, as appropriate, such IoT projects must be carried out in compliance with the general requirements and any unique conditions of approval under their various NCC-issued licences.

In recent times, the NCC has taken interest in the IoT space. As part of its Strategic Vision Plan (SVP) 2021–2025, the NCC has organised an IoT code camp and hackathon, with a focus on two categories:

- development of IoT solutions for kidnapping and banditry in Nigeria; and

- assistive robotics solutions for effective e-waste management.

In 2022, the NCC also held a stakeholders’ consultative forum on emerging technologies, with the theme “Regulatory Roadmap for the IoT Ecosystem in Nigeria”. At the event, key officials of the NCC were in agreement that, considering all the challenges and issues surrounding the IoT ecosystem, the regulation of the sector was of essence.

Financial services

The Blueprint recognises the IoT as an emerging trend in digital technology. The Blueprint also highlights the positive implications and the risks of adopting the IoT, and provides for minimum standards for the deployment of the IoT in the financial services sector.

Cybersecurity and data protection

The deployment of an IoT system raises a major cybersecurity challenge, as IoT devices are prolific breeding grounds for cybersecurity attacks such as distributed denial of service (DDoS) attacks.

The primary cybersecurity legislation in Nigeria is the CPPA 2015, which sets out a framework for:

- the protection of critical information infrastructure;
- the promotion of cybersecurity; and
- the protection of computer systems and networks, electronic communications, data and computer programs, IP and privacy rights.

It is the responsibility of every service provider in Nigeria to comply with all the provisions of the CPPA, and failure to comply attracts various levels of sanctions including imprisonment. Although the CPPA does not expressly provide

for the IoT, with the increasing adoption of IoT solutions, service providers in the sector need to pay particular attention to the CPPA as it affects their projects.

With respect to data protection, to the extent that IoT projects involve the processing of personal data, data controllers and data processors must process personal data in compliance with the NDPR and other relevant data protection laws.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Regulatory Landscape for Audio-Visual Media Services

Generally, the provision of audio-visual services in or from Nigeria (eg, TV or radio) is regulated under the National Broadcasting Commission Act (NBCA). Under the NBCA, the National Broadcasting Commission (NBC) may grant licences:

- in the case of a radio station, for frequency modulation, medium wave and short wave;
- in the case of television, for very high frequency and ultra high frequency; and
- for such other broadcast frequencies as the commission may, from time to time, determine.

In the exercise of its power under the NBCA, the NBC has issued the National Broadcasting Code 2016 as amended in 2020 (the “NB Code”) to further regulate the broadcasting industry. The NB Code makes it illegal for any person to operate or use any apparatus or premises for transmission of sound or vision by cable, television, radio, satellite or other medium of broad-

cast from anywhere in Nigeria, unless licensed by the NBC.

The NB Code provides that the NBC can grant broadcast licences in the following categories:

- broadcast – subscription DTH (audio and video);
- cable television subscription;
- community (radio and television);
- networking (radio and television);
- FM radio broadcasting;
- internet broadcasting;
- digital TV content aggregation;
- broadcast signal distribution;
- digital terrestrial (free-to-view) TV;
- direct satellite broadcast;
- mobile/handheld (DVB-H);
- digital subscription television;
- electronic programme guide (EPG); and
- over-the-top (OTT)/video on demand (VOD).

Although the NB Code does not define “internet broadcasting”, it defines the internet as “an international computer network through which computer users communicate and exchange information” and “broadcasting” as “transmission of programmes, whether or not encrypted, by radio waves or other means of telecommunication for reception by the public by means of a receiving apparatus.” A combined reading of both definitions incorporates video platforms with user-generated content to the extent that these platforms are internet-enabled.

Additionally, the National Broadcasting Commission Act (Amendment) Bill 2019 (the “NBC Bill”) is presently being debated in the Nigerian Senate. This bill seeks to expand the NBCA’s scope of application to incorporate newer forms of broadcasting into Nigeria’s broadcasting regulatory framework. Webcasting, which is defined as

“transmitting over the web/internet” and refers to both online and internet broadcasting, is also included in the scope of the bill. In practice, the NBC Bill would have the effect of requiring a licence from the NBC and regulating the provision of online, digital, internet or OTT broadcasting services in Nigeria under the NBC Act.

Eligibility, Fees and Charges

To provide audio-visual media services, the applicant must submit a licence application to request permission to own, establish or operate a radio, sound, television, cable or satellite station. Based on information specified on the NBC’s website, the application must be addressed to the Director General of the NBC. For each application, there is an application form fee of NGN50,000. The applicant must satisfy the following conditions:

- be a body corporate registered under the Companies and Allied Matters Act (CAMA) or a station owned, established or operated by the federal, state or local government;
- demonstrate to the satisfaction of the NBC that it is not applying on behalf of any foreign interest;
- comply with the objectives of the National Mass Communications Policy as applicable to the electronic media (that is, radio and television); and
- give an undertaking that the licensed station shall be used to promote national interest, unity and cohesion and that it shall not be used to offend religious sensibilities or ethnicity, or to promote sectionalism, hatred and disaffection among the peoples of Nigeria.

An application must be accompanied by the following:

- a certificate of incorporation;

- a certified copy of the articles and memorandum of association;
- a project study including the engineering design of the system; and
- evidence of the undertaking required under Section 9(d) of the NBCA.

It is important to note that religious organisations and political parties are disqualified from obtaining licences under the NBCA.

After the licence is granted, the applicant would be required to pay the licence fee for an initial term of five years. Subject to renewal, the licence fee for an initial term of five years is as follows.

- Category A – any location in the FCT, Lagos and Rivers State:
 - (a) radio – NGN20 million;
 - (b) open TV – NGN15 million; and
 - (c) cable TV – NGN10 million.
- Category B – any location in all other states:
 - (a) radio – NGN15 million;
 - (b) open TV – NGN11.25 million; and
 - (c) cable TV – NGN10 million.
- Public stations – NGN5 million for five years, or NGN1 million per television or radio channel per annum for five years.
- Direct broadcast satellite (single-channel) – NGN10 million for five years.
- Direct-to-home (DTH) (multichannel) – NGN25 million for five years.
- Dealer (wholesaler) – NGN120,000 per annum.
- Importer (wholesaler) – NGN120,000 per annum.
- Retailer – NGN30,000 per annum.
- Others – 2.5% of income.

Renewal Fees

Renewal fees apply as follows.

- Cable – satellite television (MMDS):
 - (a) Category A, any location in the FCT, Lagos and Rivers State – NGN5 million for five years; and
 - (b) Category B, any location in all other states – NGN4 million for five years.
- Direct broadcast satellite (single-channel) – NGN10 million for five years.
- Direct-to-home (DTH) (multichannel) – NGN50 million for five years.

NITDA Code of Practice

Video platforms with user-generated content are also required to comply with the NITDA Code of Practice for Interactive Computer Service Platforms (ICSPs) and Internet Intermediaries (IIs) (the “NITDA Code”), as discussed in **2.1 Key Challenges**.

In order to counteract online harm such as misinformation and/or disinformation, and to guarantee a secure digital environment in Nigeria, the NITDA Code specifies best practices required of digital platforms – ie, ICSPs and IIs. According to the NITDA Code, ICSPs and IIs are generally prohibited from using or modifying their platforms in a way that could compromise or obstruct the application and/or enforcement of Nigerian law. Other important compliance obligations include the need to remove illegal content within 48 hours of receiving a complaint from an authorised government agency.

Platform providers known as large service platforms (LSPs) are also required by the NITDA Code to incorporate in Nigeria, and to designate a liaison officer to serve as a conduit of contact with the Nigerian government, among other obligations.

According to the NITDA Code, failure to abide by its rules will be seen as a violation of the NITDA Act 2007, as well as of the National Broadcasting Commission (NBC) Act 2004 and the Nigerian Communications Act (NCA) 2003.

Advertising

Audio-visual media platforms providing advertising services will be regulated by the ARCON Act (see **2.1 Key Challenges**). The ARCON Act seeks to provide a regulatory framework for the advertising, marketing and communications industry. It is applicable to “individuals, organisations, body corporates or agencies of the federal, state or local government(s) that engage in, regulate, sponsor or take benefit of advertising services, advertisements and marketing communication services”. It also applies to “any person who sponsors or takes benefit of advertising, advertisements or marketing communications services within the provisions of the ARCON Act”.

With respect to licensing, the ARCON Act requires that every person or organisation, including foreigners, that intends to practise or carry out advertising, marketing and communications as a business or profession in Nigeria be registered in accordance with the provisions of the ARCON Act. Furthermore, all adverts directed or targeted at the Nigerian market are required to be vetted and approved by the Advertising Standards Panel (ASP) prior to publication. Thus, if the operations of video platforms with user-generated content in Nigeria involve advertising/marketing business or provide advertising services, they would be required to obtain a licence.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Technologies and Services that Fall Within the Scope of the Local Telecommunications Rules

All activities and operations within the Nigerian telecommunications sector fall within the scope of the local telecommunications rules, either directly or by extension. These include:

- the installation of communication masts and towers;
- international cable infrastructure and landing station services;
- internet services;
- infrastructure sharing and colocation services;
- commercial basic radio communications network services;
- electronic directory services;
- the operation of public payphones;
- internet exchange;
- sales and installation of terminal equipment (including mobile cellular phones and HF/VHF/UHF radio, etc);
- repair and maintenance of telecommunications facilities;
- cabling services; and
- the operation of cybercafes.

Pre-marketing Requirements in the Nigerian Telecommunications Industry

The NCC is the principal regulator in the Nigerian telecommunications sector. Anyone who intends to operate a communications system or facility or to provide a communications service must have been authorised and licensed by the NCC, or must have been exempted from such requirements. A separate licence is usually required for each type of telecommunications activity,

although it is also possible for several activities to be undertaken under a single licence.

As detailed in 2.1 Key Challenges, NCC licences are categorised into two categories – individual licences and class licences. Individual licences are typically bespoke licences where the terms and conditions upon which the licence is granted are specific to the activity undertaken by the licence holder; whereas for class licences, the terms and conditions upon which the licence is granted are common across all licensees.

Any person who provides a telecommunications service in Nigeria without a valid licence shall be liable to an administrative fine of NGN5 million, and NGN500,000 for each day that the contravention persists after an order to desist has been issued by the NCC. Relatedly, it is also an offence for a licensee to continue to provide a telecommunications service after the expiry of a licence duly issued by the NCC, and such offence is punishable by an administrative fine equivalent to the initial fee for the relevant licence, and an additional fine of NGN100,000 for each day that the contravention persists after the expiry of the licence.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Now more than ever, technology transfer has become an integral activity in the increasingly digital global economy. For developing countries like Nigeria, technology transfer agreements are important to ensure the lawful absorption and adoption of technologies created in developed countries for the purpose of boosting the economic performance of the relevant developing country.

This notwithstanding, in Nigeria technology transfer comes with its own challenges, which include the following.

Registration Difficulties

Foreign technology transfer agreements are subject to registration requirements under the National Office for Technology Acquisition and Promotion (NOTAP) Act. The effect of not registering a registrable contract is that the parties are restricted from making payment through, or on the authority of, the Central Bank of Nigeria, or a licensed bank in Nigeria. The challenge here is that the registration process with the NOTAP is typically protracted and, in most cases, involves a lot of exchanges between the applicant and the NOTAP regarding the terms of the contract, especially where this has been executed by the parties prior to submission for registration. Other specific application requirements which may pose challenges to the registration process include the following.

- The requirement for certain applications such as trade mark licence agreements to be accompanied by evidence of the registration or pending registration of trade marks. Where such evidence is not available, compliance with this requirement may be a challenge, especially for time-sensitive agreements and projects.
- The requirement that all technology transfer agreements involving projects of and/or by the Nigerian government be mandatorily governed by the Nigerian laws of arbitration, with Nigeria being the seat of arbitration. This requirement poses difficulty, especially for transferors of technology who would prefer that such agreements be governed by other arbitral rules.
- Registration of the relevant contracts with the NOTAP is also cost-intensive as, upon

approval of registration, applicants are required to pay a registration fee which varies depending on the value of the underlying contract.

Lack of Funds to Adapt the Transferred Technology to Local Conditions

For efficient use of the transferred technology, it is ideal that the transferee has enough financial capacity to fund the purchase of the technology as well as local research and development for the adaptation and improvement of the transferred technology. However, this is rarely the case in Nigeria as transferees often barely have the required funds for research and development for the adaptation of the technology or to train the relevant members of staff on the workings of the technology.

Lack of Local Technical Know-How

The skills and technical know-how of the recipient in a technology transfer agreement are essential for the valid utilisation and optimal performance of the foreign technology. However, the dearth in sufficient skills and know-how for the efficient adoption and utilisation of foreign technologies is a limiting factor in Nigeria.

Local Legal Framework

Generally, the procurement of technology products and services is subject to the laws of contract. As mentioned previously, the transfer of technology into Nigeria must be done within the context of the local regulatory framework, and as such the following rules and restrictions will apply.

Registration of the technology transfer agreement with the NOTAP

The NOTAP may refuse to register technology agreements:

- where the underlying technology is obsolete;
- where the underlying technology already exists in Nigeria;
- where the price is not commensurate with the value of the underlying technology sought to be transferred; and
- in instances where such transfer of technology imposes limitations on technological research or development by the transferee.

Non-registration of the relevant technology transfer agreement restricts the repatriation of funds (foreign exchange) through the official foreign exchange market. Importantly, technology agreements must be registered with the NOTAP within 60 days of the execution or signing of the contract. Agreements in the following titles and substance are required to be registered:

- technical know-how;
- technical know-how and management services;
- technical services;
- consultancy;
- management services;
- software licence;
- value-added services;
- trade mark licence;
- R&D;
- franchise;
- hotel management agreement; and
- consultancy and technical know-how.

Competition considerations

Competition issues may arise within the context of technology transfer agreements. The Federal Competition and Consumer Protection Act (FCCPA) 2018 and the Abuse of Dominance Regulations 2022 prohibit all such agreements, including technology transfer agreements, which have the effect of stifling competition.

However, where a local organisation occupies a position of dominance or attains a position of dominance in the relevant market by virtue of a technology transfer agreement, the actions of such organisation which stifle competition and/or constitute an abuse of the dominant position would be excused where such actions or conduct are indispensable for the achievement of technological or economic progress in Nigeria. Alternatively, such conduct would be excused where the anti-competitive effects of the abusive conduct are reasonably necessary for the achievement of technological or economic progress.

Data localisation requirements

Parties to a technology transfer agreement which involves personal data must ensure compliance with the localisation requirements of the data privacy laws in Nigeria. These data localisation laws provide specifically for the following:

- all ministries, departments and agencies (MDAs) of the Federal Government of Nigeria are required to host all sovereign data locally on servers within Nigeria;
- all data and information management companies are required to host all sovereign data in Nigeria;
- all network service companies in Nigeria are required to host all subscriber and consumer data in Nigeria;
- all telecommunications companies are required to host all subscriber and consumer data in Nigeria; and
- all companies that produce functional computer devices from component parts brought from other organisations are required to assemble all hardware in Nigeria and maintain fully staffed facilities for that purpose.

Importantly, the localisation laws apply to all MDAs across all tiers and arms of government, private sector institutions, multinationals and individuals to the extent that they process sovereign data.

The Public Procurement Act

The procurement of technology products and services by government or public bodies is regulated by the Public Procurement Act (PPA) 2007. The Act covers procurement of all goods and services by the federal government, public bodies and all entities which derive 35% of the funds appropriated for any type of procurement, from the Federation's share of the Consolidated Revenue Fund. The PPA focuses primarily on ensuring transparency and accountability in all procurement processes by public sector bodies.

Industries Subject to Greater Restrictions

The banking sector

In the context of technology transfer agreements, banks are subject to more restrictions due largely to the need to protect the interests of the public whose funds they deal in. Specifically, fees payable by banks for management or technical support services, which they receive from expatriates, should be tied to the actual costs of the services rendered by the expert and not to the profit or sales of the bank.

A further restriction in this regard is that expatriate staff of banks can only be paid in the local currency – ie, Naira. However, remittance abroad, in foreign currency, can be effected through the Personal Home Remittance.

Nigeria's federal government ministries, departments and agencies (MDAs)

As mentioned above, public sector entities are subject to procurement requirements under the PPA.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The COVID-19 pandemic changed global realities and led to the introduction of digital identity schemes and trust services such as electronic signatures and teleconferences. While there are no specific laws which speak to the legality, permissibility or otherwise of electronic signatures and other digital identity schemes, some major laws have been amended to accommodate these new realities. Examples of these laws, rules and regulations are listed as follows:

- the Companies and Allied Matters Act 2020 recognises the validity of an electronic signature for the authentication of a document or proceeding by a company and further provides that the signature may be by a director, secretary or other authorised officer of the company;
- the Evidence Act 2011 provides that an electronic signature would suffice where the relevant law requires a signature;
- the Nigerian Data Protection Regulation (NDPR) 2019 and the accompanying Implementation Framework recognise and govern the collection, protection, storage and processing of personal data, which is defined broadly and thus includes digital identities and electronic signatures; and
- the CPPA 2015 provides that electronic signatures appended in respect of purchases of goods and any other transactions shall be binding.

Notwithstanding the above, certain transactions and documents cannot be validly concluded and executed using electronic signatures. These

transactions and agreements include the following:

- the creation and execution of wills, and other testamentary documents;
- death certificate;
- birth certificate;
- divorce, marriage, adoption and other related matters;
- the issuance of court orders, notices and official court documents such as affidavits, pleadings, motions and other related judicial documents and instruments;
- any cancellation or termination of utility services;
- any instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature; and
- any document ordering the withdrawal of drugs, chemicals and any other material either on the grounds that such items are fake, dangerous to people or the environment, or expired.

Considerations Arising from Trust Services, Electronic Signatures and Digital Identity Schemes

Other than the aforementioned laws, there is presently no specific and comprehensive legal framework governing electronic signatures and trust services in Nigeria. However, by the existing laws referenced above, the following elements are relevant.

Legal liability

Trust services and electronic signatures present varying levels of risks, including the risk that the electronic signature or digital identity is not authentic. Here the current legal position is that whenever the genuine nature of an electronic signature is in question, the burden of proving that the signature does not belong to the purported originator of such electronic signature shall be on the contender. Indeed, for many evidential issues in Nigeria, the general legal position is that he who asserts must prove.

Fundamental rights considerations

While the introduction and general acceptance of electronic signatures and other trust services have brought ease to cross-boundary transactions and communications, the possibility of forgery of electronic signatures and digital identities has raised concerns about the potential breach of the rights of private citizens to their privacy and digital identity.

Although the Constitution of the Federal Republic of Nigeria contains a generic provision for the protection of the privacy of citizens, their correspondence, telephone conversations and telegraphic communications, the NDPR contains a more comprehensive provision safeguarding the rights of natural persons resident in Nigeria to the protection of their personal data, which by its broad definition includes electronic signatures and digital identities.

Data protection

Data protection is a major concern regarding the manner in which electronic signatures are collected, processed and stored by relevant host companies. Considering that electronic signatures validly constitute personal data, it is important that the process of collection, storage and processing in this regard complies with local data processing laws.

Templars is a full-service commercial law firm with offices in the cosmopolitan cities of Lagos, Abuja, Port Harcourt and Accra. The media, entertainment, technology, and intellectual property (METI) practice at Templars is renowned for the services it provides traversing the full range of issues in the technology sector, including: e-commerce, data protection, intellectual property licensing, patenting and protection; cloud services arrangements; cybersecurity; fintech regulation and compliance; technology licensing; acquisition; international joint ventures in the telecommunications industry; and advice on start-ups. The firm's recent experience in-

cludes: advising YouTube on its USD100 million Black Voices Fund, a global racial-justice initiative aimed at supporting black content creators and artists across different countries; advising Apple on the launch of a number of first-to-market products that are connected with its online services (including the online provision of original video-on-demand content via Apple Music); and advising American Tower Corporation (ATC) on its business entry into Nigeria through its USD1.05 billion acquisition of approximately 4,800 tower sites across Nigeria from Bharti Airtel.

Authors



Ijeoma Uju is a partner in Templar's corporate and commercial practice group. She has almost two decades' experience in providing general corporate advisory services to

clients, and in advising clients on compliance requirements applicable to the operation of their businesses in the technology ecosystem, regarding data protection, financial technology, cryptocurrency regulations, blockchain, artificial intelligence, tech policy, and start-up/organisational development. In addition to her transaction-specific work, Ijeoma regularly conducts regulatory compliance seminars and workshops for leading Nigerian and multinational tech companies. Ijeoma has also written and published articles on regulatory compliance, corporate governance and business formation in legal journals.



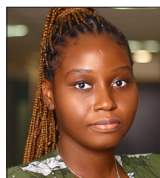
Oghomwen Akpaibor is a managing counsel in Templar's corporate and commercial practice group and METI practice group. She has a wealth of experience in media

and technology law, general corporate advisory and general regulatory advisory. Oghomwen manages the government-relations aspects of clients' regulatory compliance engagements. She also advises the various players in the tech ecosystem (locally and internationally) on subject matter-specific queries arising in respect of their businesses, including regarding labour and immigration, intellectual property, anti-corruption and privacy.



Tomisin Olanrewaju is an associate in Templar's finance practice group and METI practice group. She has been admitted to the Nigerian bar and has experience advising on

regulatory compliance, data protection and intellectual property. Tomisin provides legal support to Nigerian entities and MNEs to ensure they achieve their business objectives and remain in legal compliance with the requirements of relevant Nigerian authorities, particularly in relation to data protection, corporate restructuring, intellectual property protection, and the establishment of businesses by foreign and indigenous companies.



Victoria Oloni is an associate in Templar's corporate and commercial practice group and METI practice group. Victoria is a Certified Information Privacy Professional (CIPP/E) with the

International Association of Privacy Professionals (IAPP), where she also served as the Young Privacy Professional for the 2022 leadership cohort of the IAPP Nigeria Knowledge chapter. Victoria has written and published articles on privacy and data protection, cybersecurity, the digital economy, and general intersections of technology and law.

Templars

Fifth Floor
The Octagon Building
13A, AJ Marinho Drive
Victoria Island
Lagos
Nigeria

Tel: +234 1 270 3982
Fax: +234 1 271 2810
Email: info@templars-law.com
Web: www.templars-law.com

TEMPLARS

Law and Practice

Contributed by:

Leif Eirik Thrane and Arne Byberg

Advokatfirmaet Haavind see p.366



Contents

1. Metaverse	p.357
1.1 <u>Laws and Regulations</u>	p.357
2. Digital Economy	p.357
2.1 <u>Key Challenges</u>	p.357
3. Cloud and Edge Computing	p.358
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.358
4. Artificial Intelligence and Big Data	p.360
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.360
5. Internet of Things	p.361
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.361
6. Audio-Visual Media Services	p.362
6.1 <u>Requirements and Authorisation Procedures</u>	p.362
7. Telecommunications	p.363
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.363
8. Challenges with Technology Agreements	p.364
8.1 <u>Legal Framework Challenges</u>	p.364
9. Trust Services and Digital Entities	p.364
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.364

1. Metaverse

1.1 Laws and Regulations

Norway does not have any specific laws regulating the metaverse. The general rules that apply in the physical world will also apply in the metaverse. These include, but are not limited to, contract law, rules on personal data protection and regulations on intellectual property.

A key legal challenge when applying Norwegian law in the metaverse will be to ensure a sufficient amount of personal data protection. As Norway is part of the European Economic Area (EEA), the main rules for data protection in Norwegian law are found in the Personal Data Act and the General Data Protection Regulation (GDPR). All processing of personal data must comply with the terms set out in this regulation.

The GDPR is implemented by the Personal Data Act, which complements the GDPR on certain topics. Some specific Norwegian examples include:

- the minimum age for children consenting to the processing of their personal data in the context of information society services is 13 years, thus lower than the GDPR standard of 16 years (Section 5);
- only certain parts of the GDPR apply when the processing of data is done solely for journalistic purposes, or in relation to academic, artistic or literary purposes;
- personal identity numbers may only be processed when there is an objective need for identification; and
- a specific legal basis applies for private entities' processing of personal data relating to criminal offences.

The supervisory authority for GDPR compliance in Norway is the Norwegian Data Protection Authority (DPA). The DPA has taken its role seriously by issuing a steadily increasing number of fines in recent years.

Regulating intellectual property rights (IPR) might also be a key legal challenge in the metaverse. For example, if intellectual property is created in the metaverse, several jurisdictions may claim their IPR laws apply and these may dovetail or conflict with the terms of use for the metaverse.

Similarly, the regulation of non-physical tokens might become a legal challenge. A variety of non-physical tokens are used in e-sports and e-games as a currency in transactions. To assess such tokens in terms of commercial value in the physical world is a challenge, for example, in terms of applicable jurisdiction, tax regulation and contract law.

2. Digital Economy

2.1 Key Challenges

Norway does not have specific laws or regulations applicable to the digital economy. EU regulations, such as the Digital Services Act and the Digital Markets Act, will apply once implemented into Norwegian law.

A general challenge with the digital economy is how to apply traditional legal concepts from the analogue world to digital activity. Specifically, tax regulations and criminal regulations have proved challenging to apply in the normal context of jurisdiction, due to the geographically borderless nature of the digital economy, which needs to be reconciled with strict requirements for laws to be clear and predictable in order to be

enforceable within the areas of tax and criminal law in Norway.

Cryptocurrency has proved to be a legal challenge. Norwegian banks have long been wary of accepting deposits made in cryptocurrency. The reasoning behind the reluctance is that the normal “Know Your Customer” requirements and anti-money laundering procedures can be difficult to enforce and apply in relation to clients using cryptocurrency. Documenting the absence of money laundering or similar crimes in past crypto transactions can be almost impossible and there is no common code or practice applied across the banks in Norway yet.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Norway does not have any general legislation governing cloud and edge computing. However, specific regulations regarding the processing of personal data, financial data, archive data in the public sector and data in the health sector will influence cloud and edge computing requirements. In addition, the Norwegian Security Act may impose further requirements or restrictions based on national security considerations.

Processing of Personal Data

All processing of personal data is subject to the European Union’s General Data Protection Regulation (GDPR). The GDPR requires that the data controller must have a legal basis for the processing of personal data, including the transfer of the data to the service provider, as well as for any transfer of data to countries outside the EU and EEA.

Article 32 of the GDPR requires that the controller and the data processor ensure the safety and integrity of the data processed through technical and organisational security measures. Appropriate measures may be encryption, ability to restore the availability and access to personal data as well as internal processes for regularly testing, assessing and evaluating the effectiveness of the measures.

The requirements under Chapter 5 of the GDPR govern transfer of personal data to third countries and are therefore relevant for cloud computing. Transfer of personal data to third countries requires a transfer mechanism, and the level of protection of the data must meet EU standards.

As of the ECJ’s ruling in case C-311/18 (Schrems II), the EU-US Privacy Shield personal data transfer mechanism for transfers from the EEA to the US is invalid, and organisations must seek alternative transfer mechanisms when working with US cloud providers. For Norwegian businesses using data processors abroad, the Schrems II ruling has also caused challenges for other managed services locations outside the EU and EEA, such as India.

As far as the EU standard contractual clauses (SCCs) were concerned, existing agreements based on the old templates executed before 27 September 2021 were valid until 27 December 2022. Most data exporters will have to adopt supplementary measures to ensure that the data’s level of protection is up to EU standards. The judgment therefore entails that the use of cloud computing services from third countries can be challenging. The effectiveness of encryption is emerging as a key assessment.

The Financial Sector

The Bookkeeping Act generally requires that accounting material subject to storage requirements must be stored in Norway. According to the Bookkeeping Regulation, exceptions can be made for storage in certain EEA countries if the Tax Directorate is informed. Currently, only the Nordic countries are covered by the exemption. The bookkeeping authorities may grant exemptions for other countries in the EU/EEA on a case-by-case basis. Subsequently, the access to cloud services for accounting material is restricted. However, the Bookkeeping Act does not prevent entities from storing copies of accounting material on servers abroad, as long as the material is (in addition) legally stored and processed in Norway.

The Norwegian Regulation regarding use of Information Communication Technology (ICT) in the Finance Sector will also affect the use of cloud computing services in this business segment. The Regulation sets requirements for ICT systems used in the financial sector, and businesses will have to carry out risk assessments, ensure the Financial Supervisory Authority's right of inspection also applies to the provider, and assess whether outsourcing in general, or cloud computing services in particular, meet the Regulation requirements related to the systems' quality and business continuity. The Norwegian Regulation was last updated in December 2021, largely implementing guidelines by European authorities (European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIOPA), European Securities and Markets Authority (ESMA)).

National Security

The Security Act applies to all public bodies, as well as companies involved in classified procurements or companies that for other reasons

are subject to the Act's requirements following a decision by the relevant ministry. The Act generally allows for the use of cloud services for businesses that are subject to the Act, but use of cloud and edge services for information that could relate to national security interests needs to comply with strict requirements in the Act. The business must carry out risk assessments and assess whether use of cloud and edge computing services is safe considering the specific information that is to be safeguarded. A proactive dialogue with the security authorities should also be considered.

The Security Act has been in force for a relatively short period of time. Interpretation of its scope and restrictions remains vague and subject to public debate. It should also be noted that the application of the restrictions may change based on the geopolitical climate. The outbreak of war in Ukraine and the related energy crisis with attacks on energy infrastructure in Europe illustrates the risk and is particularly relevant as Europe's reliance on the Norwegian energy sector has increased. Both events played a part when the Norwegian oil and energy company Equinor became subject to the Norwegian Security Act in 2022.

Archiving in the Public Sector

The Archive Act applies to the public sector in Norway. It does not explicitly govern the use of cloud or edge computing but prohibits public entities from transferring or transporting archive material out of Norway. However, it must be noted that EU Regulation 2018/1807 on the free flow of non-personal data (the FFD Regulation) is currently under consideration in the EEA, including Norway. If the FFD Regulation is incorporated in the EEA Agreement, Norwegian authorities may have to revoke the prohibition. A new

Archive Act is also in process and is expected to be proposed to parliament in 2024.

For software suppliers to the Norwegian public administration, it is worth noting that the current Archive Act also mandates the use of open formats and requires that public entities carry out risk assessments of the storage systems to be used and examine whether these fulfil their archiving obligation.

The Health Sector

Entities providing, managing, or assuring quality healthcare services are subject to the Norwegian Patient Journal Act and underlying regulations, which impose strict requirements governing information security, including the use of cloud service providers. The Act also imposes functional requirements regarding documentation of healthcare, right of access, access control and deletion of data. Additionally, most healthcare providers in Norway are bound by the sector-specific standard “Normen”, a compilation of information security requirements which in some cases are stricter than requirements in law.

New EU Acts

New EU acts covering cloud and edge computing that are deemed relevant for the EEA are likely to also be implemented in Norway.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Norway does not have any general legislation governing artificial intelligence. However, specific regulations like the processing of personal data, intellectual property rights and discrimination in relation to fundamental rights are exam-

ples of relevant regulations that will apply to the use of artificial intelligence.

Further, in the field of artificial intelligence, Norway is influenced by EU regulation. The current EU proposals for harmonised regulation of AI are relevant for Norway through the EEA Agreement, and the Norwegian government has submitted its views and position in a national review note from August 2021. EU positions on civil liability – adapting liability rules to the digital age and artificial intelligence – are also likely to have impact on Norway via the EEA as they materialise and mature at European level.

Data Protection

Big data, machine learning and artificial intelligence projects will involve processing large data sets. More often than not, data sets targeted for machine learning and artificial intelligence use and contain unstructured rather than structured data. The data sets may contain non-personal data or personal data, or a mix. The GDPR will apply where such data sets contain personal data. This includes the requirement for a legal basis for the processing and a number of safeguards. Key challenges with machine learning and artificial intelligence technologies in Norway will be:

- complying with the prohibition against processing data for a purpose which is incompatible with the purpose for which it was collected; and
- biased algorithms.

Artificial intelligence, machine learning and big data are also likely to be viewed as high-risk processing activities, entailing that the controller could be required to conduct data protection impact assessments (DPIAs).

Intellectual Property

Ownership of non-personal data has yet to be broadly discussed in Norway, but the general view is that data that merely represents factual observations may not be “owned” by the collecting company or person in the traditional concept of ownership. However, databases and computer programs used for processing big data, machine learning and artificial intelligence are to some extent safeguarded by the sui generis database property right in Norwegian copyright law. The Norwegian Protection of Trade Secrets Act may also provide dovetailing protection for data if reasonable measures to avoid disclosure are implemented. As the protection offered by national rules is limited, it is important that intellectual property questions are clearly regulated by contract.

The question of ownership and intellectual property rights as regards the results generated by intelligent machines has been resolved by the European Patent Office, which also impacts Norway. Hence, an artificial intelligence-system cannot be named an inventor in Norway. Contractual regulation of IPR between parties using technology for innovation purposes will remain essential for the foreseeable future.

Discrimination

The use of artificial intelligence may affect the rights and freedoms of individuals, eg, when examination reviews or job applications are processed by automatic means. While problematic from a GDPR perspective, such automation may also be problematic under the recently adapted Norwegian Act on Discrimination, governing individuals’ rights to equal treatment and not to be discriminated against based on, for example, race, sex, religion, age or sexual orientation. We have already seen examples of such discrimination by algorithms internationally. As

discrimination is already governed by law in Norway, developers must implement safeguards to prevent discrimination when developing artificial intelligence. Further regulation by the EU with indirect application in Norway may be expected.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There is no specific Norwegian legislation regarding the internet of things (IoT), although there has been a manifest proliferation of sensor technology across industries and for personal use in Norway in the last decade. Legal requirements for data protection will limit the scope of IoT projects when it comes to personal data, as these devices usually collect a large amount of data. All devices processing personal data will have to comply with the general principles of the GDPR, including not collecting more data than necessary for the purpose of processing (data minimisation) and not processing data in a manner incompatible with the initial purposes of processing (purpose limitation).

When IoT technology is applied for non-personal data, the contracts will remain key, although severely under-regulated in a large volume of legacy contracts in Norway, which may fuel renegotiation or disputes. A joint code of conduct for the agriculture and aquaculture industries has been proposed by relevant organisations in Norway with the aim of transferring data ownership from the sensor vendor to the farmer, but adoption remains uncertain.

Certain radio and communications devices that are connected to the internet will have to meet minimum requirements in areas such as informa-

tion security, privacy and anti-fraud based on local implementation of EU cybersecurity laws.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

The Norwegian Broadcasting Act sets different requirements for set categories of audio-visual media services.

The first category corresponds to companies wishing to engage in broadcasting via ground-based transmitting facilities, and these must obtain a licence. The term “broadcasting” shall be understood to encompass “the transmission of speech, music, images and the like by electronic communications networks intended or suitable for direct and simultaneous reception by the public”. Beyond the requirement that the communication must be made via an electronic communication network, the term “broadcasting” is technology neutral.

Companies wishing to engage in other broadcasting services, ie, broadcasting services not subject to the licensing requirement, must register with the Norwegian Media Authority. This requirement is typically applicable for companies wishing to broadcast via the internet, satellite or cable. The broadcasting terms criteria of “direct and simultaneous reception by the public” entails that the registration requirement is only applicable for companies wishing to transmit live content to the public, for instance streaming live news online. On-demand audio-visual services are not obliged to register.

The third and last category covers on-demand audio-visual services, which are defined as a service “where the primary purpose is providing

audio-visual programmes that can be viewed at the moment chosen by the user and at their individual request on the basis of a catalogue of programmes and that is distributed to the general public via electronic communication networks”. This typically includes non-live online streaming and online television.

The criteria of editorial control will generally exclude media services which distribute user-generated content without interference from the service provider. However, Norwegian authorities are currently considering a proposed amendment to the Norwegian Broadcasting Act, which suggests implementing the rules from Directive 2010/13/EU (Audiovisual Media Services Directive), regarding user-generated video platform services (such as YouTube), over which the provider of the service has no editorial control.

The Licensing and Registration Processes

Application for a broadcasting licence is done by sending a completed form to the National Media Authority. Licensed parties will be subject to fees regulated by the Ministry of Culture. The fees may vary from time to time and for different providers.

Registration of a broadcasting service is done on the website of the Media Authority after creating a user account.

Other Main Requirements

The legal framework sets specific requirements for the different categories of audio-visual media services. This includes requirements for labelling age limits and advertisements, as well as rules on reporting to the authorities and protection measures for younger viewers.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Currently, the Electronic Communications Act applies to all activity relating to electronic communications as well as associated equipment (Section 1-2). The Act is neutral regarding variations in technology and therefore encompasses all forms of electronic communication. Further obligations for providers derive from the Act's corresponding regulations.

However, influenced by the EU's European Electronic Communications Code, there will likely be a new electronic communication act presented to parliament in 2023 or 2024. The final result of such a new act is not yet known, but it is implied that the scope of the telecommunication rules might be adjusted.

General Approval Requirements

There is no general requirement for regulators' approval to offer electronic communication services in Norway. However, most providers are required to register their business with the Norwegian Communications Authority (Nkom) to operate legally. The obligation to register applies to:

- providers that install, operate and give access to electronic communications networks which are utilised for offering a public electronic communication service;
- providers of telephone services available to the public; and
- providers of transmission capacity.

Other providers are not obliged to register. Examples of these are providers of content services and data transfer services that do not install or operate their own physical network and

telephony providers with a service that is not – or is only partially – designed for end-to-end connectivity. Voice-over-Internet Protocol (VoIP) systems that are not fully designed for end-to-end connectivity and instant messaging systems and use other providers' physical networks will therefore not need registering.

To register, the provider must complete Nkom's form and have it signed by a person with the authority to legally commit the company. Once the form and relevant attachments have been sent to Nkom by post or email, the provider may offer its products and services in the Norwegian market. Registered companies appear on Nkom's public list of registered providers.

Registration of electronic communications providers is free of charge, but providers of electronic communications networks, electronic communications services and associated facilities with a turnover of more than NOK35 million must, in the following year, pay administrative charges to Nkom.

Approval Requirements for Use of Frequencies in Norway – including RFID

The use of frequencies in Norway is not permitted without a licence. General licences are granted in the General Authorisations Regulation. These licences apply to anyone using the specific equipment or service, therefore allowing free use of the specific usage. The Regulation's Section 9 allows for the use of specific frequency bands for RFID equipment in co-ordination with applicable standards. Consequently, the use of RFID tags within the terms set out in the provision is not dependent on application for an individual licence.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Norway does not have general legislation for IT service agreements, although the country boasts no fewer than three families of IT standard contract templates (Statens Standardavtaler, IKT Norge and Dataforeningen). The relevant legislation to consider is the Norwegian Contracts Act, and the non-statutory principles applicable to all contracts. Compared to other jurisdictions, Norway may be considered a “hybrid” between the common law and the civil law tradition. The Contracts Act contains provisions regarding all forms of agreements, including rules on how a binding contract is concluded and rules on certain circumstances that can lead to invalidation of a contract. Commercial contracts will, however, very rarely be censored or invalidated by a Norwegian court of law following the provisions of the Contracts Act. It is therefore important that the agreement, or the choice of standard template, is well considered in advance, and that the agreement regulates the placement of risk between the parties.

The Norwegian Act relating to the Sale of Goods directly applies to the sale of goods, but the Act is to some degree seen as an expression of applicable non-statutory principles governing contracts law and may therefore apply analogously to IT service agreements, especially for matters not regulated in the contract. The Act governs the parties’ obligations and remedies in the event of breach of contract and will consequently need considering when entering into an IT service agreement. Consumers enjoy mandatory protection that cannot be varied in contract, so B2C contracts require more scrutiny than B2B contracts.

Data Protection

GDPR compliance is a typical challenge in many IT service contracts as these will often involve the processing of personal data to some extent. If the service provider will be processing data on behalf of the customer, a data processing agreement will be mandatory pursuant to Article 28 of the GDPR. Another commonly occurring challenge is complying with the GDPR requirements for data transfer if the provider processes the data in a non-EU country, which triggers Schrems II-related issues.

Regulated Industries

Regulated industries frequently use the Statens Standardavtaler templates, which are provided by the Norwegian government for use in the public sector, but they can freely be used by businesses in the private sector as well.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

As a result of the EEA, Norway has implemented the EU regulation on electric identification and trust services for electronic transactions in the internal market, through the Norwegian electronic trust services act.

Electronic signatures ID confirmation and signatures are commonly used in Norway both in the public and private sector. Most governmental platforms online require log in with electronic ID. This includes accessing tax statements, any social aid and student loans. Private corporations like banks, insurance companies, real estate agencies, unions and the Norwegian postal and freight services also prefer and rely on electronic ID confirmation and signatures.

Payment confirmation through electronic signatures is also frequently used in online retail.

The largest provider of electronic signatures and identification in Norway is BankID. BankID is jointly owned and developed by Norwegian banks and is the leading identity service provider across the market in Norway.

Other examples of providers with a foothold in the Norwegian market are Buypass and Signicat.

In the last few years, liability and responsibility for loss after fraud using electronic identification and signatures has been litigated in Norwegian courts. Recent principal judgments have concluded that the electronic identification and signature providers carry a larger part of the liability than previously assumed.

Advokatfirmaet Haavind has a nationally recognised tech practice with over 20 members of staff focusing on technology, media and IP rights. The team excels across all disciplines of TMT expertise, including tech M&A, large-scale IT projects, digital media and telecoms, privacy and data protection, new digital ventures and innovative products, and litigation. Other areas of expertise include non-personal data ownership, data lakes and AI, trade secrets, TV/film distribution, privacy enforcement, antitrust in tech and Norway's Security Act. The firm's

blend of expertise sees it regularly involved in the largest and most complex TMT matters in Norway, particularly IT outsourcing or cloud migration. Combining sector-specific knowledge and experience with a practical understanding of the increasingly complex regulatory landscape clients are facing, Haavind's tech practice frequently teams up with its corporate or commercial disputes teams for dovetailing support of clients' largest matters, and regularly advises on issues with cross-border implications.

Authors



Leif Eirik Thrane is Haavind's TMT practice lead and has been the driving force behind the long-term growth of the team. With in-house experience in the tech industry and two decades

of M&A experience, he is particularly well positioned to support tech transactions in Norway and the Nordics. Leif is a leading advisor to the software industry and a key contributor to market practice for tech M&A in Norway and beyond. In addition, Leif is experienced in negotiating large outsourcing agreements, supporting dispute resolution, advising on regulatory and compliance issues, and complex licensing.



Arne Byberg is one of Norway's most internationally experienced tech lawyers, having spent several years living and working in Silicon Valley while associate general counsel and vice-

president of Hewlett-Packard. He has also served as general counsel, board secretary and compliance officer for the Norway-based EVERY Group. Arne is a senior partner in Haavind's tech practice, where he supports complex tech transactions, strategic outsourcing, digital transformation projects and tech dispute resolution, as well as traditional software development and licensing. Arne's specialist area also covers non-personal data and data ownership issues.

Advokatfirmaet Haavind AS

Postboks 359
Sentrum
0101
Oslo
Norway

Tel: +47 22 43 30 00
Email: post@haavind.no
Web: www.haavind.no/en/



Law and Practice

Contributed by:

Yousaf Khosa, Shafaq Rehman,
Amna Anjum and Mahnoor Javed
RIAA Barker Gillette see p.385



Contents

1. Metaverse	p.369
1.1 <u>Laws and Regulations</u>	p.369
2. Digital Economy	p.369
2.1 <u>Key Challenges</u>	p.369
3. Cloud and Edge Computing	p.372
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.372
4. Artificial Intelligence and Big Data	p.376
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.376
5. Internet of Things	p.376
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.376
6. Audio-Visual Media Services	p.377
6.1 <u>Requirements and Authorisation Procedures</u>	p.377
7. Telecommunications	p.380
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.380
8. Challenges with Technology Agreements	p.382
8.1 <u>Legal Framework Challenges</u>	p.382
9. Trust Services and Digital Entities	p.383
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.383

1. Metaverse

1.1 Laws and Regulations

There are no laws or codes of conduct that regulate the metaverse in Pakistan. Prior to developing any significant laws that regulate or apply to the metaverse, it will be important for the general public and the legislature to be educated on what the metaverse is and the necessity of its regulation. Most laws in Pakistan will need to be revised/amended to apply to the metaverse.

2. Digital Economy

2.1 Key Challenges

Pakistan does not have any general laws or regulations that cover the umbrella term digital economy. The Ministry of IT & Telecom has issued a Digital Pakistan Policy in 2018 to enable the acceleration of a digitised ecosystem for expansion of a knowledge-based economy and to spur economic growth. The Digital Pakistan Policy represents a vision with objectives to have a holistic digital strategy, have sectorial digitalisation, enhance e-commerce, empower youth, promote innovation and entrepreneurship in the IT sector, increase software exports, increase foreign – domestic investment and reduce barriers for disabled persons to have online access and standardisation, among others. This policy document is not law but guides relevant departments for future development in this area.

Digital banking, an element of the digital economy, is one sector that has seen development. Developing the e-commerce industry has also been of keen interest to the government of Pakistan in recent times. Pakistan remains sceptical of cryptocurrencies, which are now an integral part of the digital economy in certain jurisdictions.

Digital Banking

The regulator for banks in Pakistan is the State Bank of Pakistan (SBP). The SBP has, under the relevant provisions of the Banking Companies Ordinance 1962, issued the Licensing and Regulatory Framework for Digital Banks, in January 2022.

A “digital bank” has been defined as a bank which offers all kinds of financial products and services primarily through digital platforms or electronic channels instead of physical branches.

Under this framework, SBP may grant two types of digital bank licences:

- Digital Retail Bank (DRB), which will provide financial solutions to retail customers; and
- Digital Full Bank (DFB), which may provide financial solutions to retail customers as well as business and corporate entities.

The following will be eligible to form and seek a licence for a proposed digital bank.

- A traditional bank with a minimum of one year of experience of delivering digital financial services (DFS) in the retail customer segments may apply either individually or with other equity participants. However, the SBP may advise an extended period of experience if the traditional bank’s performance is not considered satisfactory by the SBP.
- An international bank or international DFS entity with a successful track record of a minimum of three years of delivering DFS in the retail customer segments may apply either individually or with other equity participants.
- An Electronic Money Institution (EMI) seeking conversion into a digital bank with a minimum of one year of experience of delivering DFS in

the retail customer segments. However, the SBP may advise an extended period of experience if the EMI's performance is not considered satisfactory by the SBP. Further, the pilot phase operation period of an EMI may be counted towards the one year operations requirement for an EMI seeking to transform into a digital bank.

- Those holding majority stake in or exercising control over an MFB, EMI, international bank or international DFS entity with a successful track record of a minimum of three years of delivering DFS in the retail customer segments may apply either individually or with other equity participants.
- Any other person with a minimum of three years of experience in the financial services, financial technology, telecommunication, merchant aggregation technology platforms, information communication technology (ICT), or other pertinent digital or innovative financial and non-financial domains, when applying to form a digital bank with a minimum of 5% equity in the proposed digital bank, either individually or preferably with at least one of the individuals or entities listed in sub-clause (a), (b) and (d) being a minimum 5% equity participant in the proposed digital bank.

The digital banking regime is not, however, immediately effective – the application process will be followed by a no objection certificate, an in-principle approval, demonstration of operational readiness by prospective licensees, and thereafter a grant of a restricted licence to commence pilot operations before grant of licence to commence commercial operations. The length of time needed to obtain a licence varies according to the fulfilment of each specified criteria.

The SBP in its press release dated 13 January 2023 confirmed that it has issued no-objection

certificates (NOC) to five applicants for establishing digital banks in the country, namely:

- Easy Paisa DB (Telenor Pakistan B V & Ali Pay Holding Ltd);
- Hugo Bank (Getz Bros & Co, Atlas Consolidated Pte Ltd and M & P Pakistan Pvt Ltd);
- KT Bank (Kuda Technologies Ltd, Fatima Fertilizer Ltd and City School Pvt Ltd);
- Mashreq Bank (Mashreq Bank UAE); and
- Ragami (Kuwait Investment Authority through PKIC and Enertech Holding Co).

These are the first NOCs that have been issued by the SBP for digital banks after a thorough and rigorous assessment process as per the requirements of the framework; they will now enter the next stages mentioned above for grant of licence.

E-Commerce

There is currently no sector-specific legislation applicable to the operation of e-commerce businesses in Pakistan. E-commerce operations in Pakistan are largely governed by existing laws and regulations on general commerce. The government of Pakistan published the e-Commerce Policy of Pakistan, October 2019 (Policy) with a vision to enable an environment for holistic growth of e-commerce across all sectors of Pakistan. A policy document of such nature is not law in Pakistan. As such, this policy only acts as guidance to various government departments and entities for the future development of e-commerce operations in Pakistan.

For the purposes of the foregoing, “e-commerce” includes the buying and selling of goods or services including digital products through electronic transactions conducted via the internet or other computer-mediated (online communications network).

The policy aims to address challenges faced in the following areas:

- e-Commerce regulatory and facilitation environment;
- financial inclusion and digitisation through payment infrastructure development;
- SMEs and youth empowerment through e-commerce;
- consumer protection in a digital environment;
- taxation on e-commerce activities;
- ICT sector and telecoms services in Pakistan;
- logistics for e-commerce platforms;
- data protection and investment; and
- global connectivity and multilateral negotiations.

Digital Currencies

Under BPRD Circular No 3 of 2018 (Circular), the SBP has prohibited the banks and financial institutions it regulates from enabling persons in Pakistan to deal in cryptocurrencies. While proceedings seeking issuance of a direction of appropriate nature so as to nullify the Circular and the implementation of a regulatory framework regarding crypto-assets and crypto mining in Pakistan are pending adjudication, the Federal Investigation Agency (FIA) has launched a crackdown on cryptocurrency dealers and has written a letter to the Pakistan Telecommunication Authority (PTA) to shut down 1,600 websites for this purpose, in view of the fact that millions have been purportedly embezzled from Pakistani citizens in digital currency fraud. Apart from shutting down these websites, the FIA has also sought the PTA's assistance in taking action against the people running these websites.

The SBP is now undertaking a detailed cost and benefit analysis on launching its own digital currency, known as the Central Bank Digital Currency (CBDC). CBDCs are digital tokens, similar

to cryptocurrency, and are the digital form of a country's fiat currency. However, unlike cryptocurrency, a CBDC is issued and regulated by a nation's monetary authority or central bank. The SBP intends to launch a Quick Response (QR) Code-based Person-to-Merchant (P2M) system in the recent future to enable merchants and small businesses to receive instant payments from their customers.

Separate to the above, the SBP has also promulgated the Regulations for Electronic Money Institutions (EMIs), with the aim of promoting new technological innovations to enable the non-banking sector to deliver innovative and efficient payment services to consumers at lower costs. These regulations are primarily aimed at removing entry barriers for non-banking entities by providing them a guiding as well as an enabling regulatory framework for the establishment and operations of EMIs in Pakistan. These regulations also address potential risks in order to ensure consumer protection in line the legal framework of the country while promoting digital payments and financial inclusion.

The regulations apply to EMIs, defined as non-banking entities duly authorised to issue means of payments in the form of "electronic money". Electronic money is the monetary value as represented by a claim on the issuer which is stored in an electronic, including a magnetic device or payment instrument, issued on receipt of funds of an amount not less in value than the monetary value issued, accepted as means of payment by undertakings other than the issuer and including electronic store of monetary value on an electronic device that may be used for making payments or may be prescribed by the SBP.

The SBP may grant an EMI licence in three stages, subject to compliance of the EMI Regulations:

- an “In-Principle” approval;
- permission to commence pilot operations (limited-scale real transactions) once the EMI attains operational readiness, fulfils minimum capital and security deposit requirements and any other requirements as mentioned in the In-Principle approval; and
- full scale licence to commence commercial operations to be granted subject to satisfactory completion of pilot operations and fulfilment of all SBP requirements.

To date, four non-banking entities have been granted a full-scale licence, while several more have received in-principle approval.

Challenges

With a large and growing population, Pakistan is among the countries with the highest number of smartphone subscribers and is well-suited to move towards a digital economy. Even though the past year has seen a significant shift from traditional means of doing business, educating the masses on the purpose and benefits of digitisation remains a noteworthy challenge. Moreover, access to a faster and reliable communication network is a major challenge, especially in remote areas. This is critical for any material effort to promote digitisation to take effect in Pakistan.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

In February 2022, the Ministry of Information Technology & Communication notified the “Paki-

stan Cloud First Policy” (the Cloud Policy) to encourage cloud adoption across Pakistan, and to empower organisations to transition to cloud-based solutions. The Cloud Policy is expected to result in cloud adoption across a variety of markets and industries and foster the growth of the local ICT industry by enabling access to cloud-based technologies and complementing emerging technologies such as AI, machine learning, and the IoT.

The Cloud Policy recognises cloud service providers’ approach to information security and data privacy concerns, and further recognises different cloud service models including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS), as well as the different cloud deployment methods, including the public cloud, government cloud, private cloud and hybrid cloud.

For the implementation of the Cloud Policy, the Ministry of Information and Technology is to set up a cloud office to ensure a planned governance structure that will enable the roadmap for establishing a structured and formal organisation for cloud governance in Pakistan.

Industries with Greater Regulation

Banking sector

Pursuant to BPRD Circular No 01 of 2023, the SBP has notified a framework titled “Framework on Outsourcing to Cloud Service providers” (the Framework). The Framework overrides the previous framework titled the Enterprise Technology Governance and Risk Management Framework” which was notified vide the BPRD Circular No 5 of 2017 and amended by BPRD Circular No 6 of 2019 and BPRD Circular No 4 of 2020.

The Framework applies to all regulated entities (RE) including banks, digital banks, microfi-

nance banks, electronic money institutions, etc, and sets out minimum requirements for REs to outsource their material and non-material workloads to cloud service providers.

Permissible cloud outsourcing arrangements

Material workload under the Framework means all systems, applications and services that are fundamental for carrying out the business of an RE and that, if disrupted, have the potential to significantly impact an institution's business operations, reputation or profitability. Outsourcing of services to cloud service providers does not absolve the REs from their prime responsibilities, including managing and running the business operations effectively by adhering to the legal and regulatory requirements and the protection of consumers' data, and REs are further encouraged to give preference to onshore cloud service providers.

The REs are permitted to outsource their workload to cloud service providers in the following manner:

- all type of workloads (material and non-material) may be outsourced to reputable onshore (domestic) cloud service providers;
- electronic money institutions, non-designated payment system operators or payment service providers may outsource their material and non-material workloads to offshore (outside Pakistan) cloud service providers; and
- banks, microfinance banks, digital banks, development finance institutions and designated payment system operators or payment service providers may outsource their non-material workloads to offshore cloud service providers, although outsourcing of their material workloads to offshore cloud service providers shall be subject to SBP's approval.

Other requirements under the Framework include the following.

- REs are required to monitor and review capacity utilisation of their cloud workloads.
- REs are to provide adequate training of the cloud environment, to their end-users and privileged users.
- All security incidents/breaches are to be reported to the SBP in compliance with the requirements specified in the "Enterprise Technology Governance & Risk Management Framework for Financial Institutions" or as advised by the SBP from time to time. Further, REs are to conduct investigations to identify the root cause, take appropriate actions to prevent recurrence of such incidents in future and fix responsibility for such lapse.
- For material workloads, REs are to provide the following information to the SBP one month before placing their services with the CSPs:
 - (a) name of the CSPs, and their parent company (if any);
 - (b) description of the activities and details of data to be placed with the CSP;
 - (c) date of commencement/renewal/expiry of services;
 - (d) last contract renewal date (where applicable); and
 - (e) service and deployment models.

Internal controls in cloud outsourcing arrangements under the Framework

There are multiple safeguards and internal control guidelines provided under the Framework. These include having an overall structure and processes for managing cloud outsourcing arrangements, which is vital in maximising the benefits and managing the associated risks. REs planning to outsource need to consider adapt-

ing their organisational structure for effective and efficient oversight of cloud service providers by developing comprehensive internal policies, delegating cloud specific governance responsibilities, etc.

The Framework requires the REs to exercise reasonable care before entering into cloud outsourcing arrangements by conducting reasonable due diligence of the cloud service providers and their material subcontracting arrangements by using the defined criteria set out in the Framework.

The REs are further required to maintain an effective oversight mechanism including but not limited to the assessment of performance against desired service levels and the ongoing viability of the cloud service provider's cybersecurity practices and controls, changes in service location(s), subcontracting, change of ownership, and to review and monitor the cloud service provider's compliance with the laws and contractual obligations on an ongoing basis.

The Framework also requires the REs to establish a mechanism for security event monitoring by complying with the requirements set out in the Framework.

Processing of personal data in the context of the cloud

The Framework provides that outsourcing of the workloads to the cloud service providers does not relieve the REs from the responsibility of safeguarding data confidentiality and integrity and has laid out a set of obligations and/or responsibilities for REs to ensure the data protection.

Separately, the Ministry of Information Technology and Telecommunication is in the process of

seeking comments from stakeholders on a consultation draft (v.25.08.2021) of a personal data protection bill (PDP Bill) before it is tabled in Parliament. This bill has undergone a few iterations, and the most recent draft appears to incorporate input received from stakeholders on the earlier drafts.

If enacted, the PDP Bill will require that personal data is not transferred to any system located outside Pakistan or a system that is not under the direct control of the federal or provincial governments of Pakistan, unless it is ensured that the country to which the data is transferred offers personal data protection at least equivalent to that under the PDP Bill. Such data is required to be processed in accordance with the PDP Bill and, where applicable, consent must be given by the data subject.

Since the PDP Bill aims to regulate the processing of personal data, cloud service providers will be required to comply with the provisions thereunder; personal data stored on a cloud may only be processed with the consent of the data subject unless the processing is necessary:

- for the performance of a contract to which the data subject is a party;
- for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by a contract;
- in order to protect the vital interests of the data subject;
- for the administration of justice pursuant to an order of a court of competent jurisdiction;
- for legitimate interests pursued by the data controller; or
- for the exercise of any functions conferred on any person by or under any law.

