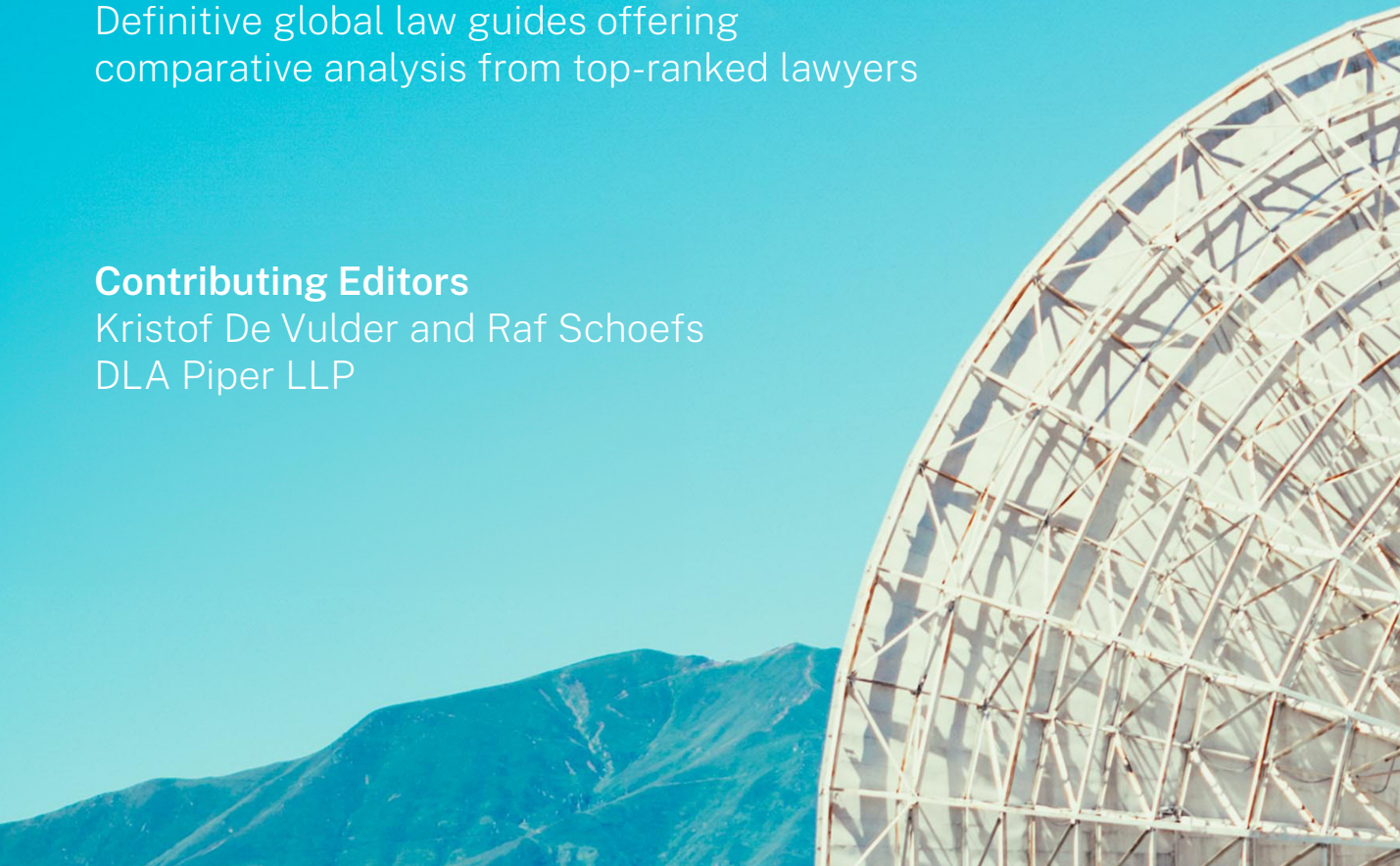

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2024

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

Contributing Editors

Kristof De Vulder and Raf Schoefs
DLA Piper LLP



Chambers

Global Practice Guides

TMT

Contributing Editors

Kristof De Vulder and Raf Schoefs

DLA Piper

2024

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, Sean Marshall, Marianne Page, Heather Palomino, Deborah Sinclair, Stephen Dinkeldein and Adrian Ciechacki

Content Coordination Manager Nancy Laidler

Senior Content Coordinator Carla Cagnina

Content Coordinator Hannah McDowell

Head of Production Jasper John

Production Coordinators Genevieve Sibayan, Pete Polanyk and Paul Cummings

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 © 2024

Chambers and Partners

CONTENTS

INTRODUCTION

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

AUSTRALIA

Trends and Developments p.10

Contributed by Webb Henderson

BELGIUM

Law and Practice p.18

Contributed by DLA Piper UK LLP

Trends and Developments p.37

Contributed by EDSON

BRAZIL

Law and Practice p.46

Contributed by Azevedo Sette Advogados

CANADA

Law and Practice p.62

Contributed by Fasken

CHINA

Law and Practice p.80

Contributed by DaHui Lawyers

Trends and Developments p.100

Contributed by DaHui Lawyers

EGYPT

Law and Practice p.107

Contributed by Shehata & Partners

FRANCE

Law and Practice p.135

Contributed by White & Case LLP

GREECE

Law and Practice p.154

Contributed by Nikolinakos & Partners

INDIA

Law and Practice p.178

Contributed by G&W Legal

INDONESIA

Law and Practice p.194

Contributed by ABNR Counsellors at Law

ITALY MEDIA

Trends and Developments p.211

Contributed by Amiconi Studio Legale

JAPAN

Law and Practice p.216

Contributed by Mori Hamada & Matsumoto

Trends and Developments p.231

Contributed by Nagashima Ohno & Tsunematsu

MACAU, SAR CHINA

Law and Practice p.240

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

MALAYSIA

Law and Practice p.254

Contributed by Skrine

Trends and Developments p.274

Contributed by Skrine

MEXICO

Law and Practice p.280

Contributed by Galicia Abogados

NETHERLANDS

Trends and Developments p.293

Contributed by Greenberg Traurig, LLP

NORWAY

Law and Practice p.303

Contributed by Advokatfirmaet Haavind AS

POLAND

Trends and Developments p.316

Contributed by Sołtysiński Kawecki & Szlęzak

PORTUGAL

Law and Practice p.326

Contributed by CS'Associados

CONTENTS

SINGAPORE

Law and Practice p.348

Contributed by Drew & Napier LLC

Trends and Developments p.367

Contributed by Rajah & Tann Singapore Ltd

SPAIN

Law and Practice p.376

Contributed by Asensi Abogados

Trends and Developments p.399

Contributed by Asensi Abogados

SWEDEN

Trends and Developments p.407

Contributed by Delphi

SWITZERLAND

Law and Practice p.415

Contributed by Lenz & Staehelin

USA

Law and Practice p.433

Contributed by Kelley Drye & Warren LLP

INTRODUCTION

Contributed by: Kristof De Vulder, Raf Schoefs and Laetitia Mouton, **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 13 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, Raf Schoefs and Laetitia Mouton, **DLA Piper**

Co-Author



Laetitia Mouton is a lead lawyer in DLA's intellectual property and technology team. Laetitia advises national and international companies on all aspects of information

technology law, with a particular focus on technology and outsourcing transactions, and has over 5 years of experience. She regularly drafts and negotiates complex IT and outsourcing agreements, taking into account the increasingly complex regulatory framework (e.g, DORA regulation, Digital Services Act etc).

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



INTRODUCTION

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

TMT 2024 Global Overview

While 2023 was undeniably the break-through year for artificial intelligence (and more specifically generative AI tools, such as ChatGPT), looking ahead into 2024, it is nearly certain that AI will continue to dominate conversations. In 2024 we also expect an increasing uptake in the deployment of 5G networks across many markets, as a consequence boosting the market for the internet of things (as IoT will benefit from high-speed connectivity), as well as leading to a further rise of cloud and edge computing deals. Many organisations will require more computing resources and more flexibility in this respect, which most will find with “hyperscalers”.

Alongside these technological advances, the world is grappling with ongoing challenges, including geopolitical tensions, environmental concerns, and economic uncertainties, all of which impact the TMT sector. In addition, cybersecurity remains a paramount concern for both businesses and policymakers, while regulatory focus intensifies on emerging technologies such as artificial intelligence, and scrutiny surrounding the digital economy and the market dominance of tech giants remains high on the agenda of lawmakers worldwide.