Furthermore, personal data is not permitted to be processed unless:

- the personal data is processed for a lawful purpose directly related to an activity of the data controller;
- the processing of the personal data is necessary for or directly related to that purpose; and
- the personal data is adequate but not excessive in relation to that purpose.

The PDP Bill also provides that critical personal data will only be processed in a server or data centre located in Pakistan. Personal data, other than that categorised as critical personal data, may be transferred outside the territory of Pakistan under a framework (on conditions) to be devised and a mechanism for keeping a copy of personal data in Pakistan, which is also to be devised by the National Commission for Personal Data Protection (which is required to be established within six months of the promulgation of the PDP Bill into law).

Additional compliance requirements

A person providing cloud computing and/or hosting services may fall within the definition of a “service provider”, “social media company” or a “significant social media company” in terms of the Prevention of Electronic Crimes Act 2016 (PECA) and the Removal and Blocking of Unlawful Online (Procedure, Oversight and Safeguards) Rules 2021 (RBUO Rules).

Pertinent definitions appearing in the PECA and RBUO Rules appear below.

- “Online information system” means an information system connected with other information systems through internet and any cloud-based content distribution services.

- “Service provider” includes a person who:
 - (a) acts as a service provider in relation to sending, receiving, storing, processing or distributing any electronic communication or the provision of other services in relation to electronic communication through an information system;
 - (b) owns, possesses, operates, manages or controls a public switched network or provides telecommunication services; or
 - (c) processes or stores data on behalf of such electronic communication services or the users of such services.
- “Significant social media company” means and includes social media companies with more than half million users in Pakistan or companies on the list specially notified by the PTA for this purpose from time to time.
- “Social media company” means any person that owns, provides or manages online information system for the provision of social media or social network service.

The RBUO Rules have been notified under the PECA and provide that service providers, social media companies or significant social media are required to:

- make available community guidelines for access or usage of any online information system, and these guidelines should easily be accessible and will inform the user of the online information system not to host, display, upload, modify, publish, transmit, update or share any content in violation of local laws;
- provide to the Federal Investigation Agency (FIA) any information, date, content or sub-content contained in any online information system owned, managed or run by the respective service provider, social media company or social media company, in decrypted, readable and comprehensible

format or plain version in accordance with the provisions of PECA; and

- deploy mechanisms to ensure immediate blocking of live streaming through an online information system in Pakistan of any online content particularly related to terrorism, hate speech, pornography, incitement to violence and that is detrimental to national security on receiving intimation from the PTA.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Technologies such as artificial intelligence and machine learning, which are at the forefront of computing, have had limited practical application until recently, but they have come to pervade daily life in a short span of time and are galvanising a technological paradigm shift. Business analytics and big data are transforming the way businesses and governments operate. Competing on analytics is the new norm, whereby competitive advantage is defined by turning proprietary and other data sets into insights using advanced algorithms. The advances in big data analytics, machine learning and the use of artificial intelligence in relation thereto may present a great opportunity for Pakistan. There is, however, no specific regulatory framework currently applicable in Pakistan that addresses the implementation and/or regulation of big data, machine learning and artificial intelligence, which may be the biggest challenge relating to the implementation of these technologies. A system or product utilising big data, machine learning and/or artificial intelligence technology is presently treated at par with any other system or product of a similar nature.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection Internet of Things

While IoT projects and services are not subject to specific requirements and do not require a special authorisation, there are certain telecommunications standards that may become relevant depending on the type of device(s) to be used and/or service(s) the provision of which is contemplated.

The regulator for the telecommunications sector in Pakistan is the PTA, which was created pursuant to the Pakistan Telecommunication (Reorganisation) Act 1996 (PTA Act). Every licence granted by the PTA may contain:

- restrictions as to the types of telecommunication system or telecommunication service to be provided by the licensee, the area and period of operation and the types of telecommunication equipment that may be included in its telecommunication system;
- the obligation to ensure that only terminal equipment approved for connection to the telecommunication system in question is connected; and
- obligations to maintain confidentiality of customer data.

Devices that utilise the radio-electric spectrum to transmit and/or receive information require a “type approval” from the PTA before they can be connected to a public-switched network (further details of this are provided in **7.1 Scope of Regulation and Pre-marketing Requirements**).

Machine-to-Machine Communications and Data Protection

Pakistan does not have a legal framework that specifically regulates machine-to-machine communications. While sector-specific regulators enforce data protection requirements as part of the law and the terms of the licences granted thereunder, the PECA criminalises the misuse of personal data without consent, and it is therefore important that machine-to-machine communications do not result in the commission of offences under the PECA. These offences include:

- unauthorised access to information systems or data;
- unauthorised copying or transmission of data;
- interference with information systems or data;
- unauthorised access to critical infrastructure information systems or data;
- unauthorised copying or transmission of critical infrastructure data;
- interference with critical infrastructure information systems or data;
- electronic forgery;
- electronic fraud;
- unauthorised use of identity information;
- unauthorised interception;
- malicious code;
- spamming; and
- spoofing.

Moreover, Protection from Spam, Unsolicited, Fraudulent and Obnoxious Communication Regulations, 2009, framed under the PTA Act, apply to all licensees of the PTA to ensure and protect the interest of telecoms consumers by preventing them from harassment, disturbance, spam, fraudulent and unsolicited communication.

Communication Secrecy

The transmission of encrypted data on a public-switched network as traffic is not permitted

under the applicable laws. Non-standard protocols of communication, including encryption, cannot be undertaken without prior approval of the PTA. Prior approval of the PTA is required for use of a non-standard mode of communication including virtual private networks (VPN) and non-standard protocols which include encrypted messages. The use of any non-standard of communication, including all mechanisms by means of which communications become hidden or modified to the extent that they cannot be monitored, is a violation of applicable laws.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

The Pakistan Electronic Media Regulatory Authority (PEMRA) – established under the Pakistan Electronic Media Regulatory Authority Ordinance, 2002 (PEMRA Ordinance) – is mandated to regulate the establishment and operation of all broadcast media and distribution services in Pakistan. It was established for the purpose of international, national, provincial, district, local or special target audience broadcasting. PEMRA regulates the distribution of foreign and local TV and radio channels in Pakistan.

For the purposes of the foregoing:

- “broadcast media” includes media which originates and propagates broadcast and pre-recorded signals by terrestrial means or through satellite for radio or television, and includes teleporting, provision of access to broadcast signals by channel providers and such other forms of broadcast media as PEMRA may, with the approval of the federal government, specify; and

- “distribution services” includes a service which receives broadcast and pre-recorded signals from different channels and distributes them to subscribers through cable, wireless or satellite options and includes Cable TV, local multipoint distribution service (LMDS), multichannel multipoint distribution service (MMDS), direct-to-home (DTH) and other similar technologies.

Licensing Regime

Operating broadcast media or providing distribution services can only be undertaken once a licence has been obtained from PEMRA. Applications are decided subject to clearance from the Ministry of Interior and frequency allocation by the Frequency Allocation Board (FAB) in relevant cases. PEMRA issues licences for broadcast media and distribution services for:

- international and national scale stations;
- provincial-scale broadcasts;
- local area or community-based radio and TV broadcasts;
- specific and specialised subjects;
- distribution services; and
- up-linking facilities, including teleporting and digital satellite news gathering units (DSNG).

PEMRA may also grant permission to a distribution service licensee for the running of an in-house distribution channel subject to such terms and conditions as PEMRA may prescribe, provided that only Pakistani content is permitted to be distributed on such channel.

A licence granted by PEMRA under the PEMRA Ordinance will be valid for a period of five, ten or 15 years subject to payment of the annual fee, as prescribed from time to time. PEMRA may renew a licence on such terms and conditions as may be prescribed and in case of refusal

to renew a licence, reasons will be recorded in writing. Subject to the terms and conditions of the licence granted by PEMRA, a licensee is not permitted to sell, transfer or assign any of the rights conferred by the licence without prior written permission of PEMRA.

PEMRA is required to process each application in accordance with prescribed criteria and hold public hearings in the respective capitals of each province or, as the case may be, in Islamabad, before granting or refusing the licence.

Every application form is required to be accompanied by a non-refundable application processing fee as set out in Schedule-B of the Pakistan Electronic Media Regulatory Authority Rules 2009 (PEMRA Rules). Applications for the grant of a licence will, in the first instance, be short-listed by considering their:

- financial viability;
- technical feasibility;
- financial strength;
- credibility and track record;
- majority shareholding and management control (which should vest in Pakistani nationals);
- prospects of technical progress and introduction of new technology;
- market advancement, such as improved service features or market concepts;
- contribution to universal service objectives; and
- contribution to other social and economic development objectives.

Ownership restrictions

PEMRA will not grant a licence to:

- a person who is not a citizen of Pakistan or resident in Pakistan;

- a foreign company organised under the laws of any foreign government;
- a company the majority of whose shares are owned or controlled by foreign nationals or companies whose management or control is vested in foreign nationals or companies; or
- any person funded or sponsored by a foreign government or organisation.

Foreign Programmes and Local Content Requirement

Licensees of PEMRA, pursuant to the terms of their licence, are required to carry all channels of Pakistan Television Corporation (PTV), the national broadcaster, and all licensed satellite TV and foreign satellite TV channels having landing rights permission from PEMRA. Such licensees, under all circumstances, will provide the “basic service”, which includes a range of satellite TV channels as determined by PEMRA, comprising channels with religious, educational, informational, news and entertainment content. A licensee will be restricted to carry or relay only those foreign satellite TV channels that have obtained necessary landing rights permission of PEMRA for “landing” into Pakistani territory. A licensee may not discriminate against any licensed TV channel or landing rights permission holder in offering its broadcast or distribution platform.

Licensees of PEMRA, pursuant to the terms of their licence, are required to offer at least one basic service package (this means the free-to-air television channels of the national broadcasters, non-commercial educational and health-related TV channels licensed by PEMRA, and such other free-to-air television channels as determined by PEMRA to be distributed by a distribution service licensee to its subscribers against a fixed minimum monthly subscription fee) that includes the must-carry channels (ie, the channels of national broadcasters, non-commercial

educational channels licensed by PEMRA and such other free-to-air television channels as determined by PEMRA to be distributed by the distribution networks including IPTV networks to its subscribers), for which it does not charge a subscription fee at a rate higher than the maximum fee prescribed by PEMRA.

PEMRA has issued a notification whereby the airing of Indian content has been banned. Further, airing programmes that are a production of international entities requires prior approval from PEMRA. PEMRA has also prohibited broadcast media or distribution service operators from broadcasting or rebroadcasting or distributing any programme or advertisement if PEMRA is of the opinion that such programme or advertisement is:

- against the ideology of Pakistan;
- likely to create hatred among the people;
- prejudicial to the maintenance of law and order;
- likely to disturb public peace and tranquillity or endanger national security; or
- pornographic, obscene, vulgar or offensive to the commonly accepted standards of decency.

Online Content/Internet-Based Platforms

PEMRA regulates the traditional distribution platforms, whereas the PTA and PEMRA jointly regulate internet-based platforms.

PEMRA has provided, on its website, Consultation Paper No Web&OTT/1- 2020 in relation to regulating web TV and over-the-top (OTT) TV; however, there is no specific legal framework to regulate such content, except for the RBUO Rules which allow the PTA to block certain online content and/or the entire online system if such

content is not removed by the service provider or social media company.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The PTA Act and the rules and regulations framed thereunder (the PTA Laws) provide a framework to regulate the operation of telecommunications systems and the provision of telecommunications services. The PTA Act provides that no person is permitted to establish, maintain or operate any telecommunication system or provide any telecommunication service unless they have obtained a licence under the PTA Act.

For purposes of the foregoing:

- “telecommunications system” means any electrical, electromagnetic, electronic, optical or optio-electronic system for the emission, conveyance, switching or reception of any intelligence within, into, or from Pakistan, whether or not that intelligence is subjected to rearrangement, computation or any other process in the course of operation of the system, and includes a cable transmission system, a cable television transmission system and terminal equipment; and
- “telecommunications service” means a service consisting of the emission, conveyance, switching or reception of any intelligence within, into or from Pakistan by any electrical, electromagnetic, electronic, optical or optio-electronic system, whether or not the intelligence is subjected to rearrangement, computation or any other process in the course of the service.

Network and Service Provider Obligations

The definitions of the above-mentioned activities are very broad – therefore, the PTA Act could apply to a wide range of entities and services.

Radio-Electric Spectrum

The PTA is also responsible for dealing with applications relating to the use of radio-spectrum frequency through its Frequency Allocation Board (FAB), which has the exclusive authority to allocate and assign portions of the radio frequency spectrum to the government, providers of telecommunications services and telecommunication systems, radio and television broadcasting operations, public and private wireless operators, and others.

Terminal Equipment/Type Approval

An approval by the PTA will be required before any terminal equipment can directly or indirectly be connected to a public switched network. The PTA may impose certain conditions on the approval, including conditions limiting its connection to specified types of telecommunication systems. The technical standards for terminal equipment and the procedure for approving test equipment, testing any terminal equipment and certifying that it complies with the relevant technical standards has been provided in the Type Approval Technical Standards Regulations 2021 and its subsequent amendment, Type Approval Technical Standards (Amendment) Regulations, 2022.

A type approval granted by the PTA signifies that particular telecommunication equipment is approved for general sale and is suitable to connect with a specific public telecommunication network.

The following categories of equipment require prior type approval from the PTA:

- tracking system devices with subscriber identity module (SIM) or international mobile equipment identity (IMEI)-based functionality and which transmit location details (eg, vehicle tracking or smart watches with SIM/tracking);
- satellite terminal equipment;
- wireless radio trans/receiver sets with more than 2 MW output power (eg, very high frequency, high frequency, ultra-high frequency and two-way radios);
- terminal devices operating in information security management (ISM) as defined by PTA ISM band regulations, global navigation satellite systems (GNSS) within the band and usage conditions prescribed by the Frequency Allocation Board (FAB) of the PTA;
- short range devices (SRD), ultra wide band (UWB), IoT devices, radio-frequency identification (RFID), Bluetooth, immobilisers, inductive loop systems, smart metering, technology telemetering, machine-to-machine (M2M), etc, as defined in PTA Regulatory Framework for Short Range Devices (SRD) and Terrestrial Internet of Things (IoT) Services, etc;
- internet protocol phones, videoconferencing, voice-over internet protocol (VoIP) systems, gateway, etc;
- private automatic branch exchange (PABX) or internet protocol private automatic branch exchange (IP-PABX); and
- SIM/IMEI/Wi-Fi-based mobile devices (eg, mobile handsets, Wi-Fi tablets, dongles, wingles).

The following types of equipment are exempted from type approval:

- networking equipment (switches, firewalls, servers, storage devices);
- laptops, desktops and personal computers;
- tablet PCs with Wi-Fi-only functionality (non-SIM based devices); and
- global positioning system-only devices.

A non-refundable processing fee of PKR5,000 (PKR2,500 for SRDs and UWBs) per application for locally manufactured terminal equipment and USD100 (USD50 for SRDs and UWBs) per case for internationally manufactured terminal equipment is charged by the PTA for all new cases, for amendments of issued certificate and for issuance of duplicate certificates.

VoIP/Instant Messaging

Given that transmission of encrypted data on the network as traffic is not permitted under the applicable laws, non-standard protocols of communication, including encryption, cannot be undertaken without prior approval of the PTA. Operators are required to obtain prior approval of the PTA if they use a non-standard mode of communication including VPNs and non-standard protocols which include encrypted messages. Furthermore, the use of any non-standard of communication, including all mechanisms by means of which communications become hidden or modified to the extent that they cannot be monitored, is a violation of applicable laws.

While it is mandatory for service providers to provide local enforcement agencies with decryption and interception abilities for encrypted services, regulation relating to messaging and VoIP is highly topical.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Technology agreements are not specifically regulated under Pakistan law and are therefore sub-

ject to being governed according to the volition of the parties in terms of the Contract Act 1872, and are generally reflective of best practices in the sector. This provides parties with the ability to reflect their interest and will in their legal relationship. A contract, however, may not be contrary to the law that is in force, and parties may be required to comply with certain obligations, which may result from sector-specific regulations.

Please also refer to the “Banking sector” and “Processing of Personal Data in the Context of the Cloud” subsections in **3.1 Cloud and Edge Computing**.

Foreign Exchange Controls

One of the greatest challenges that local organisations encounter in terms of entering into technology agreements with non-residents is in seeking an exemption from the SBP in connection with the restriction imposed on outward payments to non-residents under the Foreign Exchange Regulation Act 1947 (FERA). Pursuant to the FERA, no person located or resident in Pakistan is permitted to make any payment to or for the credit of any person resident outside Pakistan, except as may be provided in and in accordance with any general or special exemption from the provisions of FERA which may be granted conditionally or unconditionally by the SBP.

The SBP has, however, extended a general exemption to the restriction contained in the FERA, whereby scheduled banks have been given general permission to release foreign exchange up to a maximum of USD100,000 (or its equivalent in other currencies) per invoice for private sector companies incorporated in Pakistan, and branches of foreign companies operating in Pakistan with the permission of the

Board of Investment. This exemption applies when such companies/branches are undertaking permissible business/commercial activities, paying local taxes and periodically repatriating their profits abroad (subject to compliance with the relevant provisions of applicable law).

After satisfying themselves of the genuineness of the requests, and after deducting all applicable taxes, the SBP allows the above-mentioned payments for charges on account of utilisation of IT services such as:

- satellite transponder charges;
- international bandwidth charges;
- international internet service charges;
- international private line charges;
- software licence, maintenance or support fees for proprietary/specialised software; and
- subscriptions or payments for access to foreign electronic media and databases.

The SBP has also extended a general permission to scheduled banks to release foreign exchange up to a maximum of USD400,000, or equivalent in other currencies, per year (starting from the date of designation of the relevant scheduled bank), for each company/firm/sole proprietorship incorporated/established in Pakistan on account of commercial payments, pertaining to digital services, in favour of digital service provider companies.

The above permissions are subject to the fulfilment of procedural requirements, set out in the Foreign Exchange Manual (a compendium of permissions granted by the SBP with regard to FERA, from time to time).

Pursuant to EPD Circular Letter No 02 of 2023, the SBP, in a move to encourage exporters of software and IT and IT-enabled services to bring

their foreign exchange earnings into the country, has allowed 35% retention of earnings outside the country. For meeting this objective, the SBP has amended the Foreign Exchange Manual and advised the banks to mandatorily allow, until 31 March 2023, retention of 35% of their export proceeds in special foreign currency accounts. After the expiry of this period, the instructions will be reviewed in light of the export performance of the IT sector and export proceeds during this period.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Electronic Signatures

The Electronic Transactions Ordinance, 2002 (ETO) was enacted to recognise and facilitate documents, records, information, communications, transactions and signatures in electronic form, and to allow their admissibility as evidence in a court of law without witnessing being necessary.

An electronic signature under the ETO can be in the form of letters, numbers, symbols, images, characters or any combination thereof in electronic form incorporated in an electronic document with the intention of authenticating or approving the same. An advanced electronic signature under the ETO is either:

- a signature which is unique to the person signing it, capable of identifying such person, created in a manner under the sole control of the person using it, and attached to the electronic document to which it relates in a manner that any subsequent change in the electronic document is detectable; or

- provided by an accredited certification service provider and accredited by the certification council as being capable of establishing authenticity and integrity of an electronic document.

Trust Services

The federal government of Pakistan established an Electronic Certification Accreditation Council (ECAC) under the ETO, one of the main functions of which is to grant and renew accreditation certificates to certification providers, their cryptography services and security procedures, in order to establish trust through the use of accredited digital signatures.

The Certification Service Providers' Accreditation Regulations, 2008 (CSPA Regulations), framed under the ETO, provide for a mechanism for the ECAC to issue accreditation to eligible applicants to be an "Accredited Certification Service Provider". The purpose of an accredited certification service provider is to provide certification services and certificates confirming the authenticity and/or integrity of an electronic document or an electronic signature.

Digital Identity

The National Database & Registration Authority (NADRA) launched computerised and chip based national identity cards in 2012 and has recently been working to make the computerised national identity cards into digital wallets and introduce a mobile application for that purpose.

Amendments have been made in the Income Tax Ordinance, 2001, vide the Finance Act, 2022, to enable NADRA to share its records and any information with the Federal Board of Revenue for the purpose of carrying out the objectives of the Income Tax Ordinance, 2001.

In addition to the above, the ECAC facilitates regulators and authorities in Pakistan such as the SBP, NADRA, the Securities and Exchange Commission of Pakistan (SECP), the FBR, the PTA and the Election Commission of Pakistan (ECA), for use of digital identity for the integrity of electronic transactions as per the guidelines set out in the ETO.

More recently, Parliament has enacted the Pakistan Single Window Act, 2021 (PSW Act), to establish and operate a single point of submission and receipt of trade data and information to enable synchronised processing of data and information; achieve standardisation and harmonisation of documents required for regulatory control; remove legal, regulatory and operational barriers to electronic transactions for external trade; and facilitate co-ordination and partnership among all the relevant trade regulatory agencies and stakeholders dealing with international trade and trade facilitation.

The federal government, to further achieve the object of the PSW Act, framed the Pakistan Single Window Evidence of Identity (EOI) Rules, 2022 (EOI Rules), under the PSW Act. The EOI Rules apply to all individuals, sole proprietorships or bodies corporate registered with the FBR, the SECP, government organisations, diplomatic missions, foreign individuals, businesses or any other commercial and non-commercial entity engaged in cross-border trade.

The EOI Rules require all persons wishing to conduct a cross-border trade transaction to undergo an electronic verification process by subscription to a PSW system whereby the applicant upon furnishing the necessary information and payment of subscription will be issued a unique user ID electronically. The PSW system is designed to function in connection and in conjunction with the FBR, the SECP, NADRA, Pakistan Mobile Number Portability Database Company (PMD) and commercial banks, amongst others.

Challenges

While Pakistan is taking noteworthy steps towards digitising identity, the country's personal data protection laws are not yet following suit, in the absence of which the risk of misuse of a person's identity information remains significant. NADRA's database is accessed by scores of public and private service providers, from the tax department to the election commission to mobile service providers. As there is no data protection law, there is no accountability even when personal data of persons is leaked. Promulgation of appropriate data protection laws and their strict enforcement is necessary to mitigate such risks.

RIAA Barker Gillette offers the full range of corporate, commercial and dispute resolution legal services from offices in Pakistan's major cities: Karachi, Lahore, Islamabad and Peshawar. With nine partners and over 40 associates, the firm is amongst the country's largest practices. Its clients include multinational corporations, financial institutions, non-profit organisations, Pakistani conglomerates, private clients and government agencies. RIAA Barker Gillette is also the primary contact in Pakistan for many major international law firms. It has extensive experience

of complex cross-border work, and on advising across a number of industry and regulatory sectors. The firm is routinely called on to act in projects, M&A, private equity, corporate restructuring and tax advisory mandates, and on commercial disputes. In addition to the support of and access to the resources of its offices in London, New York, Dubai, Beijing, and Kabul, RIAA Barker Gillette is the exclusive member firm in Pakistan for Lex Mundi, the world's leading network of independent law firms, which has members in over 100 countries.

Authors



Yousaf Khosa is a partner of RIAA Barker Gillette, based in Islamabad. He is recognised as one of the leading lawyers in Pakistan. He has been involved in the drafting of prominent

petroleum laws in the country, and regularly advises clients on their corporate, commercial, labour and taxation matters. He is considered an expert in the telecommunication, oil and gas, and construction sectors in Pakistan.



Shafaq Rehman is a partner at RIAA Barker Gillette based in Karachi and has vast experience in assisting clients on corporate advisory and transactional matters. Her clients are primarily

comprised of multinational companies operating in Pakistan or seeking to commence operations in Pakistan. She is a key contact for foreign law firms, including several offices of Baker McKenzie, Clifford Chance and Cooley LLP. Shafaq has assisted with establishing and regularising multiple start-ups and has also acted for investors that have funded existing start-ups in Pakistan. Her practice focuses on cross-border advisory, where she routinely advises clients on matters relating to foreign exchange, M&A and corporate compliance.

Contributed by: Yousaf Khosa, Shafaq Rehman, Amna Anjum and Mahnoor Javed, **RIAA Barker Gillette**



Amna Anjum is an associate in the Karachi office of RIAA Barker Gillette. She advises local and foreign clients on all aspects of corporate, commercial, regulatory and transactional matters.



Mahnoor Javed is an associate based in the Karachi office of RIAA Barker Gillette. She regularly assists senior associates and partners in corporate advisory and transaction matters.

RIAA Barker Gillette

D67/1
Block 4
Clifton
Karachi

Tel: +92 21111 529937
Email: pk@riaabg.com
Web: www.riaabarkergillette.com/pk

**RIAA
Barker
Gillette**

Law and Practice

Contributed by:

Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran
and Raymond John S Cheng

Villaraza & Angangco see p.405



Contents

1. Metaverse	p.388
1.1 <u>Laws and Regulations</u>	<u>p.388</u>
2. Digital Economy	p.389
2.1 <u>Key Challenges</u>	<u>p.389</u>
3. Cloud and Edge Computing	p.392
3.1 <u>Highly Regulated Industries and Data Protection</u>	<u>p.392</u>
4. Artificial Intelligence and Big Data	p.394
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	<u>p.394</u>
5. Internet of Things	p.396
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	<u>p.396</u>
6. Audio-Visual Media Services	p.397
6.1 <u>Requirements and Authorisation Procedures</u>	<u>p.397</u>
7. Telecommunications	p.398
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	<u>p.398</u>
8. Challenges with Technology Agreements	p.400
8.1 <u>Legal Framework Challenges</u>	<u>p.400</u>
9. Trust Services and Digital Entities	p.402
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	<u>p.402</u>

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

1. Metaverse

1.1 Laws and Regulations

To date, the Philippine government has not yet passed a law which specifically provides rules and regulations regarding the metaverse.

Nonetheless, government agencies in the Philippines recognise the potential of virtual asset systems to revolutionise digital transactions. In particular, in 2021 the *Bangko Sentral ng Pilipinas* (BSP), which is the central bank of the Philippines, issued Circular No 1108 providing regulations for virtual asset service providers (VASPs).

Under BSP Circular No 1108, a VASP is defined as any entity that offers services or engages in activities that provide for the transfer or exchange of virtual assets, which involve one or more of the following activities:

- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets; and
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets.

The Circular defines “virtual assets” or “VAs” as any types of digital unit that can be digitally traded or transferred, and that can be used for payment or investment purposes. They can be considered as “properties”, “proceeds”, “funds”, “funds or other assets”, and other “corresponding value” that can be used as a medium of exchange or a form of digitally stored value created by agreement within the community of VA users. However, digital units of exchange are not considered as VAs where they are used for:

- the payment of goods and services solely provided by their issuer or a limited set of merchants specified by their issuer (eg, gift checks); or
- the payment of virtual goods and services within an online game (eg, gaming tokens).

The BSP has also recognised non-fungible tokens or “NFTs” as a class of virtual asset that establishes ownership of a unique asset (digital or physical) such as digital arts and music. Nonetheless, the BSP noted that NFTs in the form of gaming tokens are a form of digital units of exchange, which are excluded under the regulations of BSP Circular No 1108.

Under BSP Circular No 1108, an entity which falls under the definition of a VASP is required to secure a certificate of authority (COA) as a money service business (MSB). In the course of a COA application, the BSP shall take into account and extend its evaluation over the fitness and propriety of the VASP’s beneficial owners.

Pursuant to the provisions of the BSP Circular, VASPs are only allowed engage in transactions with other VASPs, financial institutions and/or remittance and transfer companies that are duly authorised and licensed with the appropriate regulatory authorities. The transfer of virtual assets between VASPs and other BSP-supervised financial institutions (BSFIs) shall also be considered as cross-border wire transfers. In addition, the transactions must comply with the pertinent rules on wire transfers issued by the BSP.

BSP Circular No 1108 also seeks to address challenges that are typically associated with transactions performed using virtual assets, such as having adequate cybersecurity and ensuring confidentiality and integrity of data.

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

Thus, under the Circular, VASPs are mandated to have the following, among others.

- A sound risk management system to mitigate risks arising from outsourcing.
- An internal control system commensurate with the nature, size and complexity of their business.
- Customer awareness measures to educate their customers on matters including:
 - (a) safeguarding of VAs and/or fiat currency wallets as well as protection of client information such as login credentials;
 - (b) use of the mobile platform and wallets;
 - (c) actual fees and charges related to the use of the mobile platform and withdrawal transactions; and
 - (d) problem-resolution procedures.
- Customer due diligence.

Currently, there is a moratorium for applications for VASP licences for a period of three years, starting 1 September 2022. To date, the BSP has not yet lifted the moratorium.

2. Digital Economy

2.1 Key Challenges

Laws Regulating the Digital Economy

To aid the Philippines in boosting its digital economy, various laws and regulations have been passed by the Philippine government and its agencies to provide legal validity to digital transactions, and to regulate activities provided by entities providing digital services. Among the key policies passed are the following.

The E-Commerce Act

Recognising the role of information and communications technology (ICT) in nation-building, the Philippine government enacted Republic Act

(RA) No 8792 (the “E-Commerce Act”) as early as the year 2000. This law aims to facilitate transactions, exchanges and storage of information through the utilisation of electronic, optical and similar mediums, modes, instrumentality and technology.

Through the E-Commerce Act, electronic data messages, electronic documents and electronic signatures were given legal effect, validity or enforceability. The legislation likewise recognised that contracts may be expressed in, demonstrated by and proved by means of electronic data messages or electronic documents, and no contract shall be denied validity or enforceability on the sole ground that it is in the form of an electronic data message or electronic document.

The National Payment Systems Act

RA No 11127, otherwise known as the National Payment Systems Act (NPSA), was passed and signed into law on 30 October 2018. Through said law, the government aims to promote the safe, secured, efficient and reliable operation of payment systems. Hence, all operators of payment systems (OPS) are required to register with the BSP.

To implement the provisions of the NPSA, the BSP issued BSP Circular No 1049, series of 2019, providing for the *Rules and Regulations on the Registration of OPS*. The BSP also issued BSP Circular No 1089, series of 2020, or the *Payment System Oversight Framework* (PSOF), which sets out the regulatory approach of the BSP in overseeing payment systems in the Philippines.

Pursuant to the rule-making powers of the BSP, the following activities are considered operations

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

of a payment system, and entities performing such activities are required to register as OPS:

- maintaining the platform that enables payments or fund transfers, regardless of whether the source and destination accounts are maintained with the same or different institutions;
- operating the system or network that enables payments or fund transfers to be made through the use of a payment instrument; and
- providing a system that processes payments on behalf of any person or the government.

If an OPS is also a BSFI engaged in payments and settlements, it must additionally comply with the provisions of BSP Circular No 970, series of 2017, or the *Adoption of a National Retail Payment System Framework* (NRPS). The NRPS is a policy and regulatory framework that aims to provide direction in carrying out retail payment activities through BSFIs by defining high-level policies, principles and standards, which when adopted would lead to the establishment of a safe, efficient and reliable retail payment system.

The Credit Card Law

With the objective of promoting fair and sound consumer credit practices which are aligned with global best practices, the Philippine government also enacted RA No 10870, otherwise known as the “Credit Card Law”. Said law defines a “credit card” as any card or other credit device intended for the purpose of obtaining money, property or services on credit.

Through the Credit Card Law, the BSP supervises all credit card issuers and acquirers. A “credit card issuer” refers to a bank or a corporation that offers the use of its credit card. An “acquirer” refers to the institution that accepts and facilitates the processing of the credit card

transaction which is initially accepted by the merchant.

Under the Law, credit card issuers and acquirers must establish an appropriate system for managing risk exposures arising from credit card operations. Credit card issuers are also mandated to conduct know-your-client (KYC) procedures and exercise proper diligence in ascertaining that applicants possess good credit standing and are financially capable of fulfilling their credit commitments. Further, credit card issuers are mandated to determine, based on the credit standing and financial capacity of the cardholder, the credit limit to be extended to the cardholder.

BSP regulations for electronic money issuers

Given the rise of digital payments performed online and through the use of mobile applications, the Philippine government also issued regulations to regulate such transactions. In particular, the *BSP Manual of Regulations for Non-Bank Financial Institutions* (MORNBFI) provides for regulations on the issuance and operations of electronic money (“e-money”) issuers (EMI). E-money is defined therein as monetary value represented by a claim on its issuer, and that is:

- electronically stored in an instrument or device;
- issued against receipt of funds of an amount not lesser in value than the monetary value issued;
- accepted as a means of payment by persons or entities other than the issuer;
- withdrawable in cash or cash equivalent; and
- issued in accordance with the regulations in the MORNBFI.

EMIs are entities authorised by the BSP which provide money transfer or remittance services

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

using electronic stored money value systems and similar digital financial services. EMLs are required to be registered with the BSP before they can operate.

There are no foreign equity limitations for entities that engage in the business of an EMI. Nevertheless, EMLs are required to have a minimum paid-up capital of PHP100 million.

Currently, there is a two-year moratorium on the issuance of EMI licences, which commenced on 16 December 2021. The moratorium is expected to be lifted by 16 December 2023.

The Data Privacy Act

RA No 10173, otherwise known as the Data Privacy Act (DPA) was enacted by the Philippine government to protect the fundamental human right of privacy of communication, while ensuring free flow of information to promote innovation and growth. The DPA and its implementing rules and regulations (IRR) provide that the processing of personal data shall be allowed subject to adherence to principles of transparency, legitimate purpose and proportionality.

The DPA also has extraterritorial application and therefore applies to an act performed, or a practice engaged in, in and outside the Philippines by an entity if:

- the act, practice or processing relates to personal information about a Philippine citizen or resident;
- the entity has a link with the Philippines, and the entity is processing personal information in the Philippines, or even processing outside the Philippines as long as said information is about Philippine citizens or residents; or
- the entity has other links in the Philippines.

In ensuring security of personal information, the DPA mandates personal information controllers (PICs) to implement reasonable and appropriate organisational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

Legal Challenges in Relation to the Digital Economy

The rise in digital transactions also provides challenges to its key players, which include the entities providing the digital transactions and their users. Some of these challenges include the following.

Fraudulent transactions

A common trend is the rise of fraudulent transactions facilitated through various digital platforms, such as phishing. Phishing is the fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication. In order to prevent such practices, PICs must implement appropriate security measures to catch cases of phishing and be able to prevent their occurrence for the protection of data subjects.

Protecting confidentiality of client information

Another challenge is ensuring the confidentiality of client information, especially that being processed by financial institutions. The *BSP Manual of Regulations for Banks* (MORB) mandates financial institutions to implement measures such as the following:

- having a written privacy policy in place to safeguard customers' personal information;
- ensuring that privacy policies are regularly communicated throughout the organisation;

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

- having appropriate systems in place to protect the confidentiality and security of the personal data of customers against unauthorised access;
- having appropriate policies and practices in place for employee management and training to assess and address the risks to customers' personal information; and
- having a strong IT system in place to protect customers' personal information.

Compliance with the DPA

To ensure compliance with the mandates under the DPA, various offences relating to data privacy have been identified and specific penalties provided for under the DPA. In particular, unauthorised processing, accessing due to negligence, and improper disposal of personal information and sensitive personal information are among those acts considered as offences under the DPA. The penalties for said offences range from fines to even imprisonment.

In addition, the rise of digital transactions has also resulted in incidents involving a "personal data breach" or a "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". In cases where sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorised person, the DPA requires PICs to notify the National Privacy Commission (NPC) and the affected data subjects.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

The Philippine Government's Cloud First Policy

On 18 January 2017, the Philippine Department of Information and Communications Technology (DICT) promulgated through its Departmental Circular No 2017-002 the Philippine government's Cloud First Policy (the "Cloud First Policy"). Under Section 4.1 of the Cloud First Policy, "cloud computing" was defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Through the Cloud First Policy, the Philippine government aimed to eliminate the duplication of hardware and systems, and fragmentation of databases. The policy also aims to promote within the Philippine government the use of cloud computing technology in order to reduce costs, increase employee productivity and develop excellent online services for Philippine citizens.

The Cloud First Policy mandates government departments and agencies to consider cloud computing solutions as a primary part of their infrastructure planning and procurement. In the storage, use and processing of data, all government agencies and instrumentalities of the Republic of the Philippines are required to adopt cloud computing as the preferred ICT deployment strategy, method or technology for administrative use or for the delivery of government services.

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

Government agencies are recommended to select the appropriate cloud deployment model according to the agency's specific needs and the type of data it handles. Depending on the classification of the agency's data, there will be a requirement to apply certain controls.

The Cloud First Policy provides that security and compliance responsibilities in developing cloud systems are shared between the cloud service provider (CSP) and the government agency. The level of responsibility on both parties depends on the cloud deployment model type. The contracting agency is responsible for selecting and implementing security controls for any workloads that it operates in the cloud, while the CSP is responsible for ensuring that the services used by the contracting agency are highly secure and resilient so they are available to use on demand.

The Cloud First Policy also provides that the DICT will develop a list of accredited cloud service providers. The pre-accredited list of cloud vendors would have been pre-vetted to ensure their services meet or exceed the mandatory security controls for government cloud usage.

Policy on Cloud Computing for Financial Institutions

Under BSP Circular No 808, cloud computing is considered as a migration from owned resources to shared resources in which client users receive information technology (IT) services, on demand, from CSPs via the internet "cloud".

Given the increased probability of risk and exposure to potential issues related to business operations, such as ensuring confidentiality, the BSP would only allow the use of public cloud computing models for non-core operations and business processes that do not directly involve sensitive data. These would include emails, office

productivity, collaboration tools, claims and legal management. Conversely, core operations and business processes whose importance is fundamental in ensuring continuous and undisturbed operation of IT systems used to directly perform banking and financial services are not allowed to use public cloud computing services. These would include loans, trusts and treasury systems, automated teller machine (ATM) switch operations, electronic delivery systems and systems used to record banking operations.

Under BSP Circular No 808, a financial institution should consult the BSP before making any significant commitment on cloud computing. In addition, the financial institution should understand the applicability of local laws and regulations, and ensure that its contract with a CSP specifies obligations pertaining to the financial institution's responsibilities for compliance with relevant laws and regulations.

The use of outsourced cloud services to achieve the financial institution's strategic plan does not diminish the responsibility of the board of directors and of the management to ensure that the outsourced activity is conducted in a safe and sound manner, and in compliance with applicable laws and regulations. An outsourcing policy approved by the board of directors and a rationale for outsourcing to the cloud environment are required to be in place to ensure that the board is fully apprised of all the risks identified.

In addition, financial institutions are mandated to have a vendor management process in place that proactively monitors the performance of the CSP on an ongoing basis. This is also to guarantee availability and reliability of the services provided, and the ability to provide consistent quality of service to support normal and peak business requirements.

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

Lastly, to effectively monitor services including risk and risk mitigation associated with the use of a CSP, the financial institution and the CSP should agree in advance that the financial institution shall have access to the CSP to audit and verify the existence and effectiveness of internal and security controls. In addition, the parties may also agree on the right to an audit clause via an external party as a way to validate other control aspects that are not otherwise accessible or assessable by the financial institution's own audit staff.

Processing of Personal Data in the Context of Cloud Computing

Given that cloud computing is normally outsourced to CSPs, both the entities outsourcing personal data and the CSP should ensure that the processing of the personal data satisfies the criteria for lawful processing under the DPA. Thus, in cases where the processing of personal data is outsourced to a CSP, the entity which outsourced the processing of personal data still remains primarily accountable for the protection of personal data under its control.

Under the DPA, the entity which outsourced the data processing is required to use contractual or other reasonable means to ensure that proper safeguards are in place, to ensure the confidentiality, integrity and availability of the personal data, and prevent its use for unauthorised purposes. Further, under the IRR of the DPA, the contract for outsourcing processing of personal data, including that outsourced to CSPs, must inter alia include the following:

- that the processing of the personal data shall be made only upon the documented instructions of the entity which outsourced the data processing;

- ensuring that an obligation of confidentiality is imposed on persons authorised to process the personal data;
- not engaging another processor without prior instruction from the entity which outsourced the data processing;
- at the choice of the entity which outsourced the data processing, deleting or returning all personal data to the outsourcing entity after the end of the provision of services relating to the processing; and
- allowing for and contributing to audits, including inspections conducted by the outsourcing entity.

Both CSPs and the entity outsourcing the processing of the personal data are mandated to implement reasonable and appropriate organisational, physical and technical security measures for the protection of personal data. They should take steps to ensure that any natural person acting under their authority and who has access to personal data does not process it except upon their instructions, or as required by law.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Laws or Regulations Regulating Artificial Intelligence (AI) and Big Data

Currently, there is no law in the Philippines which specifically provides regulations for AI and big data. Nonetheless, there are laws which may be applicable in relation to the use of AI and big data in the Philippines, such as the following.

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

The Intellectual Property Code (the “IP Code”)

The Philippine IP Code (RA No 8293) classifies computer programs as original intellectual creations in the literary and artistic domain whose copyright belongs to the author of the work and that are protected from the moment of their creation. A “computer program” is defined as “a set of instructions expressed in words, codes, schemes or in any other form, which is capable, when incorporated in a medium that the computer can read, of causing the computer to perform or achieve a particular task or result”.

By having a copyright, the author shall have the exclusive right to carry out, authorise or prevent the following acts, among others:

- reproduction of the work or substantial portion of the work;
- the first public distribution of the original and each copy of the work by sale or other forms of transfer of ownership; and
- rental of the original or a copy of the computer program.

The IP Code also provides for usage of computer data, which may be considered as fair use, or a non-infringement of copyright. In particular, decompilation, which is the reproduction of the code and translation of the forms of the computer program to achieve the interoperability of an independently created computer program with other programs, is considered fair use.

The Data Privacy Act

The DPA takes into account that emerging technology such as AI may process personal data, including big data, through automated processes. Thus, under the DPA, a PIC carrying out any wholly or partly automated processing operations or set of such operations intended to serve

a single purpose or several related purposes is required to notify the National Privacy Commission (NPC) when the automated processing becomes the sole basis for making decisions about a data subject, and when the decision would significantly affect the data subject. In addition, the DPA provides rights to which data subjects are entitled in relation to the automated processing of their personal information, which include the following.

Right to be informed

The data subject has a right to be informed whether personal data pertaining to them shall be, is being, or has been processed, including the existence of automated decision-making and profiling. Prior to entry of personal data in the processing system, the data subject has the right to be notified and furnished with information regarding the methods utilised for automated access and the extent to which such access is authorised, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Right to object

The data subject shall have the right to object to the processing of their personal data, including processing for direct marketing, automated processing or profiling.

Right to access

The data subject has the right to reasonable access, upon demand, to information on automated processes where the data will or is likely to be made as the sole basis for any decision that significantly affects or will affect the data subject.

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There is currently no law in the Philippines which specifically provides regulations for the internet of things (IoT), which is commonly described as a system of interconnected devices that enables objects to collect and exchange data that would allow execution of specific commands. Nonetheless, certain provisions under the DPA may apply in relation to activities involving machine-to-machine communications.

In particular, the DPA provides guidelines for “data sharing”, which is defined as the “disclosure or transfer to a third party of personal data under the custody of a PIC or personal information processor (PIP)”. For the collection and exchange of data between and among machines, the PIC will be responsible for any personal data under its control or custody, including that where the processing has been outsourced or subcontracted to a PIP.

The DPA defines a “PIC” as a natural or juridical person or any other body who controls the processing of personal data, or instructs another to process personal data on its behalf. There is control if the natural or juridical person or any other body decides on what information is collected, or on the purpose or extent of its processing. “PIP” refers to any natural or juridical person or any other body to whom a PIC may outsource or instruct the processing of personal data pertaining to a data subject.

Under the DPA, data sharing shall be allowed when it is expressly authorised by law, and there must be adequate safeguards in place for data privacy and security.

The DPA allows data sharing in the private sector if the data subject consents to data sharing, and the following conditions are complied with.

- Consent for data sharing must be required even when the data is to be shared with an affiliate or mother company, or similar relationship.
- Data sharing for commercial purposes, including direct marketing, must be covered by a data sharing agreement (DSA).
- The data subject must be provided with the following information prior to collection or before data is shared:
 - (a) identity of the PICs or PIPs that will be given access to the personal data;
 - (b) purpose of the data sharing;
 - (c) categories of personal data concerned;
 - (d) intended recipients or categories of recipients of the personal data;
 - (e) existence of the rights of data subjects; and
 - (f) other information that would sufficiently notify the data subject of the nature and extent of data sharing and the manner of processing.

The DPA also mandates that sharing between government agencies for the purpose of a public function or provision of a public service must also be covered by a DSA.

DSAs are required to provide an overview of the operational details of the data sharing, including the procedure the parties intend to observe in its implementation. Where the recipient is allowed to disclose the shared data, or grant public access to it, this must be established clearly in the DSA. Where disclosure or public access is facilitated by an online platform, the program, middleware and encryption method used should also be identified. Any other infor-

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

mation that would sufficiently inform the data subject of the nature and extent of data sharing and the manner of processing involved should also be provided.

In addition, DSAs must include rules for the retention of shared data and identify the method to be adopted for the secure return, destruction or disposal of the shared data, and the timeline therefor. Adequate safeguards to protect personal data should likewise be put in place in every DSA. Where online access to personal data is granted, the parties should ensure that said access is secure through the use of any appropriate program, software or any other means.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

No one statute or series of statutes would apply to the mass media industry as a whole. Rights, obligations and requirements are contained in different statutes and regulations which regulate this industry, including content-based regulations and regulatory requirements for an entity to provide audio-media visual services in the Philippines.

Content-based regulations on traditional media are handled by several government agencies, such as the Movie and Television Review and Classification Board (MTRCB), the Optical Media Board, and the National Council for Children's Television. Currently, the MTRCB's authority is limited only to television and movies and does not include online mass media.

Regulatory requirements for the provision of audio-visual media services fall within the pow-

ers of the Philippine Congress and the National Telecommunications Commission (NTC).

Traditional Mass Media

In the Philippines, the ownership and management of mass media (eg, TV and radio) companies is limited to Philippine nationals or corporations, partnerships or associations wholly owned by Philippine nationals only. Mass media is defined as any medium of communication (ie, newspapers, radio, television, films, movies, wire and radio communication) designed to reach the masses and set their standards, ideals and aims. Mass media services include the gathering, transmission and distribution of news, information, messages, signals and all forms of written, oral and visual communication services.

Mass media companies are required to be corporations established in the Philippines and must secure a franchise from the Philippine Congress and the appropriate permits from the NTC, particularly a Certificate of Public Convenience and Necessity (CPCN).

A Congressional Franchise is the principal authority for a mass media company to construct, operate and maintain audio-visual media services in the Philippines. The term of the franchise is set for a period of 25 years and renewable upon application, unless sooner revoked or cancelled. The franchise grantee cannot lease, transfer, sell or assign the Congressional Franchise or the rights and privileges acquired thereunder to any corporation, or merge with any corporation, without the prior approval of the Philippine Congress. A Congressional Franchise is granted in the form of a Philippine statute, is approved through the same process as any other Philippine statute, and requires compliance with publication requirements.

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

Once enfranchised, the mass media company should obtain the necessary permits by filing a petition for the issuance of a CPCN with the NTC. During the application process, the mass media company is required to prove its legal, financial and technical capabilities, as well as the economic viability of the proposed operations. The applicant may secure a provisional authority (PA) to operate from the NTC while the CPCN application is pending evaluation/assessment. Once the mass media company is granted a PA, it may commence its operations, subject to the outcome of the CPCN application. A CPCN is coterminous with the franchise unless revoked or cancelled for violation of its terms and conditions.

Online Mass Media

Except for those offences punishable under the Cybercrime Prevention Act of 2012 (RA No 10175) and the Anti-Child Pornography Act (RA No 9775), there are generally no regulations governing internet usage or online media. The Philippine government would likely apply the same requirements to digital platforms, including nationality restrictions. The controversy on whether the use of digital platforms to broadcast news, information and videos is considered mass media in the Philippines remains unsettled.

However, the Securities and Exchange Commission (SEC) clarified that the use of the internet is not considered mass media per se. It is the use of the internet as a digital platform or medium to disseminate information and ideas to the public which would constitute a mass media undertaking. Currently, the distribution of television shows and movies is covered under the term “mass media” and will be subjected to nationality restrictions against foreign ownership. Depending on the type of services being provided, an authorisation may be required to be

secured with the relevant government agencies prior to operation.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

With the 2022 amendment of the Public Service Act (RA No 11659) (PSA), several changes were made to the scope and applicability of telecommunications regulations including the relaxation of foreign ownership restrictions on public telecommunications entities (PTEs). However, operating entities are still required to undergo the same regulatory requirements to operate as a PTE. Notwithstanding the long-awaited amendment to the archaic PSA, several regulations on the telecommunications industry are still relevant and applicable.

Relaxation of Foreign Ownership

Under the amendment, PTEs are no longer classified as public utilities subject to the constitutional requirements on Philippine nationality, but as a public service owning critical infrastructure. Foreigners may now own 100% of the outstanding capital stock of PTEs provided reciprocity conditions are met. Nevertheless, nationality restrictions are still imposed under certain conditions, such as when the reciprocity requirement is not met, if the investor is an entity controlled or acting on behalf of a foreign government or foreign state-owned enterprises, and if the investor is a sovereign wealth fund or independent pending funds of states. The amendment to the PSA, however, does not appear to have removed the requirement for PTEs to obtain a legislative franchise and other licences from the NTC, including the CPCN.

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

Another telecommunications law-related change under the PSA amendment is the carving out of a value-added service (VAS) provider and passive telecommunications tower infrastructure (PTTI) provider from the term “telecommunications”. This notwithstanding, existing rules and regulations governing VAS and PTTI are still applicable.

Passive Telecommunications Tower Infrastructure

The DICT issued Policy Guidelines on the Co-Location and Sharing of PTTI (DICT Circular No 008) (the “PTTI Policy”) to govern the co-location and sharing of PTTIs by independent tower companies (ITCs) and mobile network operators (MNOs). PTTI refers to all types of outdoor non-electronic telecommunications infrastructure or civil works that are utilised for the purposes of mounting antennas, transmitters/receivers, radio frequency modules and other radio communications systems (such as macro cell sites) for the rendition of ICT services in the telecommunications network.

Except for MNOs with a Congressional Franchise and CPCN, all entities intending to establish or operate one or more shared PTTI is required to register as an ITC and secure an ITC Certificate of Registration (COR) with the DICT. The ITC COR is valid for five years, and renewable for the same period upon proper application, unless sooner revoked or cancelled due to the ITC’s violation of relevant laws, departmental orders, circulars, rules and regulations, or other justifiable reasons.

Under the PTTI Policy, an ITC applicant is required to have the relevant construction experience, registration, licence and financial capacity of, or equivalent to, a contractor falling under Category A or higher of the Philippine Contractors Accreditation Board (PCAB).

Value-Added Service

Unlike PTEs, a VAS provider is not required to secure a Congressional Franchise or a CPCN. It is, however, required to secure a COR from the NTC. “VAS provider” is defined as an entity which, relying on the transmission, switching and local distribution facilities of the local exchange and inter-exchange operators, and of overseas carriers, offers enhanced services beyond those ordinarily provided for by such carriers. The following services are classified as VAS:

- messaging services – includes all types of messaging services such as short messaging service (not more than 160 characters), messaging service (more than 160 characters), multimedia messaging service (allowing the sending and receiving of multimedia messages such as video, graphics and audio clips), and unified messaging service (allowing voice messages to be stored in the mailbox along with email, and that can be accessed through an email client or via telephone with a telephone user interface);
- audioconferencing – allows conferencing between two or more participants at different sites by using networks to transmit audio;
- audioconferencing and videoconferencing – allows conferencing between two or more participants at different sites by using networks to transmit audio and video data;
- voice mail service – refers to an email system that supports audio where users can leave spoken messages for one another and listen to the messages by extending appropriate commands in the email system;
- electronic mail service – a store and forward method of composing, sending, storing and receiving messages over an electronic communications system;
- information service – includes all types of information delivered to/accessed by users/

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

- subscribers, such as road traffic information, financial information, visa application information and other information of a similar nature;
- electronic gaming services except gambling – allows a user to play games online;
 - applications service – includes all types of applications delivered to/accessed by the users/subscribers, such as mobile banking, electronic payments, point of sale service, etc;
 - content and program service – includes all types of content delivered to/accessed by users/subscribers, such as music, ringtones, logos, video clips and other content of a similar nature;
 - audiotext service – a system where consumers dial a phone number and navigate a voicemail-like system to get desired information;
 - facsimile service – allows a consumer to send and receive documents through the electronic communications network;
 - virtual private network service – a communications network tunnelled through another network and dedicated to a specific network (secure communication through the public internet is a common application); and
 - hosting service – allows a service provider to host in its facilities websites and private branch exchanges (PBX).

The COR is valid for a maximum period of five years, subject to renewal upon application. Applicants for a VAS licence may opt to apply for a shorter period than five years, but not for less than one year.

Technologies such as Voice over Internet Protocol (VoIP) services, while considered a VAS service, are covered by separate regulations and requirements. VoIP is a type of voice communication using the internet (ie, internet pro-

ocol technology), instead of the traditional circuit switch technology. Similar to other VAS providers, VoIP service providers and resellers are required to register as such with the NTC. The COR is valid for one year, and renewable thereafter.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Undertakings, rights and obligations, liabilities, representations and warranties, termination and indemnity provisions are the most common provisions the parties will find in any agreement, whether it is a share purchase, purchase/acquisition of goods or assets, or service agreement. In the Philippines, agreements are generally governed by the contractual stipulations of the parties. However, some of the considerations, risks and look-outs that IT service providers must take into account when entering into agreements with local organisations are as follows.

Government Contracts

Governmental procurement of goods and consulting services are governed by the Government Procurement Reform Act (RA No 9184). As a general rule, governmental procurement for goods must undergo competitive bidding. However, in highly exceptional cases, alternative modes of procurement can be resorted to, such as limited source bidding, direct contracting and negotiated procurement.

Technology Transfer Agreements

IT service agreements that contain provisions regarding the transfer of technology – ie, a technology transfer agreement (TTA) – must comply with the requirements under the IP Code, and its implementing rules and regulations. An IT ser-

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

vice agreement would be considered a TTA if the contract or agreement involves the transfer of systematic knowledge for the manufacture of a product, the application of a process, or the rendering of a service including management contracts, and if it involves the transfer, assignment or licensing of all forms of intellectual property rights, including licensing of computer software, of the agreement.

TTAs are required to contain the mandatory clauses and none of the prohibited clauses listed under the IP Code. Additionally, under the IP Code, TTAs are required to contain provisions regarding tax liability of the licensor, continued access to improvement, and governing law, which should be Philippine law. In addition, if the TTA has an arbitration clause, the TTA must include the arbitration rules applicable and the seat of arbitration. The IP Code prohibits provisions and clauses which will have an adverse effect on competition and trade, such as, but not limited to:

- price fixing;
- restriction on volume and structure of production;
- free grantback;
- payment for unused or expired patents;
- non-contestability of patents;
- export restrictions; and
- hold harmless provisions.

A TTA that fails to comply with the mandatory and prohibited provisions of the IP Code is unenforceable in Philippine courts unless an application for exemption (under exceptional or meritorious cases) was filed and approved by the Documentation, Information and Technology Transfer Bureau of the Intellectual Property Office of the Philippines.

Data Privacy and Security

Data privacy and data security are global concerns that any IT service provider may face when processing the data of local organisations, particularly the personal or sensitive personal data of the clientele of local organisations. The DPA (RA No 10173) is the primary law governing the protection and processing of personal data in the Philippines. The processing of personal information is allowed subject to compliance with the requirements of the DPA and other laws allowing disclosure of information to the public, and adherence to the principles of transparency, legitimate purpose and proportionality.

It is common for PICs to outsource the processing of personal and sensitive personal data of data subjects. While being outsourced to the PIP, PICs are responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed and to prevent its use for unauthorised purposes. In processing personal and sensitive personal information, the PIP and PIC must comply with data security requirements under the DPA, which include:

- implementing reasonable and appropriate organisational, physical and technical security measures for the protection of personal data; and
- implementing security measures aimed at maintaining the availability, integrity and confidentiality of personal data and that are intended for the protection of personal data against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

Likewise, in the case of a data breach, the PIC and/or the PIP is required to report the occurrence of a personal data breach within 72 hours

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

upon knowledge thereof, or when there is reasonable belief by the PIC or PIP that a personal data breach requiring notification has occurred.

The IRR of the DPA and the issuance by the NPC set out the security-related measures, security breaches and policies on cybersecurity that local organisations and IT service providers must comply with. Thus, in order to comply with the obligations under the DPA IRR and NPC issuances, local organisations may require that specific undertakings, warranties and indemnities to carry out security measures and to report security breaches are included in the service agreement with the IT service provider.

Sector-Specific Regulations

While private-sector IT service agreements are generally governed by the contractual stipulations of the parties, IT service providers may be required to comply with certain standards and requirements for regulated industries, such as banking and insurance.

For example, the BSP has issued specific guidelines for BSFIs, such as banks and non-bank financial institutions that outsource certain services or activities, to have access to certain areas of expertise or to address resource constraints (including IT functions or services) to third parties.

While IT outsourcing transfers operational responsibility to the service provider, BSFIs retain ultimate responsibility for the outsourced activity. As such, the IT service provider may be required to comply with the BSFI's policies and guidelines on outsourcing, risk management, business continuity and IT risk management (eg, IT audit, information security, IT operations, vendor management, disaster recovery plan, etc) by

way of contractual obligations in the service level agreement.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The COVID-19 pandemic accelerated digital transformation globally, including the acceptance of the use of electronic signatures ("e-signatures") and digital signatures. With the work-from-home restrictions being imposed by the Philippine government, businesses, clients and consumers were forced to learn and to use e-signatures instead of the traditional methods of physically signing documents in "wet ink". However, the use of e-signatures existed long before the pandemic began.

In the early 2000s, the Philippines approved the E-Commerce Act (RA No 8792) and issued its IRR. This centerpiece of legislation was designed to clear up doubts regarding the validity and enforceability of the use of e-signatures.

Under the E-Commerce Act, e-signatures/digital signatures on an electronic document shall be the functional equivalent to the signature of a person on a written document for as long as it can be shown that it was made through a prescribed procedure not alterable by the parties. While used interchangeably in the Philippines, e-signatures and digital signatures are not identical and do not mean the same thing. Philippine law provides a delineation on the terms "e-signature" and "digital signature".

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

Distinction Between E-signatures and Digital Signatures

An e-signature refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to the electronic document or electronic message, where the distinctive mark was executed or adopted by such person with the intention of authenticating, signing or approving the electronic document or electronic message.

A digital signature is a type of e-signature consisting of a transformation of an electronic document or electronic message using an asymmetric or public cryptosystem. Otherwise stated, a digital signature is a type of e-signature that encrypts a document with digital codes and relies on a public-key cryptography to support identity authentication and to provide data and transaction integrity.

Digital signatures are safer and ensure greater protection for both parties to a transaction/document. The application being used to affix the digital signature creates a digital-based certification which shows that the digital signature was affixed, the identity of the signatory, and whether there were any alterations made to the electronic document/message after the transformation was made. No such protection and verification mechanisms are included in the traditional “e-signature” as this may be affixed by merely copying and pasting such signatures into the electronic document.

Notably, in 2022 the DICT created and launched the Philippine National Public Key Infrastructure (PNPKI). PNPKI is software that creates a digital certificate that identifies people, organisations and machines electronically.

Authenticating E-signatures and Digital Signatures

While there is a distinction between the application of e-signatures and digital signatures, both types of signature are authenticated in the same way, through the following:

- by evidence that a method or process was utilised to establish a digital signature, and verifying this;
- by any other means provided by law; or
- by any other means satisfactory to the judge as establishing the genuineness of the electronic signature.

Once duly authenticated, the Philippine courts admit an electronic/digital signature affixed to an electronic document as the functional equivalent of a “wet ink” signature. Likewise, when an electronic or digital signature is authenticated, the following presumptions arise (unless contradicted and overcome by other pieces of evidence).

- For an e-signature:
 - (a) the e-signature is that of the person to whom it correlates;
 - (b) the e-signature was affixed by that person with the intention of authenticating or approving the electronic document to which it is related or to indicate such person’s consent to the transaction embodied therein; and
 - (c) the methods or processes utilised to affix or verify the e-signature operated without error or fault.
- For the digital signature:
 - (a) the digital signature is that of the person to whom it correlates;
 - (b) the digital signature was affixed by that person with the intention of authenticating or approving the electronic document to which it relates or to indicate such per-

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

son's consent to the transaction embodied therein;

- (c) the methods or processes utilised to affix or verify the digital signature operated without error or fault;
- (d) the information contained in a certificate is correct;
- (e) the digital signature was created during the operational period of a certificate;
- (f) no cause exists to render a certificate invalid or revocable;
- (g) the message associated with a digital signature has not been altered from the time it was signed; and
- (h) a certificate had been issued by the certification authority indicated therein.

While this is the case, some government agencies are starting to accept documents that are electronic/digitally signed. In 2021, the SEC started accepting the electronically signed audited financial statements of companies. Likewise, the Bureau of Internal Revenue has also begun accepting the e-signatures of taxpayers in certain types of submitted forms and certificates.

A notarised document is an example of a document that requires certain formalities. Notarised documents cannot be in electronic form; consequently, e-signatures/digital signatures cannot be affixed. Notarised documents must be signed in wet ink and presented before a notary public in the Philippines.

Using E-signatures/Digital Signatures in the Philippines

Except for documents that require certain formalities, there is no requirement or restriction on using e-signatures/digital signatures. Documents such as letters, memoranda and agreements can be signed using e-signatures/digital signatures. While there is no legal impediment to doing so, not all government offices in the Philippines accept documents signed electronically. Government offices would normally still require that the documents submitted to their offices be in "wet ink".

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco

Villaraza & Angangco is a full-service law firm that has been at the forefront of the Philippine legal landscape since 1980. It offers professional services of the highest calibre, and has lawyers adept at handling the most intricate problems and providing comprehensive solutions to the full spectrum of clients' interests. Villaraza & Angangco's corporate and commercial law department is composed of six partners and 20 highly qualified lawyers. The firm's technology, media and telecommunications (TMT) practice

includes advising major Philippine telecommunications companies on transactions involving acquisitions, compliance, and project financing. The firm also advises clients in the financial technology industry, including entities engaged in online lending, electronic money issuance, cryptocurrency trading and credit card acquirers. With the complexity of the TMT transactions it handles, Villaraza & Angangco has gained recognition from multiple legal publications as the Philippines' leading law firm for TMT.

Authors



Sylvette Y Tankiang is the managing partner of Villaraza & Angangco and also the head of the firm's taxation department. She has special expertise in the fields of TMT, taxation, M&A,

banking and finance, real estate, natural resources, and power and energy. She advises clients from multiple industries, including telecommunications, energy, banking and e-commerce. She has consistently been ranked by various legal publications, including Chambers and Partners (Global and Asia-Pacific). She was the former President of the Harvard Law School Association of the Philippines, the Harvard Club of the Philippines, and the University of the Philippines Women Lawyers' Circle.



Franchette M Acosta is the co-managing partner of Villaraza & Angangco and is also currently serving as the head of the firm's corporate and commercial law department.

She is recognised as a leading lawyer by various legal publications, including Chambers and Partners (Global and Asia-Pacific). Franchette's proficiency in commercial law enables her to guide clients in foreign direct investments market entry or expansion, finance and project development, competition and data protection laws, and government contracts. She has represented clients across various industries such as telecommunications, financial services, real estate, power/energy, mining and manufacturing.

PHILIPPINES LAW AND PRACTICE

Contributed by: Sylvette Y Tankiang, Franchette M Acosta, Richard Henrick I Beltran and Raymond John S Cheng, Villaraza & Angangco



Richard Henrick I Beltran is a partner in the corporate and commercial law department of Villaraza & Angangco. His practice areas include corporate law, mergers and acquisitions,

TMT, foreign investments, banking and financial services, natural resources and data privacy. Richard has extensive experience in conducting due diligence, negotiating contracts, and preparing relevant documents for mergers and acquisitions of companies across multiple industries. He also provides legal advice to clients in the telecommunications and financial technology industries on matters relating to their regulatory compliance, including licensing applications. He also handles project financing transactions for clients from multiple industries.



Raymond John S Cheng is a senior associate of Villaraza & Angangco with expertise in M&A, banking and finance, capital markets, financial technology, foreign investments,

project financing and securities. Raymond regularly advises both domestic and international clients on regulatory matters in various industries including e-commerce, financial services, logistics, mass media and telecommunications.

Villaraza & Angangco

11th Avenue Corner
39th Street, Bonifacio Triangle
Bonifacio Global City 1634
Metro Manila
PO Box 3559 Makati Central
Philippines

Tel: +632 8988 6088
Fax: +632 8988 6000
Email: info@thefirmva.com
Web: www.thefirmva.com



**VILLARAZA
& ANGANGCO**
THE FIRM • EST. 1980

Trends and Developments

Contributed by:

Agata Szeliga, Sylwia Macura-Targosz
and Aleksandra Krześniak-Sałatczyk

Sołtyński Kawecki & Szlęzak see p.414



Expectations for Polish TMT in 2023

It can be stated with confidence that 2023 will be a year in which a lot will happen in the areas of telecommunications, media, and technology. For Poland, 2023 will be the year in which it will have to fully absorb that the biggest war in Europe since 1945 is taking place in a neighbouring state – Ukraine – and that it has again become a country on the front line with an increased risk of cyber-attacks to its infrastructure and businesses. It will also be necessary to cope with the increasing costs of energy and the potential interruption of supply. Energy-intensive technologies (including large cloud centres) will have to think about the solutions to limit their electricity consumption and ensure a continuous provision of services. Combined with growing awareness about climate change and initiatives to reduce CO₂ emissions at the EU level, this may trigger substantial innovation and developments in energy generation and consumption in these sectors.

On top of that, 2023 will be a very active year for legislators and regulators. On the EU level, a number of new legal acts have already been adopted (eg, the Data Market and Data Services Acts) or are expected (eg, the Data Act, the EU Health Data Space and the AI Act). In addition, Polish legislators will be busy in 2023 as, finally, the new Electronic Communication Law has reached the Polish Parliament and is expected to enter into force in the third quarter of 2023.

Often criticised for their insufficient protection of consumers and smaller market players, Polish regulators have started to take a more active stance. The Polish data protection authority has just announced that, in 2023, it will carry out inspections of entities running mobile and web applications. This article goes into greater detail on the approach of Polish regulators concerning influencers and the enforcement of EU legislation.

The Growing Importance of Cybersecurity

The growing cybersecurity threat has triggered legislative activity, including the EU NIS 2 Directive, which came into force on 16 January 2023. For Poland, this means that the National Cybersecurity System Act (the “Polish Cyber Act”) will have to be amended by 17 October 2024 at the latest.

NIS 2 Directive

The NIS 2 Directive is designed to make cybersecurity and response capabilities to various types of incidents in both the public and private sectors even stronger. The most significant change comes down to the expansion of the scope of obliged entities and their division into “essential entities” and “important entities”. In addition to those in the energy, transportation, banking, financial and health sectors, the essential entities will include:

- cloud computing service providers;
- data centres service providers; and
- content delivery network providers.

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

Among the categories of “important entities”, a new group has emerged: providers of social networking services and courier service providers. The obliged entities will be required to prepare and implement appropriate procedures for cybersecurity and the reporting of breaches, incidents, and cyberthreats. Under NIS 2, the Cyber Crisis Liaison Organisation Network (EU-CyCLONE) will also be established to support the co-ordinated management of large-scale cyber-attacks and crises.

The Polish approach to cyber-security

In Poland, the National Cybersecurity System aims to ensure cybersecurity at the national level, in particular, the uninterrupted provision of essential services and digital services, and the achievement of a sufficiently high level of security of the ICT systems used to provide these services. Poland has been working on an amendment to the Polish Cyber Act since September 2020. Subsequent versions of the bill have raised numerous controversies over the new obligations of participants in the national cybersecurity system; this raises significant costs for entrepreneurs. To avoid double standards, as a result of any differences between the Polish Cyber Act and NIS 2, legislators should focus on implementing the NIS 2 Directive and not on the previously proposed amendments.

Cyber-resistance of the internet of things

Complementary to the NIS 2 Directive and wider activities ensuring the security of critical supply chains is the Cyber Resilience Act (CRA), which covers the security of internet-connected devices – especially the internet of things (IoT). The CRA is intended to establish common standards for software and digital equipment manufacturers, in particular, by ensuring that:

- for the expected lifetime of the product or for five years after launch, cyber vulnerabilities are effectively addressed;
- there will be the obligation to notify the EU Agency for Cybersecurity of identified vulnerabilities in a product or service within 24 hours; and
- manufacturers of electronic equipment take into account cybersecurity principles from the design stage of their goods and services.

In Poland, the CRA bill has gone through the public consultation stage.

Cybersecurity as a service – an increasingly attractive solution

Cybersecurity as a Service (CSaaS) is an outsourced model of cybersecurity management. Due to the growing number of cyber-attacks, the awareness of Polish companies in this area is increasing. Due to a lack of in-house dedicated cybersecurity specialists, companies are turning more and more to outsourced cybersecurity services. This is, in turn, driving the emergence of companies providing cybersecurity services on the Polish market.

Increased Focus on the Consumer in E-commerce and Media Activities

On 1 January 2023, three EU directives – the [DCD Directive](#), the [SGD Directive](#), and the [Omni-bus Directive](#) – were implemented into the Polish legal system. These rules impose new obligations on entrepreneurs entering into contracts with consumers and aim to increase digital consumer protection, primarily in the face of unscrupulous marketing practices of entrepreneurs.

After Poland's significant delay in implementing these directives, Polish consumers will finally get the protection consumers in other EU member states already enjoy. This marks a major change

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Sołtysiński Kawecki & Szlęzak

for Polish e-commerce firms, which should reorganise their online operations.

Is this the end of Black Monday, Black Friday, and Black Weeks?

The new regulations are aimed at increasing consumer protection while shopping, and eliminating entrepreneurs' illegal practices. The most important is the requirement of transparent information on discounts (an entrepreneur announcing a promotion or sale will have to provide, in addition to the current price, the lowest price offered in the 30 days preceding the reduction), clear rules for placing offers in online search results, and a prohibition on suggesting that published consumer opinions are genuine if the entrepreneur has failed to introduce mechanisms to ensure their trustworthiness. The regulations impose new information obligations on entrepreneurs operating online (eg, stating if published opinions are verified and in what manner), and on shopping platforms (eg, indicating whether a given offer originates with a business or a natural person). In the coming year, it will become clear how these new regulations have affected the market and the promotions offered by entrepreneurs.

The consumer can do more

As of 2023, a consumer will be able to take advantage of the warranty concerning the "non-conformity of goods with the contract", rather than the "occurrence of a physical or legal defect in the goods", as before. What is more, concerning the non-conformity of goods with the contract, the consumer will have to demand the repair or replacement of the defective goods first, and only later a price reduction or withdrawal from the contract (the hierarchy of claims). The entrepreneur will also have a shorter time to process a consumer's complaint (the time has been reduced from 30 days to 14 days),

and the consumer will have a longer time to file a complaint (the time has been extended from one to two years from the delivery of the product). The period of the seller's liability remains unchanged and is still two years from the date of the delivery of the goods.

Digital revolution

Many changes also await the Polish market in the digital world, including a complete novelty in the regulations – ie, the appearance of a category of goods with digital elements ("smart" goods). Goods with digital elements, digital content, and digital services can be complained about in the same manner as any other goods or services. The entrepreneur will be responsible for the compliance of such digital goods (eg, games and computer programs) with their trial versions or announcements. They will also be obliged to provide consumers with updates for at least two years. Consumers will be protected not only if they pay for digital content or services with money (eg, access to applications) but also with their personal data (eg, the right to withdraw from the contract within 14 days).

Social commerce - influencers under the regulator's magnifying glass

Many consumers make purchasing decisions while browsing social media or buy a product directly through Facebook, Instagram, or TikTok. The reason for this is that many influencers promote services or products on behalf of advertisers on their social media accounts, doing so in a way that gives the impression that they are providing their own honest opinion, not that the influencer is influenced by their advertising contract. Thus, without being aware that the influencer's statement is an advertisement, consumers willingly opt for the goods or services they recommend.

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Sołtysiński Kawecki & Szlęzak

Currently, there are no regulations that directly govern how to tag advertising material on social media. Nevertheless, the law clearly states that advertising content must not mislead consumers. To protect consumers, the Polish President of the Office of Competition and Consumer Protection (OCCP) announced the “Recommendations pertaining to the tagging of advertising content by influencers on social media.” Despite their lack of legal force, these Recommendations are another step in the fight against unfair market practices in social media, and will certainly contribute to increased legal awareness among influencers, to the benefit of consumers.

According to the Recommendations, an influencer should tag advertising materials published on their social media channels in a way that is clear, unambiguous, and understandable for every recipient. Among other things, such tags must be placed in a prominent place (and not, for example, only after the user expands the description of the post), written in a clear font that is not too small, and not merge with the colour of the background. Two-level tagging is recommended; namely, using both the platform’s functionality and single tagging (eg, in the description, in a photo or video, or in the narration of the material). The OCCP also recommends using specific words to designate advertising material. The method of concluding a contract between an influencer and advertising agency or an advertiser and a form of compensation (eg, cash, products or services, discounts on the purchase of products or services) is not relevant when it comes to recognising the content as commercial. Self-promotion also must be tagged as an advertisement.

The OCCP’s actions as regards an influencer’s marketing on social media have initiated positive changes in the proper labelling of commercial

content. The next step is to verify the labelling of content published on websites. However, this appears to be only the beginning of the OCCP’s activities in this area as it has announced that all possible steps will be taken to ensure that internet users are protected from hidden advertising and have the opportunity to make a conscious choice about whether they want to read commercial content.

The New Electronic Communications Law is finally coming

A major change, not only for telecommunications industry entities, will be the entry into force of the new Electronic Communications Law (ECL) and the Law Introducing the Electronic Communications Law. Without a doubt, this will be one of the most important legislative events in the TMT area in Poland in 2023. The ECL is an implementation of the European Electronic Communications Code (Directive (EU) 2018/1972 of 11 December 2018) and is to fully replace the existing act of 16 January 2004 (the “Telecommunications Law”). The scope of the ECL is much broader than that of the Telecommunications Law as it will comprehensively regulate the market for electronic communications services. The new regulations apply not only to the traditional telecommunications services sector, but also to interpersonal communication services not using numbers. This mainly involves instant messaging services (eg, Messenger or WhatsApp) as well as email. The planned changes will also cover the rules for the provision of electronic services (sending unsolicited marketing information), direct marketing (cookies), or processing the personal data of electronic communications services users. As of now (the second half of January 2023), the draft ECL is being debated by Parliament. It is expected it will enter into force in the third quarter of 2023 (six months after its official pub-

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

lication). The ECL and the implementing act will amend more than 50 Polish legal acts.

New powers for law enforcement agencies

One of the most widely discussed proposals consists of obliging instant messaging providers (eg, Messenger or WhatsApp) to store their users' data to the same extent that telecommunications entrepreneurs are currently required to store such data (eg, the place and time of login). Under the new regulations, instant messaging providers will be required to store data "clearly identifying a user of the network" for 12 months. In practice, this may be all the data that the provider of a particular service has collected on a user. Also, the providers would have to make available traffic data (including real-time location data of users) and, most likely, the content of the communication, upon request of law enforcement authorities without any involvement of the providers' personnel. If the provider does not comply with this obligation, it may be banned from the Polish internet. There is a common opinion that such broad rights being given to law enforcement agencies is incompatible with EU law (including the EU Charter of Fundamental Rights).

Direct marketing - will the previous consents be valid?

Consent to online or phone marketing collected by data controllers under the existing regulations will remain in force if the original method of expressing consent meets the conditions stated in the ECL. The companies will have to verify the consents on which they rely and decide whether it will be necessary to collect them once more.

Guidelines for direct billing

Direct billing – ie, fees for services which are added to telecommunications bills (eg, for subscriptions to VOD platforms) – will be regulated.

This applies to both one-time charges (eg, renting a movie from a VOD library) and recurring charges (subscription). The service is to be available to users with their prior consent "on a durable medium." This is supposed to further protect consumers from "unknowingly" launching a particular service. It also proposes introducing a limit (PLN35 per month), above which additional services can no longer be added to the bill.

Must carry/ must offer

A lot of controversy surrounds the bill introducing the ECL, in particular, changes to the "must carry must offer" (MCMO) obligation, which is currently regulated under the Broadcasting Law. The MCMO obligation is the requirement put on certain broadcasters to make their channels available (must offer) to operators that distribute TV channels. The operators, in turn, have an obligation (must carry) to distribute these channels or pay a fine.

The proposed amendments are to change the scope of the channels covered by the MCMO, excluding privately owned channels and limiting them only to the channels of the public broadcaster, owned by the Polish State. In addition, the Chairman of the National Broadcasting Council is to be given very broad powers to determine the list of additional channels covered by the MCMO. These changes are the subject of heated discussion, including on the grounds of incompatibility with EU law and the Polish Constitution.

New Liability Rules for Online Content-Sharing Service Providers

Another important legislative development in 2023 will be the implementation of the Copyright Directive (Directive (EU) 2017/790 of 17 April 2019) on copyright and related rights in the Digital Single Market. In Poland, this amend-

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

ment has been widely commented on, among other things, due to the content of Article 17 – ie, the use of protected content by online content-sharing service providers. The mentioned article was challenged before the CJEU by Poland and several other member states. The new legislation was referred to in the media as “ACTA 2”.

The implementation of the Copyright Directive will take place in Poland by amendment to the Act of 4 February 1994 on Copyright and Related Rights. The bill also introduces new rules for the liability of online content-sharing service providers – ie, administrators of web pages on which users can publish content (eg, photos, videos or text). Under the new rules, platform providers will be liable for copyright infringement regarding the content distributed by their users unless they meet conditions exempting them from such liability.

How will the new liability rules work?

The new regulations indicate that, as a general rule, a provider may distribute content uploaded by its users if the right-holder allows it. If such consent has not been obtained, indemnification from liability for the unlawful dissemination of content is possible, but more difficult, as a provider of online content services will be required to demonstrate that:

- it exercised due diligence to obtain the consent of the right-holder;
- it exercised due diligence in accordance with high standards of professional diligence in the sector to prevent access to a given work if the right-holder has delivered information appropriate and necessary to achieve that purpose; and
- it acted promptly after receiving a duly justified request from the right-holder to block access to that work or remove it from its web-

sites, and exercised due diligence to prevent future access to that work.

Merely responding to reported infringements will no longer be sufficient. Providers of online content services will be required to take a number of proactive measures to avoid liability.

Excluded providers

The bill also identifies categories of providers that will not be subject to the new liability rules. These include cloud services, online sales platforms, search engines, online encyclopaedias, scientific or educational repositories, or open-source software development platforms. However, this catalogue is closed so all other entities meeting the threshold will be covered by the new rules.

Further Development of 5G Networks

Further development of the 5G network in Poland is likely to continue in 2023. The 5G network is designed specifically for smart cities and the internet of things. Admittedly, the largest mobile network operators in Poland have already launched 5G networks and are offering an increasing number of devices (smartphones, modems, etc) to connect to modern base stations. Nevertheless, an auction of bandwidth dedicated only to 5G networks has not yet taken place.

According to the activity plan for the Office of Electronic Communications (Poland’s regulatory authority), one of the Office’s goals in 2023 is to make frequencies in the 3.6 GHz band available for the deployment of 5G technology. In practice, this means holding the aforementioned auction, including conducting a selection procedure for operators and issuing reservation decisions. The Office also plans to take steps to increase the percentage (up to 77%) of households within

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Softysiński Kawecki & Szlęzak

reach of internet access with a backhaul capacity of at least 100 Mbps.

New Wave of State Subsidies?

Investment in the telecommunications and technology space, especially taking into account the deployment of the 5G network, will be substantial. In the past, a lot of jurisprudence in state aid matters was related to financing the public remit or the development of broadband networks.

One of the biggest burdens in the last year was related to the release of the 700 MHz band by the terrestrial television services to make it available to develop the internet of things. One of the first decisions in which the European Commission approved aid was to replace the frequency-dependent equipment for broadcasting in the context of migration from the 700 MHz band that was issued for Spain (case SA.51080) and Czechia (case SA.55742). It is expected that similar aid may also be granted to some Polish broadcasters in 2023. However, the Commission also opened the formal procedure to investigate

the aid granted by Czechia for terrestrial television parallel broadcasting in a new standard – ie, DVB-T2/HEVC. The Commission argues that the support granted to the terrestrial television services went beyond the scope needed to release the 700 MHz band, but allowed them to upgrade their network to make it capable of providing additional services and of better quality, while operators providing television transmission services on alternative platforms allegedly have invested in the transition to DVB-S2/MPEG4 (capital and operating costs) with private resources. As a result, there is a risk that the operators of terrestrial television services received a preference (case SA. 64153). Thus, it cannot be ruled out that, if aid is awarded to Polish operators of terrestrial television releasing 700 MHz, similar complaints will also appear.

Moreover, additional complaints may be triggered if the MCMO obligation is adopted in the way currently envisaged in the ECL as it may constitute an undue advantage for the Polish State broadcaster.

POLAND TRENDS AND DEVELOPMENTS

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Softysiński Kawecki & Szlęzak

Softysiński Kawecki & Szlęzak (SK&S) is one of Poland's leading full-service law firms. With more than 180 attorneys, the firm provides the highest standard of legal services in all areas of business activity, and is reputed for the quality of its work and innovative approach to complex legal problems. Since the 1990s, SK&S has been closely associated with the ever-changing new technology sector, especially the dynamic IT industry. SK&S provides high-quality legal

services to both individuals and companies, covering the full scope of TMT issues. The firm's TMT practice works alongside fintech, IP/IT, privacy, and tax teams to provide an innovative interdisciplinary service. SK&S helps businesses use state-of-the-art technologies in a safe and cost and time-effective manner. It was a founding member of the New Technologies Association.

Authors



Agata Szeliga has been a partner at SK&S since 2009. She specialises in new technologies and personal data protection, as well as in state aid laws. She advises on cloud computing,

especially in its deployment in the financial sector. As a data protection lawyer, she advises on implementation of new data protection processes within organisations, handling sensitive personal data protection requests, as well as breaches and complaints. She is a member of the Expert Group at the European Commission on B2B Data Sharing and Cloud Computing.



Sylwia Macura-Targosz is a senior associate who joined SK&S in 2008. She specialises in intellectual property law, IT, new technologies as well as e-commerce law. She is

experienced in the field of IT systems implementation projects and licensing issues. Her fields of expertise also include personal data protection and privacy matters. She has advised in a number of IT and employment projects in which the personal data were of importance. She also acts as a Data Protection Officer for certain SK&S clients and supports entrepreneurs in proceedings conducted by the President of the Personal Data Protection Office. She is a member of the Polish New Technologies Law Association.

POLAND TRENDS AND DEVELOPMENTS

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk,
Sołtysiński Kawecki & Szlęzak



Aleksandra Krześniak-Sałajczyk is an associate at SK&S and an advocate trainee at the Warsaw Bar Association. She has been working with SK&S since 2021. She

specialises in intellectual property cases (copyright, industrial property, combating unfair competition and IT systems implementation contracts), as well as regulatory issues in telecommunications and broadcasting law. Aleksandra supports entrepreneurs in proceedings conducted by Polish regulatory authorities (eg, the President of the Office of Electronic Communications and the National Broadcasting Council).

Sołtysiński Kawecki & Szlęzak

Jasna 26
00-054
Warszaw
Poland

Tel: +48 22 608 70 00
Fax: +48 22 608 70 01
Email: office@skslegal.pl
Web: www.skslegal.pl



Law and Practice

Contributed by:

Alina Popescu, Daniel Alexie,
Flavia Stefura and Cristina Crețu
MPR Partners see p.429



Contents

1. Metaverse	p.417
1.1 Laws and Regulations	p.417
2. Digital Economy	p.417
2.1 Key Challenges	p.417
3. Cloud and Edge Computing	p.418
3.1 Highly Regulated Industries and Data Protection	p.418
4. Artificial Intelligence and Big Data	p.420
4.1 Liability, Data Protection, IP and Fundamental Rights	p.420
5. Internet of Things	p.421
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection	p.421
6. Audio-Visual Media Services	p.425
6.1 Requirements and Authorisation Procedures	p.425
7. Telecommunications	p.426
7.1 Scope of Regulation and Pre-marketing Requirements	p.426
8. Challenges with Technology Agreements	p.427
8.1 Legal Framework Challenges	p.427
9. Trust Services and Digital Entities	p.428
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes	p.428

1. Metaverse

1.1 Laws and Regulations

Romania does not currently have specific regulation on the metaverse. However, legislation specific to intangible assets (such as intellectual property, e-commerce, data protection, cybersecurity, cloud, etc) would apply to the development, marketing and operation of software pertaining to the metaverse, whereas hardware (networks, devices) used for the metaverse would be governed by relevant legislation (eg, legislation on the authorisation of producers of 5G equipment).

When using NFTs in the context of metaverse, it should be borne in mind that the Romanian fiscal authorities have issued guidance on taxing NFTs. Individuals who obtain income from the sale, on specialised blockchain platforms, of content in the form of digital files (NFTs) or royalties from such sales have the obligation to declare these forms of income, regardless of whether they are made in Romania or abroad; these individuals must also pay revenue tax on these income streams.

Moreover, as Romania is in the process of adopting legislation for digitalisation of public services, the metaverse is not at present on the agenda of Romanian legislators. Difficulties may arise due to the lack of dedicated legislation, at least until EU legislation is adopted in the field.

2. Digital Economy

2.1 Key Challenges

Romanian Law no 365/2002 on e-commerce transposes into national legislation Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of infor-

mation society services, in particular electronic commerce, in the Internal Market (the “e-Commerce Directive”) and thus applies to e-commerce as part of the digital economy.

The provisions of this law are in line with the e-Commerce Directive and thus very much focus on consumer protection, regulating, for example:

- the provision of information society services (which is not subject to any local authorisation procedures);
- commercial communications, which cannot be made without prior consent (similar to the provisions of the legislation transposing the ePrivacy Directive – it remains to be seen whether the new ePrivacy Regulation will bring about changes concerning commercial communications and if consent will remain the only legal basis applicable in such cases);
- information that an e-commerce supplier must provide to the client prior to contracting (eg, technical steps to follow to conclude the contract, technical means for identifying and correcting input errors prior to the placing of the order, languages offered for the conclusion of the contract); and
- the means by which e-commerce contracts may be concluded.

Government Emergency Ordinance no 134/2014 regarding the rights of consumers in contracts concluded with professionals transposes into national legislation Directive 2011/83/EU of the European Parliament and of the Council on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. The ordinance thus regulates consumer rights resulting from distance contracts, mainly

the right to withdraw from the contract within 14 days.

Government Emergency Ordinance no 141/2021 on certain aspects regarding contracts for the supply of digital content and digital services (the “Digital Content and Digital Services Ordinance”) transposing Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services entered into force on 9 January 2022.

The stated purpose of the Digital Content and Digital Services Ordinance is to contribute to the harmonisation at the EU level of the specific, essential, and binding contractual rights of consumers in the EU, along with boosting the digital economy.

In line with the EU legislation, the Digital Content and Digital Services Ordinance:

- applies to any contracts whereby digital content or digital services are provided;
- establishes subjective and objective conformity requirements for digital content and services, such as being in line with the expectations usually associated with the specific type of content/services and to be provided along with updates and all required accessories meant to ensure functionality; and
- regulates consumers’ rights specific to digital services and content, such as the suppliers’ obligation to correct the content/services for lack of functionality or breach of intellectual property rights.

Last but not least, as certain provisions of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amend-

ing Directive 2000/31/EC (the “Digital Services Act”) and Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (the “Digital Markets Act”) have entered into force (in October and November 2022), it can be argued that Romania is fairly well equipped for the digital economy from a legal perspective.

Therefore, challenges will more likely result from a practical and economical perspective rather than from a legal one, as Romania ranks last among all EU member states in the 2022 Digital Economy and Society Index. Nevertheless, according to public sources, Romania’s digital economy is expected to grow significantly in the next number of years, with certain reports claiming that by 2030 Romania’s digital economy sector could represent approximately 10% of its GDP.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

In 2022, cloud computing became a major focus point for Romanian regulators. The National Recovery and Resilience Plan for Romania after the COVID-19 pandemic, for which the EU allocates funds, includes a major overhaul of public sector services by the creation of a government cloud.

In June 2022, the Romanian government adopted Emergency Ordinance no 89/2022 regarding the establishment, administration and development of cloud IT infrastructures and services used by public authorities and institutions, which represents the general framework for creating

the government cloud platform. Secondary legislation has just been enacted in February 2023. However, final touches need to be added through tertiary legislation, which is pending.

In regulated industries such as banking and insurance, using the cloud has specific rules. Cloud services are currently defined in Romanian insurance legislation as services provided via cloud computing technologies to allow universal, convenient, on-demand network access to a common set of configurable computing resources, which can be quickly made available and launched with minimal effort of management from, or interaction with, the service provider. The legislation also defines the following types of cloud:

- public cloud – IT infrastructure available for free use by the general public;
- private cloud – IT infrastructure available for use exclusively by one company; and
- hybrid cloud – IT infrastructure consisting of two or more distinct cloud infrastructures.

The legislation referred to above also imposes certain obligations that will be discussed below.

In addition, a guide on the externalisation of cloud services was released by the Financial Supervisory Authority in August 2021 for the attention of fund administrators and other entities that work with investment funds.

The guide applies from 31 July 2021 to all cloud outsourcing commitments concluded, renewed, or modified on or after this date. The relevant entities had to review and amend existing cloud outsourcing commitments to ensure that they comply with this guide by 31 December 2022. In a nutshell, relevant companies must allocate clearly delineated responsibilities for managing

outsourcing contracts. Furthermore, they must monitor the outsourcing contracts on a risk-approach basis.

In the insurance sector, specific norms implement the guidelines on outsourcing to cloud service providers of the European Insurance and Occupational Pensions Authority. Companies are subject to an obligation to evaluate their cloud outsourcing partners in terms of risks posed by the cloud outsourcing activity. Insurance companies are also obliged to document their outsourcing relations in a separate registry, where the information must be kept for two years after the contractual relationship with the outsourcing partner has ended.

These norms on cloud outsourcing also provide minimum contractual provisions that must be included in the cloud outsourcing agreements. Insurance companies are obliged to ensure that cloud service providers comply with legal requirements and appropriate security standards. All critical and significant outsourced cloud operations must be notified in writing to the Financial Supervisory Authority.

Processing personal data in a cloud falls under the principles stated in the General Data Protection Regulation (GDPR). Considering the Guidelines 07/2020 on the concepts of controller and processor in the GDPR issued by the European Data Protection Board (EDPB), the cloud providers mainly act as processors (ie, processing personal data under the instructions and on behalf of the controller), even where they offer standardised cloud services. In all cases where cloud providers act as processors, the parties must conclude a data processing agreement setting forth the conditions of the processing.

Following the invalidation of the EU-US Privacy Shield through the decision of the Court of Justice of the European Union in *Schrems II*, special attention should be paid to the transfers of personal data to third countries.

Whilst the first step is to ensure that the personal data is stored and processed entirely within the European Economic Area, due to the potential extraterritorial effect of surveillance laws governing third countries, the standard transfer tools provided by the GDPR might not be sufficient.

In this respect, the EDPB issued recommendations on supplementary measures to be used to ensure that the transferred data benefits from the same level of protection as that ensured in the EU.

However, following the recent draft adequacy decision for the EU-US Data Privacy Framework, published by the European Commission on 13 December 2022, it is to be expected that the hurdle related to the transfers in the US will come to an end, at least until a new *Schrems III* (potentially) invalidates the new framework.

It is expected that, in the next six months, a new adequacy decision for the EU-US Data Privacy Framework will be adopted by the European Commission and put an end to the current problems generated by the potential transfers in the US.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

The discussions on the draft AI Regulation have advanced, with the Czech Presidency present-

ing in November 2022 the final version of the compromise text on AI Regulation adopted by the Council on 6 December 2022.

The compromise text voted for by the Council of Europe:

- provided for a narrower definition of an AI system;
- extended the prohibited AI practices;
- regulated the general purpose of AI systems;
- made explicit references to the exclusion of national security, defence and military purposes from the scope of the regulation;
- clarified that the regulation does not apply (except for the transparency obligations) to AI systems and their outputs used for the sole purpose of research and development or when used for non-professional purposes; and
- increased transparency.

As the next steps, the European Parliament will need to express its views on the text, aiming to vote on it in the first quarter of 2023. Following the vote, it is expected that the AI Regulation will enter into the trilogue process in April 2023.

Given the substantial reach of the data protection rules when dealing with AI, in June 2021 the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) also expressed their concerns with regard to the content of the draft AI Regulation.

In this respect, the two European authorities underlined the need for the AI Proposal to expressly state that the data protection legislation in force applies to all processing of personal data which falls under the scope of the AI Proposal.

At the same time, given the high risks posed by the identification of natural persons in public places by using remote biometric techniques, both the EDPB and EDPS called for a general ban on using AI that allows for automated recognition of human features in public places. The same ban should apply where AI systems use biometrics to cluster individuals on grounds such as ethnicity, gender, and political or sexual orientation.

The EDPB and EDPS also call for a prohibition against using AI:

- in order to infer human emotions, except for specific cases where the recognition of emotions plays an important role for health reasons, such as health purposes; and
- for any type of social scoring.

It remains to be seen if the final version of AI Regulation will address these concerns while ensuring sure that its provisions will not hinder innovation in the field of AI.

Civil Liability

There are currently no specific rules with regard to AI. Thus, the general rules on civil contractual liability and tort law apply, as well as those on administrative liability, the assessment being made on a case-by-case basis.

For instance, under the Romanian Civil Code, there is an obligation for one party to repair the damages incurred by another party as a result of the use of an object. The liability sits with the person who owns or has control over the object or who uses the object in their own interest. Such a person would be held liable regardless of whether there was any fault on their behalf. It is thus not unlikely for a person owning or using AI tools to be held liable for any damages that

might result from events caused independently by the AI programme, even if the latter did not receive direct instruction to that specific end.

It should be noted that on 28 September 2022, as part of the European AI Strategy, the European Commission adopted a proposal of the Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). Its aim will be to put in place uniform rules regarding certain aspects of non-contractual civil liability for damage caused by the involvement of AI systems.

In 2022, the Senate of Romania found that the proposal for a Directive of the European Parliament and of the Council on the adaptation of the rules on extra-contractual civil liability to artificial intelligence (Directive on AI liability) – COM (2022) 496 respects the principles of subsidiarity and proportionality.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Big data, machine learning and artificial intelligence are currently not regulated in Romania. Nevertheless, there is increased interest from certain authorities in relation to these fields.

Internet of Things

At the moment, the internet of things (IoT) is not regulated in Romania. Nevertheless, when implementing IoT projects, one must bear in mind various pieces of legislation, examples of which are given below.

Data protection

As IoT products generally collect and process large quantities of personal data, every such product should be thoroughly assessed to ensure its compliance with GDPR requirements, including those referring to data processing impact assessment (DPIA).

The Romanian National Supervisory Authority for Personal Data Processing has put large-scale processing of personal data generated by sensor-based devices transmitting data through the internet or through other means (IoT applications, such as smart TVs, connected vehicles, smart metering, intelligent toys, intelligent cities or other such applications) on the list of data-processing operations for which conducting a DPIA is required prior to deployment.

Cybersecurity

As the IoT implies the use of new technology that may be subject to security vulnerabilities, IoT-based projects might also need to consider compliance with cybersecurity legislation, such as:

- Law No 362/2018 on ensuring a high common level of security of networks and information systems transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the European Union (the “NIS Directive”); and
- Regulation (EU) 2019/881 of the Parliament and of the Council of 17 April 2019 on ENISA (the “European Union Agency for Cybersecurity”) and on information and communications technology cybersecurity certification and repealing of Regulation (EU) No 526/2013 (the “Cybersecurity Act”), which was directly applicable in Romania as of 28 June 2021.

The new Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the EU, repealing Directive (EU) 2016/1148 (the “NIS 2 Directive”) introduces the concept of “important entities” and adds new sectors where such important entities operate that would fall within the revised scope of the NIS Directive. One such sector is the manufacturing of certain critical products, such as:

- computer, electronic and optical products;
- electrical equipment;
- other machinery and equipment not elsewhere classified;
- motor vehicles, trailers and semi-trailers; and
- other transport equipment.

To this end, following the transposition of the NIS 2 Directive into the national legislation (by 17 October 2024), the manufacturers of IoT devices that fall under the scope of the same will need to take key risk-management measures to manage risks to the security of network and information systems.

In 2022, Law no 242/2022 regarding data exchange between IT systems and the creation of the National Interoperability Platform was adopted. It regulates the creation, operationalisation and administration of the tools/means necessary for the delivery in an integrated format of several electronic services by implementing the interoperability platform.

Big Data *Competition*

In 2021, the Romanian Competition Council published a document called a “Study on the effects on competition of the usage of Big Data platforms” (the “Study”).

The need for the Study arose both from the rapid evolution of digital markets and the impact of big data on the economy. The absence of sufficient information in that respect caused the Romanian Competition Council to start working on the Study in 2018.

The Study has identified not only the strengths and opportunities arising from the use of big data (ie, economy of time and resources, innovation, efficiency and productivity, real-time information), but also the threats posed by such usage (ie, in the area of data confidentiality, data protection, legitimacy of data usage and control over data quality).

Following the Study, the Romanian Competition Council concluded that, despite the positive impact of big data on economic growth (mainly through increased productivity and efficiency), the same has the potential to affect competition through abuse of dominance by restricting or refusing access to data or through collusion.

Intellectual property

In relation to intellectual property, one issue is whether algorithms used in big data can be protected through intellectual property rights. The answer so far seems to be that such algorithms are excluded from protection under EU copyright laws, since “ideas, procedures, methods of operation or mathematical concepts” are not protected under EU copyright rules.

Patent protection of algorithms is also excluded. However, to the extent algorithms are used in the creation of computer-implemented inventions that are new, involve an inventive step and are susceptible to industrial application, the possibility of patentability, although still uncertain, is not excluded.

It is debatable whether algorithms can benefit from sui generis protection under database protection laws. In order for such protection to be granted, substantial investments must be made in either the obtaining, verification, or presentation of the contents to prevent extraction and/or re-utilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database. It is unclear whether protecting algorithms can be linked to their role in obtaining or evaluating data.

Algorithms may, however, be protected as trade secrets, as long as they remain secret. However, the lack of transparency in algorithms creates its own set of issues, especially in the context of automated decision-making.

Another issue raised by AI algorithms is that of authorship. In Europe, the European Patent Office has refused two patent applications on the grounds that a machine, instead of a human, was named as inventor. This line of reasoning is likely to be followed by countries such as Romania.

Data protection

The GDPR is based on observing key principles, such as lawfulness, fairness, transparency, purpose limitation, data minimisation, storage limitation, integrity, and confidentiality.

At the opposite end, big data implies:

- collecting a huge amount of information;
- combining data from various sources; and
- further usage of the data in order to analyse and make decisions based on it.

Thus, ensuring that big data does not infringe on GDPR principles can be a challenge.

Given the significant volume of information scattered across multiple systems, a company must have in place procedures and mechanisms enabling the swift location, extraction, rectification, restriction and/or erasure of the personal data concerned.

Open data

In 2022, Law no 179/2022 on open data and reusing information from the public sector was adopted. The purpose of the initiative was the full transposition into national legislation of Directive (EU) 2019/1024 of the European Parliament and of the Council of June 20, 2019, regarding open data and the reuse of public sector information. The legislation aims at facilitating the use of available data from the public sector for the creation of innovative IT products, solutions and services by private companies and strengthening the free flow of information.

Artificial Intelligence

National strategic framework

Romania has plans to develop a “national strategic framework in the field of artificial intelligence” through the project “strategic framework for the adoption and use of innovative technologies in public administration 2021-27 – solutions for business efficiency”.

In 2021, as a first step in the development of the national strategic framework, the Romanian Authority for the Digitalisation of Romania (ADR) in partnership with the Technical University of Cluj-Napoca launched a public consultation on AI. The public consultation was open to academia, businesses, consumers, professionals, and public sector entities that work with AI or for which AI represents a strategic element in the further development of Romania. The purpose of the public consultation has been to obtain qualitative data on the respondents’ view of AI.

This initiative is in line with the European vision on AI, especially in light of the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (the “Artificial Intelligence Act”) and amending certain union legislative acts.

From 2023, Romania will be contributing to the NATO Innovation Fund, a multi-sovereign venture capital fund meant to provide strategic investments in start-ups developing dual-use emerging and disruptive technologies in critical areas for allied security.

Competition

The Romanian Competition Council’s Study concluded that, due to the ability of machine learning to learn constantly and adapt following the processing of real-time data, there is a risk of collusion between companies using such machine learning, for example, based on the rapid adaptation to a competitor’s prices. However, in order for a cartel to exist, the will of more than one undertaking in this regard must still exist.

Intellectual property

Please see the **5.1 Machine-to-Machine Communications Secrecy and Data Protection** (Big Data) for potential intellectual property aspects, equally touching on AI.

Data protection

In April 2021, the European Commission put forward a Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on AI (the “AI Proposal”) with an aim to provide a co-ordinated European approach to the human and ethical implications of AI.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

The main pieces of legislation regulating audio-visual media services in Romania are Law No 504/2002 on audio-visual content (“Audio-visual Law”) and Decision No 220/2011 on the Code of regulation of audio-visual content (“Audio-visual Code”).

Analogue programme services may only be provided by a broadcaster under Romanian jurisdiction on the basis of the analogue audio-visual licence and, as the case may be, of a broadcasting licence.

Digital terrestrial programming services through a broadcasting/television multiplex operator under Romanian jurisdiction may only be provided on the basis of a licence for the use of radio frequencies in a digital terrestrial system, for the benefit of digital audio-visual licence holders.

Procedure for Granting Audio-Visual Licences

The procedure for granting audio-visual licences is provided in Decision 277/2013 of the National Audio-visual Council (CNA) on the procedure for granting, amending, extending the validity and assignment of the licence and the audio-visual authorisation decision, except for those for digital terrestrial broadcasting, as well as the conditions for the broadcasting of local programmes, retransmissions, or takeover programmes of other broadcasters.

For terrestrial frequencies, the licence is granted based on competition among providers. If the service is provided via electronic communica-

tion networks, the licence is granted by decision of the CNA. Both analogue or digital audio-visual licences are granted for a period of nine years, for both radio and television. They can be renewed every nine years.

The holder of the broadcasting licence or the licence for the use of radio frequencies in the digital terrestrial system has an obligation to pay, annually in advance, a tariff for the use of the spectrum.

Video-on-demand services are governed by CNA Decision No 320/2012 regarding the provision of video-on-demand services. The decision does not apply to websites that provide user-generated audio-visual content for sharing, or sharing within a community of interest, such as YouTube.

The provision of on-demand audio-visual media services through electronic communications networks using digital terrestrial television systems is possible only on the basis of a digital terrestrial audio-visual licence granted by the CNA in accordance with the law. Other than that, any person intending to provide on-demand audio-visual media services has an obligation to notify the CNA of this intention at least seven days before the start of the activity.

The provisions of the Audio-visual Law and the Audio-visual Code apply accordingly to the audio-visual programmes broadcast on demand, considering their specificity to be viewed on request and at the time chosen by the user.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Scope of Telecommunications Rules and Approval Requirements

Government Emergency Ordinance No 111/2011 on electronic communications (GEO 111/2011) transposes the main EU legal provisions in the field of electronic communications and covers all activities in the field of electronic communications networks and services.

According to GEO 111/2011, an electronic communications service is a service normally provided for remuneration which consists wholly or mainly of the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excluding services providing or exercising editorial control over content transmitted using electronic communications networks and services.

The provision of electronic communications networks and services is subject to a general authorisation regime and, where applicable, licences for the use of limited resources for the provision of electronic communications networks and services (such as radio frequencies, numbering resources and other associated technical resources). The provision of electronic communications networks and services by persons in the European Union may be limited only for reasons related to defence, public order and national security or public health. The limitation of the freedom to provide electronic communications networks and services is motivated and notified to the European Commission. The provision of electronic communications networks and services by persons outside the European Union may be limited for objective and justified

reasons, by decision of the National Authority for Management and Regulation in Communications (ANCOM).

The procedure to become an electronic communications network and/or services provider under the general authorisation regime is free of charge and consists of a notification to ANCOM. Providers of interpersonal communication services that are not based on numbers do not have the obligation to notify ANCOM.

In 2023, ANCOM aims to amend the general authorisation framework to bring it in line with the new amendments to the GEO 111/2011 brought by the transposition into the national legislation of Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (“European Electronic Communications Code”).

Instant Messaging

The European Electronic Communications Code, which came into force on 21 December 2018, extended the scope of electronic communication services. According to this European enactment, electronic communication services encompass the following types of services:

- internet access services;
- interpersonal communications services; and
- services consisting wholly or mainly in the conveyance of signals, such as transmission services used for the provision of machine-to-machine services and for broadcasting.

The concept of interpersonal communications services is new and refers to services normally provided for remuneration that enable direct interpersonal and interactive exchange of information via electronic communications networks

between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipients. This concept does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

There are two types of interpersonal communications services, namely:

- number-based interpersonal communications services, where the interpersonal communications service connects with publicly assigned numbering resources or enables communication with a number or numbers in national or international numbering plans; and
- number-independent interpersonal communications service, where the interpersonal communications service does not connect with publicly assigned numbering resources or does not enable communication with a number or numbers in national or international numbering plans.

The number-independent interpersonal communications services include instant messaging services such as WhatsApp and Facebook Messenger. According to the European Electronic Communication Code, the national regulatory authorities (NRAs) have powers with regard to instant messaging services consisting of, among other things, submitting requests for information, settling dispute resolutions (including potential cross-border disputes), monitoring the market and protecting end-user rights with regard to non-discrimination, providing information in contracts, ensuring transparency and the quality of service.

The European Electronic Communication Code was transposed into GEO 111/2011 through Law

198/2022 for the modification and completion of some normative acts in the field of electronic communications and for the establishment of measures to facilitate the development of electronic communications networks.

Voice over Internet Protocol

In Romania, Voice over Internet Protocol (VoIP) services using numbering resources are electronic communication services similar to fixed telephony services provided over public switched telephone networks (PSTNs). VoIP services are subject to GEO 111/2011 in terms of numbering resources, number portability, interconnection, quality of service and access to emergency services.

Radio-Frequency Identification Devices (RFIDs)

The National Authority for Management and Regulation in Communications Decision No 311/2016 on radio frequencies and frequency bands, exempted from the licences regime, sets the technical specifications applicable to RFIDs.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

In Romania, technology agreements are not regulated as separate contracts in the Civil Code, the general law of contracts in Romania. However, specific regulations can be found in fields such as those identified below.

Competition – Technology Transfer Agreements

In competition law, technology transfer agreements refer to licences where the licensor allows the licensee to exploit the technology that is the subject of the licence for the production of

goods or the provision of services. Competition law provisions regulate how technology transfer agreements can take place if the transaction has a national scope. EU provisions are also incident when the transfer has an EU dimension.

Data Storage Location

In relation to the soon-to-be-built government cloud, a draft government decision states that the government cloud services are hosted and offered on a core infrastructure located on the territory of EU member states.

Financial Institutions

Please see the 3.1 **Highly Regulated Industries and Data Protection**.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Electronic Signatures

From the perspective of electronic signature and trust services, in Romania, Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS Regulation") is applicable.

Romania also has a national law, Law 455/2001 on electronic signatures, which is obsolete. The Romanian legislature is in the process of drafting a new national law for electronic signatures, focused on the areas where the eIDAS Regulation allows for member states to follow their own approaches.

Digital Identity

In a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, the European Commission found that the eIDAS Regulation has not achieved its potential, given that:

- only a limited number of electronic identifications (eIDs) have been notified, limiting the coverage of notified eID schemes to about 59% of the EU population;
- the acceptance of notified eIDs at the level of both member states and service providers is limited;
- only a few of the services accessible through domestic eID are connected to the national eIDAS infrastructure; and
- the added value of the eIDAS Regulation with regard to electronic identity is limited due to its low coverage, uptake and usage.

Therefore, a reform is expected to increase the usage of electronic identification.

So far, Romania is testing a pilot program of issuing electronic identity cards, which is currently ongoing in Cluj county (at least 4,200 electronic identity cards issued); this will be extended to Bucharest in 2023.

MPR Partners is an internationally recommended and award-winning law firm with a client-friendly, business-oriented and innovative approach. The firm's recognition comes from outstanding client feedback and reputed legal ranking and business publications at both international and local levels, as well as from its peers. With swift access to an extensive network of legal and tax professionals throughout the European Union and worldwide, an award-

winning management team, competitive business terms and outstanding feedback from large corporations and international law firms, MPR Partners is a firm of choice for proficiently-handled business law, tax and insolvency matters across the EU and beyond. Find out more on the firm's official websites: www.mprpartners.uk (London office) and www.mprpartners.com (Bucharest office).

Authors



Alina Popescu is the founding partner of MPR Partners. She is an internationally commended lawyer with extensive expertise in legal management, M&A, competition law, technology and

commercial and corporate projects, as well as in regulatory and international arbitration matters. Alina's diverse expertise, her ability to co-ordinate cross-border projects and her capacity to lead 365-degree, multi-angled assessments and strategies brings added value to the most intricate transactions and disputes. As a result, she has garnered outstanding feedback from major corporate clients and international law firms. She has been a qualified lawyer since 2004 and is a member of the International and Competition Sections of the New York State Bar Association, the International Bar Association, the International League for Competition Law and the Bucharest Bar.



Daniel Alexie provides valuable assistance to major corporate clients at MPR Partners with regard to various legal advisory matters, spanning IP, IT and telecoms, data privacy (assisting

clients on adapting their corporate policy to comply with EU and Romanian privacy laws, including the GDPR) as well as advertising and consumer protection aspects. His expertise covers the M&A, corporate and commercial, competition and employment areas of practice. Daniel represents international and local clients in various sectors such as industry, services, entertainment and healthcare. He is a versatile and adaptable professional, and a team-player with good strategy skills.

Contributed by: Alina Popescu, Daniel Alexie, Flavia Stefura and Cristina Crețu, **MPR Partners**



Flavia Stefura is part of MPR Partners' advisory department, being primarily involved in IP, data privacy, competition, consumer protection and M&A matters. She previously worked

for reputed international law firms in the Romanian market, and deals with corporate and commercial, employment, regulatory as well as administrative matters. She advises high-profile clients that are active in various industry sectors, such as retail, fast-moving consumer goods (FMCG), banking and finance. Flavia is a highly focused professional, delivering cross-departmental assistance in a timely manner.



Cristina Crețu is a seasoned technology law and data protection expert, with over 16 years of experience in the TMT sector. She has worked with the Romanian telecoms regulatory

authority (ANCOM), has been a regulatory expert with Deutsche Telekom's Romanian subsidiary as well as a regulatory manager and data protection officer with Liberty Global in Romania, and is now a Senior Technology and Data Protection Consultant with MPR Partners' Bucharest and London offices. Cristina is also a Vice Chair of the American-Romanian Chamber of Commerce's Data Protection Task Force. She co-heads the firm's task force on the Romanian National Council for Digital Transformation and is part of the European Data Protection Board "Support Pool of Experts" List.

MPR Partners

6A Barbu Delavrancea Street
Building C
Ground Floor
1st District
011355 Bucharest
Romania

Tel: +402 1310 1717
Fax: +402 1310 1718
Email: office@mprpartners.com
Web: www.mprpartners.com



MPR PARTNERS

Trends and Developments

Contributed by:

Alina Popescu, Daniel Alexie,
Flavia Stefura and Cristina Crețu
MPR Partners see p.436

Introduction

The acceleration of the digitisation and digitalisation trends that started during the COVID-19 pandemic and continued throughout a troublesome 2022 has led not only to a more urgent need for access to public and private services via digital means, but also to more pressing concerns regarding cybersecurity and potential threats from third-party state actors.

While the new technologies and the rapid development of the interoperability and interconnectivity of essential fields of activity are a driver for economic growth and social development, the associated challenges are not easy to overcome. These include fragmentation, red tape around permits for network constructions, low digital skills, and exposure to cyber-risks.

Nevertheless, the reforms and investments provided in its National Recovery and Resilience Plan (PNRR) under the Digital Transformation component aim to ensure that Romania will have a coherent and integrated digital infrastructure to help transition to a more digitalised economy and society.

The importance of the topic is reflected in the budget allocated in Romania's PNRR (endorsed by the European Commission in September 2021) to digital transformation-related investments, which represent 20% of the total amount allocated under the plan.

In addition, Romania has continued to make headlines with its flourishing technology sector;

among such headlines has been the Bucharest venue of the EU Cybersecurity Competence Centre starting to take shape. Moreover, Romania hosts business and regulatory conferences for the technical sector, such as GoTech World.

Technologies such as IoT, artificial intelligence, machine learning and 5G have started to play an important role in Romania's economic growth, offering numerous opportunities for investments.

Digital Transformation in the Public Sector

The digitalisation of public administration plays a key role in Romania's PNRR, with an emphasis on areas such as justice, employment and social protection, environment, civil service management and skills development, public procurement, cybersecurity, tax, and customs. All these add up to a plan to build a secure government cloud infrastructure and to support the deployment of electronic IDs.

Romania also plans to invest in both:

- the digitalisation of health by developing an integrated e-Health system, which will help connect over 25,000 healthcare providers and telemedicine systems; and
- the digitalisation of education, by improving digital pedagogical skills, educational content, equipment and resources.

Digital transformation is mainly focused on:

- setting up the government cloud;
- ensuring interoperability;

- improving connectivity;
- increasing the protection and cybersecurity of public and private entities; and
- increasing the digital competence of the public sector.

The process to ensure the digital transformation is to go hand in hand with the amendment of the Occupations Classification Code for the same to include the definition of new digital occupations.

Government Cloud

The Government Cloud was envisioned to promote two reforms.

- “Development of a unitary framework for defining the architecture of a government cloud”.
- “Increasing digital competence for public service and digital education throughout the life of citizens” – this reform includes one investment which covers the deployment of the Government Cloud Infrastructure.

The PNRR provided two legal enactments which were needed to develop a unitary framework for defining the architecture of a government cloud, namely:

- the Information Systems Interoperability Law, detailing the uniform set of standards and rules that public entities are supposed to apply for the development of applications in a secure and sustainable environment – this law has been enacted in the form of Law 242/2022 on the exchange of data between IT systems and the creation of the National Interoperability Platform; and
- the Government Cloud Act, setting out the responsibilities and tasks regarding the design, implementation, development and management of the cloud infrastructure, tech-

nologies and services – this normative act has been enacted in the form of Government Emergency Ordinance 89/2022 regarding the establishment, administration and development of cloud IT infrastructures and services used by public authorities and institutions.