For those both within and outside the sector, staying abreast of major technological and legal developments can be challenging. This guide aims to offer valuable insights into the legal frameworks governing key aspects of the TMT sector. Acknowledging the dynamic nature of the TMT field, this Chambers TMT Guide focuses on being topic-driven rather than providing an exhaustive overview. Our aim is to address common questions that lawyers and in-house counsel frequently encounter 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. Apple has recently also entered the arena by launching a mixed reality headset.

No specific laws for the metaverse have been introduced yet, but it raises many questions relating to intellectual property, enforcement, privacy, and (cyber)security.

Digital economy

Until the adoption of the EU Digital Markets Act (DMA) and the EU Digital Services Act (DSA) in 2022, there were only limited rules for digital services. This led to the introduction of a whole range of soft law instruments and legal uncertainty. The DSA became applicable on 17 February 2024 and as of 7 March 2024 the companies designated as “gatekeepers” will have to comply with the DMA. It remains to be seen how these instruments will be implemented in the EU member states over the next year and how significant the impact on the TMT sector will be.

Cloud and edge computing

In today’s interconnected world, the concept of “cloud” permeates every aspect of our daily lives, from entertainment and finance to communication and commerce. This pervasive integration brings forth a delicate balance between

INTRODUCTION

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

accessibility and control, with licensing models often superseding traditional notions of ownership. Organisations may have more flexibility and more easy access to computing resources but will at the same time be confronted with an increased level of dependency on their service providers and additional business continuity and security risks.

This shift towards cloud and edge computing introduces myriad legal considerations, from sector-specific regulations to data protection and liability concerns.

Artificial intelligence

The rise of artificial intelligence continues to reshape industries and societies, with innovations such as ChatGPT pushing the boundaries of what machines can achieve. However, this rapid advancement brings complex legal and societal challenges with it, including questions of liability, data protection, intellectual property, and fundamental rights. As businesses harness the power of AI, navigating the legal landscape (including the new European AI Act) becomes paramount to ensure responsible and ethical deployment of these technologies.

Internet of things (IoT)

IoT is a small acronym for something so large. The internet of things (IoT) expands its reach into every aspect of our lives, from smart homes to connected vehicles and industrial sensors. However, this proliferation of connected devices also introduces new security risks and legal considerations. As hackers target vulnerable IoT devices, the need for robust cybersecurity measures becomes increasingly urgent. Legal frameworks must adapt to address challenges such as data protection, communications security, and regulatory compliance in this rapidly evolving landscape.

Audio-visual media services

The digital transformation has democratised content creation, allowing organisations of all sizes to establish digital communications channels. However, this proliferation of online content triggers regulatory considerations, particularly regarding audio-visual media services. Understanding the applicability of regulations to online video channels and user-generated content is essential for compliance and risk management in this evolving legal landscape.

Telecommunications

Telecommunications regulations have evolved to encompass new technologies and communication methods, from voice-over IP (VoIP) to instant messaging and 5G networks. Compliance with regulatory frameworks is essential for organisations delivering electronic communication services, ensuring adherence to obligations related to network security, privacy, and consumer protection. As technology continues to advance, staying abreast of regulatory developments remains crucial for successful and compliant service provision.

Challenges with technology agreements

Navigating technology agreements in a global economy requires careful consideration of specific requirements and restrictions. From data localisation requirements to price-revision mechanisms, understanding the applicable legal frameworks is essential when selecting technology providers and negotiating contracts. By staying informed and proactive, organisations can mitigate risks and maximise opportunities in their technology agreements.

Trust services and digital identity

As online transactions become increasingly prevalent, trust services and digital identity schemes play a critical role in authentication and

INTRODUCTION

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

identification. Understanding the legal framework surrounding these technologies is essential to ensuring secure transactions. By staying informed about applicable regulations and best practices, organisations can navigate the evolving landscape of trust services and digital identity with confidence.

AUSTRALIA

Trends and Developments

Contributed by:

Ish Omar, Ara Margossian, Angus Henderson and Jordan Cox

Webb Henderson



Webb Henderson is a specialist firm with offices in Australia and New Zealand, regularly advising across the Asia-Pacific, Middle East and beyond. Its areas of expertise are TMT, competition and regulation, disputes, and corporate and finance. The firm has more than 50 lawyers, who are known for combining deep industry knowledge and legal expertise with experience gained from market-leading assignments. The TMT team is among the region's largest specialist digital teams, and assists TMT companies, digital infrastructure investors, gov-

ernments and regulators on their most important corporate, commercial and regulatory projects. Recent highlights include advising NBN Co in Australia on its ground-breaking 30-year Special Access Undertaking and on its Wholesale Broadband Agreement; advising a leading hyperscaler on a range of global subsea cable projects, acting for Spark NZ on its NZD900 million tower sale, build and leaseback deal with Ontario Teachers' Pension Plan; and advising Starlink on Australian and New Zealand regulatory and commercial matters.

Authors



Ish Omar is a partner in Webb Henderson's TMT practice and works at the intersection of law and digital transformation. He assists leading telecoms operators to structure, purchase

and supply digital infrastructure access services. He is a lead external adviser to NBN Co and Spark NZ, assisting on their key projects for over a decade. Ish has also advised on regulatory, commercial and corporate projects for telecoms operators, digital infrastructure investors and regulators across South-East Asia, the Middle East and North America, assisting with digital transformation, industry shifts and regulatory reform in a variety of economies.



Ara Margossian is one of the region's leading practitioners in the TMT sectors, with extensive experience in advising clients on strategic corporate, commercial and regulatory projects. He has

been involved in some of the most high-profile TMT transactions in Australia, the Asia-Pacific and the Middle East, including projects on wireless technologies, fibre networks, undersea cables, structural separation, MVNOs, network sharing and interconnection, as well as competition law and regulatory clearance matters. Ara's current practice focuses on corporate and commercial transactions supporting the delivery of large-scale infrastructure projects, including next generation access networks, intercity and long-haul terrestrial networks, undersea cable systems and next generation satellite systems.

AUSTRALIA TRENDS AND DEVELOPMENTS

Contributed by: Ish Omar, Ara Margossian, Angus Henderson and Jordan Cox, **Webb Henderson**



Angus Henderson is the co-founding partner of Webb Henderson and has over 30 years' experience in communications regulatory, wholesale and commercial transactions in Australia, the Asia-Pacific, Middle East and beyond. He has worked for leading operators on some of the largest telecoms, pay-TV and broadband deals. Working extensively on prominent fibre-related projects in Australia, Singapore and Malaysia, he has particular expertise in developing and implementing regulatory frameworks that support those investments. Angus also acts for international telecoms and digital infrastructure companies rolling out satellite, 5G and global connectivity services. He is a leading individual in Chambers Asia-Pacific 2024 (Band 1).



Jordan Cox is a specialist TMT partner at Webb Henderson. His expertise spans a wide range of commercial and regulatory matters, including the development and supply of wholesale next generation access networks; digital infrastructure; and the design, operation and reform of telecommunications regulatory frameworks. He advises TMT clients and others in these areas across New Zealand, Australia, Asia and the Pacific Islands. Jordan also advises regularly on competition law matters, and works closely with Webb Henderson's corporate and finance group to advise on New Zealand competition law aspects of mergers and acquisitions.

Webb Henderson

Level 18
420 George St
Sydney NSW 2000
Australia

Tel: +61 2 8214 3500
Email: enquiries@webbhenderson.com
Web: www.webbhenderson.com

**webb
henderson**
LEGAL AND REGULATORY ADVISORS

TMT in Australia: An Introduction

Three trends are shaping Australia's digital landscape more than any others:

- the adoption and emerging regulation of AI;
- the continued expansion of large-scale digital infrastructure investments; and
- industry shifts from the entry of LEOSat networks.

AI adoption and regulation

Australians are enthusiastic early adopters of technology, and AI is no exception. Businesses and governments are racing to deploy and experiment with the latest AI tools (primarily generative AI). At the same time, executives have been wary of making decisions that embed path dependencies that might cause problems under future regulation. So the Australian government's AI regulatory announcement in January 2024 brought some welcome clarity. It not only provides a degree of certainty, but it also seems measured, helping decision makers to push forward with their AI ambitions.

The January announcement was an interim response to the Australian Department of Industry's discussion paper six months earlier, on Safe and Responsible AI in Australia.

In contrast to the forthcoming EU AI Act, the Australian government is not proposing sweeping legislation that addresses AI as a singular topic across many domains. It is also not seeking to set up a comprehensive scheme to categorise every use of AI into a pyramid of risk levels from low-risk through unacceptable risk.