The legislative process is ongoing and is particularly intense concerning the Government Cloud. The secondary legislation has already been adopted by the government, and tertiary legislation should be developed shortly. Following that, the tenders for building the Government Cloud infrastructure will begin.

5G networks

High-capacity networks and the necessary measures to ensure the transition to EU 2025 connectivity targets are both required for the digital transformation.

Stimulating private investment for the deployment of high-capacity networks, including through the acceleration of the national roll-out of 5G networks and the provision of broadband coverage for white areas, has therefore become crucial.

In 2022, Romania transposed into national legislation Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. Following the transposition, in November 2022, Romania organised the tender for the 5G spectrum, with 420 MHz of spectrum allocated as a result of the tender.

Thus, the rate of adoption of 5G technology in Romania remains to be seen. This aspect will determine whether the level of investment for rolling out 5G networks will surpass the minimum required through the 5G licences. This will also

determine whether further tenders to allocate the remaining 5G spectrum will be organised soon.

Broadband coverage and speeds

In 2022, more than eight out of ten households in Romania have had access to internet at home, an increase of 1.3 percentage points compared to the previous year according to the Romanian National Institute of Statistics.

Romania's vision is to implement 5G broadband as soon as possible, as described in:

- the National Strategy Digital Agenda 2020;
- the National Plan of Development of the NGN infrastructure;
- the Strategy for Digital Communications 2020; and
- the Strategy for implementing 5G in Romania.

Romania has already take steps in the right direction by adopting measures involving the simplification of the building authorisation process for broadband networks and organising the 5G tender. In addition, Romania is setting up partnerships for the development and testing of 5G uses. For the moment, seven potential pilot projects are being planned, one for each development region of Romania, following interviews with businesses, academics and public sector representatives.

However, one of the biggest issues for Romania's electronic communication sector remains the lack of universal coverage. To ensure the provision of broadband coverage for white areas, the PNRR envisages the implementation of a scheme to support the use of communication services through different types of instruments for beneficiaries, with a focus on white areas. This scheme is meant to help with the provision of coverage for very high-speed internet

access, namely, at least 100 megabits per second (Mbps) delivered through fibre-to-the-premises (FTTB/H) and/or 5G networks to those areas where the market cannot deliver these services on its own (ie, disadvantaged rural areas).

Investments are to be made in passive infrastructure and active network elements, back-haul and access segments, and in deploying new networks and upgrading the existing ones to address:

- the areas not covered with fixed networks which have a demand for services; and
- the fixed networks that do not provide the necessary speeds to offer proper electronic communication services.

eHealth and telemedicine system

The pandemic triggered an increase in the demand for telemedicine solutions. Although changes in the legal framework have been made to accommodate telemedicine, investments are needed to increase the access of rural and small urban areas, as well as of vulnerable groups, to specialised consultations via telemedicine.

The digitalisation of the National Health Insurance House and putting in place measures designed to ensure the cybersecurity of the Health Insurance IT Platform are two further important tasks for the Romanian authorities. In this respect, investments are planned to allow the integration of health institutions through digital infrastructure which will help to reduce fragmentation and increase the quality of health data.

In 2022, secondary legislation concerning telemedicine was enacted. Since presently approximately 50% of medics are concentrated in only six municipalities in Romania (Bucharest,

Craiova, Timișoara, Cluj, Târgu Mureș, and Iași), it seems that, even though the main restrictive effects of the COVID-19 pandemic have ended, there is no reason that telemedicine should not be widely used. However, certain difficulties may arise from the lack of digital education of both medics and patients.

Potential New Obligations on Cloud Operators

Although not covered by the telecoms framework, the recent transposition of the European Electronic Communication Code included an obligation for the providers of electronic hosting services with IP resources to support law enforcement bodies and bodies with powers in the field of national security in the implementation of technical surveillance methods or authorisation acts, namely:

- allowing lawful interception of communications by the relevant authorities, at provider's cost;
- conveying to the authorised bodies, on request, the encrypted content of the communications made on the provider's network which is identified by lawfully issued warrants; and
- to allow the relevant authorities access to the provider's own computer systems, in order to copy or extract (exclusively) the data identified in lawfully issued warrants.

Whether cloud operators will be included in the scope of this obligation remains to be seen, as the National Regulatory Authority for Communications and Information Technology of Romania (ANCOM) must publish on its website the types of electronic hosting services for which the providers with IP resources must observe the above-mentioned obligations.

Cybersecurity

Bucharest is the host of the European Cybersecurity Industrial, Technology and Research Competence Centre (the "EU Cybersecurity Centre"), which should play an important role in connecting public stakeholders with the relevant researchers and private sector. The EU Cybersecurity Centre held its first offline meeting in Bucharest in June 2022 and featured a discussion of its priorities and the necessary steps for ensuring its full operability in Bucharest.

Another important development in the cybersecurity field is the adoption and entry into force in 2022 of the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 ("NIS 2 Directive"). The member states, including Romania, will have until 2024 to transpose the Directive into national legislation.

The NIS 2 Directive regulates the cybersecurity of supply chains, sets reporting obligations, and introduces harmonised sanctions. It also establishes an EU Cybersecurity Crisis Response Framework (EU-CyCLONe). As with most directives, it may be unlikely to see Romania implement the NIS 2 Directive before its deadline in 2024.

Artificial Intelligence

In November 2022, the Romanian government instituted the Romanian Committee for Artificial Intelligence, created under the patronage of the Prime Minister, with the technical secretariat being provided by the Ministry of Research, Innovation and Digitalization. The declared role of the Committee will be to stimulate the participation of private, academic, and civil society

Contributed by: Alina Popescu, Daniel Alexie, Flavia Stefura and Cristina Crețu, **MPR Partners**

actors, together with the Romanian authorities, in exploiting AI for the benefit of Romanian society.

The budget of the Committee for Artificial Intelligence is approved through the Smart Growth, Digitization and Financial Instruments Program.

MPR Partners is an internationally recommended and award-winning law firm with a client-friendly, business-oriented and innovative approach. The firm's recognition comes from outstanding client feedback and reputed legal ranking and business publications at both international and local levels, as well as from its peers. With swift access to an extensive network of legal and tax professionals throughout the European Union and worldwide, an award-

winning management team, competitive business terms and outstanding feedback from large corporations and international law firms, MPR Partners is a firm of choice for proficiently-handled business law, tax and insolvency matters across the EU and beyond. Find out more on the firm's official websites: www.mprpartners.uk (London office) and www.mprpartners.com (Bucharest office).

Authors



Alina Popescu is the founding partner of MPR Partners. She is an internationally commended lawyer with extensive expertise in legal management, M&A, competition law, technology and

commercial and corporate projects, as well as in regulatory and international arbitration matters. Alina's diverse expertise, her ability to co-ordinate cross-border projects and her capacity to lead 365-degree, multi-angled assessments and strategies brings added value to the most intricate transactions and disputes. As a result, she has garnered outstanding feedback from major corporate clients and international law firms. She has been a qualified lawyer since 2004 and is a member of the International and Competition Sections of the New York State Bar Association, the International Bar Association, the International League for Competition Law and the Bucharest Bar.



Daniel Alexie provides valuable assistance to major corporate clients at MPR Partners with regard to various legal advisory matters, spanning IP, IT and telecoms, data privacy (assisting

clients on adapting their corporate policy to comply with EU and Romanian privacy laws, including the GDPR) as well as advertising and consumer protection aspects. His expertise covers the M&A, corporate and commercial, competition and employment areas of practice. Daniel represents international and local clients in various sectors such as industry, services, entertainment and healthcare. He is a versatile and adaptable professional, and a team-player with good strategic skills.

ROMANIA TRENDS AND DEVELOPMENTS

Contributed by: Alina Popescu, Daniel Alexie, Flavia Stefura and Cristina Crețu, **MPR Partners**



Flavia Stefura is part of MPR Partners' advisory department, being primarily involved in IP, data privacy, competition, consumer protection and M&A matters. She previously worked

for reputed international law firms in the Romanian market, and deals with corporate and commercial, employment, regulatory as well as administrative matters. She advises high-profile clients that are active in various industry sectors, such as retail, fast-moving consumer goods (FMCG), banking and finance. Flavia is a highly focused professional, delivering cross-departmental assistance in a timely manner.



Cristina Crețu is a seasoned technology law and data protection expert, with over 16 years of experience in the TMT sector. She has worked with the Romanian telecoms regulatory

authority (ANCOM), has been a regulatory expert with Deutsche Telekom's Romanian subsidiary as well as a regulatory manager and data protection officer with Liberty Global in Romania, and is now a Senior Technology and Data Protection Consultant with MPR Partners' Bucharest and London offices. Cristina is also a Vice Chair of the American-Romanian Chamber of Commerce's Data Protection Task Force. She co-heads the firm's task force on the Romanian National Council for Digital Transformation and is part of the European Data Protection Board "Support Pool of Experts" List.

MPR Partners

6A Barbu Delavrancea Street
Building C
Ground Floor
1st District
011355 Bucharest
Romania

Tel: +40 2131 01717
Fax: +40 2131 01718
Email: office@mprpartners.com
Web: www.mprpartners.com



MPR PARTNERS

Law and Practice

Contributed by:

Marina Villalonga

Asensi Abogados see p.458



Contents

1. Metaverse	p.439
1.1 <u>Laws and Regulations</u>	p.439
2. Digital Economy	p.440
2.1 <u>Key Challenges</u>	p.440
3. Cloud and Edge Computing	p.444
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.444
4. Artificial Intelligence and Big Data	p.446
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.446
5. Internet of Things	p.449
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.449
6. Audio-Visual Media Services	p.451
6.1 <u>Requirements and Authorisation Procedures</u>	p.451
7. Telecommunications	p.453
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.453
8. Challenges with Technology Agreements	p.454
8.1 <u>Legal Framework Challenges</u>	p.454
9. Trust Services and Digital Entities	p.456
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.456

1. Metaverse

1.1 Laws and Regulations

The Metaverse and its Regulation

The metaverse could be considered the greatest technological revolution of recent years. Since its recent inception, it has become the central focus among technological advances. This concept refers to a three-dimensional virtual reality, where individuals can interact through avatars much like they do in reality. The metaverse will allow us to study, hold work meetings, attend concerts, go shopping and engage in a long list of activities, many of which are currently beyond the imagination. The reality is that the metaverse is still early in its development. Certainly, it is mainly used today for the development of leisure activities and especially for video games, but its applications will continue to grow exponentially.

There is no doubt that the evolution of the metaverse is unstoppable, so it is becoming urgently necessary to regulate the legal aspects that derive from it, encompassing matters such as data protection or cybersecurity.

Currently, regulatory frameworks exist both at Spanish and European levels, which can serve as a basis for the resolution of potential problems that may occur in the development of the metaverse. In the EU, the General Data Protection Regulation (GDPR), the Digital Services Act, the Digital Markets Act and the Cybersecurity Act are all pertinent, among others. In Spain, the *Ley Orgánica de Protección de Datos y garantía de los derechos digitales* (LOPDGDD), which transposes the GDPR, and the *Ley de Servicios de la Sociedad de la Información* (LSSI), which regulates the electronic procurement of goods and services, constitute the main regulations to deal with the metaverse phenomenon for the time being.

Obviously, these rules do not cover the abundance of situations and conflicts that will have to be resolved in the coming years; for now, the aforementioned pieces of legislation will have to be subsidised with the common Spanish contractual and consumer protection law.

The *Agencia Española de Protección de Datos* (AEPD), the Spanish data protection authority, has recently focused on the metaverse and its privacy risks. This body acknowledges that the metaverse is made possible as a result of the development and expansion of a multitude of technologies in constant evolution which interact in the metaverse, such as internet of things (IoT), artificial intelligence (AI), blockchain, 5G, digital identity techniques, cloud or edge computing, and virtual reality or augmented reality technologies.

The Challenges Posed by the Metaverse

There are two essential risks that will have to be faced in relation to the metaverse: privacy and data security.

As the AEPD points out, the metaverse can be very intrusive from the privacy point of view since the processing of data in this environment is massive. Thus, the processing of some specific categories of data will be of paramount importance and will make it possible to extract extremely detailed information from users. Such is the case with biometric data. Virtual reality glasses will be able to determine what we like and what gives us pleasure or elicits rejection with the analysis of the changes in our pupils.

Likewise, the perception of postural changes or the position of avatars in the virtual environment will reveal information of which the user is not aware. This information can be used to person-

alise marketing campaigns based on specific profiles.

So, each of the technologies that converge in the metaverse present certain privacy risks that will have to be addressed, ranging from non-consensual profiling to identity theft. Therefore, it will be essential to adopt the necessary measures based on the mechanisms provided for in both of the data protection regulations. These measures must integrate impact assessments, data security, transparency in data processing, the guarantee of the rights of the data subjects and the minimisation of data collection.

The very concept of the metaverse as a virtual reality space in which people interact as they do in the real world also entails the presence of (cyber)criminals and a space conducive to piracy. Blockchain technology, through its process validation system, can help mitigate these risks, but it cannot make them disappear, at least not on its own. It must go hand in hand with the implementation of strong cybersecurity measures that can neutralise techniques such as phishing or prevent the theft of cryptocurrencies.

However, the development of the metaverse will have to face other challenges, beyond privacy or cybersecurity. For example, there are even AI tools for image and video generation that can alter creative processes and consequently affect the work of artists.

This leads on to the potential problems related to intellectual property. Since the non-fungible tokens (NFTs) are subject to transactions in the metaverse, mechanisms must be established to verify their authenticity and identify copies or plagiarism. Some lawsuits have already been filed by luxury firms against the plagiarism of their products through NFTs.

In any case, none of the above will be a reality without the input of the big technology companies that lead the development of the metaverse. In recent months, these companies have suffered significant falls in the stock market, arising from the global situation and the false growth expectations that were born as a result of the pandemic. Mass layoffs and cost containment motivated by the fear of a recession and rising interest rates (and therefore higher financing costs) are a certainty, so it remains to be seen whether progress on the metaverse will be made as fast as expected. In any case, it seems that adverse conditions are cyclical and we are only facing a fair adjustment in the technology sector, and sooner or later the definitive impetus for the development of the metaverse will take effect.

2. Digital Economy

2.1 Key Challenges

Brief Introduction to the Concept of Digital Economy

Digital economy entails the use of technology for the production of goods and services, as well as for their subsequent commercialisation, for example, e-commerce, mobile applications or online banking. There is no doubt about the importance of the role that the digital economy plays in our lives today.

In line with the above, it is a reality that within the EU and in each of its member states, a real digital revolution is being experienced. This is confirmed by the huge number of regulations that are being adopted in recent months and the many others that are in the processing phase, precisely because more and more aspects of our lives are developing in the digital environment and the advance of technology is inevitable and occurring at a significant speed.

Digital Regulation

Before entering into detail on the regulations that expressly regulate the digital economy, it is convenient to briefly review the recently approved provisions that refer in a more general way to digital rights, essential for human beings to interact in an orderly manner in the digital environment.

Decision (EU) 2022/2481 of 14 December 2022 sets out the strategic agenda for the Digital Decade Policy Programme 2030, and is based on the communication of 9 March 2021 entitled “2030 Digital Compass” to guide the digital transformation of the EU for the coming years.

In this context, we must also refer to the declaration on European Digital Rights and Principles for the Digital Decade, adopted on 15 December 2022. It reflects the EU’s commitment to achieving a secure digital transformation, putting people at the centre, in order to achieve the objectives of the aforementioned 2030 Digital Compass.

In Spain, these digital commitments are reflected in the Digital Rights Charter, presented by the Spanish government in July 2021, which aims to protect citizens from the possible risks generated by disruptive technologies. They are not normative in nature and therefore merely constitute a frame of reference for public authorities.

This document is complemented by the Digital Spain 2026 strategy, which constitutes the update of the Spanish digital transformation roadmap launched in July 2020.

Regulation on Digital Services and Digital Markets

As previously announced, having laid the foundations that should govern any regulatory devel-

opment in the digital field, we must highlight the very recent publication of several rules that directly regulate certain aspects of the digital economy and that constitute the Digital Services Package presented by the European Commission in 2020.

This digital package basically translates into the approval of Regulation (EU) 2022/2065, of 19 October 2022, known as the Digital Services Act (DSA), and Regulation (EU) 2022/1925, of 14 September 2022, known as Digital Markets Act (DMA).

The adoption of these two rules is an essential part of the EU’s Digital Agenda and aims to create a safer digital space, both for citizens and businesses, in the face of the exponential growth of digital services, especially after the pandemic.

In the end, it is a question of establishing a specific set of uniform rules for the entire EU in order to ensure legal certainty and the proper functioning of the internal market by creating a secure and reliable online environment.

It should also be noted that the EU legislature has chosen a Regulation and not a Directive to regulate the package of digital measures, which implies its direct application as law without the need for transposition in all countries of the European Economic Area (EU plus Iceland, Norway and Liechtenstein).

Digital Services Act

The DSA aims to be a pioneer in the regulation of digital services by reformulating in detail the rights and obligations of certain intermediary service providers, users and digital businesses in order to strengthen respect for fundamental rights in the EU and establishing a new liability regime for certain platforms. In this sense,

new diligence requirements are established for intermediary services providers in terms of the actions to be carried out in the face of illegal content.

It is a necessary update because since the former Directive on electronic commerce was published in 2000 (and transposed into Spanish law by the LSSI), there have been no significant changes in these regulations, despite the fact that the transformation of digital markets and services since then has been overwhelming.

It should be noted that the new DSA does not derogate from the old Directive of the year 2000 and, therefore, the LSSI will continue to be in force in Spain regarding any provisions that do not contradict the DSA. Thus, in Spain, verification work will have to be carried out to verify the enforceability of the provisions of the LSSI that do not contradict the DSA.

As happened with the GDPR, the DSA will involve a significant effort from the operators so that they can adapt to its provisions, which is why much of its articles will not be applicable until 17 February 2024, without prejudice to the fact that the rule entered into force on 16 November 2022.

In addition, in the wake of the GDPR, the DSA affects those providers that address their services to citizens located in the EEA, including big Chinese and American technology companies. Moreover, the DSA includes a strong sanctioning regime for deterring non-compliance.

The DSA concerns the following intermediary service providers:

- Intermediary services offering network infrastructure, such as internet access providers and domain name registrars;
- hosting services, eg, cloud computing and web hosting; and
- online platforms, such as social media platforms, marketplaces and app stores.

In addition, it includes an extensive reference to very large online platforms (VLOP), which reach more than 10% of Europe's 450 million consumers, to which a specific regime will apply.

These above-mentioned services can be divided into three groups:

- those of mere conduit;
- those of caching; and
- hosting services (including online platforms).

Furthermore, the DSA incorporates three new figures:

- digital services co-ordinators shall be appointed by each member state and shall be advised by the European Board for Digital Services;
- trusted flaggers shall be appointed by the digital services co-ordinator of each member state for the purpose of recognising and flagging illegal content;
- compliance officers will need to be appointed by the VLOP, and for practical purposes, as many compliance-related positions should be appointed in large companies (eg, DPO), they will often end up outsourcing these figures to compliance companies.

One of the central components of this new regulation is the inclusion of measures to fight against illicit goods, services or online content, including a liability exemption regime ("safe harbour") that

applies to mere conduit and caching services when they are not involved with the information transmitted, and from which providers of hosting services or data storage services may also benefit if certain requirements are met. Among others, the provider should, upon obtaining actual knowledge or awareness of illegal content, act to remove or to disable access to that content. Thus, the provider will only be liable when it has actual knowledge that the activity or information stored is illicit and do not proceed to the withdrawal of said data or to disable access.

In this sense, the interpretative problems will derive from the consideration of the concept of “actual knowledge”. The practical problems will come because the removal of such illicit content must take place respecting the fundamental rights of the recipients, including the freedom of expression and the right to information. The balancing of such rights will be complicated by providers and may entail serious difficulties in determining liability in court.

So, what would happen if the platform mistakenly removes content upon notice from a trusted flagger and it turns out that content was not illegal? This could happen, for example, in the case of closure of profiles on social media platforms. It seems that the end user affected by such improper termination of their profile has no legal action according to DSA provisions to assert their rights. In this regard, it should be borne in mind that the content of profiles on social media platforms can affect many other areas, such as the intellectual property rights related to such content. Clearly, a solution to this problem will have to be found by the member states.

Digital Markets Act

The DMA aims to ensure a level playing field for digital companies by fostering competition for

the benefit of all users. That is why the position of the “gatekeeper” acquires special relevance, understanding those platforms with a significant impact on the internal market, as they act as a gateway for professional users to reach end users.

In this sense, the DMA aims to prevent gatekeepers from imposing unfair conditions on these users, whether professionals or end-users, thus prohibiting the development of unfair practices by platforms with the highest market share. This will facilitate the growth of start-ups that will be able to operate in a fairer and more equitable environment.

For example, gatekeepers will need to ensure that end users can easily unsubscribe from platform services or uninstall pre-installed services. In addition, they must allow their business users to promote their offers and enter into contracts with their customers outside the gatekeeper platform, or provide them with access to the data they generate when using the gatekeeper’s platforms.

As for prohibitions, among others, they will not be able to track end users outside the gatekeeper’s core platform service for targeted advertising purposes, without effective consent having been granted, and they will not be able to classify their products or services more favourably than those offered by third parties.

These companies shall be designated gatekeepers for at least one of the core platform services included in the DMA, which are as follows:

- online intermediation services;
- online search engines;
- online social networking services;
- video sharing platform services;

- number-independent interpersonal communications services;
- operating systems;
- web browsers;
- virtual assistants;
- cloud computing services; and
- online advertising services.

Within the framework of the DMA, as was the case with the DSA, we can refer to the creation of three figures.

- The gatekeepers – For a company to acquire the status of gatekeeper it must meet certain qualitative and quantitative thresholds provided for in the regulation.
- The High-Level Group – It will be composed of several European bodies with sufficient expertise to advise on the implementation of the DMA.
- The compliance officers, appointed by each gatekeeper.

The Commission shall be the authority empowered to enforce the provisions of the DMA. To this end, it may count on the collaboration of the authorities and courts of each member state, with whom it may act in a co-ordinated manner to carry out the necessary investigative measures.

In any case, any user who sees their rights violated in relation to the DMA may assert them before the national courts, directly invoking the violation of the provisions contained in the aforementioned legal text.

The DMA was published on 12 October 2022, entered into force on 1 November 2022 and will apply from 2 May 2023.

Brief Reference to Digital Finance

The discussion on the digital economy cannot end without including a brief reference to digital finance, given the growth of the crypto-asset market.

In order to undertake appropriate regulation in the field of digital finance, the EU has also prepared a package of rules to regulate this sector. Only one of these will be discussed here, the proposal for MiCA Regulation (Markets in Crypto-assets), pending final approval.

The future MiCA Regulation will regulate the issuance and trading of crypto-assets on platforms, excluding financial instruments and NFTs. It aims to cover the existing legal gap in the commercialisation of cryptocurrencies at European level, favouring legal certainty, consumer and investor protection, market integrity and financial stability, bearing in mind the importance that stablecoins are gaining, which will be supervised by the European Banking Authority (EBA).

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

General Perspective

Article 6 (30) of Directive (EU) 2022/2555, of 14 December 2022, concerning measures to ensure a high common level of cybersecurity across the European Union (NIS 2 Directive) defines cloud computing as “a digital service that enables on-demand administration and broad remote access to a scalable and elastic pool of shareable computing resources, including where such resources are distributed across several locations”.

Edge computing consists of cloud computer services delivered closer to where the data era being generated or collected (Recital 34 NIS 2 Directive).

Cloud service providers are considered “digital service providers” under Directive to EU 2016/1148, known as NIS 1 Directive, which was transposed into Spanish legislation by virtue of Royal Decree-Law 12/2018, on the security of networks and information systems, subsequently developed by Royal Decree 43/2021. The provisions on cybersecurity contained in that legislation are therefore applicable to cloud service providers.

In any case, the NIS 1 Directive has recently been superseded by the aforementioned NIS 2 Directive (in fact, it repeals it with effect from 18 October 2024). NIS 2 Directive, which was published in the OJEU on 27 December 2022 and entered into force 20 days after its publication, includes in its scope, as did the NIS 1 Directive, cloud computing services (Recital 33), as long as the providers provide their services or carry out their activities in the EU territory. They should therefore be subject to the new cybersecurity provisions provided for in the NIS 2 Directive, which should be transposed by the member states up to 17 October 2024.

As stated in this regulation, cloud computing services include, among others, infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) and network as a service (NaaS).

Regulated Industries

As far as the banking sector is concerned, although there are no specific regulations for cloud computing as such, the European Banking Authority (EBA) published at the end of the 2017

Recommendations on outsourcing to cloud service providers. Basically, it offers a guide to be followed by financial institutions that decide to make use of this technology.

In Spain, the Bank of Spain, as supervisory authority, ensures compliance and the correct application of these recommendations.

In the insurance sector, the European Insurance and Occupational Pensions Authority (EIOPA) published its Guidelines on Outsourcing to Cloud Service Providers in a similar sense to those applied to the banking sector.

The *Dirección General de Seguros y Fondos de Pensiones*, the supervisory body in Spain, endorsed the EIOPA guidelines by resolution of 10 July 2020 and since then has been ensuring their correct follow-up.

The European Securities and Markets Authority (ESMA) also published its guidelines on 10 May 2021 in the same sense as the previous ones.

Data Protection

The very idiosyncrasy of cloud computing implies that companies providing this type of services must respect the applicable data protection regulations as cloud computing inevitably involves the processing of data. Therefore, it will be necessary to comply with the provisions set forth in the GDPR and the LOPDGDD.

In this sense, the first issue to be resolved is the quality in which the cloud computing service provider acts, since, depending on the specific legal relationship that unites it to its client, it will be considered processor (the most common, which entails the signature of the processing agreement provided for in Article 28 GDPR), or joint-controller by exercising control jointly with

its client, with the legal consequences that this entails.

It should be borne in mind that the determination of the legal position occupied by each party determines the law applicable to the contract. Thus, when the client is controller and the provider is processor, the applicable law will be that of the client.

In any case, it will be desirable for the client that the contract with the cloud services provider includes a data portability clause in the event of termination of the agreement. The provider should facilitate such portability to the new service provider or to the client themselves.

Finally, we must not ignore the importance of cloud computing services in international data transfers, that is, with third countries outside the EEA. If such transfer takes place, all necessary measures must be taken to safeguard the processing of data by providing adequate guarantees and, if necessary, signing the standard contractual clauses in their latest approved version.

The AEPD published guidelines in 2018 for cloud computing service providers and for clients in order to resolve the doubts that may arise in terms of data protection in this type of relationship.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights Regulations on Artificial Intelligence and Big Data.

Although the concepts of big data and AI have different functionalities, they are closely related

in that both revolve around data. Thus, they share advantages, benefits and also risks.

On the one hand, AI constitutes the ability of a machine to exhibit the same capabilities as humans, allowing learning or problem solving for specific purposes. On the other hand, big data refers to the set of technologies that are used to collect and process massive amounts of data and extract valuable information through advanced analytical systems.

There has been an undeniable tremendous rise of AI and big data in recent years in all areas, thanks to the rapid evolution of technology. This has allowed the application of both technologies to a large number of sectors with fascinating results.

However, the use of intelligent systems can in turn entail enormous risks for human beings and even violate their fundamental rights.

For all the above, the public authorities have accelerated normative and institutional development to promptly control this phenomenon and make the most of all the benefits that these technologies offer, as well as to protect the individual, who must always be located at the centre of digital law, as the EU has stated in its recent regulations and those in development.

Specifically, in terms of AI, regulation is prolific both at EU level and in Spain, although currently only soft law instruments exist. In any case, every attempt at regulation is accompanied by the arduous task of trying to balance conflicting interests. On one side are the interests of technology companies in developing their systems with the fewest obstacles possible, and on the other side are those of the public authorities that, despite their interest in technological progress,

must also ensure the protection of the fundamental rights of their citizens.

EU Regulations

In April 2021, the Commission presented a proposal for a regulation that will be known as the Artificial Intelligence Act (AI Act). As pointed out above, this regulation is aimed at encouraging the development of AI by promoting investment and innovation and, in turn, focuses on the risks that this entails in order to achieve safe AI that respect fundamental rights.

Previously, several studies and guidelines had aimed to reflect on AI from an ethical perspective. Such is the case of the Ethical Guidelines for a reliable AI, of 2019, endorsed by the European Commission, or the study of the European Parliament Research Service (EPRS) entitled “European framework on ethical aspects of artificial intelligence, robotics and related technologies: European added value assessment”. Subsequently, in February 2020, the European Commission published the White Paper on Artificial Intelligence, and the European Parliament published the Resolution of 20 October 2020 containing recommendations on ethical aspects of artificial intelligence, robotics and related technologies.

In the field of insurance, the EIOPA published in 2021 “Artificial Intelligences Governance Principles: Towards Ethical and Trustworthy Artificial Intelligence in the European Insurance Sector”, with the aim of ensuring responsible and safe use of this technology within the insurance market.

In any case, all that exist so far are soft law instruments, which are not binding. The AI Act is here to change this and is the result of the EU's claim to leadership in the regulation of AI

worldwide; it is one of the essential milestones of its Digital Agenda.

The text proposed by the Council to define AI limits this definition to systems developed through machine learning and strategies based on logic and knowledge.

Four categories of IA systems are established:

- minimal risk;
- low risk;
- high risk; and
- unacceptable risk (which are prohibited).

Therefore, it is the high-risk systems that draw the focus of this rule as they can potentially pose the greatest threats to fundamental rights.

Indeed, certain sectors require the creation of a register for high-risk systems and the regulation of additional requirements for their users; however, the possibility that this would delimit the use or development of AI makes it difficult to include such provisions in the final text of the Regulation.

In order to ensure compliance with the provisions contained in the future AI Act, the regulation is completed with a strong system of fines and penalties. However, no specific mechanisms are included to protect possible violations of fundamental rights.

With all the above, on 6 December 2022 the Council laid the groundwork for “trilogue” dialogues between the Council of the EU, the European Parliament and the Commission on the proposal for the AI Act.

Finally, it should be noted that on September 2022 the Commission submitted a proposal for

a Directive on adapting non-contractual civil liability rules to AI (known as AI Liability Directive). It provides for new rules on disclosure of information and burden of proof in proceedings for claims for damages caused by AI systems. This regulation delves into an issue as important as liability for fault or negligence in the claims indicated and represents a new advance in the package of measures planned by the EU for the regulation of AI, which is completed by the proposal to revise the Directive of 25 July 1985 on liability for damage caused by defective products.

All of this is intended to adapt the rules on product liability, as well as the non-contractual civil liability regime, to the digital age and, in particular, to AI.

Spain

Spain has also taken the development of new technologies very seriously and, with regard to AI, has adopted several regulatory measures with the aim of becoming one of the pioneer countries in the regulation of digital aspects.

In 2019, the Spanish Strategy for I+D+I in AI was approved, as was the Digital Strategy for Artificial Intelligence (ENIA) in 2020, within the framework of the Digital Spain 2026 Agenda, in order to facilitate the development of inclusive, sustainable and citizen-centred AI.

Some of the measures that are provided for and have already been implemented are the creation of the Data Office and the figure of the Chief Data Officer (who has already been appointed), as well as the implementation of the Artificial Intelligence Advisory Council. In addition, the Spanish Agency for the Supervision of AI will soon be created, with headquarters located in A Coruña, and all of this in compliance with the

provisions of the Recovery, Transformation and Resilience Plan (*Plan de Recuperación, Transformación y Resiliencia* – PRTR).

In addition, the previously revised Digital Rights Charter of 2021 includes a specific section on AI rights.

Article 23 of Law 15/2022, of 12 July 2022, comprehensive for equal treatment and non-discrimination, is the first inclusion in a Spanish Law of a specific provision on AI for the purposes of establishing mechanisms so that the algorithms used by public administrations consider non-discrimination, transparency and accountability, where technically feasible. To this end, impact assessments should be carried out. It also calls for the promotion of ethical AI that respects fundamental rights. In addition, a seal of quality of algorithms, still pending regulatory development, will be promoted.

Finally, in June 2022, the government of Spain and the European Commission presented a project to implement the first EU regulatory sandbox on AI. The objective is the joint definition by the competent authorities and companies developing AI of the best practices that should serve as a basis for the implementation of the future AI Act.

Legal Aspects on AI and Big Data

Although, as indicated, there is a great interest at both EU and domestic level in effectively regulating AI, the truth is that today the legal conflicts that may arise as a result of the use of AI and big data must be resolved by resorting either to common national law in civil matters, commercial or criminal, or to sectoral legislation that regulates industrial and intellectual property, data protection or business secrets, among others.

However, we have seen that there are already several initiatives that touch on aspects as varied as product liability or the protection of fundamental rights against the interference of new technologies.

It is undeniable that both AI and big data seriously endanger privacy, even more so with the development of neurotechnology by big technology multinationals. Thus, the implications in the field of data protection are unquestionable and, in any case, the provisions of the RGPD and the LOPDGDD must be complied with.

For example, referring to big data, profiling is one of its main uses, which may involve certain risks linked to discrimination for possible data processing based on predictions. In addition, it is necessary to bear in mind the practical difficulty posed by the existence of future uses of the data not foreseen at the time of its collection and for which the user's consent is not granted.

Difficulties also arise in data sources and data reuse. An assessment of the risks and even a data protection impact assessment will have to be carried out and the data will have to be anonymised. In the end, any project involving AI and big data must respect the principle of accountability and be developed by default and by design.

In any case, the data shall be processed lawfully, fairly and in a transparent manner, and the data subjects must be duly informed about the processing of their data. In this respect, the AEPD has published a code of good practices in data protection for big data projects.

Many privacy situations may arise regarding data treatments as common today as those involving the so-called web scrapping techniques that,

wrongly relying on access to data from public sources, skip the obligations derived from the data protection regulations. All this must be aligned with the Data Governance Act (Regulation (EU) 2022/868, published in the OJEU on 3 June 2022), which establishes mechanisms for the re-use of certain categories of publicly/held protected data.

The extraction of information from websites may also entail intellectual property risks where those pages are protectable, and copyright can be invoked. The European Network and Information Security Agency (ENISA) identified in the report big data security, the different digital and cybersecurity threats for big data projects. This reinforces the transversal importance of cybersecurity in terms of AI and big data, so that the application of the regulations in this matter cannot be ignored.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection IoT and its Main Implications

On 16 September 2014, the Article 29 Working Party (now the European Data Protection Board) issued an opinion on the evolution of IoT and defined it as the infrastructure in which multiple sensors embedded in common devices record, process, store and transfer data and interact with other devices or systems, making use of its network connection capabilities.

From a data protection perspective, it should be noted that on 3 December 2020, the AEPD published an explanatory article with the implications that IoT devices could have in terms of data protection. Thus, according to this guide, there

are multiple actors involved in the processes linked to IoT devices (manufacturers, developers, cloud computing providers, telecommunications operators and social networks, among others).

Each of these agents may adopt the role of controller or processor, and, based on this, they must assume the obligations provided for each figure in the applicable data protection regulations.

Likewise, the categories of data subject to processing will be diverse, including contact data, internet usage habits, geolocation, physiological data, images, voice, and many more.

IoT devices can process not only data directly captured or provided by the user itself, but also inferred data, which is obtained from the analysis and processing of a large volume of data from various users through the use of technologies such as big data and AI.

All this can pose serious privacy risks since certain devices are able to capture habits and behaviours in an extremely detailed way, to such an extent that any hint of privacy disappears completely and the legal basis that legitimises the processing of data is completely blurred.

This is especially worrying in cases of voice-controlled devices, which can capture conversations totally unrelated to their use.

Also relevant is the incipient rise of home automation IoT devices that allow control of different elements of the home, such as air conditioning, lighting or blinds. There is already an increasing tendency to connect these devices directly to the manufacturer's cloud, which will be accessed through an app, using 5G technol-

ogy. This will imply new challenges in terms of privacy protection.

In any case, in the absence of specific regulation, and without prejudice to the provisions below, common Spanish Law must be resorted to in order to resolve possible conflicts arising from the application of the IoT, although most attention must be paid to the EU and Spanish regulations on data protection. Especially relevant are Articles 21 and 22 GDPR relating to the right to object to data processing and automated decision-making, including profiling.

IoT Regulations

The complexity derived from IoT devices has been addressed, from the most technical point of view, from the regulation of cybersecurity. It has already become clear that any vulnerability in IoT devices can jeopardise the privacy of users, so it makes perfect sense that cybersecurity stands as the key element in protecting the rights of users of IoT devices.

Thus, in the EU, special mention should be made, on the one hand, to the NIS 2 Directive regarding network and information security, which is applicable to IoT devices, and on the other hand, to the proposal of the Cyber Resilience Act, given that it will include a regulation on cybersecurity requirements for products with digital elements to ensure more secure hardware and software products.

In Spain, the approval of Royal Decree-Law 7/2022, of 29 March, on requirements to guarantee the security of fifth-generation electronic communications networks and services, is essential for the regulation of IoT. 5G technology will be crucial for the connectivity of IoT devices.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Legislative Overview

The emergence of new forms of audiovisual content consumption led to a review of the regulation of audiovisual media services within the EU, which resulted in the approval of Directive (EU) 2018/1808, of 14 November 2018, published in the OJEU on 28 November 2018. This Directive lays down EU-wide media content rules for the provision of audiovisual media services, including traditional television broadcasts, on-demand services and platform video sharing (also known as Audiovisual Media Services Directive).

The application of this regulation aims to strengthen the safety of viewers and, to this end, for example, the regulation referring to illegal content is extended to include video-sharing platforms. It also includes measures for the protection of minors and disabled persons and encourages the adoption of codes of conduct to limit the advertising of unhealthy products intended for minors.

The Directive establishes the country of origin principle, according to which audiovisual media service providers are subject to the law and jurisdiction of the member state in which they are established.

It was transposed belatedly into the Spanish legal system by virtue of the recent Law 13/2022, of 7 July (General Law on Audiovisual Communication), and part of its most relevant content is summarised in the following points.

- Protection of children and teenagers from inappropriate content. Providers must offer an age-rating system. Thus, content not recom-

mended for children under 18 can only be broadcast between 10pm and 6am.

- Besides the television activity, it covers payment platforms in streaming and video sharing services through platforms and users of special relevance (so-called influencers), as long as they are established in Spain. As a result, platforms such as Netflix, HBO or Amazon Prime are not affected by this law.
- All the above-mentioned subjects must:
 - (a) be registered in the state registry of audiovisual communication service providers (regulations on which are still pending);
 - (b) include systems to verify users' ages;
 - (c) establish mechanisms to rate content according to age; and
 - (d) include a functionality for users who upload videos to declare whether they contain advertising.
- Subliminal advertising, tobacco and electronic cigarettes, as well as advertising that violates human dignity is prohibited.
- The advertising of esotericism or gambling, as well as alcoholic beverages, may only be carried out in certain time slots.
- Advertising is generally limited to 144 minutes between 6am and 6pm, and to 72 minutes between 6pm and 12am.
- The European audiovisual work is promoted by reserving certain percentages for its broadcasting.
- The production of audiovisual works by women is encouraged, as well as the promotion of co-official languages in Spain.

Influencers

As noted above, the new Spanish regulation includes certain obligations for users of special relevance who use video-sharing platforms.

The European Regulators Group for Audiovisual Media Services (ERGA) includes in the definition

of vlogger, content creators, streamers, influencers, or video sharing platforms.

Video sharing platforms (eg, Instagram) are those that:

- offer the general public content created by the users themselves;
- do not have editorial responsibility for such content;
- their aim is to inform, entertain or educate;
- are offered through electronic communication systems; and
- the content is organised mainly by algorithms.

That said, the users of special relevance (influencers) of video sharing platforms must meet the following requirements:

- the service they offer is an economic activity;
- they assume editorial responsibility for their content;
- they have educational, entertainment or informational purposes; and
- they have a significant number of followers or users.

Once the above requirements have been met, they must comply with the aforementioned obligations provided for in the Spanish General Law on Audiovisual Communications.

Requirements for the Provision of Audio-Visual Media Services

The provision of television and radio communication services requires, prior to the start of the activity, responsible declaration before the competent audiovisual authority in Spain (the Ministry of Economic Affairs and Digital Transformation). The service may be provided as soon as such declaration is filed without prejudice to the supervisory powers of the competent authority.

The provision of television and radio communication services by means of hertzian waves requires a prior licence granted by means of a public tender. This licence shall be accompanied by a concession for the exclusive use of the public radioelectric domain.

To be a licensee, one of the following conditions must be met:

- to have nationality of a member state or a state that recognises this right to Spanish legal persons;
- to have a registered office in a member state or in a state that recognises this right to Spanish legal persons; and
- to have a representative domiciled in Spain for notification purposes.

Licences shall be granted for a period of 15 years, automatically renewable for successive periods of equal duration if the holder has been fulfilling the requirements to be the holder of said licence and provided that there is no third party who, under certain conditions, intends to grant the same licence.

The provision of the video sharing service through platforms, including influencers who make use of these services, should only be registered in the State Register of Audiovisual Communication Service Providers, once it is put into operation, without prejudice to complying with the rest of the general obligations already explained above.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

General Regulatory Framework

The regulation of telecommunications in Spain is given by Law 11/2022, of 28 June (General Telecommunications Law), which entered into force on 30 June 2022. This regulation is the result of the transposition of Directive (EU) 2018/1972 of 11 December 2018, establishing the European Electronic Communications Code, which was part of a telecommunications laws package that included the creation of the Body of European Regulators for Electronic Communications (BEREC).

One of the main objectives of the Spanish General Telecommunications Law is the massive deployment of 5G networks, and it includes the new classification of electronic communications services provided for in the Directive, which distinguishes between:

- internet access services;
- interpersonal communications services (both number-based and number-independent); and
- services consisting of the conveyance of signals.

Over the Top

As for number-independent interpersonal communications services, ie, without public numbering resources assigned, there is the so-called OTT (over the top), whose services are provided by means of data transmission over third-party networks. This is, for example, the case of some social networks that integrate messaging services. Although OTTs are not legally considered as operators, they must first communicate their intention to provide services.

The law provides for certain obligations for OTTs, which obviously also apply to other operators, among which we can highlight the following:

- communicate the start of its activity to the Registry of Operators, whose management corresponds to the CNMC;
- comply with the obligations to provide information to the authorities;
- ensure the rights of end users; and
- adopt the necessary measures for the management of security risks.

General Requirements

Regarding the requirements for the provision of networks and electronic communications services, it is established that it may be carried out by natural or legal persons who are nationals of any country belonging to the EEA or of any other nationality when so established by international agreements.

Those interested parties must previously notify the Register of Operators of the start of their activity and submit to the conditions provided for the specific service they wish to provide. If the content of the notification does not meet the requirements, the service shall be refused. However, bear in mind that this does not apply to OTTs, which will only have to communicate the start of their activity to the Registry of Operators for purely statistical purposes.

In the development of its business, the operator should comply with any obligations regarding consumer protection rights and transparency, as well as respecting fundamental rights and freedoms.

The resolution of conflicts between operators in the Spanish market will be resolved by the CNMC. The resolution of certain cross-border

disputes shall be carried out with the intervention and opinion of BEREC.

Telecommunications Equipment

Telecommunications equipment placed on the market must comply with the legally required specifications, in accordance with the conformity assessment procedures to be established. Certain cases of mutual recognition are foreseen where the conformity of equipment has been assessed in accordance with the essential requirements of another member state. Equipment requiring concessions, permits or licences may be put into service only when it has obtained such ratings. The surveillance of the market for telecommunications equipment and its adequacy will be the responsibility of the Spanish Secretary of State for Telecommunications and Digital Infrastructures.

Installers of telecommunications equipment (and those who assume its maintenance) must submit to the Registry of Telecommunications Installation Companies a responsible declaration on compliance with the requirements for the exercise of said activity, prior to the start of it.

Use of the Public Radio Domain

The common use of the public radio domain shall not require any enabling title. The special use of the public radio domain is carried out of the frequency bands enabled for its exploitation in a shared way, without limitation of number of operators or users. The private use of the public radio domain is carried out through the exclusive exploitation or by a limited number of users of certain frequencies in the same physical area of application.

The enabling titles by means of which rights of use of the public radio domain are granted will take the form of general authorisation, individ-

ual authorisation, administrative affectation or concession. The granting of rights of use of the public radio domain will take the form of general authorisation in cases of special use of frequency bands.

The general authorisation will be understood to be granted without any further formalities than the notification to the Spanish Secretary of State for Telecommunications and Digital Infrastructures, without prejudice to the obligation to pay the corresponding fees.

Individual authorisations shall be granted for use by radio amateurs or for private use for self-provision. For the rest of the cases not contemplated above, an administrative concession will be required. The duration of the enabling title will depend on each case.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges Regulatory Framework

Technology contracts are commercial contracts that make specific reference to the use and implementation of new technologies. They often pose a challenge for the consumer or small non-specialist business as they are faced with highly technical documents imposed by large technology companies that offer no room for negotiation.

For all the above, it is important that the client takes into consideration certain crucial aspects before formalising the contract.

Technology contracts do not find a specific regulation in the Spanish legal system, so it will be necessary to resort to common Spanish

law, mainly the Civil Code and the Commercial Code, depending on whether both parties are merchants, or the client is a consumer, in which case the provisions of the General Law for the Defence of Consumers and Users will apply.

Pre-formulated Standard Agreements

Pre-formulated standard agreements (*contratos de adhesión*) acquire special relevance in the framework of technology. These are contracts in which there is an imbalance between the parties so that one party imposes the conditions that will govern the contractual relationship on the other, as the weak party has little or no negotiating capacity to refute the provisions of the document imposed on them.

In these cases, the content of the contract is integrated almost entirely by general conditions of mass traffic and, in accordance with the provisions of both the Spanish General Law for the Defence of Consumers and Users, and the Spanish Law on General Contracting Conditions, the unfair clauses that may be included in such contracts will be null and void when contracted with a consumer.

Main Challenges

The formalisation of technology contracts involves risks for the client that must be detected and, if possible, neutralised. Furthermore, it is advisable that the client has at least a minimal knowledge in this area so as to avoid unexpected occurrences.

In addition, on many occasions the contract will ultimately be reviewed by a legal advisor prior to signing (or at least that would be desirable). This implies that lawyers must be very aware of the particularities of this type of contract, and they must also have knowledge, even if it is basic, regarding the object of the contract. This means

that professionals in the legal sector have to be increasingly familiar with technological concepts in order to be able to advise correctly their clients in this growing sector.

Main features on Technology Agreement

As indicated, there are no specific provisions in the Spanish legal system for this type of contract. However, they contain certain clauses that are usually repeated or that should exist. It is important to focus on these clauses as they can complicate the execution of the contract. These clauses include the following.

- The duration of the contract and its rollover.
- The price and its possible future revisions.
- The causes of termination and the periods of notice.
- The processing of personal data. This point acquires special relevance in certain services that involve massive access to personal data. It will be necessary to analyse in each case whether it is also appropriate to sign a contract for data processing, as provided for in Article 28 of the RGPD, or if international data transfers will take place, in which case the relevant measures must be adopted.
- The liability assumed by each of the parties. In particular, it is highly advisable to clearly indicate whether the providers are subject to a best-efforts obligation or a performance obligation where the client is seeking for specific results.
- It is common to include a service level agreement (SLA) that details in depth the object of the provision and the quality standards.
- The intellectual property of the software or deliverables.
- Confidentiality obligations.
- Technical specifications, which are usually accompanied in the form of an annex.

- Penalties for non-compliance. In this sense, it is common for the provider to limit its liability economically and, in addition, exclude certain concepts such as loss of profits or indirect damages. It will be necessary to check if these limitations prevent the correct compensation of the client for the damages that may be caused.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Regulations Currently in Force

The use of electronic signatures is becoming more and more common, and contracts are increasingly being signed online for basic needs, such as buying food or clothes, or to interact with the public administration. This creates the need for electronic signature methods that generate trust among users, way beyond the simple insertion of the scanned handwritten signature.

The EU responded to this need with the approval of EU Regulation 910/2014, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market (known as eIDAS). In Spain, it finds its legal equivalent in Law 6/2020, of 11 November, regulating certain aspects of electronic trust services, which complements the eIDAS Regulation only in those aspects that have not been harmonised at European level and that must be developed by each of the member states.

The eIDAS Regulation distinguishes between the electronic signature, the advanced electronic signature and the qualified electronic signature.

We will distinguish each of the aforementioned types of signatures depending on whether it allows us to identify the signatory with certainty, security regarding the possible manipulation of the content of the contract or the technical means required for its use.

- The electronic signature is an electronic signature which, for example, consists of accepting payment and the terms and conditions in any online purchase. It is the simplest type of signature since no electronic certificate or physical devices are needed to sign. Just “click”. In this case, the real identity of the signatory is not verified, so this method offers fewer guarantees.
- As for the advanced electronic signature, it is one that meets certain technical requirements, specifically, those provided for in Article 26 of the eIDAS Regulation. An example is the biometric signature, which collects the graphics of a handwritten signature on a touch device that stores biometric data and closes with a time stamp that prevents subsequent modifications of the document.
- Finally, the qualified electronic signature is a type of advanced electronic signature created by means of a qualified device for the creation of electronic signatures which is based on a qualified electronic signature certificate. It is used, for example, in relations with public administrations. It provides the maximum legal guarantees and has a legal effect equivalent to that of a handwritten signature.

Both the advanced and qualified electronic signatures allow the signatory to be identified, prevent subsequent modifications of the document in question, display full legal effects and are admissible as evidence in judicial proceedings.

Devices qualified for the creation of electronic signatures shall comply with certain security requirements. Commission Implementing Decision (EU) 2016/650 of 25 April 2016 publishes a list of standards for the safety assessment of such devices.

Spanish legislation, on the other hand, applies to public and private providers of electronic trust services established in Spain and to those with a permanent establishment who are not supervised by the authority of another member state. The legislation regulates certain aspects, some of the most relevant of which are the following.

- Electronic certificates, for the period of validity shall not exceed five years. Legislation also describes the circumstances for verifying the identity of the signatory.
- Obligations of electronic trust service providers. They must be subject to the regulation on data protection and guard and protect the signature creation data. In addition, they must constitute a civil liability insurance for a minimum amount of EUR1,500,000, except if they belong to the public sector. Such insurance may be replaced by a bank guarantee.
- Liability regime. Certain cases of limitation of the liability of electronic trust service providers are included, for example, in cases of negligence on the behalf of the signatory in the preservation of their signature creation data.
- Information security obligations.
- Supervision and control. These tasks will be carried out by the Spanish Ministry of Economic Affairs and Digital Transformation.
- List of infractions and penalties.

The Future Digital Identity in the EU

In June 2021, a framework for a European Digital Identity was proposed by the EU to be made available to citizens, residents and businesses in the EU through a European Digital Identity Wallet.

To this end, a proposal for a Regulation amending the eIDAS Regulation was prepared. This proposal aims to ensure universal access to secure and reliable electronic identification and authentication, all through a personal digital wallet stored on the mobile phone.

The wallet shall be issued with an electronic identification system that complies with the “high” security level, all based on cybersecurity certification schemes that should provide a harmonised level of confidence in the security of the wallets. Thus, the Cybersecurity Act will be fully applicable to the Electronic Identity Regulation.

The proposed Regulation has a special impact, not only on cybersecurity, but also on the protection of personal data. Its articles include several references to the GDPR and ensure compliance with its principles by qualified trust service providers. In particular, reference is made to the obligation of member states to ensure the protection of personal data and to prevent user profiling.

“Trilogues” should now begin to reach agreement on the proposal for a regulation between the EU institutions.

Asensi Abogados is a boutique law firm specialising in the gaming and gambling sector. It represents and advises a large number of international gaming companies with interests across the Spanish and Latin American markets. The firm works for the largest online betting and casino operators, software providers, skill games operators, affiliates and payment solution providers, as well as land-based operators, slot-machine manufacturers and suppliers. Asensi Abogados has offices in Madrid,

Mallorca and Bogotá, and is part of the Spanish Digital Gaming Association (Jdigital). Its TMT practice focuses on digital challenges faced by its online gambling operators, such as data protection, digital markets, e-commerce or cloud computing. A team of two partners and nine associates operates in Spain, while the Colombian office is composed of one partner and three associates. Recent work carried out by the firm includes detailed advice for online operators in Spain.

Author



Marina Villalonga joined Asensi Abogados in October 2022 and she is leading the M&A and corporate department as well as the TMT and data protection area. She graduated in law in

2007 and she has worked for top-tier firms within the corporate department, advising both national and international companies. Marina has wide expertise in M&A, contractual law, insolvency and tourism law. She is a qualified lawyer in new technologies, e-commerce and data protection, and has worked as a data protection officer for many entities.

Asensi Abogados

Av. Jaume III, nº 1, 1º
07012
Palma de Mallorca
Balearic Islands
Spain

Tel: +34 971 90 92 19
Email: contact@asensi.es
Web: www.asensi.es

A S E N S I
ABOGADOS

Trends and Developments

Contributed by:

Marina Villalonga

Asensi Abogados see p.465

Introduction

Spain has taken the development of new technologies and improving quality in telecommunications very seriously and, although a large part of the regulations governing these aspects come from the EU, it is true that many initiatives have been taken at national level aiming to lead the technological revolution in Spain's international neighbourhood.

Thus, for example, Spain has focused much of its efforts on the development and implementation of artificial intelligence for application by private companies and the public administration.

The wide deployment of 5G technology also deserves special mention, and in Spain the 3.58 GHz and 700 MHz frequencies have already been auctioned, putting Spain among the countries with the highest levels of 5G connectivity.

This high degree of connectivity, in combination with other features such as Spain's strategic geographical position, is leading to the exponential growth of data centres in the country, a sector that is experiencing record investment figures and is seeing significant growth forecasts. Several companies, such as Amazon or Google, have either already located their data centres in Spain or are planning to do so.

This article will consider two topical examples of national regulation of specific matters that have great practical application, either at present or in the near future. Discussion will firstly cover the issues arising from the digital heritage and its transmission after the death of its owner. The

second part covers the form in which crypto-asset advertising is regulated in the Spanish territory, awaiting approval of the corresponding regulation on crypto-assets by the EU.

The Digital Will

The inheritance of digital heritage

The internet has become an indispensable and fundamental tool for the development of multiple aspects of our professional, academic and personal lives. We interact on social networks, send and receive files (music, photographs, news, etc), use email, post blogs, access forums, and more.

People's interaction with digital environments generates an enormous amount of information that accumulates throughout their lives and becomes part of the legacy of each person when they die. Such interaction results in the creation of digital identities, which is nothing more than the projection of our personalities in cyberspace.

The EU is no stranger to this reality and is therefore already working on the future European Digital Identity through a European Digital Identity Wallet, which will be stored on mobile phones. The wallet shall be issued with an electronic identification system that complies with the required high level of security; it may be used for both online and offline public and private services across the EU, such as opening a bank account, filing tax returns, renting a car or applying for a bank loan.

This implies that the factors that shape our digital identity today will increase in the coming years, as a large part of people's lives will be

managed through digital means. Therefore, what happens to an individual's digital data when they pass away is becoming concern.

As a starting point, it must be noted that digital identity as such does not integrate inheritance, but defence of the digital identity corresponds to the heirs based on the actions for the protection of the honour, privacy and image of the deceased person provided for in the Spanish Organic Act 1/1982, of May 5 of civil, on civil protection of the right to honour, personal and family privacy and self-image. In addition, Article 3 of the Spanish Organic Law on Data Protection and guarantee of digital rights (LOPDGDD), which transposes the EU General Data Protection Regulation, regulates the right of access, rectification or deletion of data of the deceased by the persons related to them (spouse, steady partner, ascendants, descendants or heirs), who may contact the data controller or the data processor to communicate the death, for the purpose of protecting the memory of the deceased.

However, and beyond the formation of a digital identity, the truth is that interactions on the internet also result in the conceptualisation of a digital heritage that is integrated by the information we send or receive, or information that which we store in the cloud. This includes aspects as diverse as ebooks, sound files, rights on music or audio-visual platforms, balances in electronic purses, cryptocurrencies, or online purchases pending delivery, among many others.

Digital heritage does have a place in inheritance and is capable of economic quantification, although the quantification proceedings can come with several complications. Thus, digital assets can be ordered through the granting of what is called a digital will. However, this term should not cause confusion. The digital will is not

a will formalised online through digital platforms; it is a document that orders the succession of digital heritage, which has already been defined. The Spanish legal system only allows the granting of a will before a public notary and never through digital means, so there is no specific means to order the succession of digital patrimony beyond the explicit provisions that may be included in the will.

Applicable regulations

In Spain, the legislature of Catalonia was a pioneer in regulating this phenomenon before any country in the EU. It did so through Law 10/2017, of 27 June, on digital wills. This rule provides that people can express their digital wills so that the heir (or the person designated for that purpose) acts before the digital service providers where the testator had active accounts after their death (or in circumstances of judicially modified capacity), promoting provisions that determine the way to handle one's presence in digital environments in the event of death. In the absence of a will, a specific document of digital wills may be granted to regulate these aspects.

Digital wills may instruct the designated person to:

- communicate the death to digital service providers;
- request digital service providers to cancel active accounts; or
- request service providers, if appropriate, to deliver a copy of the digital files stored on their servers.

The aforementioned Catalan law also regulated the creation of an electronic registry for digital wills, so that persons with a legitimate interest could determine the existence of a digital will document. However, the creation of such regis-

try was declared null and void and against the Spanish Constitution on the grounds that the competence for the establishment of registers lies with the State. This being the case, it should be the central government that takes the initiative for the creation of this registry for the whole country, which would be desirable in view of the growth in importance of digital wills that is expected in the coming years.

In any case, the relationship between digital assets and the protection of personal data is undeniable since, as noted above, one of the most common provisions of the digital will is the regulation of access by heirs to the accounts and digital profiles of the deceased.

Thus, it is logical that Article 96 of the LOPDGDD regulates the right to a digital will, which must be construed as a reinforcement of the provisions of the aforementioned Article 3 of the LOPDGDD. This precept empowers those related to the deceased, heirs or executors to contact the digital service providers in order to access the information and give the appropriate instructions regarding said information according to the will of the deceased embodied in their digital will. It should be noted that Article 96 is the only provision that contains a reference to the digital will and applies to the entire Spanish territory.

Difficulties and challenges

Although the regulations presented are concise, the truth is that the digital heritage faces a wide range of problems and issues that hinder the implementation of the succession of digital heritage and are resolved as the need arises.

Thus, for example, where the deceased is the holder of cryptocurrencies, they must ensure that their heirs know of its existence, as well as the access codes; in the absence of a regis-

try that the heirs can consult, they may not be aware of the assets if they have not been previously informed of them or if they have not been expressly identified in the will. Likewise, since they are not legal tender, they must be converted to calculate their value in the inheritance.

In relation to emails, there is a personal contract between the account holder and the service provider. Therefore, the account will not be transferable and, of course, the heir will not be able to send emails from the address of the deceased. However, the heir must be able to access the content of the emails for the sole purpose of verifying whether content with patrimonial relevance capable of forming part of the inheritance has been transmitted (whether sent or received). For such access, a court order will be required.

Social networks with profiles that, like email, cannot be transmissible may be used for the exchange of content that is eligible for protection under intellectual property laws. In this case, the heirs must be able to access information with patrimonial content but not the personal data of the account profile. Profiles can be closed or kept active to honour the memory of the deceased. In any case, it is becoming clear that some kind of intervention is needed, as the number of active profiles corresponding to deceased people is increasing exponentially.

For influencers and people with YouTube channels that generate income, digital inheritance acquires a particularly relevant role.

Another difficulty to be faced relates to the identification of and access to the multiple and changing profiles of the deceased after the digital will has been granted. Many profiles are created under pseudonyms, which makes it difficult to identify the person behind them.

Consider also that passwords may be changed without the knowledge of the heirs. For all of the above reasons, it is necessary to establish mechanisms that, based on blockchain technology, allow interested parties to consult existing profiles and request passwords. Some of these problems could be solved if social networks were to require digital identification for the creation of profiles, in connection with the above-mentioned European Digital Entity.

Anyway, casuistry is endless, and every day new issues arise that require a legal solution (eg, purchases that have not yet been received, accounts on online gaming and gambling sites or contracts for SaaS services). Additionally, although there is no great urgency with regard to this subject because digital heritage is mainly held by people who are not of testing age, it is highly probable that the interest in regulating digital inheritance will grow significantly as a great part of our assets become digital.

The Advertising of Crypto-Assets

The growing presence of crypto-assets in the financial market is an incontestable reality and, although it opens a window for opportunities, the current scarcity in terms of regulation poses a risk for investors who decide to opt for these assets because they are still not adequately protected.

There are many small non-professional investors who enter the cryptocurrency market without having sufficient information as to the risks involved in these investments, including their complexity, volatility and potential lack of liquidity.

It cannot be ignored that the phenomenon of social networks and influencers affects users who are carried away by the financial recommendations of those who use these platforms

to promote this type of investment without the necessary knowledge and training.

In order to fight the legal uncertainty that still surrounds transactions involving crypto-assets, the EU is finalising, within the framework of its Digital Finance Package, the proposal for a Regulation on markets in crypto-assets (known as the MiCA Regulation), which results from its aim to develop and promote new technologies in the financial sector, particularly blockchain and distributed ledger technology (DLT). Thus, the MiCA Regulation defines crypto-assets as digital representations of value or rights and focuses mainly on:

- transparency and information requirements for their issuance and trading;
- the regulation applicable to crypto-assets providers;
- consumer protection rules; and
- the establishment of measures to ensure the integrity of markets in crypto-assets.

However, while waiting for the entry into force of the MiCA Regulation, the National Securities Market Commission (*Comisión Nacional del Mercado de Valores* – CNMV), the Spanish authority for supervising and inspecting the securities markets, published the Circular letter 1/2022, of 10 January in force since 17 February 2022, which focuses on regulating a very specific aspect of crypto-assets – their advertising.

Despite the specificity of its purpose, this rule is particularly relevant because it includes a definition of crypto-asset in the Spanish legal system for the first time. Specifically, it defines it as the digital representation of a right, asset or value that can be transferred or stored electronically, using distributed ledger technologies or similar technology.

As can be seen, both definitions, that of the MiCA Regulation and that of the Circular, are practically identical.

Scope of application of the Circular

Before entering fully into the regulation of the Circular regarding the requirements for the advertising of crypto-assets, it is worth mentioning the elements outside its scope of application. For this, it is important to be clear that crypto-assets are divided into different types, the following being some of the most relevant in the context of this article.

- Cryptocurrency – This is a digital medium of exchange that uses encryption to ensure ownership and the integrity of transactions.
- Security tokens – They grant their holder a right equivalent to a financial instrument, represent a property right or a share in a project, and allow holders to participate in future increases in the value of the issuer.
- Utility tokens – They are designed for a particular purpose and they grant their holders the right of access to a specific application, product or service through an infrastructure developed in blockchain. They are not accepted as a means of payment for other goods or services and, in general, are not issued as an object of investment.
- Non-fungible tokens (NFTs) – They represent unique assets and are not interchangeable with each other.

It should be noted that the Circular regulates advertising activity related to crypto-assets for investment purposes but excludes from its scope:

- security tokens (as they are considered financial instruments they are regulated in Circular 2/2020 of the CNMV on advertising of financial products and services);

- utility tokens;
- NFTs;
- white papers published for the issuance of certain crypto-assets;
- corporate advertising campaigns with generic information;
- presentations aimed solely at analysts or institutional investors;
- publications of independent financial analysts that are not sponsored or promoted; and
- advertising on seminars or courses on crypto-assets that are not offered free of charge or for a symbolic price and that do not encourage investment in them.

The exclusion criteria provided for in the Circular are broad and relatively generic, which could constitute a source of interpretative problems when it comes to discerning which products are or are not included in the scope of the regulation.

As for the subjects affected, the Circular will apply to:

- crypto-asset service providers that carry out advertising activities for crypto-assets;
- advertising service providers, including influencers; and
- anyone else who advertises crypto-assets.

For the Circular to apply, in addition, the advertising must be addressed to investors in Spain, regardless of the nationality or domicile of the provider. It is presumed that this is the case when it is done through physical means in Spain (including web pages and domains) and when the advertisements are made in Spanish or in any other official language of Spain.

Conditions for advertising activity

In general, advertising of crypto-assets in Spain, included in the scope of the Circular, must comply with the following conditions.

- It should use simple and easy-to-understand language, so as to be clear, unbiased and not misleading.
- Sponsored posts should clearly state this fact. For audio or videos, this must be indicated at the beginning.
- Information about the risks of the product must be included in a format or position that guarantees its relevance in the advertising piece. Where there are space limitations, a link to this information must be included.
- For mass advertising campaigns (ie, aimed at more than 100,000 people), prior communication to the CNMV will be required at least ten working days before their execution. Such communication must conform to the model for this purpose provided by the CNMV.
- The obliged subjects must keep a register with information on the current campaign and those that have been carried out in the last two years, which must be available to the CNMV for inspection, if required.

The application of the Circular and its effectiveness

As noted above, the Circular arises from the need to regulate certain aspects related to crypto-assets and, in particular, for the protection of investors until European regulations are passed.

Thus, the CNMV focuses its efforts on making potential investors aware of the risks linked to these assets. In August 2022, the Spanish authority published a study that revealed the current low penetration of crypto-assets as an investment object. However, the same study indicated that 40% of investors in cryptocur-

rencies believe that legal regulation exists in this regard, while 29% consider that the investment is not riskier than other assets. Only 17% of investors consider that the liquidity of cryptocurrencies is scarce. This is striking because these percentages indicate that the population most familiar with this type of investment is not aware of its real risks and its lack of regulation.

However, the truth is that the inclusion of the advertising warnings provided for in the Circular attracts the attention of more than half of the investors, many of whom decide to seek additional information about cryptocurrencies after such warnings.

Moreover, the CNMV, being aware of the weight and scope of the activity of influencers in social networks, has set its sights on them and the investment recommendations they issue while identifying themselves as experts in the field. Thus, these influencers are requested to include clarifications on their activity and are required to fully comply with the provisions of the Circular.

The new Securities Markets and Investment Services Act

Although it is not directly related to the advertising of crypto-assets, it is worth including a final note in relation to the draft of the new Spanish Securities Markets and Investment Services Act, the text of which was published on 12 September 2022.

It should be noted that this draft includes distributed ledger technology for the registration, clearing and settlement of negotiable securities and financial instruments. In addition, the relevant provisions are contemplated taking into account the forthcoming approval of the MiCA Regulation. In this sense, the CNMV is designated as the competent authority for the supervision of compliance with the MiCA Regulation.

Contributed by: Marina Villalonga, **Asensi Abogados**

Asensi Abogados is a boutique law firm specialising in the gaming and gambling sector. It represents and advises a large number of international gaming companies with interests across the Spanish and Latin American markets. The firm works for the largest online betting and casino operators, software providers, skill games operators, affiliates and payment solution providers, as well as land-based operators, slot-machine manufacturers and suppliers. Asensi Abogados has offices in Madrid,

Mallorca and Bogotá, and is part of the Spanish Digital Gaming Association (Jdigital). Its TMT practice focuses on digital challenges faced by its online gambling operators, such as data protection, digital markets, e-commerce or cloud computing. A team of two partners and nine associates operates in Spain, while the Colombian office is composed of one partner and three associates. Recent work carried out by the firm includes detailed advice for online operators in Spain.

Author



Marina Villalonga joined Asensi Abogados in October 2022 and she is leading the M&A and corporate department as well as the TMT and data protection area. She graduated in law in

2007 and she has worked for top-tier firms within the corporate department, advising both national and international companies. Marina has wide expertise in M&A, contractual law, insolvency and tourism law. She is a qualified lawyer in new technologies, e-commerce and data protection, and has worked as a data protection officer for many entities.

Asensi Abogados

Av. Jaume III, nº 1, 1º
07012
Palma de Mallorca
Balearic Islands
Spain

Tel: +34 971 90 92 19
Email: contact@asensi.es
Web: www.asensi.es

A S E N S I
ABOGADOS

Law and Practice

Contributed by:

Lim Chong Kin

Drew & Napier LLC see p.483



Contents

1. Metaverse	p.467
1.1 Laws and Regulations	p.467
2. Digital Economy	p.469
2.1 Key Challenges	p.469
3. Cloud and Edge Computing	p.471
3.1 Highly Regulated Industries and Data Protection	p.471
4. Artificial Intelligence and Big Data	p.473
4.1 Liability, Data Protection, IP and Fundamental Rights	p.473
5. Internet of Things	p.475
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection	p.475
6. Audio-Visual Media Services	p.476
6.1 Requirements and Authorisation Procedures	p.476
7. Telecommunications	p.478
7.1 Scope of Regulation and Pre-marketing Requirements	p.478
8. Challenges with Technology Agreements	p.480
8.1 Legal Framework Challenges	p.480
9. Trust Services and Digital Entities	p.481
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes	p.481

1. Metaverse

1.1 Laws and Regulations

At present, a patchwork of legislation is available to tackle issues relating to data protection, prevention of online harm, and digital assets in the metaverse.

Data Protection and Privacy

The Personal Data Protection Act 2012 (PDPA) is the primary legislation in Singapore that governs the protection of personal data by organisations. An “organisation” includes any individual, company, association or body of persons, corporate or unincorporated, whether or not they (i) are formed or recognised under the law of Singapore; or (ii) are resident, or have an office or a place of business, in Singapore. The PDPA will generally not apply to individuals acting in a personal or domestic capacity, employees acting in the course of their employment with an organisation, and any public agency in relation to the collection, use or disclosure of personal data.

Therefore, in the virtual world, organisations shall have to comply with the obligations set out in the PDPA. Some notable obligations include the consent obligation where, subject to exceptions, an organisation must obtain an individual’s consent before collecting, using or disclosing their personal data for a purpose and the protection obligation which requires an organisation to protect personal data in its possession or under its control by making reasonable security arrangements.

Section 48J of the PDPA provides that if an organisation fails to comply with the obligations under the PDPA, the Personal Data Protection Commission (PDPC) is empowered to impose the following financial penalties:

- in the case of a contravention by an organisation whose annual turnover in Singapore exceeds SGD10 million, the PDPC may impose financial penalties up to 10% of the annual turnover in Singapore of the organisation; and
- in any other case, the PDPC may impose financial penalties up to SGD1 million.

Online Harm

The Protection from Online Falsehoods and Manipulation Act 2019 (POFMA) aims to prevent the electronic communication of false statements of fact, suppress support for and counteract the effects of such communication and to safeguard against the use of online accounts for such communication and for information manipulation. Further, the Foreign Interference (Counter-measures) Act 2021 (FICA) empowers the Minister for Home Affairs to issue directions to various entities such as internet access service providers to help the authorities investigate and counter hostile communications activity that is of foreign origin.

With respect to the online safety of users, the Protection from Harassment Act 2004 (POHA) covers offences relating to the publication of personal information in order to harass, threaten or facilitate violence against a person.

When the Online Safety (Miscellaneous Amendments) Act 2022 (the “Online Safety Act”) comes into operation from 1 February 2023, the Broadcasting Act 1994 will be amended to contain measures that allow the government to improve online safety for users in Singapore, combat harmful content in online services accessible to users in Singapore, and empower users with the necessary information and tools to protect themselves from harmful or detrimental content.

The amended Broadcasting Act now contains provisions to regulate providers of Online Communication Services (OCS). OCS refer to an electronic service (or part of an electronic service) having the characteristics of a social media service, which may be provided in or from Singapore, or from outside Singapore. Such an OCS enables end-users to access or communicate content on the internet or deliver content to end-users. Under the amended Broadcasting Act, OCS with significant reach and impact in Singapore may be designated as Regulated Online Communication Services. The providers of such Regulated Online Communication Services has the duty to take all reasonably practicable steps to comply with applicable Codes of Practice and implement measures on their services to mitigate the risks of danger to Singapore users from exposure to harmful content and provide accountability to their users on such measures.

Further, under the amended Broadcasting Act, the Infocomm Media Development Authority (IMDA) is empowered to issue directions to deal with egregious content that can be accessed by Singapore users on an OCS. For instance, the IMDA may issue directions to an OCS provider to disable access by Singapore users to the egregious content on the service or to ensure that a specified account cannot continue to communicate to Singapore users. Moreover, the amended Broadcasting Act empowers the IMDA to issue directions to internet access service providers to block access by Singapore users to the non-compliant OCS if an OCS provider fails to comply with the IMDA's direction.

Digital Assets

Two types of digital assets are likely to play prominent roles in the metaverse: cryptocurrencies and non-fungible tokens (NFTs). Cryptocurrencies or NFTs may be regulated by the

Monetary Authority of Singapore (MAS) under the Payment Services Act 2019 (PSA) or the Securities and Futures Act 2001 (SFA).

Under the SFA, the offer or issue of digital assets such as cryptocurrencies or NFTs may be regulated if they constitute capital market products under Section 2(1). Capital markets products include any securities, derivatives contracts and contracts or arrangements for purposes of leveraged foreign exchange trading.

Digital assets which fall within the scope of digital payment tokens (DPTs) are subject to the regulatory regime under the PSA. The PSA defines a DPT as any digital representation of value that:

- is expressed as a unit;
- is not denominated in any currency, and is not pegged by its issuer to any currency;
- is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt;
- can be transferred, stored or traded electronically; and
- satisfies such other characteristics as the MAS may prescribe.

Subject to applicable exemptions provided for in the PSA, the PSA requires a person who carries on a business of providing a DPT service as defined under Part 3 of the First Schedule to the PSA (ie, dealing in DPTs or facilitating the exchange of DPTs) to apply for either a standard payment institution licence or a major payment institution licence.

On top of compliance with the PSA, licence holders must also take note and comply with the MAS's guidelines and notices such as the Guidelines on Provision of Digital Payment

Token Services to the Public. The MAS also intends to tighten the rules on cryptocurrency and has released a consultation paper on Proposed Regulatory Measures for DPT Services in October 2022.

In the metaverse, NFT trading is likely to become more commonplace and a part of transacting in the virtual space. While there is no legislation which specifically target NFTs, issues such as ownership continue to be governed by intellectual property and contract law principles. A contract for the purchase of NFTs usually contains three distinct subject matters which are capable of ownership by different people. The first is the code on the blockchain which may identify and authenticate the asset. The second is the asset itself. The third is the intellectual property rights in respect of the asset. The relevant intellectual property right is commonly copyright as most NFTs constitute a form of artistic expression that is afforded protection under the Copyright Act 2021 (CA). Therefore, contracts may include the assignment of copyright or a licence. Assignments of copyright must comply with the formalities stipulated in the CA and be in writing and signed by or on behalf of the assignor. However, this requirement can easily be met even in the virtual space through the application of the Electronic Transactions Act 2010 (ETA). See **9. Trust Services and Digital Entities** for more details on the ETA.

Furthermore, the law in relation to NFTs is evolving rapidly. Most notably, the Singapore High Court recently held that NFTs are property and can be subject to proprietary injunctions. With the growing prominence of NFTs, courts and legislation can be expected to explore and address complex and novel legal issues raised by NFTs in the upcoming years.

2. Digital Economy

2.1 Key Challenges

At present, a patchwork of legislation is available, including in relation to consumer protection, sale of goods and services, payment services and personal data protection.

Digital Payment Solutions

Under the PSA, providers of digital payment solutions (such as e-wallet services) may need to apply for either a standard payment institution licence or a major payment institution licence (see **1. Metaverse** (Digital Assets section)) if they offer the following services:

- account issuance service which involves issuing a payment account or any service relating to any operation required for operating a payment account;
- domestic money transfer service which involves providing a local fund transfer service;
- merchant acquisition service which involves accepting and processing payment transactions and payment receipts for and on behalf of a merchant; or
- e-money issuance service which involves issuance of e-money for persons to make payment transactions.

The PSA also imposes a stock and flow cap on personal payment accounts issued by major payment institution licensees to protect customers by limiting a customer's potential loss from the customer's account. Personal payment accounts issued by a MPI are subject to a load capacity of SGD5,000 and an annual transaction flow cap of SGD30,000. However, recognising that there may be changes in consumer behaviour, usage of e-wallets, and e-wallet business models in Singapore over time, the MAS

released a consultation paper on 18 October 2022 proposing amendments to the currently prescribed stock and flow cap. In the consultation paper, the MAS proposed to raise the stock cap to SGD20,000 and raise the flow cap to SGD100,000.

E-Commerce

Further, e-marketplaces and e-retailers should ensure that they conform with the Consumer Protection (Fair Trading) Act 2003 (CPFTA). The CPFTA applies where the consumer or supplier is resident in Singapore or where the offer or acceptance relating to the consumer transaction is made in or is sent from Singapore. Therefore, in the digital economy where cross-border transactions are the norm, the CPFTA will apply where this nexus to Singapore is established.

The CPFTA accords customers rights and prohibits sellers from engaging in unfair practices or selling defective goods. If a supplier engages in unfair practices such as making false representations, deceiving consumers or taking advantage of consumers in certain circumstances, the consumer may take legal action against them under the CPFTA. Additionally, where a good does not conform to the agreement between the parties, the consumer has a right against the supplier to demand repair or replacement of the good at the supplier's expense or alternatively, a price reduction or refund.

Moreover, in June 2020, the first national standard for e-commerce transactions, Technical Reference 76 (TR 76), was issued by Enterprise Singapore and the Singapore Standards Council. TR 76 serves as a practical reference for e-retailers and online intermediaries to build trust and transparency in online transactions. Recently, the TR 76 was revised to include additional anti-scam guidelines for e-retailers and e-commerce

marketplaces, to offer better protection for consumers transacting online.

The Competition and Consumer Commission of Singapore (CCCS) has also updated its guidelines in relation to digital markets. For instance, the CCCS Guidelines on Market Definition have clarified issues related to market definition that are particularly relevant in digital markets which feature multi-sided platforms. Notably, the CCCS provided the definition of a “multi-sided platform” as an undertaking acting as a platform that facilitates interactions between two or more groups of users and creates value for sellers or buyers on one side of the platform by matching or connecting them with buyers or sellers on the other side of the platform.

The PDPA strikes a balance between safeguarding consumer's personal data and commercial needs. Notably, while organisations are required to obtain the consent of individuals to collect, use or disclose personal data, the PDPA provides for exemptions to the consent obligation that may be useful to e-commerce providers. For example, the business improvement exception under the PDPA allows organisations to use, without consent, personal data for the purposes of:

- improving any goods or services provided;
- improving methods or processes for the operations of the organisation;
- learning the behaviour and preferences of the individual or another related individual in relation to the goods or services provided by the organisation; and
- identifying any goods or services provided by the organisation that may be suitable for the individual or another individual.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

There are limitations placed on organisations that seek to entrust certain processes or data to the cloud, although most of these limitations are in the context of personal data protection.

Applicable Laws and Guidelines

The main legislation governing the protection of personal data is the PDPA. “Personal data” is defined under the PDPA as data, whether true or not, about an individual who can be identified (i) from that data, or (ii) from that data and other information to which the organisation has or is likely to have access. The PDPA is administered and enforced by the PDPC.

There are cross-border data transfer restrictions in the PDPA. Under Section 26 of the PDPA, an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with prescribed requirements to ensure that the transferred personal data will be accorded a standard of protection that is comparable to that under the PDPA (the transfer limitation obligation).

The prescribed requirements, as set out in the Personal Data Protection Regulations 2021 (PDPR), require the transferring organisation to ensure that the recipient of the personal data is bound by legally enforceable obligations. These “legally enforceable obligations” include any laws in the jurisdiction to which the personal data is transferred, contracts, binding corporate rules (BCRs), and any other legally binding instrument.

BCRs may be used for recipients that are “related” to the transferring organisation (eg, a parent

company or subsidiary), whilst contracts may be used for data transfers to any party. In particular, the BCRs and contracts must specify the countries and territories to which the personal data will be transferred under the BCRs or contract.

In addition, under the PDPR, an overseas recipient of personal data is taken to be bound by legally enforceable obligations to provide comparable protection for the transferred personal data if it holds an Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules (CBPR) System or Privacy Recognition for Processors (PRP) System certification (which is granted or recognised under the laws of the country or territory to which the personal data is transferred). That said, transferring organisations that are seeking to rely on this transfer mechanism should ensure that they carry out the necessary due diligence to determine that the overseas recipient is indeed CBPR or PRP-certified under the laws of the country or territory in question.

Furthermore, the PDPC has published a chapter on cloud services in its non-legally binding Advisory Guidelines on the PDPA for Selected Topics which clarifies the application of the PDPA in respect of cloud services (the “Cloud Services Guidelines”). Specifically, an organisation should ensure that the cloud service providers (CSPs) that it engages only transfer personal data in accordance with the PDPA – namely, to locations with comparable data protection regimes – or otherwise has legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data.

Industry Standards and Codes of Conduct

The Multi-Tier Cloud Security (MTCS) Singapore Standard (SS584) is the primary local industry standard for determining the level of cloud security provided by CSPs. The MTCS has three

levels of security with Level 1 being the base standard and Level 3 being the most stringent standard. The adoption of the MTCS is voluntary for CSPs unless they are participating in bulk tenders for government procurement of public cloud services.

Per the PDPC's Cloud Services Guidelines, MTCS Level 3 certification could provide organisations assurance of the CSP's ability to comply with the protection obligation under the PDPA.

The PDPC has also published the 2018 Guidelines for Cloud Outage Incident Response (COIR) (TR 62:2018). Under the voluntary COIR framework, cloud service customers (CSCs) can choose appropriate outage protection measures that would complement their business continuity/discovery recovery capabilities through a set of guidelines which assist CSCs in identifying, evaluating and negotiating protection needs with CSPs to incorporate into their service-level agreements, and sharing of COIR practices by CSPs through the same set of common parameters.

While the adoption of the COIR guidelines is voluntary, CSPs are encouraged to self-disclose their service support capabilities with respect to service outages.

Sector-Specific Regulation

Apart from the PDPA and the Cloud Services Guidelines, the use of CSPs in the financial sector is subject to additional regulation by the sectoral regulator: the MAS. In this respect, the MAS has published guidelines for financial institutions (FIs) which set out its position on cloud computing and cloud outsourcing arrangements:

- Technology Risk Management Guidelines;

- ABS (Association of Banks in Singapore) Cloud Computing Implementation Guide 2.0;
- Guidelines on Outsourcing; and
- Advisory on Addressing the Technology and Cyber Security Risks Associated with Public Cloud Adoption.

In general, these guidelines provide guidance to FIs on maintaining data, infrastructure and network security; sound practices on risk management of outsourcing arrangements; and the use of cloud computing platforms. FIs are encouraged to conduct appropriate due diligence on CSPs and evaluate the risks before entering into a cloud outsourcing arrangement. The risk assessment should also be performed periodically on existing outsourcing arrangements, as part of the approval, strategic planning, risk management or internal control reviews of the outsourcing arrangements of the FI.

Specific Issues Regarding Personal Data Protection

The transfer limitation obligation under the PDPA requires the contract or BCRs to expressly state the locations to which the personal data may be transferred. However, in the context of a CSP cloud outsourcing arrangement, an organisation may have to agree to a CSP's standard contractual terms, which may include a term that confers discretion onto the CSP as to the exact jurisdictions to which personal data may be transferred.

According to the PDPC's Cloud Services Guidelines, in such a situation, the organisation may be considered to have taken appropriate steps to comply with the transfer limitation obligation if:

- the CSP based in Singapore is certified or accredited as meeting relevant industry

standards (such as MTCS Level 3 and ISO 27001); and

- the CSP provides assurances that all the data centres or sub-processors – in such overseas locations that the personal data is transferred to – comply with these standards.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

At present, there is no specific legislation regulating the use of big data, machine learning and artificial intelligence (AI) technologies in Singapore. However, various government and regulatory agencies have developed non-legally binding frameworks to provide industry guidance on these subjects.

Applicable Frameworks

Examples of these frameworks include:

- the PDPC's Model AI Governance Framework and its companion guide, the Implementation and Self-Assessment Guide for Organisations, which provide organisations with practical recommendations in implementing ethical principles and adopting responsible AI governance;
- the MAS's Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of AI and Data Analytics in Singapore's Financial Sector, which provides a set of principles for the use of AI in decision-making in the provision of financial products and services; and
- the MAS's Veritas Initiative, which assists FIs in evaluating their AI and data analytics solutions against the MAS's FEAT principles.

Notably, the PDPC's Model AI Framework represents the efforts of Singapore's policymakers and regulators to articulate a common approach, and a set of consistent definitions and principles in the governance of AI. Broadly, it sets out principles in four key areas, including the following.

- Internal governance structures and measures – organisations should ensure that there are clear roles and responsibilities as well as risk management and internal controls in place for the ethical deployment of AI.
- AI decision-making models – organisations should consider the risks of different AI models and determine the appropriate degree of human oversight based on the expected probability and severity of harm.
- Operations management – organisations should understand the lineage, provenance and quality of data used, as well as the transparency of algorithms chosen.
- Stakeholder interaction and communication – organisations should seek to build trust and maintain open relationships with individuals regarding the use of AI through general disclosure, transparency and policy explanations, and careful design of human-AI interfaces.

Furthermore, on 25 May 2022, the IMDA and PDPC launched A.I. Verify, which is the world's first AI governance testing framework and toolkit for companies that wish to demonstrate responsible AI in an objective and verifiable manner. Developers and owners can verify the claimed performance of their AI systems against a set of principles through standardised tests. A.I. Verify packages a set of open-source testing solutions together, including a set of process checks into a toolkit for convenient self-assessment. The toolkit will generate reports for developers, man-

agement, and business partners, covering major areas affecting AI performance.

In 2018, the Advisory Council on the Ethical Use of AI & Data was established to advise the government on ethical, policy and governance issues arising from the use of data-driven technologies in the private sector and to support the Government in providing general guidance to businesses to minimise ethical, governance and sustainability risks, and to mitigate adverse impact on consumers from the use of data-driven technologies.

Autonomous Vehicles

In the context of autonomous vehicles (ie, self-driving cars), the Road Traffic (Autonomous Motor Vehicles) Rules 2017 provide that the trial or use of an autonomous motor vehicle on any road is prohibited unless specific authorisation is obtained. Parties wishing to do so must submit an application to the Land Transport Authority (LTA) stating matters such as the trial's objectives, the type of autonomous vehicle to be used and its intended purposes. The LTA has the discretion to accept or reject the application and/or impose conditions.

Fake News

In the context of fake news and misinformation, POFMA was enacted to, amongst other things, prevent the electronic communication in Singapore of false statements of fact. Notably, POFMA prohibits the making or alteration of an automated computer program (ie, an AI "bot") with the intention of using it to communicate or enabling any other person to communicate a false statement of fact in Singapore (Section 8, POFMA).

Data Protection

The collection and use of large datasets for big data analytics, machine learning and AI may trig-

ger data protection concerns, especially where such data sets involve personal data (see 3. **Cloud and Edge Computing** for the definition of personal data). Moreover, it is not uncommon for AI systems to utilise data mining solutions to obtain data from third-party sources, in some cases without having obtained consent from the affected individual.

Another significant data protection challenge is the increasing ease with which researchers can re-identify individuals from previously pseudonymised or anonymised datasets by matching them against publicly available information or other datasets.

Intellectual Property

At present, it remains unclear whether and how existing intellectual property frameworks may be applied in protecting AI-generated works. Under Singapore copyright law, the creative elements of a work must be attributable to a natural person in order for copyright protection to vest.

AI-related inventions may, however, be patentable. In April 2019, the Intellectual Property Office of Singapore (IPOS) launched an Accelerated Initiative for Artificial Intelligence (AI2) scheme under which AI-related patent applications may be granted on an accelerated basis if various conditions are satisfied – most notably, the application must be an AI invention. Additionally, under the Patents Act 1994, in order for an invention to be patentable, it must be new, involve an inventive step, and be capable of industrial application.

Furthermore, the new Copyright Act 2021, which came into force on 21 November 2021, includes a new exception to copyright infringement for the purpose of computational data analysis (regardless of whether commercial or non-commercial).

This exception allows inventors seeking to use lawfully accessed data in their AI machines for computational data analysis, under certain conditions, without the fear of being liable for copyright infringement.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

While Singapore has not enacted any laws which specifically govern the internet of things (IoT), there are existing laws and regulations which may apply to various aspects of such IoT projects or applications. Additionally, the IMDA and the IT Standards Committee's IoT Technical Committee have developed and published Technical References in this area (eg, TR 47:2016, TR 50:2016 and TR 64:2018).

Telecommunications

Firstly, the IMDA, as established under the Information Communications Media Development Authority Act 2016 (IMDA Act), is responsible for regulating, amongst others, the telecommunications sector in Singapore pursuant to its exclusive privilege under the Telecommunications Act 1999 (TA).

Under the TA, "telecommunications" is defined very broadly as any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems whether or not such signs, signals, writing, images, sounds or intelligence have been subjected to rearrangement, computation or other processes by any means in the course of their transmission, emission or reception.

As the primary legislation governing the telecommunications industry in Singapore, the TA sets out the broad licensing and regulatory framework for the telecommunications sector. Unless an exemption applies, the IMDA's jurisdiction may potentially extend to the licensing of IoT projects or applications if such projects or applications may be regarded as involving the operation or provision of telecommunications systems or services under the TA. Where applicable, such persons would therefore need to comply with the general obligations and any specific conditions of approval under their respective licences which have been granted by the IMDA (see 7. **Telecommunications** for more details on the licensing of telecommunication systems and services).

Data Protection

The applicability of the PDPA may be triggered insofar as the IoT device in question can be used to collect personal data in Singapore and transfer it wirelessly through the network. In such a case, the organisation that collects or transfers the personal data (which may be an IoT service provider) will need to comply with the data protection obligations in respect of such data, unless an exception applies.

Cybersecurity

The primary cybersecurity legislation is the Cybersecurity Act 2018 (CA), which sets out a framework for the designation and monitoring of critical information infrastructure (CII) in essential sectors such as energy, info-communications, media, water, healthcare, banking and finance, security and emergency services, aviation, land transport, maritime, and services relating to the functioning of the Government.

Under the CA, a computer or computer system may be designated by the Commissioner of Cybersecurity as CII if it is:

- necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore; and
- the computer or computer system is located wholly or partly in Singapore.

Owners of CII are subject to various obligations under the CA, including reporting of cybersecurity incidents, conducting of regular cybersecurity audits and risk assessments, and furnishing of relevant information.

Recently, on 11 April 2022, the licensing framework for cybersecurity service providers came into effect, along with the Cybersecurity (Cybersecurity Service Providers) Regulations 2022. The licensing framework, which covers cybersecurity service providers providing penetration testing services and managed security operations centre monitoring services, aims to improve the standard of cybersecurity service providers and address the information asymmetry between consumers and service providers.

With the increasing adoption of IoT solutions amongst various stakeholder groups – including consumers, enterprises and governments – organisations which deploy IoT projects or solutions in the essential sectors discussed above may wish to pay particular attention to the possibility of their systems being designated as CII and subjected to the obligations under the CA.

The IMDA has also published an IoT Cyber Security Guide which provides baseline recommendations, foundational concepts and checklists relating to the security aspects of IoT systems.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Regulation of the Media Sector

Similar to telecommunications, the IMDA is also responsible for the regulation of the media (including broadcasting and film) sector. With regard to the media sector, “media” is defined in the IMDA Act as:

- a film (as defined in the Films Act 1981);
- a newspaper (as defined in the Newspaper and Printing Presses Act 1974);
- a broadcasting service (as defined in the BA);
- a publication (as defined in the Undesirable Publications Act 1967); or
- such other medium of communication of information, entertainment or other matter to the public (or a section of the public) as the Minister may specify by order in the Gazette.

Generally, the provision of audio-visual services in or from Singapore (eg, TV or radio) would be regulated under the BA and the IMDA may grant a broadcasting licence for the provision of:

- free-to-air nationwide, localised and international television services;
- subscription nationwide, localised and international television services;
- special interest television services;
- free-to-air nationwide, localised and international radio services;
- subscription nationwide, localised and international radio services;
- special interest radio services;
- audiotext, videotext and teletext services;
- video-on-demand services;
- broadcast data services; and
- computer on-line services.

In addition, the BA provides for a class-licensing regime, under the Broadcasting (Class Licence) Notification and Broadcasting (Class Licence – Broadcasting to Digital Display Panels) Notification 2020, for:

- audiotext, videotext and teletext services;
- broadcast data services;
- virtual area network computer on-line services;
- computer on-line services that are provided by internet content providers and internet service providers; and
- distribution network digital display panels services.

In particular, it should be noted that “internet content providers” is broadly defined under the Broadcasting (Class Licence) Notification to include any individual in Singapore who provides any programme, for business, political or religious purposes, on the World Wide Web through the internet, as well as any corporation or group of individuals (whether registrable or incorporated under Singapore law or not) who provides any programme on the World Wide Web through the internet.

In such cases, it is possible that companies operating video-sharing platform services on YouTube, for example, may be automatically deemed to be class-licensed, and must comply with the conditions of the class licence and the Internet Code of Practice. Amongst other requirements, broadcasting class licensees may be asked by the IMDA to remove or prohibit the broadcast of certain programmes which the IMDA has deemed to be against the public interest, public order or national harmony or to offend against good taste or decency.

Furthermore, from 1 February 2023, the amended Broadcasting Act will contain measures to regulate providers of OCS. The IMDA will also be empowered to issue directions to deal with egregious content that can be accessed by Singapore users on an OCS (see **1. Metaverse** for more details on the Online Safety Act).

Eligibility, Fees and Charges

In general, broadcasting companies are required to be Singapore-incorporated companies or the registered local branches of a foreign company in order to hold a “relevant licence” (unless exempted by the Minister for Communications and Information).

A “relevant licence” (which excludes class licences) refers to any free-to-air licence or any broadcasting licence under which a subscription broadcasting service may be provided, and which permits broadcast which is capable of being received in 50,000 dwelling-houses or more.

Different types of broadcasting licences may come with different licence fees, for instance:

- for free-to-air nationwide television service licences, licensees must pay 2.5% of their total revenue or SGD250,000 per annum, whichever is higher, and provide a performance bond of SGD200,000;
- for free-to-air nationwide radio service licences, licensees must pay 2.5% of their total revenue per annum, and provide a performance bond of SGD200,000 in the form of a banker’s guarantee;
- for subscription international television service licences (for satellite television service broadcasters), licensees must pay SGD5,000 per annum, and provide a performance bond of SGD50,000 in the form of a banker’s guar-

antee, if they are not based or registered in Singapore;

- for nationwide subscription television service licences, licensees must pay 2.5% of their total revenue or SGD50,000 per annum, whichever is higher, and provide a performance bond of SGD200,000; and
- for niche television service licences (which applies to providers of television services targeting niche market segments and over-the-top television services delivered through the internet), no licence fee is required.

For completeness, yearly fees are payable for certain types of services under the Broadcasting (Class Licence) Notification as follows.

- Teletext services – SGD2,000.
- Computer on-line services by internet access service providers – SGD1,000.
- Computer on-line services by non-localised internet service resellers – SGD100 (if less than 500 user accounts) or SGD1,000 (for 500 accounts or more).
- Computer on-line services by localised internet service resellers – SGD100 for each premise at which the computer on-line services are provided.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

As noted in the definition of “telecommunications” (see 5. Internet of Things), the licensing and regulatory framework for telecommunication systems and services under the TA is sufficiently broad to cover almost every technological application, even if there are no specific references to individual applications such as RFID tags, Voice over Internet Protocol (VoIP) or instant messag-

ing. That said, service-specific issues may be covered in various regulations, codes of practice, standards of performance, directions, advisory guidelines and licences issued by the IMDA pursuant to its powers under the TA.

For instance, issues pertaining to the licensing and use of the radio frequency (RF) spectrum and the operation of radio stations and networks are regulated under the Telecommunications (Radio-communication) Regulations, while the Telecommunications (Dealers) Regulations set out the framework in relation to the manufacturing, importation and sale (amongst other things) of telecommunication equipment.

It should also be noted that although the IMDA was formally established on 1 October 2016 as a converged regulator for both the info-communications and media sectors, in general, the telecommunications and media sectors continue to be governed by separate regulatory frameworks. For instance, the TA does not presently apply to the licensing of broadcasting services or any broadcasting apparatus, which falls under the Broadcasting Act 1994 instead. On 2 May 2022, the Code of Practice for Competition in the Provision of Telecommunication and Media Services 2022 (Telecom and Media Competition Code) came into operation. The Telecom and Media Competition Code was issued by the IMDA to promote the efficiency and competitiveness of both the media and telecommunications industry.

Licensing for the Operation and Provision of Telecommunication Systems and Services

Generally, licences for the operation and provision of telecommunication systems and services in Singapore would fall into either of two categories, namely facilities-based operations (FBOs) or services-based operations (SBOs),

and where RF spectrum is required for the provision of wireless services, additional licensing is required under the Telecommunications (Radio-communication) Regulations.

Taking the provision of VoIP services as an example, it is noted in the IMDA's Guidelines on Licensing and Regulatory Framework for IP Telephony Services in Singapore that applicants need to first obtain either an FBO or SBO licence from the IMDA in order to provide IP telephony services. IP telephony services are defined as any VoIP services offered using an E.164 telephone number allocated to customers in Singapore, which allow customers to make and receive voice, data and/or video calls using the same IP telephone number from any domestic or overseas location where broadband internet access is available.

An FBO licence is required if applicants intend to deploy and/or operate any form of telecommunication network, systems and/or facilities for the purpose of providing telecommunication (eg, IP telephony services) and/or broadcasting services outside of their own property boundaries to third parties (which may include other licensed telecommunication operators, business customers or the general public).

In contrast, only an SBO licence is required if applicants intend to lease telecommunication network elements from any FBO licensee to provide telecommunication services (eg, IP telephony services), or to resell the telecommunication services of such FBO licensees to third parties.

While there are two licensing schemes under the SBO framework (ie, class-licensing and individual licensing), operators that lease international transmission capacity for the provision of their services are usually required to obtain an SBO

(Individual) Licence. The SBO (Class) Licence is a licensing scheme where the terms and conditions are gazetted in the Telecommunications (Class Licences) Regulations. Anyone who provides the services within the scope of the SBO (Class) Licence will be deemed to have read and agreed to the terms and conditions of the class licence.

The IMDA's licensing framework is formulated on a hierarchical basis, with FBO licences placed on a higher level than SBO licences. This means that FBO licensees are able to offer telecommunication services that would ordinarily require an SBO licence without having to obtain a separate SBO licence, but not vice versa. If an SBO licensee subsequently wishes to undertake FBO-related activities – such as deploying or operating any telecommunication network, systems or facilities – it will need to apply for a new FBO licence to replace its existing SBO licence.

Eligibility, Fees and Charges

In terms of eligibility, the IMDA's current practice is to issue FBO licences only to Singapore-incorporated companies, although such companies can be wholly owned by a foreign entity. In the case of SBO (Individual) licences, local registered branches of foreign companies are eligible to apply, while SBO (Class) licences may also be held by limited liability partnerships or limited partnerships. Further details regarding the application process for an FBO or SBO licence and the information required can be found in the respective application guidelines issued by the IMDA on their website.

In terms of applicable fees and charges, FBO licensees are subject to a minimum annual recurrent licence fee of SGD80,000 or SGD200,000 (depending on whether the licensee is an FBO or a designated public telecommunication licen-

see), with further fees chargeable as a percentage of their incremental annual gross turnover (AGTO) exceeding SGD50 million as follows:

- 0.8% of the incremental AGTO between SGD50 million and SGD100 million; and
- 1% of the incremental AGTO above SGD100 million.

SBO (Individual) licensees are subject to a minimum annual recurrent licence fee of SGD4,000, with further fees chargeable as a percentage of their incremental AGTO exceeding SGD50 million as follows:

- 0.5% of the incremental AGTO between SGD50 million and SGD100 million; and
- 0.8% of the incremental AGTO above SGD100 million.

As of the time of writing, there are no annual recurrent licence fees for SBO (Class) licensees. Depending on the type of services provided, SBO (Class) licensees may need to make a one-time payment of SGD200 upon registration with the IMDA.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Data Security

One challenge that some organisations may face when entering into IT service agreements relates to obligations surrounding data security, particularly where personal data is involved. It is common for organisations seeking to engage third-party IT service providers to enter into a written data processing agreement which sets out each party's roles and responsibilities in relation to the

personal data in question, as well as the specific security measures that would be put in place.

In addition, the PDPC requires organisations to design and organise their security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach, and identify reliable and well-trained personnel responsible for ensuring information security.

In cases where the contract for IT services is with an FI, for instance, the organisation should be aware that FIs in Singapore are also subject to the regulations and guidelines promulgated by the MAS. These regulations and guidelines include but are not limited to the MAS's Guidelines on Outsourcing, Notice on Technology Risk Management, Notice on Cyber Hygiene, and Technology Risk Management Guidelines, which, amongst other things, may require FIs to exercise strong oversight of arrangements with third-party service providers to ensure system resilience as well as maintain data confidentiality and integrity. As a result, there may be a need for organisations entering into IT service agreements with FIs to include applicable provisions in relation to the conduct of security audits and reporting with regard to breaches or cyber-attacks.

Data Localisation

In Singapore, there are no express laws in relation to data localisation or data residency. The PDPC has notably taken a stance against data localisation and emphasised the importance of the free flow of data through coherent and efficient cross-border data transfer mechanisms.

Where the IT service agreement involves a cross-border transfer of personal data (eg, storage of data in the cloud or in a data centre located out-

side of Singapore, or the solution involves cloud computing), the organisation should also consider compliance with cross-border data transfer requirements under the PDPA and PDPR (see **3. Cloud and Edge Computing** (Specific Issues Regarding Personal Data Protection section) for more details on the transfer limitation obligation and specific issues for CSPs).

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Digital Identity

Launched in 2003, SingPass is a secure personal authentication system that allows users to access various government services online. Under the National Digital Identity initiative, SingPass, MyInfo (a service that automatically fills out selected personal details for online forms) and MyInfo Business (a service that enables businesses to manage the use of its corporate and applicant's personal data for simpler online transactions) were brought together to provide greater transactional security and ease of use. All SingPass users are automatically provisioned with a MyInfo profile which allows users to provide personal data once to digital services and then consent to have their personal data retrieved from government sources to pre-fill forms for digital transactions.

As SingPass and MyInfo are managed by the Government Technology Agency ("GovTech"), the data protection provisions in the PDPA do not apply to them and other public agencies. Instead, data management by public agencies is governed by the Public Sector (Governance) Act 2018 and guided by the Government Instruction

Manual on Infocomm Technology & Smart Systems Management (previously known as IM8).

However, private organisations utilising SingPass and MyInfo to facilitate their transactions are subject to the obligations under the PDPA. As personal data on these platforms is often sensitive data, organisations should take into account the sensitivity of the personal data and implement robust policies and procedures to ensure appropriate levels of protection and security. For instance, when collecting national identification numbers, organisations should comply with the Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers issued by the PDPC.

Electronic Signatures

The ETA makes a distinction between electronic signatures, secure electronic signatures and digital signatures.

An electronic signature could conceivably take various forms such as a scanned physical signature or typing one's name where a signature is required.

According to Section 18 of the ETA, an electronic signature will be recognised as a "secure electronic signature" if, through the application of a specified security procedure or a commercially reasonable security procedure agreed to by the parties, it can be verified that, at the time the signature was made, it was:

- unique to the person using it;
- capable of identifying such person;
- created in a manner or using a means under the sole control of the person using it; and
- linked to the electronic record to which it relates in a manner such that if the record

were changed the electronic signature would be invalidated.

The key difference between a secure electronic signature and an electronic signature is that the former raises the following statutory presumptions pursuant to Section 19 of the ETA:

- In any proceedings involving a secure electronic record, it is presumed, unless evidence to the contrary is adduced, that the secure electronic record has not been altered since the specific point in time to which the secure status relates.
- In any proceedings involving a secure electronic signature, it is presumed, unless evidence to the contrary is adduced, that the secure electronic signature is the signature of the person to whom it relates; and the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

Furthermore, the ETA defines a digital signature as an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine: (i) whether the transformation was created using the private key that corresponds to the signer's public key; and (ii) whether the initial electronic record has been altered since the transformation was made. A digital signature can be treated as a secure elec-

tronic signature if the digital signature was created during the operational period of a valid certificate and is verified by reference to the public key listed in such certificate. The certificate must also meet the prescribed requirements under the ETA and be considered trustworthy.

On 5 November 2020, GovTech launched the "Sign with SingPass" service. This was rolled out through GovTech's subsidiary, Assurity Trusted Solutions, an accredited Certification Authority under the ETA. The "Sign with SingPass" service allows SingPass users to electronically sign certain documents with some government agencies and private sector businesses. Signatures made using the "Sign with SingPass" service can be regarded as secure electronic signatures under the ETA.

However, the use of electronic or digital signatures in the following matters warrants further consideration:

- the creation or execution of a will;
- the creation, performance, or enforcement of an indenture, a declaration of trust or a power of attorney, with the exception of implied, constructive and resulting trusts;
- any contract for the sale or other disposition of immovable property or any interest in such property; and
- the conveyance of immovable property or the transfer of any interest in immovable property.

Drew & Napier LLC has a highly regarded TMT Practice Group, consistently ranked as the leading IT, telecommunications, broadcasting and multimedia legal practice in Singapore. The firm possesses unparalleled transactional, licensing and regulatory experience in the areas of telecommunications, technology, media, data protection and cybersecurity. Its Data Protection, Privacy and Cybersecurity Practice Group has been at the forefront of data protection law in Singapore since 2013, and has worked on significant data protection enforcement cases and appeals, including cases that involve cyberse-

curity elements. The firm established the Drew Data Protection & Cybersecurity Academy in 2020 to offer additional services related to data protection and cybersecurity compliance, including training, data protection consulting and external Data Protection Officer (DPO) services. Drew & Napier is the preferred counsel of many regional companies, multinationals, associations, government bodies and industry regulators, and regularly assists them on a wide range of matters in Singapore and ASEAN member countries.

Author



Lim Chong Kin heads Drew & Napier's highly regarded TMT practice group. His clients include the telecoms and media regulators, global carriers, technology market leaders, global broadcasters and content providers. Chong Kin has worked on every significant development in the Singapore TMT market. He

plays, and continues to play, a key role in the development of sectoral competition regulation in Singapore. He was the lead external counsel in the liberalisation of the telecommunications, media and postal sectors, and he has assisted regulators in conceptualising and drafting "first-of-its-kind" sectoral competition legislation and frameworks.

Drew & Napier

10 Collyer Quay
10th Floor
Ocean Financial Centre
Singapore
049315

Tel: +65 6531 4110
Fax: +65 6535 4864
Email: chongkin.lim@drewnapier.com
Web: www.drewnapier.com



SOUTH KOREA

Law and Practice

Contributed by:

Doil Son, Kum Ju Son,
Seung Hyuck Han and Sun Hee Kim
Yulchon LLC [see p.502](#)



Contents

1. Metaverse	p.485
1.1 Laws and Regulations	p.485
2. Digital Economy	p.486
2.1 Key Challenges	p.486
3. Cloud and Edge Computing	p.488
3.1 Highly Regulated Industries and Data Protection	p.488
4. Artificial Intelligence and Big Data	p.490
4.1 Liability, Data Protection, IP and Fundamental Rights	p.490
5. Internet of Things	p.493
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection	p.493
6. Audio-Visual Media Services	p.494
6.1 Requirements and Authorisation Procedures	p.494
7. Telecommunications	p.495
7.1 Scope of Regulation and Pre-marketing Requirements	p.495
8. Challenges with Technology Agreements	p.498
8.1 Legal Framework Challenges	p.498
9. Trust Services and Digital Entities	p.499
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes	p.499

1. Metaverse

1.1 Laws and Regulations

In Korea, there are no laws or regulations that are generally applicable to the metaverse. However, various laws may apply depending on the specific activities and interactions taking place in the metaverse.

Laws Applying to Platform Businesses

Transactions in the metaverse

The Act on the Consumer Protection in Electronic Commerce Transactions (the “E-Commerce Act”) applies when goods or services are traded electronically. Thus, if goods or services are traded in the metaverse, the E-Commerce Act will apply.

Under the E-Commerce Act, a business operator who is engaged in or conducts electronic commerce is referred to as an “Online Seller”, and a business operator that intermediates an online order between the parties to a transaction by providing an online platform is referred to as a “Platform Operator.” In this context, the metaverse operators who sell goods or services directly to users will be considered Online Sellers, and those who provide the metaverse platform for users to sell goods or services to other users will be considered the Platform Operators under the E-Commerce Act.

Please refer to **2.1 Key Challenges** for the obligations of the Online Seller and the Platform Operator under the E-Commerce Act.

Obligation of the metaverse operator

There are no established obligations or liabilities specific to metaverse operators. However, several laws that apply to the operators of online platforms would apply to metaverse operators.

The Telecommunications Business Act (TBA) requires the operators of value-added telecommunications businesses (as which metaverse operators are likely to be categorised) to delete or otherwise prevent the distribution of certain illegal content, such as child pornography, etc. Failure to comply with this obligation may result in penalty surcharges of up to 3% of annual revenue imposed by the Korea Communications Commission.

In general, the Copyright Act prohibits copyright infringement, such as unauthorised copying and transmission of copyrighted works. However, online service providers can be protected from liability for the copyright infringement of their users if they satisfy certain statutory conditions under Article 102 of the Copyright Act. As metaverse operators are likely to be considered online service providers, the same limitation of liability would apply to metaverse operators as well.

In addition, other laws, such as the Act on the Promotion of Information and Communications Network Utilization and Information Protection (the “Network Act”), would also apply to metaverse operators to take certain actions against illegal content on the internet. Please refer to **2.1 Key Challenges** for more details.

Intellectual Property

Trade marks

Under the Trademark Act, trade mark infringement occurs when an unauthorised person uses a registered trade mark within the range of protection (ie, the designated goods) and as a trade mark (ie, to show the origin of the goods).

However, there is no established principle on how trade marks will work on virtual goods. As the trade mark is registered for certain design-

nated goods in principle, the validity of a trade mark on virtual goods is still in question. The Korean jurisprudence is to evaluate primarily in relation to the possibility of confusion, while taking into account various factors such as the quality, shape, and purpose of the goods. However, what constitutes trade mark infringement in the metaverse is still unclear under Korean law.

Copyright

Under the Copyright Act, any expression of human creativity may enjoy copyright protection. In a recent case, the Court ruled that creating a virtual golf course for virtual golf games based on a real-life golf course constitutes an infringement of the architectural copyright. This case shows how a virtual recreation of the real world on the metaverse could trigger risks of copyright infringement.

Publicity right

The publicity right (ie, the right to use one's image for profit) is protected under the Unfair Competition Prevention and Trade Secret Protection Act. To be more specific, unauthorised commercial use of an individual's name, likeness, voice and other recognisable characteristics is prohibited as an act of unfair competition. It is expected that the publicity right will be recognised as a new type of property right by the introduction of relevant laws.

Data Protection

Under the Personal Information Protection Act (PIPA), data controllers are, in principle, required to obtain prior consent from data subjects to collect and process their personal information. If the metaverse operators collect and process the personal information of their users, it should comply with the PIPA. Please refer to **2.1 Key Challenges** for the PIPA's requirements for the processing of personal information.

2. Digital Economy

2.1 Key Challenges

The digital economy in Korea is regulated by various laws and regulations concerning electronic commercial transactions, financial transactions (payment), and consumer protection in the digital space.

Electronic Commercial Transactions

The E-Commerce Act stipulates the obligations of business operators to protect consumers in e-commerce. To sell goods or services by providing information on the sale of goods or services online and to receive a consumer's order by means of telecommunications, a business operator must register with the Fair Trade Commission or the relevant local government as an Online Seller.

Online Sellers are subject to certain obligations to protect the customers. For instance, when placing an indication or advertisement for its goods or services, an Online Seller must disclose the following information:

- trade name and the name of its representative;
- address;
- telephone number;
- email address; and
- the business registration number.

Moreover, the Online Seller shall inform or notify its customers about the specific terms of the transaction before concluding a contract, and upon the conclusion of a contract, the Online Seller shall provide a document that includes such information before supplying the goods or services.

Meanwhile, Platform Operators must notify beforehand that it is not a party to electronic transactions so that the customers can easily recognise such fact.

Electronic Financial Transactions

The Electronic Financial Transactions Act (EFTA) regulates “electronic financial transactions” which enable users to utilise financial products and services provided by a financial company or an electronic financial business entity through electronic means in a non-facing and automated manner.

Depending on the specifics of the business, the EFTA requires different types of licences to provide electronic financial transaction services in Korea. To issue and manage electronic currencies, permission from the Financial Services Commission (FSC) is required. For other types of electronic financial services, including electronic funds transfers, electronic debit payment means, electronic prepayment means, and electronic payment settlement agencies, registration with the FSC is required.

Moreover, an electronic financial transaction service provider is subject to certain security measures to ensure the secure handling of electronic financial transactions. To be more specific, the specific security measures for human resources and physical facility capability as well as financial soundness for conducting electronic transactions, etc, are outlined in the FSC’s Regulation on Supervision of Electronic Financial Transactions (the “E-Transaction Regulation”).

User Protection

Content regulation

The laws to regulate illegal content in the digital space, such as the Network Act, the TBA and the Copyright Act, will apply to business pro-

viders and require them to take certain actions against illegal content.

Under the Network Act, when information violates a person’s privacy or defames someone, the victim may request the online service provider to delete the information or publish a correction statement, and the online service provider must comply with such request without delay. If there is any media product harmful to children in violation of labelling regulations or any advertisements for such content, the online service provider shall delete such content without delay. Also, circulation of “unlawful information (such as obscene content, defamatory content, criminal content, etc)” through an online network is prohibited, and the Korea Communications Commission may order an online service provider to reject, suspend or restrict management of unlawful information.

Additionally, the TBA regulates the circulation of “illegally filmed material”, which includes pictures taken without permission, deepfake images, and child sexual exploitation material. Where an online platform realises that any “illegal filmed material” is circulated on its platform, it should, without delay, take necessary measures to block the circulation of such material (ie, deleting the information, blocking access, etc).

The Copyright Act also states that any person who claims that their copyright or other rights are infringed due to reproduction or interactive transmission of works, etc, through the services provided by an online service provider may demand the online service provider to suspend the reproduction or interactive transmission of the works, and the online service provider shall take necessary actions without delay.

Personal information

When business operators who are data controllers collect the personal information of their customers, they should prepare a privacy policy in accordance with the PIPA and disclose the privacy policy on their websites. Also, the business operators are required to obtain explicit and separate consent from the data subjects for the collection and use, third party provision, and overseas transfer of personal information in accordance with the form and manner stipulated in the PIPA.

Please note that in addition to ordinary provisions, the PIPA has special provisions for online service providers. The online service providers are companies that engage in e-commerce or operate a company website to provide information about their products. For example, an online service provider meeting a certain threshold must regularly (at least once a year) notify their users of how their personal information has been used.