Instead, the Australian government is proposing more targeted legislation – building on existing laws that already regulate high-risk settings or introducing new domain-specific laws, to ensure

they address the new dimensions of risk introduced by the deployment of AI. It is a proportionate approach that has several strengths to recommend it, as follows.

- By regulating only those areas where there is an identified risk, it limits regulation to domains where there is a proven need, allowing a great degree of freedoms to explore in other areas. With AI at a nascent stage and its upside potential not yet apparent, putting the brakes on innovation would be a terrible missed opportunity. Google, Amazon, PayPal, Uber and Canva might not have succeeded against powerful industry incumbents if their opportunities to innovate had been harshly curtailed by well-meaning but too-early legislation.
- Regulating high-risk areas without banning the use of AI outright will allow responsible actors to innovate in a socially sanctioned and transparent manner. The alternative in a global market would be Australians vacating the field or becoming ever-less competitive against their international peers. This has already happened in the media space, with increasingly convoluted regulatory frameworks being introduced to prop up flailing Australian companies.
- By adopting a domain-specific approach, risks can be regulated in a technology-neutral way. For example, the EU AI Act proposes to ban AI practices used by public authorities for social scoring. While there may be widespread consensus that social scoring is unacceptable, it is unclear why the practice would only be banned when AI is involved.
- Domain-specific regulation should also help minimise or avoid red tape from regulatory overlap. This has been a recent issue with overlaps between telco-specific network

security legislation and economy-wide security of critical infrastructure legislation.

- Finally, embedding AI-driven rules in domain-specific regulation should help domain experts to quickly integrate the new rules into their existing risk and compliance frameworks, and to shape the new rules to be responsive to industry and process-specific considerations in their domain.

Of course, these benefits could be diluted or lost through poor implementation. Much remains unknown.

An initial list of high-risk settings in which AI might be regulated includes:

- recidivism prediction in law enforcement;
- employment applications;
- self-driving vehicles; and
- robotic surgery.

This list is from the government's announcement, which notes that other areas might also be considered high-risk. The final list of areas for regulatory action is as yet unknown; even when more information is available, it is reasonable to expect that new areas will be added over time, as new risks are identified.

When specific AI-driven regulation is ultimately introduced, the government has flagged that it will likely take the following forms.

- Frontier model-specific regulation, entailing specific obligations on cutting-edge AI systems development, deployment and use. This is likely to affect only large hi-tech companies and a small number of educational and government agencies specialising in the field.

- Testing obligations, requiring testing before and after deployment, to ensure AI systems in high-risk settings operate as intended.
- Transparency obligations, requiring a range of measures, such as notices to advise users that they are engaging with AI systems in high-risk settings and labelling of AI-generated content in high-risk settings.
- Accountability obligations, requiring safety officers (much like privacy officers) and training for employees of organisations that develop or deploy AI systems in high-risk settings.

The government has flagged further consultation and expert agency work to develop various guidance tools to assist businesses and government agencies with safe deployment. It has also noted that it continues to consider the impacts of AI in its ongoing "business as usual" legislative reform agenda, citing ongoing updates to the Online Safety Act and privacy laws.

For now, most decision makers can continue to experiment with AI and adopt it within their businesses, applying usual best practice risk management frameworks and adopting a few key principles, as follows.

- Develop and document rigorous testing of AI deployments, and ensure testing is ongoing or regular, much like business continuity testing. This may require external validation.
- Label the use and outputs of AI, both within organisations and externally. This need not be onerous – the ChatGPT interface simply says "ChatGPT can make mistakes. Consider checking important information". If external stakeholders like customers are likely to be unhappy with outputs directly from an AI system (eg, automated loan decisions), this is an indication that:

- (a) it may be an inappropriate or premature use of AI;
 - (b) it should be intermediated by an employee who understands the limitations of the system, can explain outcomes where they are right and is empowered to overturn it if wrong; or
 - (c) more detailed disclosures and paths for redress are needed where the external stakeholder is unhappy with the interactions or outputs.
- Take a nuanced and incremental approach to AI deployment. Conceptually, replacing a step in a process is easier and more likely to succeed than replacing the whole process. An incremental approach like this also maximises experimentation and minimises path dependencies. It is easier to swap out vendors or re-architect processes without business disruption.
 - Develop in-house expertise to help understand the opportunities and risks of AI tools in the context of the organisation's specific goals, internal responsibilities for achieving those goals, and internal responsibilities for assessing and managing risk for specific AI deployments in the context of surrounding business processes and interactions. Allocate a specific person on project and management teams to be responsible for the safe deployment of each AI system, and ensure they have proper training.
- interaction and output oversight and training (noting that embarrassing or illegal acts or statements are no less damaging whether made by an employee or an AI tool);
 - privacy and data security;
 - data sovereignty, control and availability (especially where compute loads and storage are offshore or in cloud environments controlled by third parties); and
 - the security of critical infrastructure (including "safety brakes" but also fall-back systems and processes that can be invoked if automation fails).

These approaches can be augmented, particularly in high-risk settings, as further regulation and best practice guidelines are developed over the coming year. The government has not announced specific consultation or legislation timelines.

Digital infrastructure investment expansion

The second of the three most defining trends in the Australian digital landscape is continued and expanded investment in digital infrastructure. Current focuses are submarine and terrestrial backbone cables and data centres, together with their attendant power infrastructure needs. These infrastructure types are seeing a dynamic landscape of investors including hyper-scalers, superannuation and pension funds, and investment banks.

Risk management frameworks applied to AI deployment should take the following into account:

- design-making oversight (noting that directors and officers must ultimately be able to understand and agree with decisions made by, or on behalf of, an organisation);

In parallel, traditional network operators continue to do the hard work of driving fibre ever-deeper into fixed and mobile access networks, and a small number of global players are building out LEOSat networks (which are discussed below). This traditional telco activity continues to be dynamic, with continued competition, new technologies, kaleidoscopic network alliances and active government reviews of universal

service funding models (discussed below, with LEOSats). However, at a macro level, investors and key players in the access network are reasonably stable.

By contrast, new investors and investment structures are continuing to evolve to fund submarine and terrestrial backbone cables and data centres. There are a few key reasons for this investment dynamism.

- Demand for this infrastructure continues to materially outstrip supply, offering investors good returns. AI is just one of the many technologies requiring ever-increasing data centre capacity. Others include the now mature but not-yet-finished migration of business computing off premises and into the cloud, and the increasing number and size of pipes required for the latest high definition gaming and video entertainment.
- The immense demand means that active participation from the largest incumbents does not preclude the entry or expansion of other sector participants. This creates opportunities for investors with different size investment appetites to participate in a variety of differently sized projects and in independent operators hungry for new sources of investment.
- New investment activity is required by geographic constraints. This includes the partial or complete saturation of existing connectivity hubs like Singapore and heightened geopolitical risks – both of which seem set to drive new digital infrastructure investments towards Australia (and New Zealand), amongst other relatively stable and safe investment jurisdictions.
- As these new opportunities drive the need for investment, large suppliers of data centre inputs, like original equipment manufacturers

(OEM), are increasingly seeking to move up the stack and manage ever-higher layers of the compute and storage stack on behalf of their data centre customers (much as mature TowerCos are seeking to manage more of the actives and power on behalf of telco customers). The scale of these suppliers and their financing capabilities can help those data centre operators that do not have vertically integrated hardware manufacturing capabilities compete with vertically integrated players like hyper-scalers. Whether these OEMs can keep up with the demand for cutting-edge chips is yet to be seen. Bans adopted by the US, Japan and the Netherlands on exporting key chip and chip-making equipment to China may help cutting-edge manufacturers like TSMC dedicate demand to OEMs seeking to serve mid-tier markets like Australia faster than would otherwise be the case, but time will tell.

Investors in these infrastructure types are sophisticated. They do not approach their investments as standalone projects, but rather as elements in a rapidly maturing and integrated ecosystem. Submarine cable companies are fusing cable landing stations with data centre capabilities. Data centre operators are seeking to build in proximity to existing and planned backbones and inter-city networks, and to secure backbone network operators as anchor tenants for their builds.

It is not uncommon to see large segments of a data centre dedicated to terminating infrastructure for a major cable system. This, in turn, makes it easier to secure tenancies from other operators seeking to interconnect with the major cable system. And this then needs to be enabled by power and cooling, both of which are increasingly difficult problems to solve.