Terms and conditions

The Act on the Regulation of Terms and Conditions regulates the terms and conditions, a contract prepared in advance by the business operators to enter into with multiple users. Under this law, a business operator shall prepare the terms and conditions in Korean and disclose important terms and conditions in a manner easily recognisable and understood by customers. Also, the Act specifies the types of “unfair clauses” that are unreasonably unfavourable to consumers and states that these unfair clauses shall be deemed null and void, and thus unenforceable.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

General Laws and Regulations

The Cloud Computing Act

In Korea, there are currently no laws or regulations that directly regulate the cloud computing industry. However, the Act on the Development of Cloud Computing and Protection of its Users (the “Cloud Computing Act”) aims to promote cloud computing industry by setting forth the general principles and the government’s responsibilities to promote the development and use of cloud computing.

The Cloud Computing Act defines the term “cloud computing” as an information processing system that makes it possible to flexibly use integrated and shared resources for information and communications, such as devices for information and communications, information and communications systems, and software, through information and communications networks in accordance with changes in users’ requirements or demands.

The Act further states that electronic computer systems (including equipment, facilities, etc) that are subject to authorisation, permission, registration, designation, or any similar action under other laws shall be deemed to include cloud computing services unless the relevant laws expressly prohibit the use of cloud computing services, or the cloud computing services cannot meet the technical and physical requirements of such relevant laws.

Criteria for information protection of cloud computing services

Under the Cloud Computing Act, cloud computing providers must endeavour to enhance the

quality and performance of cloud computing services and the level of information protection.

Under this law, the Minister of Science and ICT has the power to determine and publicly notify the standards for the quality and performance of cloud computing services, and the standards for the protection of information (including managerial, physical, and technical measures for information protection) (the “Criteria for Information Protection of Cloud Computing Services”), and to recommend cloud computing service providers to comply with the Criteria for Information Protection of Cloud Computing Services.

Personal information

If personal information is stored or processed by cloud computing services, the PIPA will apply to cloud computing service providers. In most cases, cloud computing service providers will be considered third-party data processors as they tend to carry out the outsourced data processing tasks (including storage) on behalf of data controllers who collected personal information for their purpose in the first place.

Under the PIPA, when personal information is transferred from a data controller (outsourcer) to a third-party data processor (outsourcee) for the benefit and business purpose of the data controller, and such transfer is consistent with the original purposes of the collection and use of personal information, it is considered the “outsourcing” of personal information processing. For the outsourcing, the third-party data processor must use the received personal information only to perform the work outsourced by the data controller, and the data controller will not be released from its obligation to monitor, supervise, and train the third-party data processor regarding the protection of the transferred personal information.

While consent from data subjects is not required for the outsourcing of personal information processing, the data controller is required to enter into a written contract with the third-party data processor (typically in the form of a data processing agreement) that includes the following terms and conditions:

- prohibiting personal information processing outside the scope and purpose of outsourcing;
- technical and managerial measures to protect personal information; and
- other matters regarding the safeguarding of personal information as prescribed by the Enforcement Decree of the PIPA.

Additionally, the data controller must disclose the following information on the privacy policy posted on its website at all times: the details of processing outsourced, and the information about the third-party data processor.

In case of overseas outsourcing of data processing (including storage), the data controller can be exempted from the consent requirement only if the following information must be disclosed in the third-party data processor’s online privacy policy, or notified to users via electronic mail, or other similar means as prescribed under the relevant Presidential Decree:

- items of personal information transferred;
- the country to which such personal information is being transferred, along with the date and method of such transfer;
- the name of the recipient (if the recipient is an entity, the name of the entity and the contact information of the person responsible for the management of personal information for that entity);

- the purpose for which the recipient makes use of the transferred personal information;
- the period during which the transferred personal information will be used/retained by the recipient; and
- the fact that the user has the right to refuse consent and any possible disadvantages resulting from such refusal.

Industry-Specific Laws and Regulations

Financial companies

There are special regulations for the use of a cloud service by a financial company, specifically in the FSC's E-Transaction Regulation.

According to the E-Transaction Regulation, when a financial company intends to implement a cloud service, it must evaluate the importance of the tasks to be carried out by the cloud service, and the soundness and security of the cloud computing service provider. Based on these evaluations, the financial company must establish and implement a business continuity plan and necessary security measures.

A financial company must also report the use of cloud services to the Financial Supervisory Service (FSS) within three months from the execution of a new service contract with a cloud computing service, or the date of any significant changes with the service provider or the cloud computing services.

Medical institutions

According to the Medical Service Act, medical personnel and medical institutions may keep medical records in the form of an electronic document with a digital signature (the "Electronic Medical Records").

For the management and retention of Electronic Medical Records, the Enforcement Rule of the

Medical Service Act and the Standards for Facilities and Equipment Necessary for Management and Preservation of Electronic Medical Records set forth specific requirements and standards for equipment and retention facilities.

When Electronic Medical Records are stored on cloud servers located outside of a medical institution, the cloud service provider of such servers must implement the equipment that enables real-time monitoring of the servers (and spare equipment to be used in an emergency), install monitoring equipment such as closed-circuit television, etc, and set up disaster prevention facilities. However, please note that since Electronic Medical Records must be stored in Korea at all times, they cannot be stored on servers located overseas.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

General Laws and Regulations

The Act on the Promotion of Data Industry and the Activation of Data Use (the "Data Industry Act") provides the basic legal principles in relation to the derivation of economic value from data and the development of the data industry. Also, the Act on the Promotion of the Provision and Use of Public Data states that certain public data must be disclosed to the public and become freely accessible, while other public data must not be disclosed to the public and become accessible only if the user files an application to the competent public institution.

In Korea, there are no statutory laws specifically regulating the use of AI. Instead, guidelines on relevant issues have been published

by various governmental agencies, such as the FSC's Guidelines for Artificial Intelligence in the Financial Sector, the Personal Information Protection Commission's Artificial Intelligence Personal Information Self-Checklist, the Korea Communications Commission's Basic Principles for User Protection in AI-Based Media Recommendation Services, and the Ministry of Science and ICT's (MISCT) Ethical Standards for Artificial Intelligence. These guidelines set out the basic principles for activities involving particular issues in using AI in each respective field.

In addition to these guidelines, the existing laws and regulations governing personal information, intellectual property, credit information, and liability and insurance, will apply.

Specific Application of Laws and Regulation

Personal information

The PIPA will apply if an AI processes personal information or if personal information is used for machine learning. Under the PIPA, different types of personal information are regulated differently.

Personal information under the real name

Personal information under the real name refers to the information that identifies a particular individual or may be easily combined with other information to identify a particular individual. If an AI processes personal information under the real name, the general principles of the PIPA will apply. This means that the data controller must explicitly obtain the consent of each data subject if it wishes to collect and use the personal information, or provide such information to a third party, unless there are any other legal grounds upon which the absence of such consent could be justified, such as when special provisions exist in other laws or it is inevitable to observe legal obligations.

Pseudonymised information

Pseudonymised information refers to personal information that is pseudonymised and thereby becomes incapable of identifying a particular individual without the use of or combination with additional information for restoration to the original state. A data controller may process pseudonymised information without the consent of data subjects for statistical purposes, scientific research purposes, and archiving purposes in the public interest. Under the PIPA, "processing" includes the collection, use, and provision of information, which means that for pseudonymised information, the data controller may carry out these activities without the data subject's consent, as long as the purposes of processing are limited to the above.

Anonymised information

Anonymised information refers to information that no longer identifies a certain individual even when combined with other information, reasonably considering time, cost, technology, and other factors. Since anonymised information cannot identify an individual, such information is not considered personal information; therefore, the PIPA does not apply. This means the data controller may process anonymised information without any limitations as to the purpose of processing.

Expected amendment of the PIPA

The amendment bill of the PIPA, which is scheduled to be passed by the legislature in early 2023, introduces provisions on the data subject's right to object to or request clarification regarding a decision based on the processing of personal information by a fully automated system, including AI technology, when such decision significantly affects the rights or obligations of the data subject.

Intellectual property

Protection of data and databases

Data used for machine learning and processed by AI, as well as the processed results, generally exist in the form of a “database”. A “database” means a compilation of systematically arranged or composed data, such that the data may be individually accessed or retrieved. Under the Copyright Act, a database is recognised as a copyrightable object; thus, producers of a database hold the rights to reproduce, distribute, broadcast, or interactively transmit the whole or considerable parts of the relevant database.

The Unfair Competition Prevention and Trade Secret Protection Act (the “Unfair Competition Prevention Act”) regulates the unfair use of “data” as an “act of unfair competition”, such as the acquisition of data by theft, deceit, unauthorised access, or other illegal means by a person without access authority, or use and disclosure of such acquired data. The term “data” in this context refers to technical or business information that is provided to a specific person or a specific number of people in the course of business, electronically accumulated and managed in a significant volume, and not managed as confidential. Such act of unfair competition is subject to criminal penalties.

Crawling

AI often uses “crawling” to collect big data necessary for machine learning. Crawling is an act of extracting data from a web page as it is, so it basically accompanies reproduction of data, which may be interpreted as an act that infringes upon the database producers’ right to reproduce, or as an unfair use of data that is an act of unfair competition.

Although the relevant legal principles have not yet been clearly established, there was a recent

Supreme Court case which found that crawling was not considered an infringement of the database producer’s rights under the Copyright Act. The Court reasoned that an infringement of the right to reproduce is less likely to be found if the information is already known or has already been made public and does not require significant cost or effort to collect. Also, the Court stated that a violation of a database producer’s rights must be judged by considering factors such as the volume of reproduced data in comparison to the volume of the entire database, and whether the database producer has made a significant investment in human or physical resources in the production of the database.

Liability and insurance

In Korea, whether the Product Liability Act applies to the damages caused by AI is still widely debated. If the Product Liability Act applies, the manufacturer of the AI would be liable for the damages to the life, body or property of a person caused by a defect of an AI. However, the manufacturer would be exempted from such liability in some circumstances, such as when the defect could not be identified with the scientific and technical knowledge available at the time the product was supplied by the manufacturer.

The Compulsory Motor Vehicle Liability Security Act states that if an insurance company compensates for losses or damages that result from the death or injury of any third party or the damage of the property of a third party caused by a defect in an autonomous driving motor vehicle, the insurance company may seek indemnity from any person who is legally liable to such losses or damages for the relevant amount. Also, under the Act, the manufacturer of an autonomous driving motor vehicle should attach a recording device that records autonomous driving information, and the owner of such vehicle should retain

the recorded information for at least six months. The insurance company may request access to the recorded information and its analysis results.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection Regulation in Relation to the Internet of Things and Machine-to-Machine Communications

No laws or regulations specifically regulate the IoT or machine-to-machine communications (M2M). However, if the IoT or the M2M falls under the definition of an existing term or meets requirements under the existing laws, such existing laws will apply.

The IoT or M2M service operators would likely correspond to the “Facilities-Based Telecommunications Business” under the TBA and would be required to register with the MSICT to conduct business in Korea. To register, the IoT or M2M service operator should meet the requirements for both financial and technical eligibility and have a user protection plan, in addition to the business plan, including details of major business facilities and network configuration.

Moreover, any IoT or M2M devices that utilise radio waves such as Bluetooth or Wi-Fi would be subject to the conformity assessment requirement in accordance with the Radio Waves Act (RWA). Under the RWA, anyone who intends to manufacture, sell, distribute or import broadcasting and communications equipment or products that cause electromagnetic interference or are affected by electromagnetic waves (hereinafter referred to collectively as “broadcasting and communications equipment”) shall, with regard

to the relevant equipment, receive a conformity assessment. The assessment standards include technology requirements, human exposure levels, and electromagnetic compatibility. The National Radio Research Agency (NRRA), a government agency under the MSICT conducts the conformity assessment under the RWA.

Under the RWA, a party or product is deemed to have received the conformity assessment if the party or product has received or completed one of the following.

- Conformity Certification – required for:
 - (a) equipment likely to cause harm to the spectrum environment and to the broadcasting and communications networks, etc; and
 - (b) equipment that causes significant electromagnetic interference or which is affected by electromagnetic waves to the extent that its normal function may be compromised.
- Conformity Registration – required for any broadcasting and communications equipment, etc, which is not subject to the conformity certification obligation.
- Interim Certification – in case there is no established conformity assessment standards or conducting the assessment is impracticable, according to the NRRA, an Interim Certification is applicable to only a few exceptional cases; therefore, such certification has not been issued frequently.

The specific requirement for certification/registration varies based on the type of product.

Communication Secrecy and Data Protection

No specific laws or regulations govern communication secrecy in relation to the IoT or M2M.

If the IoT or M2M collects personal information, the PIPA will govern such collection of personal information through the IoT or M2M. The applicable laws may differ according to the types of personal information. For instance, the Act on the Protection and Use of Location Information would apply to the collection of personal location information, and the Credit Information Use and Protection Act would apply to the collection of credit information. Under the Act on the Protection and Use of Location Information, a business operator that intends to engage in location information business or location-based service business would be required to register with or report to the Korea Communications Commission.

Moreover, as stipulated in the Protection of Communications Secrets Act (PCSA), no person or entity shall censor any mail, wiretap any telecommunications, provide communication confirmation data, or record or listen to any conversation between others that is not made public, except as provided in the Act, the Criminal Procedure Act or the Military Court Act.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

General Laws and Regulations

Korea's major audio-visual media services include terrestrial broadcasting (ie, television broadcasting, radio broadcasting, and mobile multimedia broadcasting), cable television (CATV) broadcasting, satellite broadcasting, and internet multimedia broadcasting (IPTV) services. The audio-visual media service industry, including the requirements for entry into the industry is regulated by law, including the Broadcasting Act

and the Internet Multimedia Broadcast Services Act (the "IPTV Act").

The Korea Communications Commission (KCC) and the MSICT are in charge of the authorisation of media services in Korea. The KCC issues licences to terrestrial broadcasting businesses, which are subject to stronger public interest considerations, whereas the MSICT issues licences to more commercial broadcasting businesses, such as CATV broadcasting, satellite broadcasting, and IPTV broadcasting businesses.

On the other hand, video-sharing platform services are currently not subject to licensing requirements under the TBA. A video-sharing platform service provider can commence its business after reporting to the MSICT as a value-added telecommunications business without obtaining a license. Additionally, video-sharing platform service providers whose total capital amount is at most 100 million KRW are exempted from the reporting requirement.

Under the Broadcasting Act, a country, a local government, or a person who is not a corporate entity, as well as those who violated an applicable regulatory requirement, such as the restrictions on ownership and foreign capital investment, are prohibited from operating a broadcasting business (eg, terrestrial broadcasting business, CATV broadcasting business, and satellite broadcasting business entity). The restriction on ownership prohibits a person from obtaining ownership of a terrestrial broadcasting business entity exceeding 40%. The restriction on foreign capital investment prohibits foreign investment in a terrestrial broadcasting business and a foreign investment exceeding 49% in CATV broadcasting or satellite broadcasting businesses.

Under the IPTV Act, a country, a local government, or a business corporation of which over 49% of the shares are held by a newspaper publisher, a news agency, or a foreigner is prohibited from operating an IPTV service business.

On the other hand, the TBA does not specify the grounds for disqualification of OTT service providers that are value-added telecommunications business entities.

Approval/Authorisation Procedure and Fees, etc

General approval/authorisation procedure

The KCC and the MSICT adopted a system under which they establish a basic authorisation plan for broadcasters within its jurisdiction in order to authorise or deny terrestrial broadcasting, general CATV broadcasting, satellite broadcasting, and IPTV broadcasting services through various steps, including notice of application, receipt of applications, receipt of viewers' opinions, and evaluation by the review committee.

For the authorisation of a terrestrial broadcasting business, which uses radio frequency for transmission, the KCC is also required to request and take into account a technical review of the establishment radio station under the Radio Wave Act from the MSICT as part of the evaluation.

Those who intend to conduct CATV broadcasting business must obtain authorisation from the MSICT by securing facilities and technologies that satisfy the standards prescribed by Presidential Decree of the Broadcasting Act.

Satellite broadcasting service providers must obtain broadcasting station authorisation from the MSICT as prescribed by the Radio Waves Act. IPTV broadcasting service providers must

also be authorised by the MSICT as prescribed by the IPTV Act.

The authorisation for a terrestrial broadcasting business is valid for five years. On the other hand, the validity period of authorisation for CATV broadcasting, satellite broadcasting, and IPTV broadcasting is seven years. However, these validity periods may be shortened by the KCC and MSICT by two years or less if the KCC or MSICT determines such adjustment is necessary for the protection of the viewers' interest, an undertaking of public responsibility, and the establishment of fairness and public interest.

Fee

When applying for authorisation for terrestrial broadcasting and satellite broadcasting, a fee, ranging from KRW75,000 (less than 100Watt) to KRW590,000 (exceeding 100kW), based on the size of the transmitters determined by the antenna power must be paid (the Radio Act, Article 95(1) (Annex 12)). There is a fee of KRW200,000 for the application for the CATV broadcasting authorisation (The Enforcement Decree of the Broadcasting Act, Article 671). On the other hand, there is no application fee required for IPTV business authorisation or reporting fee for value-added telecommunications businesses.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Telecommunication Business Under the Local Telecommunications Rules

Telecommunications business, regulated by the TBA, is subcategorised into the following two groups: facilities-based telecommunications business and value-added telecommunications business. Under the TBA, facilities-based tele-

communications business (FBT) means a business that provides telecommunications services for transmitting or receiving voice, data, images, etc, without any change in the form or details thereof, and services for leasing telecommunications line equipment to enable transmission or reception of voice, data, images, etc, such as telephone services or internet services.

Value-added communication business means a value-added telecommunications service provider other than facilities-based telecommunications service providers.

Requirements for Licence/Approval/Authorisation *FBT*

Pursuant to the TBA, an FBT must register with the MSICT upon satisfying the below requirements in relation to financial capability, technical capability, and plans for protecting users.

However, businesses deploying a telecommunications service in order to primarily engage in a business other than telecommunications will not be required to obtain a telecommunications registration but will be subject to an obligation to file a relatively simple report. Such enterprises will be deemed to “make ancillary use of core telecom services” where:

- even if the use of the telecommunications service were eliminated from the product or service offered, the business is still capable of supplying the product or service; and
- the telecommunications service at issue includes communication with a machine or other objects, without the possibility of voice reception/transmission (except in case of emergency).

There are certain minimum capital requirements and minimum technical staff requirements for each FBT type.

- For large-scale wired business, the minimum capital is KRW5 billion, and it is necessary to have three engineers specialising in several designated categories of telecom, broadcast and radio communications (“telecom engineers”) and two technicians specialising in several categories of telecom, broadcast and radio communications (“telecom technicians”).
- For small-scale wired business, the minimum capital is KRW500 million, and it is necessary to have one telecom engineer and one telecom technician.
- For switched resale business, the minimum capital is KRW3 billion, and it is necessary to have three telecom engineers and two telecom technicians.
- For switchless resale business, the minimum capital is KRW300 million, and it is necessary to have one telecom engineer or technician.
- For mandatory wholesale service resale businesses that only provide the services of transmission and reception of data with things, the minimum capital is KRW300 million, and it is necessary to have:
 - (a) three telecom engineers and two telecom technicians when exchange equipment is installed; and
 - (b) one telecom engineer or telecom technician when exchange equipment is not installed.
- For in-premises telecommunications business, the minimum capital is KRW300 million, and it is necessary to have one telecom engineer and one telecom technician.

Value-added telecommunications business

Pursuant to the TBA, a person who intends to operate a value-added telecommunications business must properly report to the MSICT, and those who intend to operate a special value-added telecommunications service business must register their business with the MSICT. “Special value-added telecommunications service” means:

- value-added telecommunications services provided by a special online service provider (“P2P operator”) who mainly enables interactive transmission of works and other subjects using computers between other persons; and
- value-added telecommunications services through which text messages are sent by directly or indirectly connecting a text-message system to telecommunications business equipment of a telecommunications business operator (“ISMS operator”).

Different minimum capital requirements and requirements for personnel and facilities apply in relation to P2P operators and ISMS operators.

- For P2P operators, the minimum capital is KRW300 million and the following requirements for personnel and facilities apply:
 - (a) the operator must designate and announce a copyright protection manager, youth protection manager, and information protection manager who have executive-level or department head-level or higher authorities, and concurrent positions are allowed;
 - (b) the operator must appoint at least two employees dedicated to monitoring the distribution of illegal information, harmful information, and illegal works 24 hours a day, and must secure one additional employee per 4,000 upload or sharing ac-

counts per day; and

- (c) the operator must be equipped with electronic computer systems and various computer programs necessary to provide special value-added telecommunications services smoothly and to implement a technical measures implementation plan pursuant to Article 22(2)(1-2) of the TBA.
- For ISMS operators, the minimum capital is KRW50 million and the following requirements for personnel and facilities apply:
 - (a) the operator must appoint at least one dedicated employee in charge of preventing false subscriptions, registering and managing outgoing numbers, verifying and providing the transmission path of text messages with falsely marked telephone numbers, and suspending the provision of telecommunication services to the relevant line by the person who transmitted such messages; and
 - (b) the operator must be equipped with electronic computer systems and various computer programs necessary to provide special value-added telecommunications services smoothly and to implement a technical measures implementation plan pursuant to Article 22(2)(1) of the TBA.

The TBA requires those value-added telecommunications business operators that do not have a local business address or a branch office in Korea, of which (i) the average number of domestic users per day in the three months immediately before the end of the previous year is more than 1 million, and (ii) the average daily domestic traffic generation for the three months immediately prior to the end of the previous year accounts for more than 1% of the total nationwide daily traffic generation for the same time frame, to designate in writing a person who has an address or office in Korea (“domestic agent”)

as an agent responsible for user protection and compliance of the data submission orders.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges Technology Agreements

Technology agreements are required to abide by the general contract laws.

Although there are no specific laws or regulations that apply to technology agreements in general, the Software Promotion Act (SPA) provides general principles related to the execution of software agreements. The SPA stipulates that the parties to a contract for software project (including a subcontract and a re-subcontract) shall enter into the contract fairly on an arms-length basis by mutual agreement and perform the obligations under the contract in good faith. The parties to a contract for a software project shall, when entering into the contract, clearly set forth the material terms of the contract, including the purpose and scope of the contract, the contract period and the fees, etc, in the contract, and affix their signatures (including digital signatures) thereto or exchange and keep the signed and sealed copies of the contract. If any terms of a contract for a software project are notably unconscionable to either party and fall under any of the following cases, such terms shall be null and void:

- if either party does not accept any modification of the contract amount or the contract period caused by changes to the assigned tasks or changes in economic conditions after the conclusion of the contract without good cause, or transfers the relevant burden to the other party;

- if either party transfers responsibility to the other party for any matters that are difficult to predict at the time of signing the contract, in light of all related circumstances including the terms and conditions of the contract;
- if the specific terms and conditions of the contract are not determined or, in the event of a disagreement between the parties, the terms or conditions of the contract are determined at the sole discretion of either party, which thereby prejudices the legal interests of the other party;
- if either party's liability for damages resulting from its non-performance of the contract is excessively reduced or augmented, which thereby prejudices the legal interests of the other party; and
- if the rights of the other party acknowledged by the Civil Act and other applicable statutes or regulations are excluded or restricted without good cause.

The MSICT provides standard contract forms for software projects including those for information system development and establishment of businesses, information system maintenance businesses, and the employment of software employees.

Moreover, there is a list of technologies that are subject to export control under the Korean law, the violation of which may even expose a foreign company to criminal sanctions. Under the Foreign Trade Act, any person/entity that intends to export "strategic item" designated by the Ministry of Trade, Industry, and Energy (MTIE) must obtain export permission from the MTIE or the relevant administrative agency. Even if an export good does not fall under the ambit of "strategic item", any person who intends to export goods that are highly likely to be appropriated for manufacturing, developing, using, or

storing weapons of mass destruction or missiles as carriers of such weapons must obtain “situational permission” from the MTIE or the relevant administrative agency.

Finally, the Act on Prevention of Divulgence and Protection of Industrial Technology prevents the export of “National Core Technology”, a technology designated by the MTIE that could have a material adverse effect on national security and the development of the national economy if divulged. If an entity that possesses national core technology intends to export the national core technology, it has to obtain approval from or report to the MTIE.

Data Localisation Requirements

There are no general data localisation requirements, but as discussed in **3.1 Highly Regulated Industries and Data Protection**, technology agreements in certain industries may be subject to the specific laws and regulations.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Electronic Signatures and Certification Service

The Electronic Signature Act (ESA) stipulates the basic legal framework for electronic signatures. Prior to the amendment in 2020, the ESA classified electronic signatures into:

- certified electronic signatures; and
- uncertified electronic signatures.

Certified electronic signatures had to be certified by public key certification, a system licensed by an authorised entity designated by the MSICT.

However, the amended ESA abolished the public key certificate system and allowed various other electronic signature methods.

The amended ESA stipulates that the effect of the electronic signature will not be denied due to its electronic form. Where an electronic signature is selected as a means of writing a signature, signature and seal, or name and seal under the provisions of any statute or an agreement between parties concerned, the electronic signature will have the same effect as a hand-written signature, signature and seal, or name and seal.

The MSICT establishes the operational standards for electronic signature certification services and publicly notifies the standards in consideration of internationally recognised standards. A certification service provider has to undergo an assessment by the assessment body and then obtain accreditation for its compliance with the operational standards from the accreditation agency designated by the MSICT. According to the ESA, a certification service provider has to be a national agency, local government or legal person.

The ESA also recognises and accepts international assessment standards. The ESA stipulates that the MSICT may publicly notify internationally-accepted assessments standards and recognise compliance with the operating standards. A certification service provider is deemed to have obtained an assessment of an assessment body if it has obtained an internationally-accepted assessment. In this case, the certification service provider may apply to the accreditation agency for an accreditation of compliance with the operating standards without separate assessment by a domestic assessment body.

A certification service provider must protect the personal information of the users in relation to the storage and distribution of their electronic documents, as prescribed by the relevant statutes. If a certification service provider inflicts a loss on a user in relation to the storage of electronic documents, it must compensate the user for such loss, unless it proves that the loss was not caused by intentional or negligent conduct. A certification service provider is required under the law to be insured to compensate users for such loss.

Electronic Documents

The Framework Act on Electronic Documents (FAED) specifically regulates electronic documents. The FAED stipulates that an electronic document is not denied legal effect as a document solely because it is in an electronic form. All documents would in principle be allowed to be executed in an electronic form using an electronic signature except the following documents, which are required to be executed only by wet ink signature and cannot be executed by digital signature.

- **Guaranty Agreement** – The Civil Act prohibits a declaration of intent to provide a guaranty in an electronic form, and thus, the provision of a guaranty by digital signature does not have any effect. However, if an “institutional guaranty” provided by an institution is engaged in the provision of a guaranty agreement, the execution of the guaranty agreement in an electronic form is allowed. The term “institution” means a specific financial institution making a guaranty agreement as its own business, such as the credit guarantee fund or the construction guarantee co-operative.
- **Will by holographic (handwritten) document** – To execute a will by holographic document, the testator must write the content of the

will, date, and the testator’s domicile and full name in their own handwriting and must affix seal to it.

- **Documents required to be submitted to the government offices that are required by such government offices to be affixed with the registered seal and accompanied by a certificate of the registered seal** – documents that are specifically required by the government offices to be submitted in such a manner cannot be submitted in an electronic form or with an electronic signature.

In addition, the documents that are specifically required to confirm “the actual identity of the signer” may be conditionally allowed to be executed in an electronic form using an electronic signature. In that case, the electronic signature for such documents would be considered effective only if the specific requirement is met. Examples of the foregoing include the signature of the agency transactions agreement and the signature of written documents for subcontracting transactions.

An entity specialised in the storage of electronic documents may be designated as a certified electronic document centre by the MSICT. A certified electronic document centre ensures safety and accuracy in the storage of electronic documents. Documents kept in the certified electronic document centre will be presumed as unmodified by the law. Additionally, a certified electronic document centre must protect the personal information of the users in relation to the storage and distribution of their electronic documents, as prescribed by the relevant statutes. Similar to a certification service provider’s duty described under the heading Electronic Signatures and Certification Service, if a certified electronic document centre inflicts a loss on a user in relation to the storage of electronic

documents, it must compensate the user for such loss, unless it proves that the loss was not caused by intentional or negligent conduct. A certified electronic document centre is required under the law to be insured to compensate users for such loss.

Digital Identity

Although there are no specific laws or regulations that apply to digital identity, the government expressed its support for promoting a digital identification system. On 27 January 2022, the Ministry of the Interior and Safety and the Korean National Police Agency jointly launched the mobile driver's licence, which has a legal effect identical to the plastic licence card. The government aims to expand the types of mobile IDs and launch mobile IDs for the national honoree, the disabled, foreigners, and teenagers.

Yulchon LLC is one of the premier law firms in the South Korea and is headquartered in Seoul. It has more than 600 professionals across all its offices and practice areas, and its expertise spans the full suite of legal services. Yulchon's clients range from the top ranks of Korean conglomerates and global MNEs to emerging companies, family-run businesses and high-net-worth individuals. Yulchon's TMT practice team has approximately 60 professionals including attorneys, IT and security experts, and policy

and administrative specialists who deeply understand changes in both the national and international markets and possess up-to-date knowledge of technical and legal issues. Yulchon's TMT practice team delivers comprehensive and differentiated legal advisory service to its clients, both in the conventional TMT sector and the new technology fields emerging in the wake of the Fourth Industrial Revolution involving AI, big data, cloud, fintech, blockchain, mobility, and gaming.

Authors



Doil Son is the head of Yulchon's Technology Practice. He is the most recognised Korean TMT lawyer globally and a leading legal expert in the data industry. He serves in various

organisations, in positions such as co-chair of Technology Law Committee of the International Bar Association, co-chair of the TMT Committee of the Inter-Pacific Bar Association and council member of the Korea National Data Policy Committee. He has been consistently recognised as a leading individual in the TMT area by Chambers and Partners.



Kum Ju Son is a partner at Yulchon, primarily practicing in information and communications technology (ICT) platforms, antitrust, broadcasting/communication, energy,

personal data protection and data-based AI. From 2001-09, Mr Son was a judge of the various courts in Korea. From 2009-16, as a partner at Yulchon in the TMT field, Mr Son served as advisory attorney at the Korea Communications Commission (KCC) and the Ministry of Science and ICT, and represented KT, SKT and other communications and broadcasting operators. Elected to the 20th Korean National Assembly in 2016, Mr Son served four years and returned to TMT practice in 2020.

SOUTH KOREA LAW AND PRACTICE

Contributed by: Doil Son, Kum Ju Son, Seung Hyuck Han and Sun Hee Kim, **Yulchon LLC**



Seung Hyuck Han is a partner at Yulchon who mainly practices in the areas of antitrust law, telecommunications and broadcasting, and information and communication technology.

Since joining Yulchon in 2007, Mr Han has dealt with a range of proceedings before the Korea Fair Trade Commission, the Korea Communications Commission, the Ministry of Science and ICT, and the Korea Fair Trade Medication Agency, as well as various other civil, criminal and administrative proceedings.



Sun Hee Kim is a partner at Yulchon who focuses her practice on data protection, e-commerce, information and communications technology (ICT) and fintech. She also has

extensive experience in cross-border M&A. Sun Hee's data protection practice includes advising clients on data protection and management, including cross-border data transfers, data processing agreements, data protection training, and conducting gap analysis through compliance projects. Sun Hee also advises on data protection issues in the context of M&A transactions and is actively involved in the International Bar Association as an officer of the IBA's Asia Pacific Regional Forum.

Yulchon LLC

Parnas Tower, 38F
521 Teheran-ro,
Gangnam-gu
Seoul
Republic of Korea
06164

Tel: +82 2 528 5200
Fax: +82 2 528 5300
Email: mail@yulchon.com
Web: www.yulchon.com



Attorneys at Law
YULCHON

Law and Practice

Contributed by:

Lukas Morscher and Nadja Guberan-Flühler

Lenz & Staehelin see p.520



Contents

1. Metaverse	p.505
1.1 <u>Laws and Regulations</u>	<u>p.505</u>
2. Digital Economy	p.506
2.1 <u>Key Challenges</u>	<u>p.506</u>
3. Cloud and Edge Computing	p.507
3.1 <u>Highly Regulated Industries and Data Protection</u>	<u>p.507</u>
4. Artificial Intelligence and Big Data	p.511
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	<u>p.511</u>
5. Internet of Things	p.511
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	<u>p.511</u>
6. Audio-Visual Media Services	p.512
6.1 <u>Requirements and Authorisation Procedures</u>	<u>p.512</u>
7. Telecommunications	p.514
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	<u>p.514</u>
8. Challenges with Technology Agreements	p.515
8.1 <u>Legal Framework Challenges</u>	<u>p.515</u>
9. Trust Services and Digital Entities	p.518
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	<u>p.518</u>

1. Metaverse

1.1 Laws and Regulations

In Switzerland, there is no specific regulation in relation to the metaverse. The Swiss legislature strives to keep laws technology-neutral, thus the general rules apply, including as regards risks, liability, intellectual property, anti-money laundering and data privacy. There are, however, existing regulations that are particularly relevant in the context of the metaverse.

Switzerland has a suitable, proven and balanced legal framework; hence, only limited and targeted adjustments as regards metaverse/distributed ledger technology (DLT)/blockchain applications are currently contemplated. While the Swiss legislature is aware that the possibilities offered by the metaverse/DLT/blockchain go far beyond their application to alternative financing, there is a legislative focus on the financial sector.

As regards the application of the existing regulations on initial coin offerings (ICOs), the Swiss Financial Market Supervisory Authority (FINMA) published corresponding guidelines on 16 February 2018. Generally, FINMA focuses on the economic function and purpose of the tokens, as well as whether they are tradeable or transferable, in order to classify the tokens broadly into three “archetypes”:

- payment tokens (which include cryptocurrencies);
- utility tokens; and
- asset tokens.

The classification of the individual token impacts the applicable legal and regulatory framework—ie, tokens do not constitute a separate regulatory category. Since then, FINMA has issued further

guidelines on money laundering on the blockchain and, most recently, also on stable coins.

In December 2018, the Swiss Federal Council published a report on the legal framework for blockchain and DLT in the financial sector, which noted that the Swiss legal framework is, in principle, well suited to deal with new technologies.

The DLT Act

In September 2020, parliament adopted the Federal Act on the Adaption of Federal Law to Developments in Distributed Ledger Technology (the “DLT Act”), with which various federal laws were adapted in order for Switzerland to continue to develop as a leading, innovative and sustainable location in the context of the metaverse and, in particular, for blockchain and DLT activity.

The amendments include:

- a civil law amendment aimed at increasing legal certainty regarding the transfer of DLT-based digital assets;
- the possibility of segregation of digital assets in the event of bankruptcy; and
- the introduction of a “DLT trading facility” (as a new authorisation category), which may offer trading, settlement and clearing services in relation to digital assets.

Overall, these legislative amendments are expected to increase market access to fintech companies working in the field of DLT/blockchain technologies by improving legal certainty and removing certain regulatory barriers. The provisions enabling the introduction of uncertificated register securities that are represented on a blockchain entered into force on 1 February 2021, and the remaining provisions of the DLT Act entered into force on 1 August 2021.

Anti-money Laundering

Transactions made within the context of the metaverse and particularly transactions in cryptocurrencies may be carried out on an anonymous basis and related money-laundering risks are accentuated by the speed and mobility of the transactions made possible by the underlying technology. The “know your customer” (KYC) principle is the cornerstone of the anti-money laundering (AML) and combating the financing of terrorism (CFT) due diligence requirements that are generally imposed on financial institutions where AML/CFT legislation is aligned with international standards. KYC requires that financial institutions duly identify (and verify) their contracting parties (ie, customers) and the beneficial owners (when their contracting parties are not natural persons) of such assets as well as their origin. Together with transaction monitoring, KYC ensures the traceability of assets (ie, paper-trail) and allows the identification of money laundering and financing of terrorism indicia.

With respect to the metaverse, including DLT/blockchain applications, one of the challenges is that KYC and other AML/CFT requirements are designed for a centralised intermediated financial system, in which regulatory requirements and sanctions can be imposed by each jurisdiction at the level of the financial intermediaries operating on its territory (ie, acting as gatekeepers). By contrast, virtual currency payment products and services rely on a set of decentralised, cross-border, virtual protocols and infrastructure elements, none of which has a sufficient degree of control over, or access to, the underlying value (asset) and/or information, meaning that that identifying a touch-point for implementing and enforcing compliance with AML/CFT requirements is challenging.

Swiss AML legislation does not provide for a definition of virtual currencies. However, since the revision of the FINMA AML Ordinance in 2015, exchange activities in relation to virtual currencies, such as money transmitting (ie, money transmission with a conversion of virtual currencies between two parties), are clearly subject to general AML rules. Furthermore, the purchase and sale of convertible, virtual currencies on a commercial basis and the operation of trading platforms to transfer money, or convertible virtual currencies, from the users of a platform to other users are subject to Swiss AML rules.

Since DLT-trading facilities (the separate licence category introduced by the DLT Act as an amendment to the Financial Market Infrastructure Act (FMIA); see above) can carry out activities that qualify as financial intermediation under the Anti-Money Laundering Act (AMLA), they are to be included in the AMLA as specifically regulated financial intermediaries.

Data Protection

Personal data must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is processed or stored. Anyone processing personal data must ensure its protection against unauthorised access, its availability and its integrity, including in the metaverse environment (see 3. Cloud and Edge Computing regarding data protection principles).

2. Digital Economy

2.1 Key Challenges

Under Swiss law, there are no rules specifically applicable to the digital economy. There are, in particular, no regulations particularly regarding digital services, digital markets or content reg-

ulations. The Swiss legislature strives to keep laws technology-neutral, thus general rules (including as regards data protection) apply to the digital economy (see also **1. Laws and Regulations** regarding the metaverse; **4. Artificial Intelligence and Big Data** and **9. Trust Services and Digital Entities**).

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Cloud and Edge Computing

Under Swiss law, there are no rules specifically applicable to cloud and edge computing. There are, in particular, no regulations prohibiting, restricting or otherwise governing cloud and edge computing. The Swiss legislature strives to keep laws technology-neutral, thus general rules (including as regards data protection) apply to cloud and edge computing.

Personal data must be protected by appropriate technical and organisational measures against unauthorised processing regardless of where it is stored. Anyone processing personal data must ensure its protection against unauthorised access, its availability and its integrity. The use of cloud services may qualify as an outsourced processing service and, in cases where the servers of the cloud are located outside Switzerland and the personal data is not fully encrypted during transfer and storage, as an international transfer of personal data (see below). The Swiss Federal Data Protection and Information Commissioner (FDPIC) has issued a non-binding guideline setting out the general risks and data protection requirements with respect to the use of cloud services.

The Federal Act on the Surveillance of Mail and Telecommunication Traffic of 18 March 2016, as amended (*Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs*, BÜPF), applies to providers of derived communication services, which includes cloud service providers. Where telecommunication services are involved in criminal investigations, service providers are obliged to tolerate surveillance measures and to provide access to their data processing systems upon order by competent authorities. Specific rules may apply in regulated markets, such as the banking sector (eg, Circular 2018/3 relating to outsourcing, issued by FINMA, which applies to banks, insurers and securities firms organised under Swiss law, including Swiss branches of foreign banks, insurers and securities firms subject to FINMA supervision).

In the event a customer of a cloud services provider is subject to compliance requirements as set out above or respective contractual obligations towards a third party, applicable obligations have to be set out in writing in the contracts with the cloud services provider. This applies, in particular, to compliance with data protection regulations as imposed on the customers of cloud services providers.

Data Protection Legislation

Switzerland has dedicated data protection laws. The Federal Data Protection Act of 19 June 1992, as amended (DPA), and the Ordinance to the Federal Act on Data Protection of 14 June 1993, as amended (DPO), govern the processing of what in Switzerland is referred to as “personal data” by private parties or federal bodies. Processing of personal data by cantonal authorities is subject to separate state legislation. In addition, several other federal laws contain provisions on data protection, which further address the collection and processing of personal data,

especially as regards the processing of personal data in regulated industries (such as financial markets and telecommunications).

The Swiss Federal Code of Obligations sets forth restrictions on the processing of employee data, and Ordinance 3 to the Swiss Federal Employment Act (Employment Act) limits the use of surveillance and control systems by the employer.

The Swiss Federal Act on Telecommunications of 30 April 1997, as amended (TCA), regulates the use of cookies.

The Swiss Federal Unfair Competition Act regulates unsolicited mass advertising by means of electronic communications such as email and text messages.

Statutory secrecy obligations, such as banking secrecy (set forth in the Banking Act), financial institutions secrecy (set forth in the Financial Institutions Act (FinIA)), financial market infrastructure secrecy (set forth in the FMIA) and telecommunications secrecy (set forth in the TCA) apply in addition to the DPA.

The Banking Act, the FinIA and the Swiss Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector stipulate specific duties to disclose information.

The Swiss Federal Act regarding Research on Humans, the Swiss Federal Act on Human Genetic Testing and the Swiss Federal Ordinance on Health Insurance set out specific requirements for the processing of health-related data.

Personal Data

The DPA and DPO apply to the processing of any data relating to an identified or identifiable person, irrespective of its form – ie, to personal data

pertaining to natural persons (individuals) and personal data pertaining to legal entities (companies). A person is identifiable if a third party having access to the data on the person is able to identify that person with reasonable efforts. Pursuant to the DPA, “sensitive personal data” and “personality profiles” are to be considered as special categories of personal data that are subject to stricter processing conditions. Sensitive personal data is data on:

- religious, ideological, political or trade union-related views or activities;
- health, the intimate sphere or racial origin;
- social security measures; and
- administrative or criminal proceedings and sanctions.

A personality profile is a collection of personal data that permits an assessment of the essential characteristics of the personality of a natural person.

As a general principle, personal information must always be processed (this includes collection and usage) lawfully. Such processing is lawful if it is either processed in compliance with the general principles set out in the DPA (including, among others, the principle that the collection of personal information and, in particular, the purpose of its processing, must be evident to the data subject at the time of collection) or, if non-compliant with these general principles, is justified (eg, by the data subject’s voluntary informed consent or by law). The disclosure of personal information to third parties is generally lawful under the same conditions.

Cross-Border Data Transfers

Personal data may only be transferred outside Switzerland if the privacy of the data subject is not seriously endangered; in particular, due to

the absence of legislation that guarantees adequate protection in the jurisdiction where the recipient resides. The FDPIC has published a list of jurisdictions that provide adequate data protection. The countries of the EEA and Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, Monaco, New Zealand and Uruguay are generally considered to provide an adequate level of data protection as regards personal data relating to individuals (however, many do not as regards personal data relating to legal entities), while the laws of all other jurisdictions do not provide adequate data protection.

As regards data transfers to the USA, the Swiss-US Privacy Shield (which replaced the US-Swiss Safe Harbour Framework in 2017), under which Swiss companies were able to transfer personal data to their US business partners without the need to procure the consent of each data subject or to put additional measures in place, was declared invalid by the FDPIC in September 2020. The FDPIC concluded that although the Swiss-US Privacy Shield guarantees special protection rights for persons in Switzerland, it does not provide an adequate level of protection for data transfer from Switzerland to the USA pursuant to the DPA. As a result, Swiss companies can no longer rely on the Swiss-US Privacy Shield for the transfer of personal data from Switzerland to the USA without additional safeguards or justification (see below). Further, prior to any data transfer from Switzerland to the USA or any other country not providing adequate data protection, data controllers are advised to perform a so-called data transfer impact assessment, assessing the risks associated with such transfer. The FDPIC has taken note of the Trans-Atlantic Data Privacy Framework, which has been recently negotiated between the EU and

the USA and is currently reviewing this new data privacy framework.

In the absence of legislation that guarantees adequate protection, personal data may only be transferred outside Switzerland if, inter alia:

- sufficient safeguards (in particular, standard contractual clauses) ensure an adequate level of protection abroad;
- the data subject has consented in the specific case;
- the processing is directly connected with the conclusion or the performance of a contract (and the personal information is that of a contractual party); or
- disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules (ie, binding corporate rules).

In practice, in order to ensure an adequate level of data protection, data transfer agreements or data transfer clauses (ie, binding corporate rules) are regularly used. It is the responsibility of the data transferor to ensure that an agreement sufficiently protecting the rights of the data subjects is concluded. The FDPIC provides a model data transfer agreement which can be accessed on its website. The model data transfer agreement is currently being revised by the FDPIC. The model data transfer agreement is based on Swiss law and reflects, to a large extent, the former version of the standard contractual clauses of the European Commission for data transfers (SCC).

The FDPIC recognises the new set of SCC, issued by the European Commission on 4 June 2021, for data transfers to countries not providing adequate data protection level, provided that

the necessary adaptations and amendments are made for use under Swiss data protection law. Since 1 January 2023, data transfers must be based on the new SCC or the revised model data transfer agreement once available (the old SCC as well as the model data transfer agreement may no longer be used for such transfers).

The FDPIC has to be notified of the use of such agreements accordingly. Furthermore, in the case of regular processing of particularly sensitive data or personality profiles, or regular disclosure of personal data to third parties (whereby group companies qualify as third parties within the meaning of the DPA), the respective data files must be registered with the FDPIC. The data files have to be registered prior to being established. However, there are exemptions from this registration duty; in particular, if the respective data is processed as a matter of law or in the case of a voluntary appointment of a data protection officer. A list of business organisations that have appointed a data protection officer is publicly accessible on the FDPIC's website.

Data Protection Officers

The appointment of a data protection officer is not mandatory in Switzerland. However, the registration of data collections is not required if the owner of a data collection has appointed a data protection officer that independently monitors data protection compliance within the owner's business organisation and maintains a list of data collections. The appointment of a data protection officer will only result in a release of the duty to register data collections if the FDPIC is notified of the appointment of a data protection officer. A list of business organisations that have appointed a data protection officer is publicly accessible on the FDPIC's website. The data protection officer has two main duties. First, the data protection officer audits the processing of

personal data within the organisation and recommends corrective measures if they find that the data protection regulations have been violated. They must not only assess compliance of the data processing with the data protection requirements on specific occasions, but also periodically. The auditing involves an assessment of whether the processes and systems for data processing fulfil the data protection requirements, and whether these processes and systems are enforced in practice. If the data protection officer takes note of a violation of data protection regulations, they must recommend corrective measures to the responsible persons within the organisation and advise them on how to avoid such violations in the future. The data protection officer does not, however, need to have direct instruction rights. Second, the data protection officer maintains a list of the data collections that would be subject to registration with the FDPIC. The list must be kept up to date. Unlike the data collections registered with the FDPIC, the internal data collections do not have to be maintained electronically nor must they be available online. However, they must be made available on request to the FDPIC and to data subjects.

Swiss Alignment with International Data Protection Standards

Switzerland is a state party to certain international treaties regarding data protection, such as the European Convention on Human Rights and Fundamental Freedoms and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention ETS 108) and its additional protocol of 8 November 2001. Although Switzerland is not a member of the EU and, hence, has neither implemented the EU Data Protection Directive 95/46/EC nor is directly subject to the EU General Data Protec-

tion Regulation 2016/679 (GDPR), it has been officially recognised by the European Commission as providing an adequate level of protection for data transfers from the EU.

The Swiss parliament recently adopted a revision of the DPA. The revision of the DPA aligns the DPA with international rules on data protection in order to comply with the revised Convention ETS 108 and the GDPR. This will allow Switzerland to uphold its status as a country adequately protecting personal data from an EU perspective, which allows for easier transfer of personal data from the EU and the ratification of Convention ETS 108.

The revised DPA largely follows the regime provided by the GDPR with some reliefs and very limited “Swiss finishes” (ie, rules that go beyond the requirements of the GDPR – most importantly, every country to which personal data is transferred to will have to be explicitly named). The revised DPA will enter into force on 1 September 2023.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Big data and artificial intelligence (AI) offer new opportunities to develop social or scientific knowledge and can be the basis for further forms of value creation by companies. In general, there is no cross-sector regulation in Switzerland regarding big data or AI. As regards the processing of personal data, the right to privacy and the protection of personal data must be safeguarded (see 3. **Highly Regulated Industries and Data Protection** regarding data protection principles). While government authorities periodically review

developments as regards big data and AI, it is acknowledged that any regulation should be technology-neutral in order to accommodate new developments within the existing legal and regulatory framework. This enables businesses located in Switzerland to make optimal use of upcoming technologies and advances, and to efficiently adapt their business models and processes as required or desired.

The Federal Council has set up a federal working group on artificial intelligence under the direction of the State Secretariat for Education, Research and Innovation (SERI), which facilitates the exchange of knowledge and opinions and the co-ordination of Switzerland’s positions in international bodies. Based on a report of SERI submitted to the Federal Council outlining existing measures, an assessment of possible fields of action and considerations on the transparent and responsible use of AI, the Federal Council concluded on 13 December 2019 that Switzerland is, in general, well suited to address AI applications, business models and challenges. Thus, there is no immediate need to adapt the existing legislative framework, subject to certain specific areas (such as mobility, security policy, education and research) in which, however, a multitude of measures have already been initiated to address corresponding challenges. Further, on 25 November 2020, the Federal Council adopted guidelines for dealing with AI in the Federal Administration.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

The internet of things (IoT) refers to objects and devices which are connected to a network such

as the internet and which use the network to communicate with each other or make information available. The connecting device may be a modem, network-attached storage (NAS), a webcam, intelligent light switches or smart TVs connected to an internal network or the internet. The Swiss regulatory framework encourages digital services – in particular, due to the technology-neutral approach of the legislator – thereby allowing for ample room for development for technology-driven business models and companies. Hence, there are generally no regulation-induced impediments to technological innovation under current law. Government authorities periodically review developments in technology and generally emphasise the importance of making use of technological progress. Considerable efforts are undertaken to further facilitate lower barriers to market entry for technology-driven business models.

As more and more intelligent devices are connected to the internet, not only has the number of communications participants involved grown but also the number of vulnerable devices that may be misused by hackers (eg, for sending spam emails). Such devices need to be adequately protected (eg, by using individual passwords or restricted access) and respective software has to be kept updated. Between objects and devices that communicate with each other, large amounts of information and data are typically exchanged. This may also have an impact on the protection of personal data and the general rules of data protection apply. Any data subject is protected from their personal data either being processed in a way that is not in compliance with the law or used for purposes other than those communicated or apparent to the data subject, unless the data subject consents to this processing or unless another statutory justification

applies (see **6. Audio-Visual Media Services** regarding key data protection principles).

To protect critical information and communication infrastructure in Switzerland, the Federal Council has commissioned the Reporting and Analysis Centre for Information Assurance (*Melde- und Analysestelle Informationssicherung*, MELANI) which is part of the National Cyber Security Centre (NCSC). To prevent devices within the IoT from being misused by hackers, MELANI recommends preventive measures on its website. These measures include:

- the establishment of a separate network segment for devices connected to the internet and devices connected to personal data;
- restricting access from the internet to the device;
- using protocols allowing only encrypted connection; and
- using complex passwords and two-factor authentication.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Broadcast Media Regulation

The broadcasting sector has three main authorities responsible for the granting of licences. The Federal Council is the licensing authority for the Swiss Broadcasting Corporation (SBC). With respect to other licences, licensing competence has been delegated to the Swiss Federal Department for the Environment, Transport, Energy and Communications (DETEC). The Federal Office of Communications (OFCOM) puts the licences out for tender and consults interested groups. OFCOM further fulfils all sovereign and regulatory tasks related to the telecommunications and

broadcasting (radio and television) sectors. It fulfils an advisory and co-ordinating function for the public and policymakers. It also guarantees that basic services are provided in all parts of the country and throughout the population.

The Federal Media Commission (FMEC) advises the Federal Council and the Federal Administration in relation to media issues. The Federal Radio and Television Act of 24 March 2006, as amended (RTVA), provides for an Independent Complaints Authority for Radio and Television, which deals with complaints that relate to the editorial programme and rules on disputes over denied access to a programme. In Switzerland, apart from the communications sector, regulation of the media sector is also dealt with at a federal level. The broadcasting, processing and reception of radio and television programme services are regulated by the RTVA, the Federal Ordinance on Radio and Television of 9 March 2007, as amended (RTVO), and related regulation.

Licensing Requirements

Broadcasters of programme services are, in principle, required to obtain a licence. Broadcasters that neither request the splitting of revenue nor guaranteed wireless terrestrial distribution may operate their service without a licence. However, such broadcasters need to notify OFCOM. Also, broadcasters of programme services of minor editorial importance (such as programme services that can only be received by fewer than 1,000 people at the same time) do not fall under the scope of the RTVA and do not need a licence or registration. If the broadcaster of a radio programme service is granted a licence under the RTVA, it is at the same time granted a licence under the TCA for use of the frequency spectrum (no separate application is needed). Cable TV operators are under a duty to broadcast, in

the respective coverage area, the TV programme services of broadcasters that have been granted a licence. Licences are awarded by public tender. There are no rules specifically applicable to the operation of an online video channel (such as a YouTube channel). Since the Swiss legislature strives to keep laws technology-neutral the general rules apply to the operation of online video channels. To be awarded a licence, the applicant must:

- be able to fulfil the mandate;
- possess sound financial standing;
- be transparent regarding its owners;
- guarantee compliance with employment law regulations and the working conditions of the industry, the applicable law and in particular the obligations and conditions associated with the licence;
- maintain a separation of editorial and economic activity; and
- have registered offices in Switzerland.

In general, the number of licences a broadcaster and its group companies may acquire is limited to a maximum of two television and two radio licences (this does not apply to SBC). If there are several applicants for one licence, preference will be given to the candidate that best fulfils the performance mandate. Often, independent applicants (ie, those not belonging to a media corporation that already possesses other licences) are deemed to be better able to fulfil this criterion by DETEC. The fee per year for a broadcasting licence amounts to 0.5% of the gross advertising revenue that exceeds CHF500,000. Furthermore, administrative charges will incur in relation to the radio and TV licence as well as to the telecommunications licence. These charges are calculated on the basis of time spent. A reduced hourly rate applies to the granting, amending or cancelling of a licence for the broadcasting of a

radio or television programme service as well as for the radio communications licence.

Investment Obligation in Swiss Film Production

On 15 May 2022, the introduction of an investment obligation in Swiss film production for streaming services was approved by the Swiss people. The amendment of the Film Act entails adjustments to the existing Film Ordinance and requires a new ordinance with implementing provisions for the implementation of the European quota and the obligation to invest in Swiss film-making (*Verordnung über die Quote für europäische Filme und Investitionen in das Schweizer Filmschaffen*, FQIV). The amendments include:

- an obligation for streaming service provider to invest 4% of its revenue generated in Switzerland in Swiss film productions;
- the investment may be made either directly in Swiss film production or by payment of a substitute levy which will be used to support Swiss film production; and
- an obligation for streaming service provider to broadcast at least 30% of series or films produced in Europe.

The consultation by the Federal Council will last until 17 February 2023.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

In Switzerland, the telecommunications sector is regulated at federal level. The main source of law is the TCA, which governs any transmission of information by means of telecommunications techniques, except for television and radio programme services. Further sources of law include

the Federal Ordinance on Telecommunications Services of 9 March 2007, as amended (OTS), and the Federal Ordinance on Telecommunications Installations of 25 November 2015, as amended (TIO). As regards electronic communications equipment, Swiss requirements are largely in line with international and, particularly, European standards. The Federal Council can adopt technical regulations on telecommunications installations, particularly basic technical requirements for telecommunications, evaluation, certification or declaration of conformity. OFCOM regularly designates technical standards. Compliance with these standards fulfils the basic requirements set out by the Federal Council. The telecommunications law framework applies to telecommunications service providers (TSPs), which are providers of services qualifying as telecommunications services. The TCA defines TSPs as services transmitting information for third parties using telecommunications techniques, which include the sending or receiving of information by wire, cable or radio using electrical, magnetic, optical or other electromagnetic signals.

In the telecommunications sector there are two regulatory agencies: the Federal Communications Commission (ComCom) and OFCOM. Fixed line and mobile telephony/satellite services are regulated by the TCA and its implementing ordinances.

The latest TCA revision, which entered into force on 1 January 2021, includes improvements in the area of consumer protection (including in relation to international roaming, open internet, unfair competition and protection of children and adolescents) and provides for deregulation and administrative simplification (including abolition of the general notification and licensing requirements). Under the revised TCA, among other

things, the registration obligation for TSPs is limited to TSPs which, for the provision of telecommunications services, use:

- radio frequencies that require a licence; or
- resources administered on a national level (eg, short numbers that are assigned to emergency calls or rescue and breakdown services).

All other TSPs, while still having to comply with the obligations of the TCA, are no longer required to register with OFCOM. ComCom awards one or more universal service licences to TSPs to ensure that universal service is guaranteed for the whole population of Switzerland in all parts of the country.

Providers of Voice over Internet Protocol (VoIP) services remain unregulated if they provide online services only, without transmitting data using telecommunications techniques. If the provider qualifies as a TSP (eg, where a VoIP customer can also be reached by way of a fixed line telephone number as part of the public switched telephone network), the TCA applies. However, ComCom does not require such VoIP providers to fulfil all the obligations the TCA imposes on regular TSPs; for example, they are under no duty to enable free carrier pre-selection (since there is no close link that needs to be broken between a network and a service operator) or the identification of the caller's location in the case of emergency calls (which would be technically difficult to establish).

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Under Swiss law, there is no specific regulation in relation to IT service agreements. However, there are statutes governing the general outsourcing of services to (IT) providers in certain industries, eg, the financial industry, telecommunications and the public sector. As regards financial services, the sector-specific regulation set out below applies to the outsourcing of business areas (infrastructure or business processes).

Swiss Banking Secrecy

Article 47 of the Swiss Federal Banking Act of 8 November 1934, as amended (the "Banking Act"), on banking secrecy, protects customer-related data from disclosure to third parties and applies to all banking institutions in Switzerland. Any disclosure of non-encrypted data to a supplier is only allowed with the express consent of each banking customer. Consent can be given under the bank's general terms of business if they are made an integral part of the contract between the bank and its customers. The Banking Act does not prohibit the transfer of encrypted data (where the supplier cannot identify individual customers).

The FINMA Outsourcing Circular

Circular 2018/3 (the "Outsourcing Circular") relating to outsourcing issued on 21 September 2017 by FINMA (the supervisory authority for banks, insurers, reinsurers, stock exchanges, securities firms, collective investment schemes and audit firms) applies to banks, securities firms and insurers organised under Swiss law, including Swiss branches of foreign banks, securities firms and insurers which are subject to FINMA supervision. As of 1 January 2021, the Outsourcing Circular also applies to managers of

collective assets organised under Swiss law, including Swiss branches of foreign managers of collective assets and fund management companies with a registered office and ahead office in Switzerland as well as to self-managed *sociétés d'investissement à capital variable* (SICAVs).

Before outsourcing significant business areas, these institutions must comply with the detailed measures set out in the Outsourcing Circular, including:

- the obligation to keep an inventory of all outsourced services, which must include:
 - (a) proper descriptions of the outsourced function;
 - (b) the name of the service provider and any subcontractors;
 - (c) the service recipient and the person or department responsible within the company;
- careful selection, instruction and control of the supplier; and
- conclusion of a written contract or a contract in some other format that can be evidenced in text form with the supplier setting out, among other things, security and business continuity requirements and audit and inspection rights.

The customer remains responsible for the outsourced business areas, so it must ensure their proper supervision. Swiss banks, securities firms and insurers must also consider that outsourcings to independent service providers are generally considered to increase operational risks and therefore lead to additional capital requirements for them.

Essential Service Outsourcing

A financial market infrastructure subject to the FMIA and the implementing ordinance (FMIO), as amended (which includes a stock exchange,

multilateral trading facility, central counterparty, central securities depository, trade repository or payment system), must obtain prior approval from FINMA if it wishes to outsource essential services such as risk management. If such an outsourcing is proposed by a financial market infrastructure that the Swiss National Bank (SNB) considers to be systemically important, FINMA must consult with the SNB beforehand.

When outsourcing an essential service, the financial market infrastructure must:

- carefully select, instruct and control the service provider;
- integrate the outsourced service into its internal control system; and
- monitor the services rendered by the service provider on an ongoing basis.

Reciprocal rights and duties must be set out in a written agreement with the service provider. If a financial market infrastructure outsources its services, it remains responsible for maintaining compliance with its duties under the FMIA. Outsourcing services to another jurisdiction also requires the application of appropriate technical and organisational measures to ensure the observance of professional confidentiality and data protection law. Contracting parties of financial market infrastructures whose data is to be sent to a service provider abroad must be informed. The financial market infrastructure, its internal audit function, the external audit firm, FINMA and (if systemically important) the SNB must be able to inspect and review the outsourced service.

Consolidated Rules on Outsourcing

Since 1 January 2020, consolidated rules on outsourcing also apply to both financial institutions regulated by the new Financial Institu-

tions Act (FinIA) and its implementing ordinance (FinIO), as amended and financial service providers regulated by the new Financial Services Act (FinSA) and its implementing ordinance (FinSO), as amended.

Financial institutions (which include portfolio managers, trustees, managers of collective assets, fund managers and securities firms), under the FinIA and FinIO, may only delegate tasks to third parties that have the necessary skills, knowledge, experience and authorisations to perform such tasks. The financial institution must therefore carefully instruct and supervise any such third parties. FINMA may make the delegation of investment decisions to a third party located abroad subject to an agreement on co-operation and information exchange between FINMA and the competent foreign supervisory authority (particularly if such an agreement is required under the other country's laws). If a financial institution outsources significant functions, the outsourcing service provider will be subject to information and reporting duties to, and audits by, FINMA.

The liability of financial institutions and their corporate bodies is subject to the CO. If a financial institution outsources a task to a third party, it will be liable for any damage caused by the outsourcing service provider, unless it can prove that it has diligently selected, instructed and monitored the provider (special rules may apply to fund management companies).

Financial services providers (which include client advisers and producers and providers of financial instruments), under the FinSA and FinSO, may only delegate tasks to third parties that have the necessary skills, knowledge, experience and authorisations to perform such tasks. The financial services provider must therefore care-

fully instruct and supervise the third parties. If a secondary (sub-contracted) financial services provider is required to provide a financial service for the principal's clients, the principal financial services provider will remain liable for:

- the completeness and accuracy of the client information;
- fulfilling the duties in relation to the information;
- the adequacy and suitability of the financial services; and
- documentation and accountability.

If the secondary financial services provider has reasonable grounds to suspect that the client information is incorrect or that such duties were not fulfilled by the principal financial services provider, it may provide its service only after it has ensured the completeness and accuracy of the information and compliance with the code of conduct.

Personal Data Protection

The outsourcing of services to an IT service provider may also impact the protection of personal data. Any data subject is protected from their personal data being processed in a way that is not in compliance with the law or used for purposes other than those communicated or apparent to the data subject, unless the data subject consents to this processing or unless another statutory justification applies (see **3. Cloud and Edge Computing** regarding data protection principles). However, personal data may be given to outsourcing suppliers based on a contract or statutory law if the customer ensures that the supplier will only process data in a way that the customer is itself entitled to, and that the supplier will comply with the applicable data security standards, and if no statutory or contractual secrecy obligations prohibit this data processing.

As the customer remains liable towards the data subject for the compliant handling of personal data by the supplier, and reflecting the growing importance of data protection, there is a tendency not to apply a liability cap for breaches of data protection or other regulatory requirements in outsourcing agreements. This is particularly the case when sensitive data such as business secrets or bank customer data are involved.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Trust Services, Electronic Signatures

The CO sets out the principles governing e-signatures and refers to the Electronic Signatures Act (ESA) for the technical details, which in turn refers to its respective ordinance. An electronic signature is defined as electronic data that is joined or linked logically to other electronic data and which serves to authenticate such other data.

The ESA distinguishes four levels of e-signatures:

- regular e-signatures;
- advanced e-signatures;
- regulated e-signatures; and
- authenticated e-signatures.

The authenticated e-signature in combination with an authenticated time stamp is deemed equivalent to a handwritten signature. Regulated e-signatures are not deemed equivalent to handwritten signatures; however, they may be used, for example, to evidence the authenticity of electronic invoices or to guarantee the integrity of electronically archived documents. Both

authenticated and regulated e-signatures can only be obtained from a recognised provider of certification services. A list of all such providers in Switzerland is available on the competent federal authority's website.

Authenticated e-signatures are treated like handwritten signatures. Therefore, e-signatures cannot be used where the law sets out additional formal requirements, for example, in the case of a will (which must be handwritten in its entirety) or real estate deals (requiring a public deed). Additionally, authenticated and regulated e-signatures are only available for natural persons, not for legal entities. Natural persons can, however, electronically sign on behalf of a legal entity using their personal authenticated e-signature. In addition, entities in possession of a unique business identification number may obtain a regulated electronic seal, which is essentially equivalent to a regulated e-signature.

Although e-signatures were introduced more than ten years ago, their use in Switzerland is limited. To date, only a small percentage of the population actually has an e-signature. This may be explained by Swiss law's freedom of form, enabling parties to contract without formal requirements in most cases, as well as the relatively high cost and complicated application of e-signatures and the prepayment policy applied by many online businesses, shifting the risk to the customer, who needs to trust that the other party will indeed fulfil its contractual obligations. Since payment has already been received, the online businesses generally do not have the need to verify the other customer's identity.

Electronic Identification

Following the dismissal of the Federal Act on Electronic Identification Services in the popular vote of 7 March 2021, the Federal Council

instructed the Federal Department of Justice and Police to draft a proposal for a secure governmental electronic identification (eID). From 2 September to 14 October 2021, the Federal Office of Justice conducted an informal public consultation resulting in 60 submissions. Based on the results of the consultation, the Federal Council defined the principles for the implementation of a new governmental eID and has now opened the consultation on the eID Act. The eID Act foresees, among others, that:

- the federal government shall provide an app for smartphones in which the eID can be securely managed;
- the federal government shall be responsible for issuing the eID and shall operate the infrastructure serving as a basis for the eID;
- users shall have the largest control possible over their data (self-sovereign identity) and data protection shall be ensured, among others, by the system itself (“privacy by design”) and also by minimising the required data flows (principle of data minimisation) as well as by decentralised data storage;

- the Swiss eID system shall meet international standards so that it may also be recognised and used abroad in the future;
- the use of an eID shall be voluntary and free of charge; and
- all authorities, including cantons and municipalities, shall be obliged to accept the eID when they conduct an electronic identification, eg, when issuing a confirmation of residency or an extract from the debt enforcement register.

The governmental infrastructure to be created for the purpose of the eID shall also be made available for use by municipal and cantonal authorities as well as private parties.

Lenz & Staehelin provides tailored services to clients operating and investing in all areas of the TMT sector, through a dedicated and multidisciplinary TMT team. It advises start-ups, investors, technology companies and established financial institutions in their TMT activities. Drawing, as required, on experts in various practice groups for effective and cost-efficient advice, Lenz & Staehelin strives for long-term trusted relationships with clients, becoming a partner

in the development and marketing of their services, throughout their various life cycles. Reflecting the diverse nature of TMT projects, the multidisciplinary team covers the full range of relevant legal services while successfully navigating the regulatory environment through close contacts with regulators, including in the areas of banking and finance, TMT and outsourcing, corporate and M&A, commercial and contracts, competition, tax and employment.

Authors



Lukas Morscher is a partner and the head of the technology and outsourcing practice and co-head of the fintech practice in the Zurich office of Lenz & Staehelin. He is also an expert

on digitisation in the financial services industry. He practises in transactional and regulatory matters, outsourcing (IT and business process transactions), TMT, internet and e-commerce, data privacy, fintech, blockchain and digitisation. A member of SwissICT, SWICO, the Swiss-American Chamber of Commerce and the International Technology Law Association (ITechLaw), Lukas is a frequent speaker on topics related to fintech and digitisation.



Nadja Guberan-Flühler focuses her practice on the fields of technology, media, telecommunications and corporate law as well as outsourcing transactions,

licensing, e-commerce and data protection matters. She works as an associate in the Zurich office of Lenz & Staehelin and is a member of the firm's technology and outsourcing, corporate and M&A, intellectual property and real estate practice groups.

Lenz & Staehelin

Brandschenkestrasse 24
CH-8027
Zurich
Switzerland

Tel: +41 58 450 80 00
Fax: +41 58 450 80 01
Email: zurich@lenzstaehelin.com
Web: www.lenzstaehelin.com

The logo for Lenz & Staehelin, featuring the firm's name in a white, sans-serif font on a dark blue rectangular background. A thin red horizontal line is positioned above the text.

LENZ & STAEHELIN

Law and Practice

Contributed by:

John Formichella, Naytiwut Jamallsawat, Onnicha Khongthong
and Gawin Vattanatham

Formichella & Sritawat see p.534



Contents

1. Metaverse	p.522
1.1 <u>Laws and Regulations</u>	p.522
2. Digital Economy	p.522
2.1 <u>Key Challenges</u>	p.522
3. Cloud and Edge Computing	p.525
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.525
4. Artificial Intelligence and Big Data	p.526
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.526
5. Internet of Things	p.527
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.527
6. Audio-Visual Media Services	p.528
6.1 <u>Requirements and Authorisation Procedures</u>	p.528
7. Telecommunications	p.529
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.529
8. Challenges with Technology Agreements	p.531
8.1 <u>Legal Framework Challenges</u>	p.531
9. Trust Services and Digital Entities	p.532
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.532

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

1. Metaverse

1.1 Laws and Regulations

Thailand currently has no specific law or regulation relating to the metaverse. As a result, the metaverse is governed by general laws and regulations such as the Civil and Commercial Code (CCC), the Electronic Transactions Act B.E. 2544 (2001), the Personal Data Protection Act B.E. 2562 (2019) (PDPA), IP laws and the Cyber Security Act B.E. 2562 (2019) (CSA).

As the metaverse has a persistent virtual environment that allows access to and the co-working of many individual virtual realities, it is likely that a legal relation or a legal dispute may arise in the metaverse. Any agreement or contract made in the metaverse is considered valid under Thai law if the electronic signature can be identified and verified by the signatory as being their own, and if the method/channel used for the signing is reliable for the purpose for which the data is generated or sent, taking into account the circumstances of an agreement between the parties under the Electronic Transactions Act B.E. 2544 (2001).

Furthermore, the relevance of the PDPA may be triggered insofar as personal data is used in the platform. In addition, real-time interaction activities that may occur are likely to involve biometrics data in connection with motion or sentimental expression considered as sensitive data. Consequently, metaverse developers must include a channel/methodology to obtain explicit consent from the user prior to collecting and processing data, and to ameliorate data protection measurements by complying with the PDPA.

Looking into transactions, metaverse platforms necessitate the use of digital assets as a form of payment for goods and services. However, the

legislation to facilitate the use of digital assets as a means of payment in Thailand is inadequate.

With respect to IP in the metaverse, Thailand has ensured rights regarding IP in the Copyright Act B.E. 2537 (1994) (CRA), the Patent Act B.E. 2522 (1979) (PA) and the Trademark Act B.E. 2537 (1994). As a result, certain assets in the metaverse, such as computer software, NFTs, software processes, etc, will be protected under Thai IP law, subject to compliance with the relevant laws.

Even though there is legislation in Thailand covering this cutting-edge technology, the laws tend to be defensive instruments rather than preventative as most of them, such as the CSA, designate a committee to create plans or measurements to handle issues that may arise. Following the introduction of the metaverse, Thailand's government sector is currently in the primary stage in matters regarding this, such as law enforcement, jurisdiction, legislation, etc.

2. Digital Economy

2.1 Key Challenges

Master Plan for Digital Economy B.E. 2561-2565 (2018–2022)

Thailand currently has the Development of Digital Economy and Society Act B.E. 2560 (2017), under which the Master Plan for Digital Economy B.E. 2561-2565 (2018–2022) was prescribed. The plan focuses on four strategies:

- to improve digital manpower;
- to enhance the Thai economic sector towards a digital Thailand;
- to drive communities into the digital economy; and

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthong and Gawin Vattanatham, Formichella & Sritawat

- to improve infrastructure to support digital innovations.

In order to accomplish these goals, the plan drives the following ten programmes:

- Digital Manpower;
- Digital Citizen;
- Digital Transformation;
- Digital Industry Promotion;
- Digital Startup;
- Digitalised Community;
- Social Digital Innovation;
- Smart City;
- Big Data and Innovation; and
- Cyber Security.

According to the Performance Report produced by the Digital Economy Promotion Agency, three of the strategies have met the target, but the improvement of infrastructure to support digital innovations has not occurred. Moreover, amendments and updates to certain laws and regulations have been planned, as follows:

- tax measures to promote the use of computer programs by Small and Medium Business Entrepreneurs, such as a two-time Corporate Income Tax exemption when purchasing or utilising software services;
- a 2.5-times Corporate Income Tax exemption for training or providing training sessions for employees to enhance skills in science, technology, engineering or mathematics (STEM);
- amendments to laws and regulations that hinder investments, such as pushing forward the CCC to attract foreign investors to invest in start-ups in Thailand, such as Venture Capital;
- issuing a notification and development manuals for a smart city to promote investment and tax benefits for the development of smart

city areas and smart city system developing businesses; and

- legislating a royal decree for Capital Gains Tax exemptions in targeted companies.

Master Plan for Digital Economy B.E. 2566-2570 (2023–2027)

This was recently prescribed, with the aim of developing a strong, resilient and dynamic digital economy and society with advanced human capital, technology and innovation. This recent plan focuses on four strategies:

- to adjust human capital to cope with the digital economy and society;
- to change the old-fashioned economy to a high-value digital economy;
- to provide opportunities to spread prosperity equally; and
- to enhance the efficiency of digitalised innovation infrastructure.

Digital Asset Businesses Emergency Decree B.E. 2561 (2018) (DAB)

The DAB was promulgated to address the rising trend of cryptocurrency usage and investments with an exorbitant amount of capital in various digital currency brokers in recent years. The DAB empowered the Securities and Exchange Commission (SEC) to prescribe policies for encouragement and development, together with regulating digital currency and digital currency operators.

After the DAB was enforced, substantial numbers of businesses associated with cryptocurrencies and digital tokens have obtained applicable licences from the SEC. The licence categorises the operators into the following types of business operation:

- Digital Asset Exchange;

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

- Digital Asset Broker;
- Digital Asset Dealer;
- ICO Portal;
- Digital Asset Advisory Service; and
- Digital Asset Fund Manager.

Digital asset businesses

Digital asset businesses under the DAB are categorised into three types:

- Digital Asset Exchange;
- Digital Asset Broker; and
- Digital Asset Dealer.

Those who intend to operate a digital asset business shall be approved by the Minister of Finance upon recommendation of the SEC. In undertaking digital asset businesses, the approved operators shall comply with the rules, conditions and procedures as specified in the notification of the SEC, such as:

- having adequate sources of capital covering business operation and other several risks;
- having reliable operating systems and data security systems;
- maintaining records of assets belonging to individual clients;
- segregating clients' assets from their own assets; and
- conducting Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures.

When any digital asset business is in a situation where its financial condition or operation may cause damages to the public or is in violation of relevant regulations, the SEC is empowered to order such business to rectify the problem or it can temporarily suspend the business operation wholly or partially. If the digital asset business still fails to comply or has repeated the violations, the Minister of Finance is empowered to

revoke business approval, upon a recommendation from the SEC.

Preventing the exploitation of digital assets to facilitate illegal transactions

The DAB obliges issuers of digital tokens who are willing to accept cryptocurrencies in the offering process, or operators of digital asset businesses who are willing to accept cryptocurrencies from the counterparties in any transaction, to only accept cryptocurrencies obtained from or deposited with operators of digital asset businesses that are regulated/licensed under the DAB. The rationale is to preserve the integrity of markets by ensuring that the cryptocurrencies being transacted come from traceable sources.

Furthermore, the DAB states that digital asset businesses and ICO portals are considered "Financial Institutions" under the Anti-Money Laundering Act B.E. 2542 (1999), to prevent the exploitation of digital assets as a channel for money laundering.

Maintaining financial and economic stability

Where transactions, business operations or other activities related to digital assets may significantly affect the stability of the national financial system or economy, the Minister of Finance, upon approval of the Cabinet, is empowered to prohibit digital asset businesses from engaging in any digital asset-related activity, or to suspend their operations wholly or partially.

Preventing unfair trading practices

The DAB imposes offences of unfair trading in relation to the purchase, sale or exchange of digital assets taking place in a Digital Asset Exchange in a similar manner to the corresponding provisions in the Securities and Exchange Act B.E. 2535 (1992), such as false dissemination, insider trading, front running and market

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

manipulation. This is to ensure that secondary markets for digital assets are fair, transparent and efficient, market integrity is preserved, and investors are protected.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Electronic transaction services using cloud and edge computing are common in Thailand due to the rapid advancement of technologies in the country. The notification regarding Guidelines for Using Cloud Services B.E. 2562 (2019) (NGCS) was issued by the Electronic Transactions Commission (ETC) under the Electronic Transactions Act (ETA) B.E. 2544 (2001).

The NGCS provides cloud computing service guidelines, as follows.

Technical Precautions

Service providers shall have safeguards for technical security and reliability, such as Virtual Infrastructure, access control identity verification, System Development Life Cycle (SDLC), maintain the security in software development and Application Programming Interface (API), etc.

Service Efficiency

A cloud computing user shall consider the efficiency of the service in the Service Level Agreement, which covers points such as availability, response time, capacity, service support and an exit plan.

Security

A cloud computing user shall consider the security measurements of the service in the Service Level Agreement, which covers points such as international standard reliability, authentication

level and outsourcing, data classification and key access control policy, security management and incident reports, data entry and system usage verification, vulnerability assessments and penetration testing, and good governance.

Data Management

A cloud computing user shall consider the Service Level Agreement in regard to data classification, data reserve and recovery, data cycle and data transfer.

Financial Institutions

The Bank of Thailand (BOT) has notified the Criteria for Supervising Information Technology Risk, SorNorSor. 21/2562 (2019) ("BOT notification"), which focuses mainly on regulating the IT outsourcing of finance institutions, such as cloud computing, which must be the subject of an annual IT report submitted to the BOT. The BOT notification also prescribes the Third-Party Risk Management Implementation Guideline ("BOT Guideline"), under which finance institutions must comply with the BOT notification. The BOT Guideline mainly targets risk governance, third-party risk management and BOT IT outsourcing reports.

In regard to cloud computing, financial institutions shall maintain the confidentiality of clients' personal data, as prescribed in the PDPA and the BOT notification regarding Market Conduct B.E. 2563 (2020) ("Market Conduct notification"). The Market Conduct notification focuses on supervising the protection of clients' personal data and the disclosure thereof to a third party.

Insurance

The Office of Insurance Commission (OIC) notified the OIC notification regarding the criteria to supervise and manage the information technology risk of insurance companies B.E. 2563 (2020)

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

(“OIC notification”). Consequently, the Guideline of Supervising the Use of IT Outsourcing Service B.E. 2564 (2021) (“OIC Guideline”) was prescribed to comply with the OIC notification. The OIC Guideline mainly targets the supervision of IT outsourcing, the risk management of IT outsourcing, the criteria involved in outsourcing, the model for insurance companies to manage unexpected scenarios, business continuity management (BCM), outsourcing security and IT outsourcing reports.

In regard to cloud computing, the company shall have an international data protection standard, such as data encryption and key management. In addition, the company shall have measurements to recall all user data from the outsourcer and ensure that the outsourcer is competent to destroy users’ data after the termination of service. Moreover, the outsourcer shall maintain data protection standards that comply with the relevant laws and international standards.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Thailand has no specific law or regulation relating to artificial intelligence (AI) and big data. As a result, AI and big data are governed by general laws and regulations, such as the CCC, intellectual property law and personal data protection law. This represents a challenge for those involved with these subject matters, as the general laws must be used and applied in any disputes that arise. Regarding personal data, the data controller must comply with the specific regulations under the PDPA, which will apply across all businesses that involve the collection, disclosure and/or utilisation of personal data.

There are debates in Thailand on the status of AI as a property or non-property. However, the CCC defines “property” as corporeal objects and incorporeal objects that are susceptible of having a value and of being appropriated. Therefore, AI may be considered as property (incorporeal object) under Thai law if it has a value.

AI as a property is protected by the intellectual property law. To begin with, the CRA protects computer programs, which it defines as instructions, sets of instructions or any other things that are used with a computer so as to operate the computer or to generate an output, whatever the computer language is. Therefore, the CRA only protects the source code, and not the algorithm. If a product was created by AI, the copyright of the product would belong to the owner of the AI.

However, the PA does not protect the invention of computer programs and scientific or mathematical rules or theories. “Algorithm” has been defined in academic circles as a part of a scientific or mathematical theory, so AI is not protected under the PA.

Looking into the liabilities in the event that AI causes damages, the injured person can take action under general laws such as tort law under the CCC, with the liability stipulated by law falling to the AI controller or possessor unless it can be proved that the injury results from force majeure or is the fault of the injured person.

Thai laws apply specific requirements – such as insurance, minimum capitalisations or individual licences – on the primary business operation alone, without further considering the technology or platform with which the business operates. As a result, business operators are not subject to additional regulations, particularly those pertaining to AI and big data.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

There is currently no specified law to regulate internet of things (IoT) devices in Thailand. The CSA focuses on regulating, planning, coping with and minimising cyber threats to the security of the state, government services, banking and finance, media and telecommunications, logistics, energy and public utilities and public health, through committees under the CSA.

The Industrial Product Standard Act B.E. 2511 (1968) (ISPA) – which indicates industrial product standards and prevents price competitions among manufacturers that lead to lower product quality – cannot be a tool to regulate IoT importers or manufacturers regarding systems or personal data due to the ISPA targeting the regulation of physical products.

However, there are laws and regulations related to the IoT, as follows.

Computer-Related Crime Act B.E. 2550 (2007) (CRCA)

The CRCA prescribes preventative and suppression measures in the event of a person (or persons) causing a computer system to not operate as ordered or to operate incorrectly, or illegally accessing another person's computer data in order to modify or destroy the data or utilise the computer system to disseminate false computer data or obscene images, causing damage affecting the economy, society and state security, including peace and the good morals of the people.

The IoT is defined as a computer system under the CRCA, and is therefore subject to crimi-

nal punishments. However, the CRCA cannot be considered as a mechanism to protect the preventative use of IoT devices and the safety of use, nor for requiring IoT devices to have appropriate security systems in order to prevent offences committed against an IoT device.

PDPA

The PDPA indicates the obligations for organisations that collect, use or disclose personal data to be cautious and maintain the standards of data security as prescribed by the PDPA. Moreover, the PDPA prescribes data subject rights regarding requests to:

- access or copy personal data;
- disclose personal data for which consent has not been given;
- delete or destroy personal data;
- modify personal data so that it cannot be identified.

As a result, the data controller that received the personal data via the IoT must obtain consent from the data subject in order to collect, use or disclose said data without causing any damages or operating beyond the consent of the data subject. Failure to comply with the PDPA may lead to complaints and administrative or criminal penalties.

The PDPA may assure IoT users of the obligations that require IoT device manufacturers to create a path to obtain consent in each utilisation of IoT devices. However, some IoT devices require users to give consent in several accesses of personal data, such as location tracking, cookies and internet usage, which leads to abundant personal data; if the user or data subject did not give consent, the IoT device could not be used under the terms and conditions imposed by the IoT service provider.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthong and Gawin Vattanatham, Formichella & Sritawat

The Radio Communications Act B.E. 2498 (1955) (RCA)

The RCA requires a business operator who performs transactions (such as producing, possessing, trading, importing and exporting) on radio communication equipment to obtain a licence from the National Broadcasting and Telecommunications Commission (NBTC) before commencing any such transaction. Such transactions must be reported to the NBTC or subject to an importation licence obtained from the NBTC.

There is a licence exemption for specific radio communication equipment, such as that using Wi-Fi 2.4GHz. The NBTC may also issue a Notification on exemptions on a case-by-case basis. In addition to the licence requirement, such radio communication equipment must meet the technical and safety standard prescribed by the NBTC. Therefore, each radio communication equipment's technical and safety standard shall be specified in the NBTC Notification.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

In Thailand, audio-visual media services (eg, TV, radio) are regulated by the NBTC under the Broadcasting and Television Business Act B.E. 2551 (2008) ("Broadcasting Act"). The content of films, videos and their advertising media are also regulated under the Film and Video Act B.E. 2551 (2008). Therefore, a censorship committee of officials will review, approve or censor the content of films, videos and advertisements, and approve other film and video-related activities in Thailand, such as the production or distribution of foreign films.

The Broadcasting Act categorises licences for audio-visual media service into three types, each of which has the following foreign ownership restrictions.

- Licence to operate public services: a licence issued for business operations, the main objectives of which are to provide public services (only available to government entities and specific associations, charities, foundations and educational institutions, and not to private sector operators). This licence can be divided into three types, as follows:
 - (a) Type One Public Services Licence, which shall be issued for sound broadcasting business or television business mainly intended for enhancing knowledge, education, religions, art and culture, science, technology, the environment and agriculture, and for promoting other occupations, health, sanitation, sports or the quality of life of the public;
 - (b) Type Two Public Services Licence, which shall be issued for sound broadcasting business or television business mainly intended for state security or public safety; and
 - (c) Type Three Public Services Licence, which shall be issued for sound broadcasting business or television business mainly intended for distributing news and information for:
 - (i) the promotion of good understanding between the government and the public, and between the National Assembly and the public;
 - (ii) distributing news and information for the promotion and support of the dissemination and provision of education to the public with regard to the administration under the democratic form of government with the

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

- King as Head of State;
- (iii) providing news and information services publicly beneficial for the disabled, underprivileged or interest groups who conduct social activities; or
- (iv) providing news and information services for other public interests.

- Licence to operate community services: a licence for business operations that have the same objectives as those of public services businesses, provided they must provide a benefit that meets the needs of the community or locality receiving the services (only available to government entities and specific associations, charities, foundations and educational institutions, and not to private sector operators).
- Licence to operate business services: where the main objective is to generate profit, these are subdivided into three levels: national, regional and local. Foreign ownership is limited to 25%. The foreign ownership restriction under this sector-specific law applies above the general Foreign Business Act, so the holder of such licence may only have up to 25% of its shares held by non-Thai shareholders.

An applicant must be of Thai nationality, must not be on a probationary period restricting them from using the licence, and cannot have exceeded three years of a licence withdrawal period. The approval process usually takes up to 60 days after submitting all the necessary documents. If approved, the applicant will be granted the right to operate under the express terms of the given licence. A broadcasting schedule may be allocated to other licensed broadcasters if the broadcaster complies with the rules and regulations prescribed by the NBTC.

The NBTC will grant a seven-year term for sound broadcasting licensees and five years for television broadcasting licensees. Licences may be renewed 90 days before expiry. Licensees must pay annual fees for their respective licences.

Under the Notification regarding Broadcasting and Television Business Licence fee, there are fees for a licence application consideration (which depends on the type of licence) and an annual fee. The annual fee is collected at progressive rates, as follows:

- 0.5% of the first THB5 million (~USD150,000) income;
- 0.75% between THB5 million and THB50 million (~USD1.5 million) income;
- 1% between BHT50 million and BHT500 million (~USD15 million) income;
- 1.75% between THB500 million and THB1 billion (~USD30 million) income; and
- 2% above THB1 billion income.

These requirements do not apply to video-sharing platform services or over-the-top (OTT) services (eg, video platforms with user-generated content or videos on demand). According to the NBTC, the scope of what constitutes “broadcasting” will be determined with the goal of regulating OTT Services. OTT operators have been informed that they must register themselves with the NBTC and that they would be governed by specific rules and regulations, regardless of nationality.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Organisation to Assign Radio Frequency and to Regulate Broadcasting and

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

Telecommunications Services Act B.E. 2553 (2010) (“NBTC Act”)

The NBTC Act defines “Telecommunications service” as a service that sends, transmits or receives signs, letters, figures, pictures, sounds, codes or anything else made comprehensible by frequency waves, wireless, lighting, electro-magnetic systems or any other systems, or other activities prescribed by law to be telecommunications services. Therefore, a device that meets this definition is deemed to fall within the scope of Thai telecommunications rules.

The NBTC Act establishes the NBTC as an independent broadcasting and telecommunications business regulator. Subject to supervision by the NBTC, the Telecommunications Committee regulates telecoms business in compliance with the Telecommunications Business Act B.E. 2543 (2001) (“TA”), which applies to operators of telecommunications services.

Telecommunications licences are divided into the following three types:

- Type 1 licence, for telecommunications business operators who provide telecommunications services without operating a telecommunication network;
- Type 2 licence, for operators who provide services to a specific group of customers with or without operating a telecommunication network; and
- Type 3 licence, for operators who operate a network providing services to the general public.

The TA imposes various foreign ownership restrictions for each type of telecoms licence, as follows:

- Type 1 licence – no ownership restrictions apply, so operators with a Type 1 licence are only subject to the Foreign Business Act, and a foreign business licence is required;
- Type 2 licence – foreign ownership is limited to 49% of the total shares, so a Type 2 licence holder may only have up to 49% of its shares held by non-Thai shareholders; and
- Type 3 licence – the restrictions for Type 3 licence holders are the same as for Type 2 licence holders.

The different categories of licences cover various services as indicated in the operator’s licence application. The applicant must be a legal person as established under Thai law, and must not be a bankrupt or a party that has previously had a telecommunications licence revoked. In addition, technical and commercial information relating to the business operations of the applicant – including the network structure, financial investment plan, marketing plan, service details and equipment details – must be provided to the NBTC for its consideration.

The approval of all types of licences usually takes approximately 60 to 90 days after all necessary documents and information have been submitted to the NBTC. If approved, the applicant will be granted the right to operate strictly under the express terms of the licence. Licensees must pay annual fees for their respective licences.

NBTC Inspection

Business operators who wish to manufacture, sell or import devices that have been inspected and approved by the NBTC shall not be required to provide samples of such devices for the NBTC’s inspection and approval; they can skip the inspection process and go straight for the manufacture, sell or import certificate.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

However, the operator must provide samples of any devices that have not yet been inspected or approved by the NBTC to the NBTC for inspection and approval prior to obtaining the certificate required for its business operation. This will require some extra time (approximately ten working days) and effort from the applicant, especially for brand-new devices with new technology that is unknown to the NBTC. After the consideration, the NBTC will notify the result to the applicant within seven days.

In addition to the NBTC inspection and approval, operators who wish to manufacture, sell or import certain telecommunication devices that have obtained certain international inspections/approvals (such as certain ISO marks) may file documentation relating to the international approval (such as the ISO certificate) to the NBTC for its consideration rather than submitting product samples for the NBTC's inspection/approval. The goal is to shorten the process to obtain the relevant certificate required (whether manufacture, sell or import) prior to operating such telecommunication business in Thailand.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

There are no specific laws and regulations that apply to technology agreements, and there is currently no particular law or regulation that requires data to be stored locally in Thailand. Nevertheless, industry-specific regulations mandate that some data is to be available or processed within Thailand. The banking industry, for example, requires banks to process debit card transaction data and make electronic payment system data available in Thailand.

As there is no direct legal requirement for the terms and conditions in a technology agreement, the challenge is to establish an agreement with terms and conditions that cover all the necessary elements. The provisions stated therein shall be based on the intention of the parties and the work for hire concept under the CCC. Except for the specific commercial and technical terms prescribed in the service agreement, the following terms should be noted and stated therein:

- terms and conditions regarding personal data protection should be prescribed in the service agreement if there are performance results in the collection, use or disclosure of the individual's personal data under the PDPA;
- the scope of work must be specified;
- the timeframe of the services – or milestones – and delivery methods must be specified;
- there must be a provision regarding the confidential information of the parties, such as trade secrets, know-how methods, etc; and
- there must be a provision regarding intellectual property, and the ownership thereof must be clearly specified. Under a standard work for hire agreement, the hirer (the customer who hires the service provider) is considered the owner of the work products, but a service agreement can specify the owner of specific intellectual property, so as to protect the ownership of the works and assets.

Banking and Insurance

The BOT and the OIC) have notified the terms that should be stated in the business partner (ie, outsourcing) agreement, as follows:

- details regarding scope of service, responsibility, risk management, internal control systems and the financial institution's asset security system;

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthong and Gawin Vattanatham, Formichella & Sritawat

- the service level agreement to indicate the standards of services in both common and uncommon situations;
- the business continuity plan;
- the process to follow, examine and evaluate efficiency;
- service fee;
- the timeframe, terms and conditions regarding the termination, amending and renewal of the contract;
- the scope of responsibility in case of service interruption;
- the data security, confidentiality and data privacy of customer and financial institution, including access rights and data ownership, such as methods to transmit information and data storage, etc, as well as an indication of penalties in the event of information disclosure;
- no prohibition on providing the same services to other financial and insurance institutions;
- compliance with Thai laws;
- conditions to subcontract under BOT and OIC regulations; and
- an indication of the rights of BOT and OIC under BOT and OIC regulations.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The Royal Decree on Security Procedures regarding Electronic Transactions B.E. 2553 (2001) (SPET) is prescribed under the Electronic Transactions Act B.E. 2544 (2001) (ETA) and mainly indicates the criteria of a reliable electronic transaction and divides the security procedure into three levels: strict, intermediate and basic. These three levels are categorised under the notification regarding the standard for

maintaining information security, which mainly focuses on the establishment of administrative security, information security in respect of personnel, physical security and the environment, etc.

The Royal Decree regarding the supervision of services related to licensed digital authentication B.E. 2565 (2022) (“Digital Authentication Decree”) was promulgated on 22 December 2022 under the ETA, and will become effective 180 days after the promulgation date. Digital authentication service providers are subject to be approved for a licence by the Electronic Transactions Development Agency (ETDA). Services deemed to fall within the scope of such a licence are authentication services, issuing and managing authentication services and information exchange services for the authentication and verification of digital identity. However, the authentication of electronic signature service providers under the ETA does not fall within the scope of a licence under the Digital Authentication Decree.

Therefore, digital authentication service providers are obliged to comply with the regulations under the Digital Authentication Decree, including the duty to report and comply with notifications notified by the ETDA regarding authentication data outsourcing, change of corporate structures, cessation of service, lawsuits against the service provider, director or manager qualifications, minimum company limited or public company limited registered capital, business and authentication system assessments, etc.

Regarding the use of electronic signatures, the ETA prescribes that the method of electronic signature must be:

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

- capable of identifying the signatory and indicating that the signatory has approved the information contained in such data message as being their own; and
- reliable and appropriate for the purpose for which the data message is generated or sent, having regard to the surrounding circumstances or an agreement between the parties.

Therefore, electronic signatures are legally effective and enforceable in Thailand, except in those transactions prescribed by a Royal Decree to exclude electronic signatures under the ETA (ie, transactions relating to family and succession).

Regarding digital identity, the Royal Decree regarding Digital platform service business that must notify B.E. 2565 (2022) (“Digital Platform Decree”) was promulgated on 22 December 2022 under the ETA and will become effective 240 days after the promulgation date.

The Digital Platform Decree prescribes that any digital platform that provides a service in Thailand and has an annual income of more than THB1.8 million (~USD53,000) for a natural person operator or THB50 million (~USD1.5 mil-

lion) for a juristic person operator, or any platform that provides to more than 5,000 users per month, must provide the ETDA with information concerning the operator, digital platform, users, co-ordinator (if a digital platform operates overseas), etc. The definition of digital platform service is wide, so most digital platform services in Thailand are deemed to fall under the Digital Platform Decree.

Furthermore, the co-ordinator must not be a foreign business operator, and a digital platform entity establishment is not required. In addition, the ETDA is empowered to restrict the digital platform in the event of non-compliance with Thai laws and regulations. The digital platform must inform the terms and conditions of use and provide mitigation and compensation measures to compensate those who have been damaged through the digital platform operation. In order to cease operation, the co-ordinator must notify the ETDA under the regulation prescribed by the ETDA. However, any digital platform that needs to notify the ETDA and operated before the effective date of the Digital Platform Decree is able to notify the ETDA within 90 days after the effective date.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

Formichella & Sritawat has been advising international clients on commercial transactions and regulatory matters within the TMT industry for more than 20 years. In addition to data privacy, cybersecurity and TMT/corporate practices, the firm has a litigation practice that represents international corporations in complex business and commercial disputes within the various courts of Thailand. Formichella & Sritawat regu-

larly advises on current legal structures and the rapid development of the technology and commercial practices and current regulatory frameworks and policies of the government of Thailand. It also specialises in advising clients on regulatory practices and devising tailor-made strategies and solutions that fit each client's circumstances.

Authors



John Formichella is a US-trained attorney and a leading expert in the TMT sector in East and Southeast Asia. He has over 25 years' sophisticated technology transaction

experience (five in Taiwan, and more than 20 in Thailand), covering technology transactions, fintech, data privacy issues, telecommunications law, media, e-commerce and payment systems. John is a regular contributor to Mondaq, Lexology, The Law Reviews and other industry publications regarding cybersecurity, telecommunications, space law and data privacy. His recent publications include "Getting the Deal Through: Telecoms and Media" in 2017–22.



Naytiwut Jamallsawat heads the corporate and regulatory practice at Formichella & Sritawat, and focuses particularly on data privacy, cybersecurity,

telecommunications, satellite and space law, and energy sector issues. He advises multinational enterprises from North America, Europe, Singapore, Hong Kong SAR and Mainland China on diverse regulatory matters. His practice includes advising on corporate structuring for foreign direct investment and regulatory compliance in cybersecurity, data protection, media and telecommunications. He is a regular contributor to Mondaq, Lexology, The Law Reviews and other industry publications.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat



Onnicha Khongthon is a senior associate at Formichella & Sritawat, and has seven years' experience in corporate law, the TMT sector, data privacy, cybersecurity and space law,

including corporate and commercial matters. She continues to strengthen her knowledge in wide-ranging matters, from general commercial and TMT issues to research into cybersecurity, satellite and data privacy law. Onnicha also guides foreign businesses through the often-complex process of establishing themselves in Thailand, including company registrations, BOI applications, American Treaty registrations, telecommunication licensing, and obtaining Foreign Business Licences and Foreign Business Certificates.



Gawin Vattanatham is a junior associate at Formichella & Sritawat. He mainly assists senior lawyers and partners in providing legal advice on corporate matters, data

protection, cybersecurity, TMT and laws regarding medical services in Thailand. He joined the firm after receiving an LL.B. (1st Class Honours) from the prestigious Chulalongkorn University.

Formichella & Sritawat

399, Interchange 21 Building
23rd Fl., Unit 3, Sukhumvit Road
Klongtoey-Nua
Wattana
Bangkok 10110
Thailand

Tel: +66 2 107 1882
Email: info@fosrlaw.com
Web: www.fosrlaw.com

FOSR

Trends and Developments

Contributed by:

John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon
and Gawin Vattanatham

Formichella & Sritawat see p.542

Overview of the Telecom Market in Thailand

In October 2022, the National Broadcasting and Telecommunications Commission (NBTC) approved a proposed merger between TRUE and DTAC, two of the biggest telco operators in Thailand. The two companies are now in the process of preparing the merger plan.

This merger may have a tremendous impact on Thailand's telecommunications market, as there were previously three big competitors in the market and soon there will be two. As a controversial topic in Thailand, there were concerns and criticisms that the service fee will rise considerably and that the telecommunications market will be monopolised.

Nonetheless, the NBTC indicated that certain measures would be implemented, such as pricing control, supporting smaller-scale operators to compete in the market, regulating the quality of service, spectrum utilisation and infrastructure sharing, and a digital divide. Moreover, the NBTC specifically stated that TRUE and DTAC must keep the brands separate for three years, in order to maintain consumers' freedom of choice.

The consequences of this merger between two big telco operators are yet to be seen. According to the Securities and Exchange Commission (SEC), the new company's name will be TRUE Corporation and the registered capital will be THB138,208,403,204, which is equivalent to the registered capital of TRUE and DTAC combined. In addition, 34,552,100,801 common shares will

be allocated to the shareholders of TRUE and DTAC on the book closing date.

Personal Data Protection Act

The Personal Data Protection Act B.E. 2562 (2019) (PDPA) has been fully enforced since 1 June 2022; all business sectors are required to comply with the PDPA. This compliance was a controversial issue after the PDPA become fully enforced, as it requires major changes to business operations, especially customer engagement. The PDPA's provisions are somewhat similar to those of the GDPR and other data privacy laws in various jurisdictions. Nonetheless, some of the provisions in the PDPA remain unclarified, awaiting for notifications to be prescribed by the Personal Data Protection Commission (PDPC).

The criteria and method by which to notify a data breach have recently been notified under the PDPA. The notification mainly prescribes the procedure and list of details that must be included in the data breach notice, along with the time-frame in which it must be submitted to the Office of the PDPC. However, several notifications have not yet been notified under the PDPA, such as the criteria and method to transfer personal data to foreign countries, which may cause difficulties and issues in the practice of data transferring. More ancillary laws for the PDPA are expected to be issued in 2023 to address remaining and new issues that may arise with the new technologies.

Recent update to space law

Nowadays, space-related technology is increasingly applied to daily life, benefiting both the

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

public and the private sectors, with more than 35,600 enterprises operating space-related businesses in Thailand, generating an income of approximately THB56.122 billion. The technology that these companies produce helps to mitigate and prevent national disasters, including floods, drought and other climate crises. The technology has also been applied to issues brought about by the COVID-19 pandemic, and has helped to identify different locations for commercial and medical activities.

As space businesses and activities involve cross-border operators and international organisations, Thailand requires transparent, up-to-date and adequate space laws to enable proper, legal operation of space activities and to gain trust from all operators.

A draft Space Affairs Act (“Draft Act”) has been proposed by the Geo-Informatics and Space Technology Development Agency (GISTDA), and was approved by the Cabinet on 13 July 2021. It is now undergoing the legislation process and will be sent to the Office of the Council of State and Parliament for consideration and approval before becoming effective.

The Draft Act mainly focuses on regulating a natural or juristic person who is involved in space affairs to apply for a direct space activity licence or space-related activity licence. This will also be applied to space affairs carried out before the Draft Act becomes effective. In this event, the natural or juristic person must apply for a licence within 60 days of the Draft Act becoming effective. Furthermore, space objects must be registered under the Draft Act.

The Draft Act also prescribes that the Thai government is responsible for damages that occur outside Thailand related to space activities,

space objects or space-related activities by a Thai individual or a Thai juristic person to a third party, regardless of whether the activity or object is licensed or registered. If the government has settled a dispute and paid compensation to a third party, it will have the right of recourse to the individual or the juristic person who caused the damage. More updates from the government regarding the Draft Act are expected in 2023.

Over-the-top (OTT) service in Thailand

OTT contents have been a rising trend all around the world, especially in the widespread pandemic period. More than one-third of Thailand’s population selected to utilise OTT platform, with approximately 1.4 billion hours per month spent on the platforms. Accordingly, Thailand’s OTT market is considered one of the biggest in Southeast Asia.

However, OTT service platform remains unregulated by a specific broadcasting and television law like the traditional media of radio, films, television and advertisement. Therefore, only existing laws and regulations in other relevant laws will be applicable in regards to OTT service.

The NBTC’s attempt to regulate OTT platforms by requesting the operators to register themselves under the NBTC was heavily criticised by the public and OTT platform operators, as well as technology-related NGOs. In consequence, the NBTC withdrew its requests to OTT operators.

Therefore, OTT operators who operate in Thailand must be aware of regulatory risk. On a case-by-case basis, the operators should be active and ensure that the content is in compliance with the relevant laws and regulations in forces in Thailand.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

Illegal contents, such as pornography, lèse-majesté and fake news are regulated under the Computer Crimes Act; operators who allow such illegal contents on their platforms may be blocked, banned and penalised by the Thai authority. No major changes to the existing laws are expected in 2023, but it is likely there will be some changes to the related laws in the future.

Thailand National AI Strategy and Action Plan (2022–2027)

According to the Government Artificial Intelligence Readiness Index 2020, Thailand was ranked in 60th due to the lack of policy and action plan relating to AI. In consequence, the Cabinet approved the (Draft) Thailand National AI Strategy and Action Plan (2022–2027) (“AI Plan”) on 26 July 2022, under the vision “Thailand has an effective ecosystem to promote AI development and application to enhance the economy and quality of life within 2027”.

The AI plan is aimed to build human capacity and technology, economic growth, and social and environmental impact. The AI Plan will be implemented under the following five strategies:

- preparing Thailand’s readiness in social, ethics, law and regulation for AI application;
- developing national infrastructure for sustainable AI development;
- increasing human capability and improving AI education;
- driving AI technology and innovation development; and
- promoting the use of AI in the public and private sectors.

Focusing on laws proposed by the AI plan, the intention of the law is to create guidelines and regulations in order to promote AI as being socially beneficial, ethical, trustworthy, secure

and private, fair, and emphasising human well-being. Moreover, the laws will be enacted to be in compliance with the PDPA, with consideration of data subject rights.

The intention is to create policy regulations and standards, and to enact laws that are relevant to AI. The laws will be by design, and can be divided into the following seven topics:

- to prescribe obligations for personnel who are related to AI technology;
- to secure and assure that the AI technology is used in compliance with the laws and regulations relating to privacy and data protection;
- to be transparent and verifiable in AI processing;
- to eradicate discrimination in the utilisation of AI;
- to be fair and equal for various types of personnel accessing AI technology;
- to assure the safety of society; and
- to obligate the AI creator, utiliser and AI-related entrepreneurs to ensure the accuracy of information, rights to the information assets along with the ownership and responsibility, and to create clear boundaries of AI compulsory rights.

After the enforcement of the aforementioned laws, the AI plan states that ethics in utilising AI technology and the development and effects of AI utilisation should be addressed in the primary stage of Thai education. Furthermore, the capabilities of AI entrepreneurs should be enhanced by setting standards for data storage, data verification, robotics or medical devices related to AI, in order to be in compliance with AI laws, ethics and international standards.

The AI-related laws and regulations in Thailand are clearly in the primary stages. However, AI

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

is becoming a controversial topic. Thailand's government and business sectors are pushing to regulate this cutting-edge technology for the benefit of Thailand's economic and society. Only the insurance and finance sectors regulate and put out criteria and measures for utilising AI tools as an IT outsourcing service to mitigate unexpected scenarios that technology may cause.

Trading Forex in Thailand

Forex was a hot issue in Thailand in 2022, as it was involved in one of the biggest scandals in Thailand, Forex 3D. According to official reports, the damage in this case is up to THB2.5 billion, with more than 80,000 investors. It is nearly clear that fraud has been committed, with the suggestion that investors would receive 10–15% monthly from the invested capital and 5% from capital invested by invitees.

Looking into Forex regulation in Thailand, there are no laws and regulations that indicate Forex is illegal Thailand. Nonetheless, no licences have been granted for non-banks to be Forex brokers in Thailand, even though there are laws regulating this issue. Therefore, Thai investors are capable of opening an account with foreign Forex brokers.

As there is no Forex broker regulation under Thai law, Forex investors in Thailand are not protected under Thai law. It is beyond Thailand's jurisdiction to file a lawsuit against the broker if damages occur with a foreign broker. An individual investor is responsible for pursuing damages by themselves.

According to the Bank of Thailand, a ministerial regulation was recently issued under the Exchange Control Act B.E. 2485 (1942) to amend the regulation covering transaction business relating to foreign means of payment, to

enhance the regulation and reliability in the international aspect, but this does not directly affect Forex brokers.

Notice and takedown policy

As technology changes and evolves rapidly, various illegal contents are published on the internet. Thailand recently issued a notification in regard to the notice and takedown policy ("Notification") under the Computer-related Crime Act B.E. 2550 (2007) and its amendment (CCA). The purpose of this Notification is to amend the notice and takedown policy, so that it is stricter and up to date.

The main characteristics of the Notification are as follows:

- website and social media operators must provide the notice and takedown policy, which contains the contact details of the operator or agent;
- any person is able to file a report with the police, with evidence, if website and social media operators are deemed to be violating the CCA, and any person can file a report attached to the notice issued by the police to the internet service provider;
- if a person files such a report, the internet service provider must delete the computer data within 24 hours;
- a dispute process for deletion is not provided for under the Notification; and
- a competent officer from the Ministry of Digital Economy and Society (MDES) is able to instruct internet service providers to cease the spread and use of computer data that violated the RCA – if the internet service provider fails to comply as instructed, it will be deemed to co-operate with, support or consent to the offence, which will lead to a criminal penalty.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

These main characteristics differ from the previous notice and takedown notification, especially the final point, as the competent officer was previously not authorised to directly instruct operators to take content down. Nonetheless, the Notification has been criticised as being contrary to the presumption of innocence (until proven guilty), which is assured by the Constitution of Thailand. However, the Notification will be enforced in mid-2023.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

Formichella & Sritawat has been advising international clients on commercial transactions and regulatory matters within the TMT industry for more than 20 years. In addition to data privacy, cybersecurity and TMT/corporate practices, the firm has a litigation practice that represents international corporations in complex business and commercial disputes within the various courts of Thailand. Formichella & Sritawat regu-

larly advises on current legal structures and the rapid development of the technology and commercial practices and current regulatory frameworks and policies of the government of Thailand. It also specialises in advising clients on regulatory practices and devising tailor-made strategies and solutions that fit each client's circumstances.

Authors



John Formichella is a US-trained attorney and a leading expert in the TMT sector in East and Southeast Asia. He has over 25 years' sophisticated technology transaction

experience (five in Taiwan, and more than 20 in Thailand), covering technology transactions, fintech, data privacy issues, telecommunications law, media, e-commerce and payment systems. John is a regular contributor to Mondaq, Lexology, The Law Reviews and other industry publications regarding cybersecurity, telecommunications, space law and data privacy. His recent publications include "Getting the Deal Through: Telecoms and Media" in 2017–22.



Naytiwut Jamallsawat heads the corporate and regulatory practice at Formichella & Sritawat, and focuses particularly on data privacy, cybersecurity,

telecommunications, satellite and space law, and energy sector issues. He advises multinational enterprises from North America, Europe, Singapore, Hong Kong SAR and Mainland China on diverse regulatory matters. His practice includes advising on corporate structuring for foreign direct investment and regulatory compliance in cybersecurity, data protection, media and telecommunications. He is a regular contributor to Mondaq, Lexology, The Law Reviews and other industry publications.

Contributed by: John Formichella, Naytiwut Jamallsawat, Onnicha Khongthon and Gawin Vattanatham, Formichella & Sritawat

Authors



Onnicha Khongthon is a senior associate at Formichella & Sritawat, and has seven years' experience in corporate law, the TMT sector, data privacy, cybersecurity and space law,

including corporate and commercial matters. She continues to strengthen her knowledge in wide-ranging matters, from general commercial and TMT issues to research into cybersecurity, satellite and data privacy law. Onnicha also guides foreign businesses through the often-complex process of establishing themselves in Thailand, including company registrations, BOI applications, American Treaty registrations, telecommunication licensing, and obtaining Foreign Business Licences and Foreign Business Certificates.



Gawin Vattanatham is a junior associate at Formichella & Sritawat. He mainly assists senior lawyers and partners in providing legal advice on corporate matters, data

protection, cybersecurity, TMT and laws regarding medical services in Thailand. He joined the firm after receiving an LL.B. (1st Class Honours) from the prestigious Chulalongkorn University.

Formichella & Sritawat

399, Interchange 21 Building
23rd Fl., Unit 3, Sukhumvit Road
Klongtoey-Nua
Wattana
Bangkok 10110
Thailand

Tel: +66 2 107 1882
Email: info@fosrlaw.com
Web: www.fosrlaw.com

FOSR

Law and Practice

Contributed by:

Mike Ryan, Aaron Burstein,

Mike Dover and Patricia Werner

Kelley Drye & Warren LLP see p.560



Contents

1. Metaverse	p.544
1.1 <u>Laws and Regulations</u>	p.544
2. Digital Economy	p.545
2.1 <u>Key Challenges</u>	p.545
3. Cloud and Edge Computing	p.547
3.1 <u>Highly Regulated Industries and Data Protection</u>	p.547
4. Artificial Intelligence and Big Data	p.551
4.1 <u>Liability, Data Protection, IP and Fundamental Rights</u>	p.551
5. Internet of Things	p.553
5.1 <u>Machine-to-Machine Communications, Communications Secrecy and Data Protection</u>	p.553
6. Audio-Visual Media Services	p.554
6.1 <u>Requirements and Authorisation Procedures</u>	p.554
7. Telecommunications	p.556
7.1 <u>Scope of Regulation and Pre-marketing Requirements</u>	p.556
8. Challenges with Technology Agreements	p.557
8.1 <u>Legal Framework Challenges</u>	p.557
9. Trust Services and Digital Entities	p.558
9.1 <u>Trust Services and Electronic Signatures/ Digital Identity Schemes</u>	p.558

1. Metaverse

1.1 Laws and Regulations

Laws and Regulations

The US legal and regulatory landscape governing the metaverse is rapidly evolving. The laws and regulations that are implicated by the metaverse are numerous and potentially create a range of legal issues. There are currently no US laws that specifically apply only to the metaverse – however, in some situations existing laws apply; in other situations, new laws and regulation are likely to be developed over time.

Intellectual Property

Intellectual property laws are key to metaverse governance. The creation of new types of digital assets, such as non-fungible tokens (NFTs), raises novel intellectual property issues including those summarised below.

Copyright

Copyright is a type of intellectual property that protects original works of creators. In the metaverse, this covers user-generated digital content such as avatars, virtual buildings, and digital artwork. The owner of a copyrighted item has the exclusive right to reproduce the work, display it, distribute copies and display it publicly. Copyright also provides the owner the right to authorise others to exercise these exclusive rights. If an artist creates content in the metaverse that is similar to copyrighted content in the physical world, then they may be liable for copyright infringement. For example, an avatar or an NFT in the metaverse that is similar to a copyrighted avatar or NFT outside the metaverse could trigger a copyright infringement claim.

Trade marks

A trade mark is a word, phrase, logo, design, or slogan that indicates the source of goods and

services. Trade mark law protects against the unauthorised use of a trade mark by third parties that would cause a consumer to believe that the trade mark owner either was the source of the goods or services, or endorsed or sponsored such goods or services, in a manner that may dilute or disparage the trade mark.

Many companies register their brands with the US Patent and Trade Office (USPTO) for use in connection with virtual offerings as well as those in the physical world. These companies obtain registered trade mark protection for things like virtual goods, retail store services featuring virtual goods, NFTs, and digital tokens.

Patents

A patent for an invention is the grant of a property right to the inventor. Generally, a new patent is valid 20 years from the date on which the application for the patent is filed in the United States. US patent grants are effective only within the United States, its territories and possessions. A company developing metaverse-related technologies will need to consider whether to seek patent protection and whether its technology might infringe on the patents of other parties in the same way as technology providers outside of the metaverse.

User-Generated Content Litigation

The proliferation of user-generated content creates risks of unauthorised use of third-party trade marks and brand dilution. For example, some metaverse spaces operate as an online economy, allowing users to create their own virtual worlds, to develop intellectual property, to sell branded creations, and/or to build an online business presence sell their products in the real world. Using another party's trade marks in these ways can trigger a trade mark infringement claim.

There have already been a number of challenges regarding intellectual property incorporated into user-generated content in the metaverse, including a case alleging trade mark infringement and dilution as a result of a company minting NFTs using trade marks belonging to other companies (Nike, Inc v StockX LLC and Hermès v Mason Rothschild).