Power is difficult because existing energy generators and grids are already saturated. Expanding them is not easy – the shift to green generation, the incorporation of batteries and distributed generation are all sapping the focus and balance sheets of energy companies. Added to these supply-side challenges are increasing demand-side challenges. AI workloads can typically require six times as much energy as traditional workloads.

This is leading data centre builders to increasingly build their own generation capacity, often co-located with the data centre itself. Where conditions permit, it is not unusual to have the same amount of land dedicated to energy generation as to the data centre to which the energy is being supplied. The green demands of the largest data centre customers often mean this new generation capability is usually renewable, including solar, wind and hydro energy. All of this, of course, increases the size of the investment and the opportunities for investors.

Many of the same trends are making cooling more difficult. Higher energy use for AI workloads means more heat, and this is exacerbated by AI systems benefitting from being closer together, leaving less room for passive cooling. Chilled water, water and air conditioning systems, captured heat transfer and co-location with water treatment plants are all solutions being adopted where possible.

Despite these challenges, the demand for more data centre capacity in Australia and submarine cables using Australia as both a hub and a way-point seems set to continue. Continued innovation is expected in response to these demand factors. This points to vibrant opportunities for investors and suppliers alike.

LEOSats

As with AI and digital infrastructure investment, LEOSats are not an Australian phenomenon nor even being pioneered in Australia, but they do have a special relevance to the world's only island continent. Australia has a similar population to Syria, but to get from one end of Australia to the other you could cross from Syria's capital, Damascus, to London.

Communication across this sparsely populated place has always been a problem, made harder by a deeply rooted Australian insistence on striving for near-total equity between the city and the bush. In 2009, the Australian government established the National Broadband Network Company (NBN Co), with a mandate to serve 100% of homes and businesses in Australia with broadband over fibre, fixed wireless and satellite technologies and offer "postage stamp" pricing – at a wholesale level, a broadband connection would cost the same in the most far-flung islands off the Australian coast (including the Cocos Islands, over 2,000 km from the mainland) as in the centre of Australia's biggest cities. This implied a massive cross-subsidy from the city to the bush. The average cost to serve a premises in the city was initially estimated to be ~AUD2,500 (with a full fibre connection capable of delivering 1 Gbps), whereas the average cost to serve a premises in remote areas was estimated to be closer to ~AUD45,000 (with a connection capable of closer to 100 Mbps).

The advent of LEOSat networks has almost inverted the cost calculations. The latest satellite connections still cannot compete with the capacity or speed of fixed line connections. Crucially, however, the networks are global by their nature, so they are built to serve the population of Europe (~600 million people) and, almost as a by-product of the technology, a large portion of that capac-

ity is available over the Pacific (46 million people total, 26 million in Australia). This implies that the cost per Gbps for Australians to access latent capacity in the network is likely to plummet as competition between LEOSat providers develops in the latter half of this decade. NBN Co's current satellite network is expected to come to the end of its useful life over the same time horizon.

This gives the government an unprecedented opportunity to achieve century-old universal service ambitions. In late 2023, it announced a sweeping review of universal service arrangements, with consultations closing in March 2024. There are parallel processes for refining the statutory infrastructure provider of last resort arrangements, a triennial regional telecommunications review and work being progressed by a First Nations Digital Inclusion Advisory Group. State and territory governments are also progressing trials of LEOSats and other technologies to fulfil public safety, emergency service and service delivery functions.

It seems all but inevitable that LEOSats will play a key role in digital inclusion for remote communities, particularly remote indigenous communities that continue to suffer shocking disparities in education, health and employment outcomes compared to the broader Australian community. They will also help in responding to the natural disasters that have become ever-more frequent. The police force in Western Australia has already incorporated LEOSats into its communications network, which covers a state that on its own is the size of all Western Europe.

The economics of these networks will mean that government funding for such services may change radically from the traditional models in Australia, which were developed to work with very different economic realities. Funding no

longer has to assume a single loss-making network that needs to be a heavily regulated bottleneck that is built through public funding and subject to massive ongoing cross-subsidies. With the re-balancing of the relationship to give the provider a more equal voice, it would be natural to see LEOSat providers pushing for greater regulatory harmony with the main jurisdictions in which they operate – at least for operational matters like law enforcement and security agency engagement.

Beyond the realm of government-subsidised universal services and public engagement, the same revolutionary economics also create opportunities for LEOSats. Agriculture uses an incredible 55% of the Australian landmass and is highly mechanised, and mining, which often takes place in remote areas, accounts for 14–15% of Australia's GDP. Both are likely to be eager users of LEOSats, and any material gains may flow through to the wider Australian economy, leading to a generally more prosperous Australia. This too may create opportunities for regulatory streamlining and refinement in favour of LEOSat operators in areas like spectrum management and planning rules for the deployment of VSATs and other terrestrial support infrastructure.

Conclusion

The trends shaping Australia's digital landscape are not unique: AI, digital infrastructure investment (particularly in submarine and terrestrial backbone networks, and in data centres) and the advent of LEOSat networks are amongst the most important technological trends worldwide. Harnessing these developments successfully in Australia's unique geography and economy requires a keen understanding of the nuances and implications of the technology and familiarity with the rapidly evolving commercial and regulatory landscape.

BELGIUM

Law and Practice

Contributed by:

Kristof De Vulder, Raf Schoefs and Laetitia Mouton
DLA Piper UK LLP



Contents

1. Metaverse p.21

1.1 Laws and Regulation p.21

2. Digital Economy p.22

2.1 Key Challenges p.22

3. Cloud and Edge Computing p.22

3.1 Highly Regulated Industries and Data Protection p.22

4. Artificial Intelligence p.25

4.1 Liability, Data Protection, IP and Fundamental Rights p.25

5. Internet of Things p.27

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.27

6. Audio-Visual Media Services p.29

6.1 Requirements and Authorisation Procedures p.29

7. Telecommunications p.31

7.1 Scope of Regulation and Pre-marketing Requirements p.31

8. Challenges with Technology Agreements p.31

8.1 Legal Framework Challenges p.31

9. Trust Services and Digital Entities p.34

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.34

DLA Piper UK LLP has a global intellectual property and technology (IPT) group consisting of 60+ offices, around 150 partners and 530+ 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 the firm'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 13 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.



Laetitia Mouton is a lead lawyer in DLA Piper's intellectual property and technology team. Laetitia advises national and international companies on all aspects of information

technology law, with a particular focus on technology and outsourcing transactions, and has over five years of experience. She regularly drafts and negotiates complex IT and outsourcing agreements, taking into account the increasingly complex regulatory framework (eg, DORA regulation, and the Digital Services Act).

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



1. Metaverse

1.1 Laws and Regulation

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.

A term often mentioned alongside the metaverse due to its correlation is “Web3”. The latter has to be seen as the concept of a new, decentralised internet constructed on blockchains or distributed ledgers collectively managed by participants. Although the metaverse and Web3 are different concepts, Web3 technologies can enhance the metaverse experience.

Laws and Regulations

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

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

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, impacting Book XII, are however to be expected, given the entry into force of the EU Digital Markets Act (DMA) (Regulation 2022/1925) and the EU Digital Services Act (DSA) (Regulation 2022/2065), respectively on 1 November and 16 November 2022.

The DSA establishes a new standard for the accountability of online platforms regarding illegal and harmful content, which is to be transposed in national law. In addition, it includes provisions – which are already operational – related to the transparency obligations of online platforms and the identification of very large online platforms (VLOPs) and very large online search engines (VLOSEs).

Essential for the transposition of this regime into Belgian law is the implementation of three key measures. Firstly, the draft federal law must be introduced to enact the DSA, assigning duties to the Belgian Institute for Postal Services and Telecommunications (BIPT/IBPT) – acting as both the federal competent authority and the Digital Services Co-ordinator – regarding the oversight of DSA-provisions falling under federal jurisdiction. Concurrently, decrees at the level of the federated entities are necessary to appoint their respective competent authorities responsible for supervising provisions within their jurisdictional purview. Additionally, fostering collaboration between the federal government and communities is imperative. This collaboration would involve establishing a comprehensive

agreement delineating various aspects such as the designation of the BIPT as the DSC, clarification of roles for competent supervisory authorities and the DSC, formulation of frameworks for co-operation and information exchange among competent authorities concerning the DSA, and arrangements for Belgium's representation within the broader European digital services sphere.

The DMA, in turn, targets online platforms which qualify as “gatekeepers” and therefore create a bottleneck in the digital economy, and is applicable as from 2 May 2023.