Torts

Tort law governs civil wrongs such as property damages and personal injury, which can include activity caused by users in the metaverse to other participants. A defendant could be liable for financial compensation related to an act in the metaverse. For example, defamation is a false statement presented as a fact that causes injury or damage to the character of the person it is about. In the metaverse, user-generated content that is false and causes injury to another could trigger a defamation claim.

Tax and Financial Regulations

The purchase and sale of virtual goods trigger tax implications, including sales tax and income tax. NFTs may be subject to US commodities, banking, and securities laws, due to the manner in which these assets are created and exchanged.

Contracts

In the metaverse, contract law applies to agreements between users, such as selling virtual goods to renting virtual property. Businesses entering into agreements in the metaverse need to comply with laws and regulations applicable to contracts in the physical world, including meeting all consumer disclosure requirements.

Data Protection

Data practices relating to the metaverse are subject to generally applicable US privacy and data protection frameworks, primarily the California

Consumer Privacy Act and other comprehensive state privacy laws that go into effect in 2023, Section 5 of the Federal Trade Commission Act, and state laws that prohibit unfair or deceptive acts and practices.

As with other platforms, it is important for companies that have a presence in the metaverse to understand the personal data flows involving the company, the platform, and exchanges between them. Key issues to examine include:

- whether a company collects personal data through its presence in the metaverse;
- whether the company shares any of this data with the metaverse platform; and
- whether such collection and sharing are adequately disclosed in privacy notices and covered under existing rights request processes.

Cybersecurity and Data Security

Companies face potential liability for disclosing personal data to vendors or third parties that do not maintain reasonable data security measures. Therefore, to the extent that personal data will be shared with a metaverse platform, it is important to assess the platform's cybersecurity practices in advance. In addition, if the metaverse supports operational business activities, then the platform's general cybersecurity measures, including availability guarantees and ability to resist and respond to various forms of cyberattacks, are important considerations.

2. Digital Economy

2.1 Key Challenges

Laws and Regulations

Numerous laws and regulations regulate the digital economy in the United States, including

a variety of laws, regulations and codes of conduct particular to specific industries or to the type of data and users involved. Laws and regulations at the federal, state and local level – and in some instances even laws of foreign jurisdictions – may apply to a participant in the digital economy in the USA. As a general matter, laws and regulations applicable outside of the digital economy will also apply to the establishment and operation of a digital business, in addition to those laws and regulations focused primarily on digital operations and transactions.

Terms & Conditions

A business operating a website or mobile platform will need to carefully consider the terms and policies applicable to the platform and the manner in which the terms and policies are disclosed. Even if no goods or services are being sold on the platform, the operator will generally reference the terms of use for the platform and link to the applicable policies, including as a privacy policy describing the collection, storage, use, and disclosure of personal information and policies related to the provision and use of user-generated content. The legal requirements for these policies can vary significantly depending upon the nature of the platform.

In addition to the terms of use of the platform, the operator will need to require customers to enter into appropriate binding contracts if goods or services are being sold, licensed or otherwise made available on the platform in order to specify the terms associated with the transfer of the goods and services. Courts in the United States have sometimes refused to enforce certain provisions of contracts entered into online (or the entire contract) either because the elements for valid contract formation have not been met or because certain provisions were found to be against public policy. In order to increase the

likelihood of a digital contract being enforced, the applicable terms should be prominently displayed. Operators of digital platforms generally should either:

- require potential customers to affirmatively accept the contract terms (such as by clicking on an “Accept” button clearly referencing the terms and conditions) before proceeding to use the platform; or
- provide that the contract becomes effective if the user continues to use the platform after the terms and conditions are prominently presented.

Requiring the customer to affirmatively accept the contract terms after the terms are presented to the customer will decrease the likelihood that a court in the United States will find the contract to be unenforceable as a result of the customer not having actual or implied notice of the contractual terms or the customer not having agreed to those terms. However, certain applicable statutes or common law principles may still lead a court to deny enforcement of certain provisions, such as relating to arbitration provisions or choice of law and forum selection provisions.

Intellectual Property

The digital economy also implicates intellectual property laws. Companies that offer consumers innovative experiences have to navigate IP issues including branding and trade mark protection, copyright, licences for specific software or technology, patents, trade secrets and know-how for their digital offerings.

Privacy/Data Security/Consumer Protection

Privacy, data security, and consumer protection laws play a key role in regulating commercial practices in the digital economy. The US Federal Trade Commission (FTC), which has juris-

diction over consumer protection and competition enforcement across broad areas of the US economy, based in part on Section 5 of the FTC Act, which prohibits unfair methods of competition and unfair or deceptive acts and practices. State attorneys general have similar consumer protection authority under their laws against unfair or deceptive acts and practices.

Over the past few decades, the FTC has used its Section 5 authority to establish standards for the processing of personal data through enforcement actions against specific companies, as well as non-binding guidance and policy documents. Until recently, the FTC limited its rulemaking activity to specific industries or practices for which Congress granted clear regulatory authority, such as children's privacy or the security of personal information that financial institutions handle.

The FTC, however, has indicated that the growing digital economy, coupled with business models that are based on monetising personal data, may have given rise to unfair or deceptive data practices that are prevalent. As discussed in **4. Artificial Intelligence and Big Data**, the FTC is now considering developing regulations to govern "commercial surveillance" and data security, which could apply far more broadly than the sector-specific rules mentioned above.

Industry-Specific Laws

Other federal and state regulators play an important role in the legal order surrounding the digital economy. For example, a number of federal laws applicable to entities operating in specific industries apply to the operation of a digital business in those industries, including financial institutions, health care providers and insurers (and their business associates), companies doing business with governmental entities, and educa-

tional institutions. See **3. Cloud and Edge Computing** for a summary of some of these laws.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Regulations

Entrusting processes or data to a cloud or other distributed computing environment like edge computing may implicate a variety of laws and regulation in the US depending upon the industry, data, and users involved. Laws and regulations at the federal and state level – as well as laws of foreign jurisdictions – may apply directly to providers of these services operating in the US as well as their customers. In addition, these offerings often involve providers processing data on behalf of customers that is subject to additional regulation (such as controllers of personal data). The obligations of those customers are required to be passed through to the providers in the computing contracts.

Sector-Specific Laws and Regulations and Industry Standards

Laws and standards that govern entities operating in specific industries, including financial institutions, health care providers and insurers (and their business associates), companies doing business with governmental entities, educational institutions, and telecommunications common carriers, are applicable to cloud and edge computing providers and information received by the providers. The following laws and standards are frequently implicated when such entities move processes and data to the cloud.

Financial institutions

The Gramm-Leach-Bliley Act (GLBA) is a US federal law regulating the treatment of non-

public personal information (NPI) by financial institutions, such as banks, financial advisors, and insurance companies.

The GLBA includes provisions on privacy applicable to the collection and disclosure of NPI (the “Privacy Rule”) and security provisions requiring the financial institutions to protect NPI (the “Safeguards Rule”). The GLBA applies not only to financial institutions, but may also apply to companies receiving non-public personal information from a financial institution or who perform activities that are financial in nature or incidental to financial activities. Entities subject to the GLBA generally require their providers to agree to contract terms that reflect the applicable obligations under the GLBA.

An entity subject to the GLBA utilising a third party service provider for processing will need to confirm the selection of a service provider that maintains appropriate policies and safeguards consistent with the GLBA and enter into an appropriate contract.

The Safeguards Rule (and more detailed guidelines for banks, which are not subject to the Safeguards Rule) requires financial institutions to develop and maintain a comprehensive information security programme and to exercise appropriate oversight over service providers, among other requirements. The Federal Trade Commission issued a major revision of the Safeguards Rule in December 2021.

Healthcare

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law addressing the treatment and use of individuals’ personal protected health information (PHI). HIPAA applies to healthcare providers, health insurance plans and healthcare clearinghouses

(“Covered Entities”) and their business associates (and those business associates’ subcontractors) performing certain services invoking PHI (“Business Associates”). Under the authority granted by HIPAA, the US Department of Health and Human Services has issued Privacy, Security, and Breach Notification Rules, which together establish requirements for the use, disclosure, and protection of PHI. The use of cloud and edge computing services will need to comply with HIPAA to the extent applicable.

Entities participating in federal programmes

Requirements applicable to activities by federal agencies and their contractors include the Federal Information Security Modernization Act (FISMA) and the Federal Risk and Authorization Management Program (FedRAMP). FISMA establishes federal agency roles and responsibilities for information technology security.

Educational institutions

The Family Educational Rights and Privacy Act (FERPA) provides certain privacy protections applicable to a student’s educational records. Schools covered by FERPA placing records subject to FERPA in the cloud will need to ensure that its cloud providers are contractually obligated to meet the requirements of FERPA.

Auditing standards

Standards for Attestation Engagements No 18 (SSAE 18) sets forth standards used by auditors to review certain practices of service providers. Companies offering cloud-based services in the US frequently make available to their customers on an annual basis a type of report based on SSAE 18 known as a Service and Organization Control (SOC) 2 report focusing on the principles of security, privacy, availability, processing integrity, and confidentiality. A provider providing services materially impacting the financial state-

ments of its customers will often be requested to also provide a SOC 1 report, which focuses on the service provider's financial controls.

Payment card industry standard

The Payment Card Industry Data Security Standard (PCI DSS) has been created by the Payment Card Industry Data Security Council to address data security for any company that stores, processes or transmits "Cardholder Data" or "Sensitive Authentication Data" as defined by the PCI DSS. A service provider receiving Cardholder Data or Sensitive Authentication Data will be required to meet extensive requirements to demonstrate PCI DSS compliance.

Surveillance

Several federal laws authorise law enforcement and intelligence agencies to compel cloud and edge computing providers to produce personal data and other information in response to subpoenas, court orders, and other forms of legal process. Key statutes include the Foreign Intelligence Surveillance Act (FISA) and the Electronic Communications Privacy Act (ECPA), as amended by the Clarifying Lawful Overseas use of the Data ("CLOUD Act"). The CLOUD Act permits federal authorities in certain instances to compel technology providers based in the US to provide data stored on the provider's servers located both inside and outside the US.

Given the potential multi-jurisdictional reach of cloud-based products and services, these US laws may conflict with laws of other countries claiming jurisdiction over data or computer assets. For instance, with regard to the European Union, the scope of the US legal authorities' reach, the strength of judicial and other safeguards, and the rights and protections that Europeans may exercise against government agencies seeking data stored by US-based providers

have become major issues following the Court of Justice for the European Union's July 2020 Schrems II decision. In addition to requisite processes to evaluate and respond to government demands, US-based cloud providers increasingly face demands from their customers to assess the risk of government access to the customers' data processed by the providers.

Specific Issues for Processing of Personal Data

In addition to the generally-applicable sector-specific laws and standards discussed above, several federal and state laws and regulations govern specific circumstances relating to the type of personal data collected or transmitted. These laws include broadly defined federal and state consumer protection laws, comprehensive state-level statutes, and laws designed to protect either certain categories of data collected or certain data collected on specific populations.

Federal laws

The FTC is the main consumer protection enforcement agency in the US and has long applied its authority to prevent "unfair or deceptive acts or practices" to the data protection arena. Although this authority, defined under Section 5 of the FTC Act, is not specific to data protection, the FTC has used it to bring more than 100 privacy and data security enforcement actions over approximately two decades.

State laws

Virtually every state has enacted narrow legislation to protect specific categories of sensitive personal data of its residents. However, the California Consumer Privacy Act (CCPA); Virginia Consumer Data Protection Act (VCDPA); and comprehensive privacy laws in Colorado, Connecticut, and Utah, go into effect by the end of 2023, and require contracts with service provid-

ers/processors such as cloud computing providers to limit the service provider's data use, assist with consumer rights requests and data protection impact assessments, and ensure personal data security, among other requirements. Below is a high-level description of some of these state statutory requirements.

California

The CCPA was enacted in 2018 to give Californians more control over the personal information certain businesses collect and use about them. "Personal information" is defined under the CCPA as information that identifies, relates to, or could reasonably be linked with a California consumer or their household, including name, social security number, email address, product purchasing records, online browsing history, geolocation information, and biometric data. Personal information does not include information that is publicly available, de-identified, or aggregated, as defined under the CCPA.

In addition, in November 2020, California voters approved an amendment to the CCPA called the California Privacy Rights Act (CPRA). The CPRA fully went into effect on 1 January 2023. Key amendments under the CPRA include the following.

- Higher applicability threshold to organisations that buy, sell, or share the personal data from at least 50,000 residents or households annually to at least 100,000. This modification may exclude some entities from application of the CCPA.
- New category of "sensitive personal information", which includes personal information that reveals a consumer's:
 - (a) social security, driver's license, state identification card, or passport number;
 - (b) financial account and related data;

- (c) precise geolocation within a 1,850 foot radius;
- (d) practical or ethnic origin, religious or philosophical beliefs, or union membership;
- (e) mail, email, or text messages content, unless the business is intended recipient of such information;
- (f) genetic data and/or biometric information for the purpose of unique identification; and
- (g) health status or medical conditions and sexuality, including sexual orientation.

Consumers have the right to limit or opt out of certain uses of sensitive personal information.

- In addition to limiting the use of sensitive personal data, consumers can opt-out of:
 - (a) the sale of personal information to a third party for monetary or other valuable consideration; and
 - (b) sharing of personal information with a third party "for cross-context behavioural advertising, whether or not for monetary or other valuable consideration".
- Consumers also have a new right to require businesses to correct inaccurate information "taking into account the nature of the personal information and the purposes of the processing of the personal information".

Violations of the CCPA are enforced by both the California Attorney General and the California Privacy Protection Agency, both of which have the power to impose penalties/fines of up to USD2,500 per violation or USD7,500 per intentional violation/violation involving consumers under 16 years of age. The law also affords California consumers a private right of action for breaches of sensitive personal information.

Virginia

The Commonwealth of Virginia is the second state to enact a comprehensive data privacy law, the Virginia Consumer Data Protection Act (VCDPA). The VCDPA was passed into law in 2021 and went into effect on 1 January 2023.

Virginians have comparable rights under the VCDPA as Californians do under the CCPA. However, Virginia affords additional, specific rights to opt out of targeting advertising and profiling.

Finally, there is no private right of action for Virginians to recover damages for a business's breach of the VCDPA. The Virginia Attorney General is responsible for enforcing the VCDPA and may impose penalties of up to USD7,500 per violation.

Colorado

The Colorado Privacy Act (CPA) was signed into law on 7 July 2021 and went into effect on 1 July 2023. The CPA is generally more closely aligned with the VCDPA than the CCPA. Violations of CPA will be enforceable exclusively by the Colorado Attorney General and the 22 Colorado District Attorneys and are subject to penalties of up to USD20,000 per violation under the Colorado Consumer Protection Act. There is no private right of action for Colorado consumers under the law.

Other states

Other states may enact their own laws. Given the differences among current state laws, companies will need to devote careful thought to a compliance strategy that accounts for these differences and the laws' incomplete coverage.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Entities that hold personal information about consumers and businesses should consider privacy, disclosure, equal opportunity/non-discriminatory uses, and transparency concerns. "Big data" is the collection of millions of data points of information about an individual consumer or business across a variety of sources, collected over time, and may be held or used by entities that interact directly with consumers and business (first-person data), or by data aggregators and data brokers (third-person data). "Artificial intelligence" enables machines to analyse information in big data using algorithmic processes.

While there is no comprehensive current federal statutory and regulatory structure in the US dedicated to information used in big data and artificial intelligence, several federal statutes are potentially implicated depending on the type of information at-issue. Case-by-case enforcement of these statutes have formed in the structure of consumer protection relating to big data and artificial intelligence.

At the federal level, the Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) have indicated that they may use their authority to prevent unfair or deceptive acts and practices in the AI and big data arenas. For example, in 2022, the CFPB announced that its examinations of financial institutions for unfair, deceptive, or abusive practices would include assessments of whether examinees engaged in discriminatory practices. In late 2022, the FTC issued an Advanced Notice of Proposed Rulemaking (ANPR) seeking comments from the public on proposed rules to protect against

consumer harm as a result of entities' commercial surveillance and data security practices. Following receipt of comments from the public and industry, the FTC may issue rules relating to these topics.

In addition, various states have statutory restrictions on the collection, retention, and use of personal information, generally, or with respect to specific types of personal information.

Big Data

Despite the absence of a comprehensive federal statutory and regulatory structure for big data, the Federal Trade Commission (FTC) plays a significant role in shaping entities' practices involving non-public personal information, generally, in the US using case-by-case enforcement and policy statements. The FTC has authority under Section 5 of the FTC Act to declare a business as having "unfair or deceptive acts or practices." Analysis under Section 5 of the FTC Act is fact-specific to the particular circumstances of an entities' practices. In its Report on Big Data, "Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues, FTC Report" (January 2016), the FTC described a number of specific practices as unfair or deceptive in its report on big data.

Several comprehensive state privacy laws set transparency and choice requirements in relation to profiling and automated decision-making. In 2021, Colorado and Virginia also passed generally-applicable privacy statutes relating to personal information. Those states, and Connecticut, give consumers the right to opt out of "profiling" (defined as automated personal data processing to evaluate certain individual characteristics) in furtherance of "decisions that produce legal or similarly significant effects concerning the consumer". California's privacy

regulator, the California Privacy Protection Agency (CPPA), is expected to issue regulations that address similar issues by mid-2023. In addition, the California Consumer Privacy Act (CCPA) mandates disclosure about the collection and use of "a consumer's personal information", including disclosure about what personal information is collected, the right to delete personal information, and the right to prevent the sale of the collected personal information. The CCPA also contains a right of non-discrimination for consumers that exercise their rights to protect their personal information, with certain exceptions.

Other federal and state privacy statutes are more narrowly focused on specific types of personal information. For example, the US federal Fair Credit Reporting Act regulates information collected and used by consumer reporting agencies, and federal civil rights laws regulate the use of personal information where the intent or the effect of the use of the information results in a violation of the rights of the statute's protected classes. Various states have similar and additional civil rights laws relating to this type of information. In addition, certain states provide even greater privacy protections to specific types of personal information. For example, the Illinois Biometric Information Privacy Act (BIPA) protects individuals' rights over their biometric information, such as facial recognition scans, voice and finger prints, and hand or eye scans.

As a result, entities pursuing the collection, retention, or use of information about consumers and businesses in the US should ensure that they have clear disclosures and procedures to safeguard personal information, and that these procedures are fully enforced. In addition, entities should examine the type of personal information being collected, retained, and used, as

well as the state jurisdictions applicable to the entity, to implement the appropriate federal and state privacy, disclosure, and transparency procedures and safeguards.

Artificial Intelligence

In addition to the privacy, disclosure, equal opportunity/non-discriminatory uses, and transparency considerations raised above, artificial intelligence raises an additional consideration relating to the scope of disclosure and consent. Artificial intelligence necessarily depends on algorithms that evolve or change over time. To the extent an entity provides disclosure that certain personal information is being collected, retained, and used, and the consumer provides consent for that purpose, any changes outside the scope of that disclosure and consumer's consent may violate federal and state privacy and protection laws or be considered an "unfair or deceptive act or practice" under Section 5 of the FTC Act. Entities should ensure that disclosures and consents are sufficiently specific to inform consumers of the nature of the personal information being collected, retained, or used, and periodically update these disclosures and consent in parallel with changes to their machine learning and artificial intelligence algorithmic processes.

Regulatory authorities in the United States have also increasingly become focused on the potential discriminatory impact of the use of AI in decision-making, such as when algorithms are used in connection with employment decisions or the decision to offer credit to a consumer.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

"Smart" or "connected" devices, also known as internet of things devices, follow the federal National Institute of Standards and Technology (NIST) guidelines published by the US Department of Commerce and the statutory requirements found in certain state laws. Further, pursuant to the federal Internet of Things Cybersecurity Improvement Act of 2020, compliance with the NIST guidelines is required for federal procurements.

The NIST guidelines, NISTIR 8259, provides a summary of cybersecurity and privacy risk considerations, as well as assessment tools, and NISTIR 8259A provides a baseline for how a connected device will be defined as "securable".

Connected devices raise considerations of privacy, disclosure, and cybersecurity concerns relating to information that the connected device uses, receives, stores, or transmits described elsewhere in this article, and in particular, Sections 2, 3, 4, and 8. Two additional frameworks are also significant in this arena: federal and state wiretapping laws and critical infrastructure.

Federal and State Wiretapping Laws

The federal Wiretap Act and similar state laws generally prohibit the interception of electronic communications. Although these laws contain exceptions for recipients of communications and that may allow analysis of communications for security purposes, the application of these exceptions requires fact-specific analysis. For example, some state wiretap laws require all parties to a communication to consent to interception. If this exception is the basis for intercept-

ing machine-to-machine traffic, it is important to understand whether such multi-party consent is necessary.

Critical Infrastructure

The Cybersecurity and Infrastructure Security Agency of the US Department of Homeland Security is developing cyber-incident and ransom payment reporting regulations pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Entities in the communications and healthcare sectors, among others, may be covered by these regulations. The reporting requirements, however, are not effective until the regulations are finalised.

In addition, certain states, such as California and Oregon, have statutes specifically focused on securing connected devices by requiring them to be equipped with cybersecurity safeguards which differ depending on the type of connected device. These state statutory requirements and NIST guidelines for securing a connected device should be considered in addition to privacy, disclosure, and transparency statutes, as well as general consumer protection statutes.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Radio and Broadcast Television

The Communications Act of 1934, as amended, with rules promulgated and enforced by the Federal Communications Commission (FCC), governs commercial AM, FM radio, and television broadcast authorisations. An authorisation from the FCC is required to operate a commercial AM, FM radio, and broadcast television station in the US, as described more fully on the FCC's application guidance.

An application to the FCC for a commercial AM radio station (with frequencies of 540 kHz to 1700 kHz) requires a demonstration of non-interference on the same or on adjacent frequencies as existing US or foreign-based AM stations, as well as harmonic and intermediate frequency analyses. Application and fees are required during allotment application windows.

An application to the FCC for a commercial FM radio station (with frequencies of 92.1 MHz to 107.9 MHz) requires an application for a construction permit and a concurrent petition for rulemaking to the FCC which must, according to the FCC's application guidance:

- include the proposed new channel, class, and the community to be served;
- the proposed new allotment site must meet the spacing requirements of (the FCC's rules) to other stations, prior-filed applications, and vacant allotments; and
- the proposed new allotment site must provide at least a 70 dBu signal strength over the entire community of licence.

If the petition is accepted, the FCC would then issue a notice which would permit public comment on the application. If approved, the new allotment would then be placed in an auction bid which would require the original petitioner to bid on the allotment.

Full-powered television broadcast stations are allocated through the FCC's Table of Allotment (47 CFR Section 73.622). Applicants seeking a new broadcast television station must petition the FCC and the FCC will then conduct an auction. However, at this time, the FCC states that it is not accepting new full-powered broadcast television station applications.

Video Programming by Cable and Open Video Services

Historically, video programming has been governed by state and local jurisdictions, called local franchise authorities. However, the Cable Communications Policy Act of 1984, as expanded by the Cable Television Consumer Protection and Competition Act of 1992, added cable television regulation to the FCC's authority under the Communications Act of 1934 while maintaining the primary regulatory role of the local franchise authorities, with the notable exceptions of establishing a prohibition on regulating rates for cable operators that are "subject to effective competition," as defined by the FCC, and a prohibition on exclusive cable franchises. In addition, Section 653 of the Telecommunications Act of 1996, as amended, established an "open video system" (OVS) distribution method for video programming in the absence of a local franchising authority regulatory requirement. The specific local franchise requirements vary widely across jurisdictions.

Online Video Services

The FCC's video regulations generally do not apply to IP-delivered video programming that is not provided by a multichannel video programming distributor (MVPD). There are no prior regulatory authorisation requirements to post videos online. However, entities should ensure compliance with federal, state, and local rules when making video available online. For example, a distribution of online videos may implicate the 21st Century Communications and Video Accessibility Act (CVA), 47 USC Section 613 and FCC rules where the video was previously published or shown on television. Further, interpretation of Title III of the federal Americans with Disabilities Act (ADA), 42 USC Section 12182, varies, and is subject to change through court interpretation, as to whether a website is "a place of pub-

lic accommodation" requiring equal access for individuals with disabilities, such as through the provision of closed captioning.

The federal Video Privacy Protection Act (VPPA), 18 USC Section 2710, establishes notice and consent requirements for "video tape service providers", a term that is defined with sufficient breadth to include many online streaming services as well as video-on-demand services. The VPPA generally requires a consumer's opt-in consent to disclose personally identifiable viewing history information. The VPPA provides a private right of action and has led to a significant volume of class action information against video services providers and, in some instances, advertising platforms.

With regard to the content of video posted online, pursuant to Section 230 of the Communications Decency Act, providers of an interactive computer service generally are not treated as a publisher or speaker for information provided by another information content provider. As a result, companies with video-sharing platform services will generally not be liable for civil damages for the content of videos where the provider, in good faith, restricts access to, or the availability of, material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected, or where the provider takes action to enable or to makes available technical means to restrict access to the above-described material, along with undertaking other procedural requirements of the statute.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Title II of the federal Telecommunications Act of 1996, as amended (the “Telecommunications Act”), generally governs the offer to the public of interstate and international “telecommunications”, which are transmissions by the aid of wire, cable, radio, or other like connections, through regulations promulgated and enforced by the Federal Communications Commission (FCC) 47 USC §§153(50), (53). The FCC also asserts jurisdiction over certain aspects of interconnected Voice over Internet Protocol (VoIP) services. Whether a transmission is interstate and international, on the one hand, or intrastate, on the other hand, is generally determined by the origination and termination points of the transmission. Generally, providers of telecommunications must possess authorisation from the FCC under Section 214 of the Communications Act of 1934 for interstate and international transmissions, though certain wireless carriers are relieved of the requirement to obtain Section 214 authority and broadband internet access service (“broadband”) is currently subject to distinct regulatory frameworks. All Title II telecommunications service providers and interconnected VoIP providers must obtain an FCC Registration Number (FRN) through the FCC’s website, register with the FCC, and designate an agent for service of process by filing a form with the Universal Service Administrative Company (USAC). These obligations apply to both wholesale providers and resale providers.

Individual state commissions and state and local statutes regulate intrastate transmissions. Providers of intrastate telecommunications must register with or obtain authorisation from each individual state in which the intrastate transmis-

sion occurs except where the state legislature or commission has exempted the requirement. Providers of intrastate telecommunications services are also subject to state statutory requirements, such as state statutes on unfair or deceptive acts and practices and privacy.

In contrast to federal Title II “telecommunications services”, transmissions may be subject to reduced FCC regulation if provided on a “private carriage” basis, or if the interstate or international transmission consists of “information services”. Private carriage is the transmission of telecommunications that are not offered to the public. When interstate or international telecommunications are provided on a private carrier basis, the provider is not required to obtain a Section 214 authorisation from the FCC and fewer federal compliance obligations apply. State regulators, however, generally do not recognise the concept of private carriage as an exception to authorisation or compliance obligations.

In addition, there is no requirement to obtain Section 214 authority from the FCC to provide interstate and international information service transmission. Information services are statutorily defined as “the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilising, or making available information via telecommunications” 47 USC §153(24). The definition further states that information service “does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service”. Generally, if there is a net change in the protocol of a transmission, the transmission may likely qualify as an information service 47 USC §153(50). Information services have been commonly identified as email, online gaming, web browsing, video conferencing, instant messag-

ing, and other, similar non-voice IP-enabled services. The FCC has a long-standing policy against the economic regulation of “information services”, and there is a prohibition on states subjecting information services to any state economic regulation. However, the FCC’s policy does not prohibit the application of federal and state consumer protection laws to these services.

With respect to VoIP services and VoIP service providers, there is a continuing dispute as to whether federal communications law permits states to require applications for authority; however, one or more states currently assert that authority. For the most part, states either require registrations, typically for purposes of collecting state public fund contributions, or do not impose either a registration or application requirement, although even in such cases, contributions to state public purpose funds may still be required. State economic regulation, such tax obligations, generally apply to VoIP revenues. In general, state regulation of VoIP services and VoIP services providers is limited, but registration, where it exists, varies considerably across the states with state uniquely handling the question of VoIP jurisdiction. In a number of states, legislatures have expressly removed VoIP services and VoIP service providers from the jurisdiction of the state commissions or state commissions have declined to exercise jurisdiction over VoIP services and VoIP service providers, although many such states may permit a “carve out” of residual state commission jurisdiction for purposes of state universal service fund and other public fund assessments.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges Key Challenges

Technology agreements may cover the deployment or sale of a number of different services, products, solutions and platforms, including on-premise software licences, software-as-a-service offerings, software development and maintenance, data-related product and services, artificial intelligence-enables solutions and many others. Each type of agreement will have its own challenges. However, key challenges often include performance commitments (eg, warranties and service levels), clear upfront pricing and addressing changes to prices over time, compliance with laws’ provisions, intellectual property ownership, data security and privacy, audit, indemnification and limitations and exclusions of liability.

Legal Framework

As a general matter, technology agreements will choose the laws of particular state to apply to the agreement and a court will enforce the parties’ choice of law in the contract as long as there is a reasonable relationship to the transaction or the parties, subject to certain exceptions. However, in the United States, federal law generally takes precedence over state laws. While there is no over-arching federal contract law, various federal laws will continue to apply to a technology agreement containing the choice of a specific state’s laws depending upon factors such as the subject matter of the agreement, the industry involved and the technology or data involved. For example, software and products that incorporate encryption may be subject to export restrictions under the Export Administration Regulations, a complex licensing and exemption scheme for encryption exports.

Federal, state and local governmental agencies and entities entering into technology agreements are often subject to laws and regulations applicable to the procurement process for technology agreements as well as specific requirements related to provisions contained within the agreements.

Data Protection and Cybersecurity

An increasingly important data protection and security issue concerning technology agreements is whether the parties are entering into a service provider/processor relationship, or whether personal data that is transferred pursuant to the agreement is between parties with independent rights to determine the means and purposes of processing. Comprehensive state privacy laws establish specific requirements for service provider processor contracts, similar to those under the GDPR. In addition, California requires agreements under which a party sells or shares personal data to include a subset of these provisions, including specifying the purposes of the data transfer, obligating the recipient to comply with applicable privacy laws, and providing the data source the rights to assess the recipient's compliance and remedy instances of non-compliance.

US laws generally do not require data localisation or restrict storage location (other than in relation to countries that are under sanctions or export controls), nor do they require specific measures for cross-border data transfers. However, the location of personal data storage, including the ability to enforce confidentiality provisions against employees or contractors, is often a factor in assessing a contracting party's ability to meet contractual obligations and to provide a reasonable level of data security.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Data Protection and Cybersecurity

Trust, digital identity, and similar services process personal data that may be highly sensitive because of its potential to be misused for fraud, identity theft, or account compromise. Personal data used in the course of providing such services may be subject to data breach notification laws, which have been enacted in all 50 states, the District of Columbia, and several US territories. These laws typically provide exemptions for encrypted data, provided that encryption keys are not compromised, but determining whether or not this exemption may require a forensic investigation of the relevant data security incident.

Other data protection and cybersecurity considerations that relate to trust and identity services include the following.

- **Biometric privacy laws.** At least three states have enacted laws that establish notice, consent, and retention requirements for biometric information that is used to establish individuals' identity. One of these laws, the Illinois Biometric Information Privacy Act, provides a private right of action and has given rise to a significant amount of class action litigation.
- **Comprehensive state privacy laws.** In addition to requiring heightened consent and security measures for sensitive data (including biometric information and, in California, account credentials), state privacy laws require parties to determine whether the provider or trust or identity service is acting as a service provider/processor or as a third party with independ-

ent rights to use personal data under the relevant agreement.

- State data security and disposal laws. Most states have enacted data security legislation, including secure disposal requirements, that specifically govern sensitive data such as social security numbers and state identification numbers.

Electronic Signatures

The federal United States Electronic Signatures in Global and National Commerce Act (the “ESIGN Act”), as supplemented by Uniform Electronic Transactions Acts (the “UETA Act”) and similar laws adopted at the state level, establishes that electronic records are not invalid solely because of their electronic nature when the parties have chosen to use electronic documents and signatures. The ESIGN Act permits individual states to further address electronic signatures for transactions subject to the individual state’s laws, other than in certain areas where the ESIGN Act overrules (or pre-empts) state law. While most states have adopted an act very similar to the model UETA Act, some states have modified the model act or not enacted it. In addition, the model UETA contains certain exceptions to the use of electronic signatures, such as their use with wills, codicils and certain trusts.

Generally speaking, a party to an agreement seeking to establish the validity of an electronic signature will need to:

- show that the counterparty intended to sign the document and consented to conduct business electronically;
- establish the validity of the process by which the signature was created or indicated; and
- show that a record of the electronic signature was retained and can be reproduced by all parties to the agreement.

Additional requirements apply to transactions involving consumers in some cases.

In addition to meeting the requirements related to electronic signature, an electronic contract will still need to meet the requirements for an enforceable contract under applicable state law (ie, an offer, acceptance of the offer and consideration).

Contributed by: Mike Ryan, Aaron Burstein, Mike Dover and Patricia Werner, **Kelley Drye & Warren LLP**

Kelley Drye & Warren LLP has provided carefully tailored legal counsel to its clients for more than 180 years. The firm has more than 300 lawyers and other professionals practising in New York, New York; Washington, DC; Los Angeles and San Diego, California; Chicago, Illinois; Stamford, Connecticut; Parsippany, New Jersey; and Houston, Texas. The firm's technology transactions and sourcing practice has handled some of the world's largest and most complex technology-driven transactions on all

sides of the deal spectrum and across a range of industries. The firm's communications practice assists a wide array of enterprises, ranging from global carriers to start-ups, in meeting their legal and regulatory needs. The firm's privacy and information security practice works on the leading edge of media, technology and business, helping clients understand and proactively address privacy, information security and compliance issues.

Authors



Mike Ryan chairs Kelley Drye & Warren LLP's technology transactions and sourcing practice group. His practice focuses on a variety of complex transactional matters in the

technology and business process services marketplaces. Mike has extensive experience advising clients on technology and business process services transactions, including the development and deployment of software and infrastructure using a variety of delivery models, such as cloud software-as-a-service and infrastructure-as-a-service. He also advises on intellectual property licensing transactions, resale and distribution agreements, mergers, acquisitions, joint ventures/strategic alliances and equity investments.



Aaron Burstein is a partner at Kelley Drye & Warren LLP and provides legal advice on privacy, information security, and marketing laws and best practices, including compliance

with federal and state laws throughout the USA. He has been an attorney in the Federal Trade Commission's Division of Privacy and Identity Protection and a senior legal adviser to Commissioner Julie Brill. Before joining the FTC, Aaron was a policy adviser at the National Telecommunications and Information Administration, where he was the principal drafter of the Department of Commerce's consumer privacy "green paper" and the White House's Consumer Privacy Bill of Rights report.



Mike Dover is a special counsel at Kelley Drye & Warren LLP and focuses on providing legal advice and unique legal perspectives to a variety of established and emerging

technology providers throughout the USA, including to cable, video, broadband, and other communications providers and communications infrastructure providers, relating to rights and requirements, which include cable and franchise regulations, cable transaction regulatory management, broadband deployment and infrastructure, communications infrastructure, internet of things, state commission requirements, universal service rules, and issues concerning security, privacy, licensing and performance-based breach disputes. Previously, Mike worked as a telecommunications regional network engineer, network planner, and build-out project manager for T-Mobile USA.



Patricia Werner is a special counsel at Kelley Drye & Warren LLP and member of the firm's Trademark and Copyright and Litigation practice groups. Patricia manages worldwide

intellectual property portfolios and related protection and enforcement matters for numerous brands in industries spanning consumer products, cannabis, entertainment and fashion. She handles all aspects of trade mark and copyright protection, including domestic and international trade mark portfolio management, clearing and prosecuting trade marks, licensing, IP due diligence investigations and US and foreign enforcement proceedings. In addition, Patricia is involved in corporate transactions including negotiating asset purchase and related agreements for various transactional matters.

Kelley Drye & Warren LLP

3 World Trade Center
New York
NY 10007
USA

Tel: + 212 808 7800
Fax: + 212 808 7897
Email: crubsamen@kelleydrye.com
Web: www.kelleydrye.com



Trends and Developments

Contributed by:

Tom K. Ara, James Williams,
Katherine M. Imp and Mark Radcliffe
DLA Piper LLP see p.570

Real World Meets Virtual World: Emergent Metaverse Use Cases and Attendant Legal Considerations

Over the past year, real-world businesses have rushed to develop metaverse strategies, with many even purchasing “virtual land”. The metaverse is likely to touch every industry, some minimally and others (such as real estate, entertainment and consumer discretionary) much more deeply. Yet, with the promise of a fully immersive metaverse similar to the one found in the movie Ready Player One believed to be years away, many businesses that have made the initial investment and dipped their toes in the virtual water find themselves asking, “what now?”

It is a question the e-commerce industry answered six or seven years ago with a dash of irony: propel the hi-tech online experience forward by weaving in elements of “old school” offline retailing. The result was a shift away from pureplay online-only offerings toward “clicks-to-bricks” and omnichannel models. In other words, e-commerce’s progression has been, in significant part, driven by the:

- merging of physical and digital experiences; and
- elimination of friction between physical and digital channels.

The metaverse may be following a similar path with consumer-facing industries beginning to rethink existing engagement models and test new applications developed to drive consum-

er metaverse adoption through the blurring of physical and virtual experiences.

Below is a discussion of the emerging technologies and use cases serving to increasingly blur the lines between physical and digital assets, experiences, and identity, and an examination of the potential legal issues that should be considered.

Unreal Estate: Metaverse Property

According to RubyHome (using data from a number of sources), the sales of metaverse land exceeded USD1.9 billion in 2022 on the top 10 metaverse platforms. Metaverse landowners include celebrities (such as Snoop Dogg and Deadmau5), entertainment properties (eg, The Walking Dead, Smurfs and Care Bears) and consumer brands (eg, Nike, Wendy’s and Hyundai).

While the early “generation” of metaverse buildings were quick to take advantage of the loose (or non-existent) application of real-world logic and physics, deploying features such as floating staircases, fantastical waterfalls and hallway-roaming tigers, the pendulum appears to be swinging in the other direction with the emergence of “digital twins” or metaverse assets intended to emulate their real-world counterparts.

For example, Snoop Dogg is creating a “Snoopverse” where he plans to recreate his real-world mansion in Diamond Bar, California. Likewise, the Atlanta Braves, a Major League Baseball team, last year revealed their plan to create

a digital twin of Truist Park in the metaverse. The plan opens up a slew of fan engagement opportunities for the Braves, including the ability to eventually give fans the power to view live games in the metaverse stadium via technology similar to the Netaverse Experience debuted by the NBA's Brooklyn Nets (which allows fans to experience virtual reproductions of real games in real time, from a perspective not feasible for most – or even possible – in the real world). For example, metaverse fans may be able to virtually watch games not only from dugout or court-side seats, but even from the perspective of the actual players.

As suggested above, the purpose of the digital twin strategy is not simply to create digital analogues of real-world properties, but rather to blur the line between the two. Not only are digital users able to experience the replication of live events happening in the real world, but real-world fans, through the use of augmented and mixed reality technologies, will also be able to interact with and activate metaverse elements from the real world. As an example, fans may soon be able to point their phone camera on different stadium signs to access off-limits areas via the metaverse (such as locker rooms).

Further, this digital twin strategy has applications beyond commerce, extending into educational and charitable territories. For example, it would not be a stretch to imagine Boston's Freedom Trail recreated within a metaverse environment and, conversely, the real-world Freedom Trail experience enhanced by augmented and mixed reality to deliver more vivid learning experiences.

Potential legal issues

The nature, rights and characteristics are entirely controlled by the software of the metaverse platform and that platform's terms of service

(ToS). Metaverse "virtual land" is very different from traditional land. Mark Twain's famous quote about real estate – "buy land, they are not making it anymore" – is not true in the metaverse. Generally, the current major metaverse platforms can make an unlimited amount of additional virtual land, which can affect the value of the virtual land purchased. The ToS of the metaverse platforms are generally very favourable to the platform; for example, the Sandbox ToS permit Sandbox to remove any virtual assets from its metaverse without notice for any "reason or no reason". Similarly, ToS for Decentraland permit the decentralised autonomous organisation (DAO) that runs the Decentraland metaverse to terminate the terms of service and suspend a user's accounts in its sole discretion. In the real world, businesses can, and do, negotiate co-tenancy restrictions with landlords to prevent a brand's message and foot traffic from being diverted by competitors. Given the centralised nature of current metaverse platforms and the fixed nature of their ToS, this option is not available and the projection of negotiating power some businesses enjoy in the real world may not entirely translate to the digital world. This reality will require deeper due diligence in the relevant platform's ToS, not only ensuring the intended metaverse use complies with the platform's ToS, but additionally confirming the intended use is consistent with co-tenancies; the clearest example of this is a family-oriented brand which finds that a virtual "neighbour" is launching adult entertainment offerings.

Additionally, real-world trade mark, copyright and advertising laws and regulations are likely to follow our avatars into the metaverse. Consequently, companies will need to play both virtual offence and defence, ensuring their trade marks (in the case of brand names) and copyrights (in the case of real-world architecture protected by

the Architectural Works Copyright Protection Act in 1990) are not being copied by others, as well as ensuring their offerings are compliant with real-world marketing and advertising contractual requirements and applicable law. In the case of professional sports venues mentioned above, sponsorship agreements should not only recite the rights and obligations of the team and sponsor with respect to the physical stadium, but should also address whether said rights and obligations translate to any digital iterations of the venue.

Movie Night in the Metaverse

High speed internet, 5G and the rise of streaming services have thus far revolutionised the distribution and consumption of audio-visual content for the masses. Theatrical attendance has decreased precipitously (with box office revenues remaining elevated pre-COVID as a result of increased ticket prices and plummeting post). The “movie” night as we knew it has predominantly migrated to our living rooms where the popcorn is free and the furniture germ-free. So, what is lacking from the movie-going experience, one might ask?

Film industry experts and audiences proclaim that many film genres are better enjoyed as a communal experience, particularly with strangers, and that the cinema experience itself is an immersive experience not to be lost. While a movie night in the living room lacks the communal experience a theatre may offer, the metaverse presents an opportunity for willing fans to regain that experience. Already, second screen engagement has become widespread across many streaming programs and several platforms have introduced shared viewing functionalities. Inside an immersive metaverse, fans can fully engage with others and the programming itself in the simulated theatre, sharing laughs, gasp-

ing in horror or expressing other spontaneous reactions. A couple separated by geographical boundaries can reunite and share date night at the movies, and possibly even holds hands with meaning through the use of haptic gloves. The classic “Rocky Horror Show” custom screenings can be experienced in an entirely new manner in the virtual theatre.

Companies have already begun experimenting with virtual theatres, including allowing users to experience programming available on traditional streaming platforms in immersive theatres as well as invite-only film festival screenings hosting industry professionals in the metaverse. A more interesting twist will be Hollywood-type content that will allow the user to engage, participate or even choose their own ending in an immersive setting. All of these experiences and more will develop as engagement increases in the metaverse and greater content migrates to the virtual platforms.

Potential legal issues

Creation of high-value content involves the engagement of high-level talent of various types, including writers, directors and on-screen talent, as well as various below-the-line crew (eg, make-up artists, set designers, etc) and implicates other rights as such soundtrack and licensed music incorporated into the programme. Even the simple idea of migrating a film or television programme from the big screen or small screen to the virtual screen requires an analysis of the scope of exploitation rights the party seeking to do so possesses and the financial implications (residuals, participation payments, etc) of such forms of exploitation.

Will subscribers of a traditional streaming service operating a virtual theatre also be allowed to watch the service’s programmes in the virtual

theatre at no additional cost or will a premium subscription or fee be applicable? Will admission fees be charged and into which category of revenues will those fees fall for purposes of accounting and paying any share of those revenues to various participants and entertainments guilds? Moreover, the concept of an interactive or “choose your own ending” type feature film raises the prospect of additional use fees and approval rights that talent may have based on what may be viewed as derivative or out-of-context work based on the original performance. These and many other intellectual property and commercial rights issues will be implicated as the movie-going experience migrates into the metaverse.

Virtual Moshpits: Live Musical Performances

To date, a variety of live events have been staged in the metaverse, including concerts, sporting events, interactive gaming events, trade shows, job fairs, award shows and graduation ceremonies. A number of factors have prompted the foray into such experiences in the metaverse, including:

- the ability to attend without the need to travel;
- expanded attendance capabilities;
- a more immersive experience than two-dimensional content, allowing interaction with other attendees;
- the ability of those with restricted physical mobility to easily attend and travel around the virtual space;
- real-time language translation capabilities to eliminate language barriers;
- multi-camera technology allowing attendees to participate from multiple viewpoints;
- the potential for targeted promotion designed for specific attendees based on geolocations and preference settings; and

- ancillary monetisation opportunities, including through the sale of in-experience goods such as NFTs related to the live events.

Of the different types of live events and performances that have been hosted in the metaverse, live musical performances have proved to be the most popular to date. Travis Scott’s Fortnite performance in April 2020 had over 28 million people teleporting in to view the concert. Justin Bieber’s performance on Wave, a virtual music platform, in November 2021, and Young Thug’s performance on Meta’s Horizon Venues platform in December 2021 also found great success. Other artists like David Guetta (through the Roblox platform), Calvin Harris (through the Pico VR platform) and Ariana Grande (through the Fortnite platform) have taken their metaverse concerts to another level by incorporating dance battles, puzzles, mini-games, virtual merchandise and other interactive features to their performances to further engage attendees.

The interest in live musical performances in the metaverse has also sparked a new wave of metaverse start-ups with music ambitions. For example, Popins is a start-up using volumetric video technology to turn artists into 3D avatars, which can then be viewed on mobile devices and used by fans to create their own content (such as duets). SolTunes, an NFT start-up, allows consumers to use its software to mix and match musicians, thus creating new pieces of content. MetaCities is focusing on recreating real-world locations in the metaverse, and then providing experiences in those virtual spaces that include music performances.

Some of the biggest technology and gaming companies are also expanding their music aspirations. In the last two years, Fortnite’s publisher Epic Games acquired music-games developer

Harmonix, music platform Bandcamp and music licensing start-up Lickd to expand the types of music-based metaverse experiences available to its users. League of Legends developer Riot Games has hosted hybrid concerts at its esports events, combining real-world arts with Riot Games' virtual music stars such as K/DA, True Damage, and Pentakill.

The staging of live events, in particular live musical performances, in the metaverse and on new and existing platforms will continue to be a driver of audiences to the metaverse. It will be a useful tool to engage with new and existing audiences eager to be the first to experience a particular event live that they otherwise could not or would not attend in person.

Potential legal issues

While live virtual musical performances trigger a number of different legal issues to be considered, music rights clearance tops the list. The metaverse poses various challenges to traditional forms of music licensing. For example, with traditional synchronisation licences – which are used when songs are paired with audio-visual content such as a film or television series – rights-holders know exactly how their music is being used (eg, in the opening or closing credits of a film) and negotiate fees based on such usage. In the metaverse, however, the audio-visual content to which the song is paired could be part of an evolving platform and/or user-generated content, making negotiation of a synchronisation licence far more difficult.

Performance royalties must also be considered. Traditionally, performance royalties are earned anytime a song is played publicly, including live concerts, satellite or broadcast radio stations, and restaurant or bars, and collected through performing rights organisations (PROs) or collec-

tive management organisations (CMOs). Songs performed publicly in the metaverse will presumably similarly require royalty payments or blanket licences through PROs and CMOs and this area continues to develop.

Lickd is an example of a company that has already begun to tackle the issue of music rights and licensing in the metaverse. In the last few years, Lickd has entered into licensing arrangements with publishers such as Warner Music Group and Empire so that it can provide pre-cleared music licensing for virtual content creators. By way of example, the deal between Lickd and Vegas City, a virtual world within the metaverse-based 3D world Decentraland, signed in 2022, will allow Vegas City to play background music in venues and public spaces throughout its district, the same way that consumers listen to music in restaurants and bars in the real world.

In addition to music licensing, guild and union issues must be considered. For example, if the virtual concert involves the use of performances by actual performers, that performance (including everyone from the lead singer to the background dancer) is likely covered under the Screen Actors Guild – American Federation of Television and Radio Artists (SAG-AFTRA). This means that the content creator – whether the creator is a studio, video game company, metaverse platform or other entity – will need to negotiate with SAG-AFTRA for such usage.

Another issue to consider in connection with live musical performances is censorship. The metaverse is intended to be open, transparent and inclusive, but if big technology companies ultimately control the metaverse platform then they can control the content that users see and

the information that is disseminated during the live musical performance.

There may also be other types of intellectual property besides music that must be cleared in connection with a live virtual musical performance. For example, a digital representation of a brand's mark on the clothing of an avatar or represented on the virtual stage or in the virtual arena, could have both trade mark and copyright protection requiring clearance.

Publicity rights must also be considered. Publicity rights are intended to protect a person's persona – such as their name and image – but in the metaverse, what constitutes a protectable persona gets murky. Over the years, courts have begun to protect other indicia of an individual's identity, such as look-alikes, catchphrases, caricatures, nicknames, and performance characteristics. As live virtual musical performances become more prolific, it is very likely that the scope of protection of a person's persona will also increase, or at least be brought into question.

Lastly, the terms of use of the metaverse platform hosting the live musical performance will need to be carefully considered. The dynamic nature of a live musical performance in a virtual world, where avatars of many participants may intersect with the performance, live chat functions may be operational and user contributions may actually form or distort the experience, presents unique considerations for rights-holders. If the terms of use do not contemplate these different types of contributions, then individual clearances of the participants and their contributions may need to be obtained, further complicating the clearance process.

“Identify Yourself, Avatar!”: Digital Identity and Reputation

One of the hallmark benefits ascribed to blockchain technology is the ability to own certain property and transact free from scrutiny from or control by centralised powers. This is achieved, in part, through the veil of anonymity. Transactions are trustless because the subject consensus protocol verifies the transaction terms on both sides of the equation, irrespective of party identity. But what if you wanted to trustlessly validate transactions based not on transaction terms, but on party identity?

Enter identity and reputation tokens. Depending on who you ask, these tokens may be viewed as either one of the most important developments in metaverse and blockchain evolution, or the antithesis of blockchain's reason for being – freedom from centralised control. Whatever your blockchain ideology, identity and reputation tokens are here and their use cases are likely to expand quickly. Accordingly, consumer-facing businesses should begin considering the implications, benefits and potential pitfalls surrounding merging of real world and on-chain identity. Perhaps the most promising development driving identity and reputation use cases is Soul-Bound Tokens (SBT).

On 11 May 2022, Vitalik Buterin, E. Glen Weyl and Puja Ohlhaver released a white paper titled, “Decentralized Society: Finding Web3's Soul”. The white paper describes the potential for the foundation of a fully decentralised society (DeSoc) governed by its users. SBTs would operate at the heart of DeSoc and serve as the on-chain repository of users' real-world credentials, identity and reputation.

Technically, SBTs are NFTs that certify a fact about the holder. Such facts may include the holder's:

- name;
- driver's license number;
- favourite sports team;
- résumé details (educational/work history);
- blood type;
- private club membership; and
- transaction details with respect to a specific brand.

The potential is limitless. Once SBTs are issued to a holder's wallet, they are forever bound and cannot be transferred. Possession of a medical SBT could allow an avatar to enter a metaverse clinic and immediately be recognised by the owner's real-world medical records. An SBT signifying the holder as a 2023 spring enrollee in a Philosophy 101 class at ACME university might gain the holder access to metaverse lectures and course materials. Real-world private clubs might issue SBTs to members allowing access to SBT-gated social spaces and events in the metaverse.

In addition to personal facts and history, SBTs can also serve to record and manage relationships between brands and their consumers. It is not a stretch to imagine a brand tokenising its loyalty programme and issuing SBT to customers based on both digital and real-world brand interactions. In fact, Binance has already launched an SBT called the Binance Account Bound (BAB) token. The BAB acts as an identity passport across the entire Binance network for those users who have satisfied KYC requirements. The token will also allow customers access to special projects as well as the accrual of benefits to holders who perform certain actions, giving Binance the ability to gamify customer experi-

ence and tie specific touchpoints and critical interactions to rewards.

Potential legal issues

Privacy is almost certain to become a central battleground as SBTs proliferate and evolve. On-chain identity passports containing drivers' licence numbers, medical information and the like will certainly be considered personally identifiable information (PII) under US privacy statutes, as well as personal data under the General Data Protection Regulation (Regulation (EU) 2016/679). A more nuanced review may be necessary to evaluate on-chain loyalty elements that integrate activities and data points that span across a brand's ecosystems. The matter is likely to be complicated as user wallets begin to collect SBTs from disparate sources that do not amount to PII individually, but may do so as an aggregate. Additionally, data breaches may not be a brand concern under the current vision for SBTs where data is stored in user-controlled wallets. However, if SBTs begin to be issued to user wallets custodied by a brand, breach protection will become a significant focus.

Terms of use will also need to be thoughtfully considered. Specifically, attention should be paid to SBT validation to ensure tokens are not obtained through fraud or mistake. Further, since SBTs are intended to be permanent (and given that people's minds may change about a certain affiliation throughout their lifetime), brands should provide for the means to hide tokens from public display, if so desired, or otherwise burn them. Representations should be clear around the risk factors relating to the nature of permanent tokens and the self-management of tokenised identity. Finally, in light of the potential for critical information and personal identity to be lost due to private key mismanagement or theft, thought should be given to SBT restoration

Contributed by: Tom K. Ara, James Williams, Katherine M. Imp and Mark Radcliffe, **DLA Piper LLP**

terms as well as the development of enforcement policies around tokens gained through illicit actions.

Conclusion

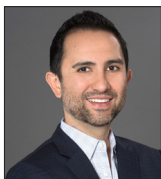
While a lifetime lived fully virtually may arise in the future, the nearer term will belong to more limited experiences as the metaverse technology evolves. As metaverse technology evolves it is likely to involve “blended worlds” which include both virtual and real-world experiences. As these “blended world” use cases continue to expand

in novel ways, so too are the legal complexities likely to multiply. Navigating these developments will require legal counsel to not only firmly grasp of the real world and virtual world legal issues as well as the manner in which the virtual world technology works so that legal counsel can synthesise these two regimes, creating issues of first impression. Counsel will need to be comfortable providing guidance in territories for which there are no maps (yet) and agile enough to anticipate issues as this nascent industry develops.

DLA Piper LLP has a highly regarded and highly ranked global media, sport and entertainment practice which advises studios, networks, financiers, investors, music publishers, record companies, production companies, video game companies, social media platforms and other stakeholders in the media and entertainment sector in all aspects of the development, financing, production and distribution of content of every type. The practice draws on the knowledge of teams throughout the firm for their experience in technology, blockchain, and digital currencies. Among its clients, the team

has represented ByteDance in its metaverse content creation initiatives for its PicoVR headset, L'Oreal and its launch of GORJS, a decentralised autonomous organisation (DAO) using blockchain to engage with customers, video game studio Smilegate in key strategic investments, Sensorium Galaxy in its in-world currency SENSO, numerous NFT platforms in content licensing deals, and many of the world's largest cryptocurrency exchanges. The firm has also developed its own digital asset creation engine, TOKO, which has been used for art auctions and online games.

Authors



Tom K. Ara is a partner at DLA Piper and co-leads its media, sport and entertainment practice. Recognised as one of the most influential business leaders shaping the global

media industry, he has led a multitude of cutting-edge transactions in media and entertainment, representing companies and industry participants of all types in complex corporate, financing and strategic industry transactions spanning the globe, from the Americas to Europe to the Middle East and Asia. He serves as advisory board member for the Blackhouse Foundation, trustee of the US-Asia Institute and is the chief editor of the Entertainment Law issue of Los Angeles Lawyer magazine.



James Williams is a partner has extensive experience navigating the intersection of corporate, securities and intellectual property law in Web3.0 and crypto content transactions. He

advises blockchain native companies on matters relating to venture financing, token generation events and airdrops, decentralised autonomous organisation (DAO) structuring and formation, protocol design and regulatory compliance with the SEC. James also routinely acts as legal and strategic advisor to many of world's well-known brands on crypto and blockchain integrations. He has represented numerous professional basketball, football and soccer teams on crypto naming rights deals, fan tokens, non-fungible tokens (NFTs) and Proof of Attendance protocols.

Contributed by: Tom K. Ara, James Williams, Katherine M. Imp and Mark Radcliffe, **DLA Piper LLP**



Katherine M. Imp is a senior associate in DLA Piper's transactional entertainment practice, with over ten years of experience representing production companies, studios

and other stakeholders in the entertainment sector in the development, production, distribution and exploitation of motion picture, television, podcast, commercial and new media content. Before joining DLA Piper, Kate gained extensive experience as production counsel for scripted and unscripted audio-visual content, negotiating agreements for over 150 different productions. She is a member of Women in Film Los Angeles and a frequent guest lecturer at the University of Southern California (USC), the University of California, Los Angeles (UCLA) and other colleges and universities in the Los Angeles area.



Mark Radcliffe is a partner in DLA Piper's Silicon Valley office. His practice is split between corporate law (particularly venture capital transactions) and intellectual property licensing

and strategy. He is well known for his work on cutting-edge legal issues from domain dispute resolution policies to open-source software licences. In 2019, the National Law Journal named him among its "Technology Trailblazers". His 20 years of experience with collaborative development in the open-source community have prepared him to work with blockchain projects. His clients range from Fortune 500 companies to unknown start-ups in a variety of industries.

DLA Piper LLP (US)

2000 Avenue of the Stars
Suite 400
North Tower
Los Angeles, CA
90067-4735
USA

Tel: +1 310 595 3000
Fax: +1 310 595 3300
Email: Tom.Ara@us.dlapiper.com
Web: www.dlapiper.com



CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com