The designation of the first organisations as “gatekeepers” by the European Commission happened in September 2023. Regulating these platforms will enhance competition and create a fairer business environment for businesses who depend on gatekeepers.

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 (eg, consumer laws, and specific laws for certain kinds of contracts). 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 of 2016 on Security of Network and Information Systems (the “NIS-1 Directive”)

(Directive 2016/1148) 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-1 Directive – ie, the requirement to adopt appropriate security measures.

This NIS-1 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, following which in 2022 a new Directive on measures for high common level of cybersecurity across the Union (the “NIS-2 Directive”) (Directive 2022/2555), and a new Directive on the resilience of critical entities have been adopted. Time-wise, the Belgian government has until 17 October 2024 to transpose both directives into national legislation and to adopt and publish all measures necessary for compliance.

The Belgian authorities, specifically the Centre for Cybersecurity Belgium (CCB), are keen on expediting the publication of the Belgian law for the transposition of the NIS-2 Directive, aiming to provide clarity to relevant entities well before that deadline. The Belgian Council of Ministers has already prepared a proposal for an implementing act and accompanying implementation decree, which are still to go through the entire legislation formation process.

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 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”) (EBA Guidelines 2019/02) 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.

As of 16 January 2023, the first major EU-wide legislation treating digital resilience entered into force, being the Digital Operations Resilience Act for the Financial sector (DORA) (Regulation 2022/2554). Its purpose is to establish uniform standards for ICT risk mitigation across all EU financial entities, more particular establishing a framework for ICT risk management, incident reporting, operational resilience testing and third-party ICT risk monitoring.

DORA goes beyond the scope of the previously mentioned EBA Guidelines (which it will replace), addressing both personnel and material aspects, and is designed to ensure digital operational resilience throughout the entire financial ecosystem. Consequently, a broader range of financial entities as well as ICT service providers (including cloud service providers) will need to adhere to the DORA conditions.

Furthermore, DORA sets forth requirements that emphasise the establishment of strategies,

frameworks, and governing processes essential for achieving digital operational resilience.

Processing of Personal Data

The General Data Protection Regulation (the GDPR) (Regulation 2016/679) 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 – as mentioned further below).

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, and 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.

According to the GDPR, the transfer of data subject to data protection outside the European Union must not compromise the level of protection guaranteed by the GDPR for natural persons. Data transfers to a third country or international organisation are permissible when the European Commission determines that the third country, specific sectors within that country, or the international organisation ensures an adequate level of protection.

A list of countries with such adequacy decisions is available. On 10 July 2023, the European Commission approved a new adequacy

decision for the United States, known as the “EU–US Data Privacy Framework”, in the wake of the Schrems-decisions taken by the CJEU in the past. The new framework aims to facilitate data export to organisations on the “*Data Privacy Framework List*” without the need for transfer instruments outlined in Article 46 of the GDPR. Data controllers transferring personal data to organisations not on the list must still use necessary transfer instruments, as stipulated in the GDPR, to ensure an appropriate level of protection, such as model contract clauses or binding corporate rules (EDPB recommendations 01/2020).

Additionally, the decision outlines remedies available to individuals whose data is transferred to the United States under the adequacy decision, should they believe the involved organisation in the US is not adhering to the Data Privacy Framework. This adequacy decision follows the invalidation of two previous decisions, Safe Harbour and Privacy Shield, by the Court of Justice of the European Union in the “Schrems I” and “Schrems II” rulings.

For Belgian businesses and organisations involved in cross-border data exchanges with the United States, this framework streamlines the process of transferring personal data without the need for additional safeguards such as Standard Contractual Clauses or Binding Corporate Rules. This simplification can lead to increased efficiency and reduced administrative burdens for Belgian companies engaging in international collaborations, data sharing, or utilising cloud services hosted in the United States.

Additionally, Belgian individuals benefit from enhanced privacy protections when their data is transferred to the United States under the EU–US Data Privacy Framework. They have specific

legal remedies available if they believe that a US-based organisation is not complying with the provisions of the Data Privacy Framework, providing an added layer of security and control over their personal information.

Another privacy-related topic can be found in the fact that in cloud computing situations, where cloud service providers come into play, the obligation to notify data breaches to both data subjects and data protection authorities typically requires more extensive involvement of the provider than in the case of merely local IT solutions, given the typically greater reliance on the former.

In cloud computing contracts, other aspects have to be carefully planned, such as the question of return or destruction of personal data, and the question of liability of the provider. In this respect, during the month of July 2023, the working group on Switching Cloud Providers and Porting Data (SWIPO) presented its Converged Code of Conduct for cloud services. Since the Data Act is in force as of January 2024, SWIPO plans to update its third Code of Conduct to address the necessary requirements set forth in the Data Act and help ensure compliance with the anticipated provisions relating to porting and switching between data processing services. Once amended, SWIPO anticipates that the Code will be eligible to be listed in the “Cloud Rule Book” as a Data Act implementation tool.

4. Artificial Intelligence

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

Artificial intelligence 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 8 December 2023, the European Parliament and the Council reached a provisional political agreement on the key points of the regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the “Artificial Intelligence Act”). The draft Artificial Intelligence Act contains a tiering of regulatory 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 a risk management system, complete and up-to-date technical documentation, designed to allow for effective human oversight and to ensure an appropriate level of accuracy, robustness and security. Different obligations will apply depending on the role of a party in the AI system’s supply chain, including requirements

applicable to providers as well as to deployers (ie, the users) of the AI system.

The question whether foundation models and/or general purpose AI systems need to be specifically regulated was a major point of discussion in the trilogue negotiations. The Commission's proposal of April 2021 did not include specific rules for foundation models or general purpose AI systems. However, with the notable market entry of several powerful general purpose AI systems since the initial proposal was published, these discussions became highly relevant. The draft Artificial Intelligence Act now contains dedicated obligations for "general purpose AI models" which are stricter depending on whether such models are considered to present "systemic risk".

After formal adoption and official publication of the draft Artificial Intelligence Act, this Regulation is expected to enter into force in the first half of 2024, following which it will gradually enter into application. All prohibited systems will need to be phased out within six months. The majority of the other requirements will then become applicable 24 months after the entry into force.

Additionally, the Commission has published a proposal for an Artificial Intelligence Liability Directive (AILD) on 28 September 2022. The proposed 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 sys-

tem 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 person) 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 infrastructure, 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) (Directive 2002/58), 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 provide for confidentiality of communications, including M2M-interactions, potentially affecting how certain organisations currently use IoT devices.

In 2023, the approval of the ePrivacy Regulation was still not realised, giving rise to uncertainties regarding the future of this proposal.

Interoperability

In the past, many companies developed IoT services or devices with their own independent infrastructure. With the increasing prevalence of IoT devices and services, the issue of interoperability – ie, ensuring seamless communication between devices, networks, and platforms – will naturally come to the forefront. A concrete (and quite literal) example of addressing this need is the introduction of a universal charger for mobile devices, expected to be implemented in 2024. Under these new regulations, consumers will not require a different charger each time they purchase a new device. Instead, they can use a single charger for a variety of small and medium-sized portable electronic devices. This common charger aims to enhance convenience by standardising charging interfaces and fast charging technology, ultimately even leading to a significant reduction in electronic waste.

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 a directive concerning audiovisual media services (the “AVMS Directive”) (Directive 2018/1808). and a directive on copyright and related rights in the Digital Single Market (the “DSM Directive”) (Directive 2019/790) 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.

The DSM Directive has been transposed in Belgium by a federal Act, changing the Belgian Code of Economic Law with a wide range of relevant topics.

In conclusion, the Belgian legal framework is composed of two federal acts, 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.
- Online content-sharing service providers must obtain authorisation from right-holders for the public access to copyrighted works uploaded by users. They are also obligated to ensure appropriate remuneration for authors and performers.

Linear providers (eg, TV and 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

The scope of the AVMS Directive includes video-sharing platforms, whereby this concept 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, ie, services with editorial control.

They must however take appropriate measures:

- to protect minors from harmful content which may impair physical, mental or moral development – eg, through age verification systems, 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;
- 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 (eg, identification principle, sponsorship, and product placement).

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The Belgian telecommunication rules, mainly found in the Belgian Act on Electronic Communications, are heavily influenced by EU rules. This has become even more the case since the adoption of the European Electronic Communications Code (the EECC) (Directive 2018/1972), and will be even more so once the EU adopts the long-awaited ePrivacy Regulation. Regarding the latter, however, it remains to be seen if, when and which form it would adopted.

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 the Open Internet Regulation (Regulation 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 services 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 (BIPT/IBPT) 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

The Belgian B2B 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;
- the legal recognition of the hardship doctrine;
- 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 XII 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 (i–iv) that is (v) created by a qualified electronic signature creation device, and (vi) 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 the 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 legal conditions 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”.

Digital Identity Schemes

While the eIDAS Regulation was ground-breaking at the time, the Regulation also included important gaps and is generally considered not to have been fully exploited in its potential.

Following a review, the European Commission drafted a proposal regarding the framework for a European Digital Identity, which would amend the EU eIDAS Regulation. This framework would introduce the “digital wallet”, which may be provided by public authorities or by private entities recognised by a member state, and which will link a citizen’s national digital identity to other personal attributes (eg, driving licence or bank account). This new framework is expected to provide a major increase of legal security and opportunities for the use of public and private online services within the EU – including in relation to electronic signatures. However, it remains to be seen how much of the proposal will have been amended once it reaches its final form as the draft was rather ambitious.

Trends and Developments

Contributed by:

Christoph De Preter and Pieter Paepe

EDSON.

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 telecommunications, media and technology industries and assists online ticketing platforms, streaming platforms, video game publishers and develop-

ers, print publishers, 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 games sector federation (IFSE). He also has expertise in IT contracts with defence and government organisations.



Pieter Paepe is an attorney at law at the Brussels Bar and a partner at EDSON., where he focuses on Belgian and EU business law, competition law and regulatory matters. Pieter

assists numerous clients with Belgian gaming law. He also advises and represents gaming clients in competition and state aid matters. In addition, Pieter has a broad commercial and competition litigation practice. He has appeared in proceedings before the Belgian courts and the Belgian Competition Authority, as well as before the EC. He has handled several cases before the ECJ, including on the Belgian government's behalf. He has helped Belgium to create ground-breaking precedents before the ECJ.

EDSON.

Lakensestraat 88
rue de Laeken
1000 Brussels
Belgium

Tel: +32 478 36 82 36
Email: christoph.de.preter@EDSON.legal.eu
Web: www.EDSON.legal.eu

EDSON.

Introduction

Governmental structure

As was the case prior to 2024, 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. With regard to video games, Larian Studios stands out as a key player, having created the very much acclaimed and almost unanimously voted game of the year for 2023, Baldur's Gate 3.

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, and an automatic wage indexation

system has brought about considerable wage increases in 2023. However, 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. Also, an increasing number of young tech professionals work as self-employed consultants.

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.

Stimulating growth with the Innovation Income Deduction

Belgium fosters an innovative environment coupled with a compelling fiscal incentive for businesses through the so-called Innovation Income

Deduction. This allows companies to deduct up to 85% of their net innovation income (ie, income derived from intellectual property (IP)) from the taxable base, resulting in a corporate taxation as low as 3.75%. This trend supports a forward-thinking strategy by boosting Belgium's competitiveness in the global innovation area with IP-rich companies.

New Opportunities in Government-Backed Digitalisation 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, obtain 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 2024 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 2024, a rise is forecast in automated negotiation and termination solutions that build on the existing e-authentication infrastructure. A notable trend is the strategic acquisition and collaboration of advanced authentication firms by identity platforms. This emphasises the need to focus on enhancing security through advanced multi-factor authentication systems, as demonstrated with the acquisition of "nextAuth" by itsme". The need for growing safe e-identification techniques is continuous, especially in government programmes, showcasing that it is

important to have strong cybersecurity plans in the digital sphere.

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

Historically, Belgium has a strong score on very high-capacity networks (VHCNs) 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) roll-out is among the lowest in Europe, with incumbent operators now making efforts to catch up. A VHCN-map (see [here](#)) can be consulted on the regulator's website. 5G roll-out in Belgium is steadily increasing – even in Brussels, which used to be a historic pain point.

A significant change in Belgium's telecommunications landscape is anticipated in 2024 with the arrival of DIGI Belgium, the nation's fourth mobile operator. A joint venture company, DIGI Belgium is the fruit of a collaboration between the Belgian local network player Citymesh and the Romanian operator DIGI. This new player will use the incumbent Proximus network to provide SIM cards and subscription services, while also developing its own network. DIGI Belgium is set to acquire 400 mobile sites from Proximus as part of the ongoing network consolidation. After the bankruptcy of EDPNet at the end of 2022, another factor to be reckoned with is the acquisition of EDPNet by Citymesh.

Legal activity, including court action, can be expected both on the wholesale and on the retail front as a result of these developments. This will range from regulatory and market prac-

tices claims between competitors to discussion over non-compete clauses and trade secrets. An illustration of this trend is the EUR1 million fine imposed by the Belgian Institute for Postal Services and Communications (BIPT) on Tel-enet because of non-compliance with the Easy Switch procedures. This penalty may serve as an indicator of more stringent regulatory enforcement.

Hardware is Hot Refurbished

The Belgian telecommunications regulator is very insistent on strict respect of the EU regulatory framework regarding terminal equipment and devices. As a result, and despite some small clarifications and improvements in the Commission's Blue Guide and legal initiatives being underway on the right to repair, continued complications can be expected in 2024 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 at the 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

Having lost two key senior members in 2022, the Belgian Data Protection Authority (DPA) now has a full director committee. The last two out of

five directors of the DPA started their mandate in July 2023.

DPA enforcement highlights

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

In 2022, the DPA published several decisions regarding the main Belgian media websites' use of cookies. Most cases ended up being settled. In 2023, the DPA reaffirmed that cookies would remain one of its main priorities: it published a checklist on the correct use of cookies and made several new settlements with Belgian media websites concerning their use of cookies. The DPA is also expected to enforce compliance with regard to cookies in 2024. Companies should therefore review their cookies policy, with the help of specialised experts.

In 2023, the DPA imposed a number of "smaller" fines on companies or individuals that were found to be in violation of the General Data Protection Regulation (GDPR), not amounting to more than EUR40,000. However, in early 2024 the DPA imposed a EUR174,640 fine on an agency that collected and brokered data on a large scale, by providing "data quality" services, without legitimate purpose, and by retaining this data over a period of 15 years without informing the data subjects accordingly. The DPA is expected to continue investigating data brokers in 2024.

In 2023, the DPA wished to support and emphasise the role of the data protection officer (DPO) as its "ally" when investigating companies. This emphasis on the role of the DPO will most certainly continue for 2024.

In February 2022, the DPA fined IAB Europe EUR250,000 for its Transparency and Consent Framework (TCF), which was held to be GDPR non-compliant. This decision has 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 European Court of Justice. The hearing of the case (C-604/22) took place in September 2023. The judgment is expected in H1 of 2024.

Judicial review

In May 2023, the DPA prohibited the transfer of tax data of Belgian Accidental Americans to the USA as per the international Foreign Account Tax Compliance Act (FATCA) agreement, considering that the FATCA did not respect several GDPR principles (namely the purpose limitation, and the principles of proportionality and data minimisation) and that it did not contain appropriate safeguards for data transfers outside the EU.

The Brussels Market Court (which has jurisdiction over the review of DPA decisions) annulled the DPA's decision on 20 December 2023, on the grounds that the decision of the DPA (*inter alia*) lacked the necessary justification. The DPA will have to issue a new decision on the FATCA's compliance with the GDPR. The DPA may revise its opinion due to the adoption, in 2023, of the adequacy decision for the EU-US Data Privacy Framework by the European Commission and its judicial review by the European Court of Justice.

Developments in (Government) Data Access *Access to government data*

The revised Data Governance Act entered into force in September 2023, and will have conse-

quences for data access in 2024 and beyond, in particular regarding geospatial and location data, health data and environment data. The updated Public Sector Information (PSI) Directive, together with the Digital Markets Act, created a push for data access from governments and gatekeepers, which will persist in 2024.

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 2024.

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 2024, 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

While 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 telecommunications space (working on FTTH). In 2024, 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 of 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 further 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 2024.

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. Collecting societies have also joined the procedure, as has the video games industry, represented by several of its associations. A decision is expected in the course of 2024.

Silence before the storm

The aforementioned 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 was no substantial change for European businesses up until halfway through 2023, when the European Commission issued a new adequacy decision for the EU-US Data Privacy Framework. The European Union recognises that the level of protection offered by the United States for personal data transferred from the EU to the USA is proportionate to European standards. Through this adequacy decision, new binding safeguards were introduced, announcing concerns raised by the European Court of Justice including limitations on access to EU data by US intelligence services and the establishment of the Data Protection Review Court available to EU individuals. Ensuring a thorough framework for transatlantic data flow, EU individuals obtain recourse procedures for mishandling of their data, and US businesses can join the framework through numerous privacy obligation commitments.

Schrems III?

The question of how durable the adequacy decision will be is bound to be settled by the CJEU in

the last months of 2024 or in early 2025. The EU-US Data Privacy Framework is expected to be under attack owing to enduring concerns over widespread surveillance practices by the US government, and the credibility of the Data Protection Review Court in processing complaints.

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 games industry in this effort. The “cultural test” criterion has been implemented in a pragmatic way, and key governmental players at both the 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 such as Walimage and VAF continue to provide interesting funding schemes to the video games industry.

Copyright remuneration scheme for the creative industry

The highly attractive Belgian copyright remuneration scheme remains in place for “artistic and literary” authors such as 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 games industry will still be eligible for this tax scheme. The same scheme should also remain available to coders and software developers contributing to video games – despite the legal reform discussed below.

Uncertainty for the software industry

Tax legislation was adopted at the end of 2022 with the intention of excluding “non-artistic and non-literary” authors such as 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 on this matter. There is a pending annulment procedure before the Constitutional Court, introduced by a number of software companies. The decision of the Court is expected to be issued in 2024. In the meantime, the tax administration has issued rulings declining software developers and engineers the benefit of the copyright remuneration scheme, on the (highly questionable) basis that software is not an artistic and literary work within the meaning of Belgian copyright law.

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 showed that large marketplaces such as Amazon favour their own products’ logistics over third-party products.

In 2024, 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 regarding the validity and enforceability of fuel surcharges and price indexations.

New Rules Underway for Gaming Sponsoring

The year 2023 witnessed significant developments in the realm of advertising for games of chance, spanning both licensed and unlicensed domains. The government issued a controversial Royal Decree on 27 February 2023, introducing stringent conditions for the promotion of licensed games of chance, particularly in the online sphere. This regulatory development has sparked debates within the gambling industry, as stakeholders grapple with the implications of these measures.

In addition, the European Court of Justice delivered a noteworthy judgment on 2 March 2023, addressing the compatibility of the prohibition on advertising in Belgium for gaming establishments located in other member states with the freedom to provide services. Annulment proceedings are currently pending against the Royal Decree of 27 February 2023, and against Article 61 of the Belgian Gaming Act of 7 May 1999, which serves as a legal basis for the Royal Decree. In addition, a law proposal is currently awaiting the vote of the Belgian Parliament that will introduce a general prohibition on advertising for games of chance in the Gaming Act, with limited exceptions to that prohibition to be adopted by the Belgian government.

Sports and Entertainment – Existing Rules Under Fire

The end of 2023 was marked by important litigation in the field of sports, with three decisions from the CJEU regarding the discretionary power of sports federations in preventing alternative competitions and implementing decisions against EU law, among others.

The recent judgments are expected to enhance alternative sports competition in sports events, potentially allowing for new organisers in the scene. National courts may have more autonomy in resolving disputes related to EU competition law in the sports context, affecting the choice of dispute resolution mechanisms and diminishing the authority of the Court of Arbitration for Sport.

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

The Court of Appeal 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 CJEU's ruling may impact on the football market, not only in Belgium but in the entire EU. The hearing took place in early 2024, and the judgment is expected to be delivered in the second half of 2024. The authors' firm represents the French and International Football Players Associations in this litigation.

Finally, 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. The Court of Appeal of Antwerp already ruled Belgian law to be inapplicable owing to its lack of TRIS-notification before its adoption in 2013. Another case concerning the resale of event tickets is currently pending before the Court of Appeal of Antwerp. The case is to be heard in June 2024.

In addition, in November 2023, the Belgian Parliament adopted several new provisions to the rigid legislation on the resale of tickets for events, granting additional powers to the authorities to make public the details of companies infringing on the ticket resale legislation, and to bargain with said companies by accepting promises to stop their violations or to adopt specific measures. It remains to be seen whether this piece of legislation will be challenged before the Constitutional Court.

BRAZIL

Law and Practice

Contributed by:

Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo

Azevedo Sette Advogados



Contents

1. Metaverse p.49

1.1 Laws and Regulation p.49

2. Digital Economy p.50

2.1 Key Challenges p.50

3. Cloud and Edge Computing p.52

3.1 Highly Regulated Industries and Data Protection p.52

4. Artificial Intelligence p.54

4.1 Liability, Data Protection, IP and Fundamental Rights p.54

5. Internet of Things p.55

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.55

6. Audio-Visual Media Services p.57

6.1 Requirements and Authorisation Procedures p.57

7. Telecommunications p.58

7.1 Scope of Regulation and Pre-marketing Requirements p.58

8. Challenges with Technology Agreements p.59

8.1 Legal Framework Challenges p.59

9. Trust Services and Digital Entities p.60

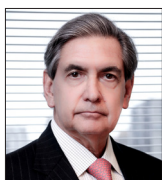
9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.60

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

Azevedo Sette Advogados was founded in 1967 and has a leading market team of over 500 professionals working in the firm's five offices located in São Paulo, Belo Horizonte, Brasília, Rio de Janeiro and Recife. 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, offering complete solutions that help clients reach their goals in accordance with their needs and strategic planning. With activities ranging

from industrial, services and commerce sectors to government, private investors, and investment funds, the firm's 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 and Camila Sabino Del Sasso, as well as the invaluable contribution of Juliana Gebara Sene Santos Ikeda and Lorena Pretti Serraglio while members of Azevedo Sette Advogados.

Authors



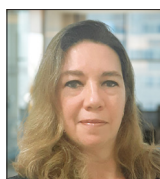
Ricardo Barretto Ferreira da Silva is a senior partner at Azevedo Sette Advogados, working in the areas of corporate, tax, M&A, IP, TMT, privacy and data protection. He

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 adviser (1992–93) of the American Chamber of Commerce São Paulo. He has also edited and co-authored numerous publications and articles on varied topics.



Ingrid Bandeira Santos is a senior associate at Azevedo Sette Advogados, qualified to practise law in Brazil and in the state of New York. Aside from working on privacy and data

protection matters, Ingrid specialises in competition law, international trade and anti-corruption compliance. She is an author and co-author in all these areas, including of a book elected by the Superior Court of Justice as an essential work for the understanding of privacy and data protection in Brazil.



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.

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**



Carolina Simioni Perdomo is an associate in the technology, media and telecommunications, and privacy and data protection practice areas at Azevedo Sette Advogados. Carolina's work

focuses on digital law and data protection matters. She is co-author of articles on technology, media and telecommunications published in Brazil and abroad.

Azevedo Sette Advogados

11th floor, International Plaza II Building
1327, Presidente Juscelino Kubitschek Avenue
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

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

1. Metaverse

1.1 Laws and Regulation

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

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

processing of personal data will have its limits 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.

Although the platform model peaked in the first two years, the metaverse has faced a proportionally huge downturn. Accordingly, there is no expectation that eventual regulation on the subject will occur at a fast pace.

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 and 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

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

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 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** – Decree 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 signa-

ture 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.
- **Metaverse** – Bill No 2,175/2023 proposes a metaverse regulatory framework with principles, guidelines and rules for the use of metaverse and the performance of legal businesses in this virtual environment.
- **Sports bets** – the recently enacted Law No 14,790/2023 regulates online betting on sports events, with several government control provisions, such as mandatory pre-licensing with fees of up to BRL30 million, requirements and prohibitions on payment transactions, tax collection at a 15% rate on income, to name just a few.

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

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

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;
- 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 the 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 those 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 stress 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

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

- 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.

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 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 back-ups. 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.
- The contractual provisions must ensure that the information in the provider's custody will be processed with confidentiality and cannot

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

be used by or provided to third parties without authorisation under any circumstances.

Recently, Ordinance No 5,950 SGD/MGI, of 26 October 2023, established a template for contracting software and cloud computing services by Federal Public Administration agencies, which is in line with the recent case law of the Federal Court of Auditors (TCU). The aim of the rule is to standardise and simplify the process of contracting software and cloud computing services, with emphasis on the security, privacy protection, integrity and governance of data held by the agencies and entities of the Information Technology Resources Management System (SISP).

The new ordinance defines specific forms of remuneration, minimum service levels, product verification and acceptance criteria and minimum security criteria. It is important to note that compliance with the aforementioned ordinance will be mandatory for contracts entered into after 30 April 2024. Nonetheless, agencies and entities may apply the standards to contracts entered into before that date. This ordinance does not apply to contracts entered into before 1 November 2023. After these deadlines, agencies will have to justify the adoption of other contracting models, but the contracting will have to be approved by the Digital Government Secretariat (SGD).

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

The use of AI is currently being discussed in Brazil through joint deliberation of Bill No 3,592/2023, Bill No 2,338/2023 and Bill No 5,691/2019. Bill 3,592/2023 discusses the use of audio-visuals

of deceased people aimed at safeguarding their dignity, privacy and rights after death. Bill No 2,338/2023 focuses on the use of AI in general. The Temporary Internal Committee on Artificial Intelligence (CTIA) was formed on August 2023 and had its work duration extended to May 2024.

Bill No 5,691/2019 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;
- 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;

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

- 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 Telecommunications 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 licence, 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

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

(ISS) is due, the rates of which vary according to the applicable municipality.

- Where 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 Telecommunications 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, which began being implemented in Brazil in 2022, is boosting the IoT market, as expected, fostering innovation and impacting local economy and society. Importantly, the minimum security requirements for 5G networks set by the Office of Institutional Security of the Republic Presidency's Normative Instruction 4/2020 are to be complied with.

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

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 station 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.

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.

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

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 the 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 13,879/2019 stipulates that concessionaires might request ANATEL to adjust the concession into an authorisation, if certain requirements are met by the interested party.

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

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

and/or restricted radiation radiocommunication equipment, provided no numbering resources are employed, and, in case of community-interest services, there are fewer 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.

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 Bra-

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

zila, 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, back-ups, 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 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.

Contributed by: Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos, Sylvia Werdmüller von Elgg Roberto and Carolina Simioni Perdomo, **Azevedo Sette Advogados**

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 government authorities and boards of trade only accept documents signed electronically or using certified digital certified signatures issued by ICP-Brasil, provided that the signatures are provided through

platforms that certify their validity via QR Code, hash or validation code. 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.

CANADA

Law and Practice

Contributed by:

Leslie Milton, Scott Prescott, Christopher Ferguson and Paul Burbank
Fasken



Contents

1. Metaverse p.65

1.1 Laws and Regulation p.65

2. Digital Economy p.66

2.1 Key Challenges p.66

3. Cloud and Edge Computing p.66

3.1 Highly Regulated Industries and Data Protection p.66

4. Artificial Intelligence p.71

4.1 Liability, Data Protection, IP and Fundamental Rights p.71

5. Internet of Things p.74

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.74

6. Audio-Visual Media Services p.75

6.1 Requirements and Authorisation Procedures p.75

7. Telecommunications p.76

7.1 Scope of Regulation and Pre-marketing Requirements p.76

8. Challenges with Technology Agreements p.77

8.1 Legal Framework Challenges p.77

9. Trust Services and Digital Entities p.78

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.78

Fasken is a leading international business law and litigation firm. With over 950 lawyers, the firm has offices in Vancouver, Surrey, Calgary, Tsuut'ina, 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

broadcasting, 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, mediation and arbitration).

Authors



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.



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, IPTV and satellite distributors, television and radio broadcasters, online streaming services and Canadian and foreign television programming services, as well as to wireline and wireless telecommunications service providers. His clients include a range of leading Canadian and international communications companies. He has been involved in numerous licensing, ownership, dispute resolution and policy proceedings before the Canadian Radio-television and Telecommunications Commission (CRTC).

Contributed by: Leslie Milton, Scott Prescott, Christopher Ferguson and Paul Burbank **Fasken**



Christopher Ferguson focuses his practice on technology, privacy and cybersecurity, and communications 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.



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 on

other commercial and regulatory matters related to technology. Paul's work involves supporting client businesses and legal teams with practical, regulatory advice for the launching of new telecommunications services and technology products. His commercial work is IT-focused and includes negotiating and drafting services, licence agreements, and 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
PO 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

Own tomorrow

1. Metaverse

1.1 Laws and Regulation

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 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 (this enhanced authority is already in place in Quebec).

In addition, the coming into force of the new Quebec law has introduced 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 that organisations collect a greater volume of potentially more sensitive personal information in the metaverse, the risks of harm 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 as metaverse users move through different metaverse platforms.

Artificial Intelligence Regulations

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

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 Parliament amended the Broadcasting Act in 2023 to (among other things) enable Canada's broadcasting and telecommunications regulator – the Canadian Radio-television and Telecommunications Commission (CRTC) – to implement a regulatory framework that would apply to digital streaming services that qualify as “online undertakings”. The CRTC has initiated several proceedings designed to implement its new mandate under the Broadcasting Act. These proceedings are expected to result in certain online undertakings being subject to obligations designed to support the creation, distribution, promotion and discoverability of Canadian and Indigenous audio and video content through monetary and non-monetary contributions and investments in Canada.

The amended Broadcasting Act provides the CRTC with the authority to impose penalties for violations of certain regulatory obligations, and grants the CRTC explicit information-gathering powers with respect to online undertakings.

In addition to the amended Broadcasting Act, the Canadian Parliament also enacted the Online News Act, which aims to require dominant digital platforms to compensate news businesses when their content is made available on their services. To achieve this goal, the Online News Act creates a bargaining framework to ensure that dominant digital platforms provide for fair compensation to news businesses, and encourages them to enter into commercial agreements with a range of news businesses in Canada.

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

Except in Quebec, there are no private sector laws of general application focused specifically on the provision of cloud services to the private sector in Canada. Quebec's law regarding information technology (AELFIT) sets limits on the liability for cloud service providers and other such intermediaries (search engine providers, internet service providers) where the provider has limited control over user-generated content. The Quebec law on information technology also targets biometric information and biometric databases, and imposes disclosure requirements in connec-

tion with such activities. Other Canadian laws of general application and certain sector-specific regulations targeted at 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 at federal entities, it has also been voluntarily adopted by many provincially regulated entities in the financial sector.

In April 2023, OSFI released a final version of a revised Guideline B-10 (the “Revised Guideline”), which sets out enhanced expectations for FRFIs in managing an expanded scope of third-party risks, and places greater emphasis on governance and risk management plans, and on specific outcomes and principles. The Revised Guideline expands the application of Guideline B-10 to “third-party arrangements”, which include any business or strategic arrangement with external entities. Examples of arrangements that will be subject to the Revised Guideline are:

- 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 Revised 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. It also includes more specific requirements for FRFIs to develop cloud-specific requirements and consider cloud portability in their contracting arrangements. The Revised Guideline will come into effect on 1 May 2024, and OSFI indicates that this transition period is intended to provide FRFIs with sufficient time to self-assess and build third-party risk-man-

agement programmes that comply with the new requirements.

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, a 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*, setting out OSFI's expectations in relation to the immediate and ongoing reporting of cybersecurity incidents, and 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*, which 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, cyber governance and risk management;
- technology operations; and
- cybersecurity.

Guideline B-13 became effective on 1 January 2024.

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:

- private sector organisations that use third-party cloud services to collect, use, store or disclose personal information of individuals on their behalf will be subject to Canadian privacy legislation if the organisation is based in Canada or has a real and substantial connection to Canada; and
- Canadian customers of cloud services will seek to have their agreements for cloud services address the requirements of Canadian privacy laws, including regarding 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 Office of the Privacy Commissioner of Canada (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 2024, PIPEDA continues to be subject to an adequacy decision by the European Commission, to ensure that personal 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, to the extent PIPEDA applies to such data.

PIPEDA applies in all provinces and territories in Canada to organisations engaged in commercial activities, except within a province or territory that has enacted substantially similar private sector legislation and that 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 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, including:

- penalties of up to CAD10 million or 2% of an organisation’s annual global revenues;
- fines of up to CAD25 million or 4% of an organisation’s annual global revenues; and
- a private right of action.

The revised Quebec law also requires organisations to undertake privacy impact assessments prior to transferring personal information outside 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. As of the time of writing, Bill C-27 remains under consideration in the parliamentary process. 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;
- define and create standards for the de-identification and anonymisation of personal information; and

- provide additional protections for the personal information of minors, including by deeming such information as sensitive personal information.

Bill C-27 would also create a new Personal Information and Data Protection Tribunal, which 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 for a private right of action to permit recourse to the courts in certain circumstances.

In response to stakeholder feedback, in October 2023 the federal government proposed amendments to the CPPA that would, among other things:

- recognise privacy as a fundamental right;
- require organisations to consider the special interests of children when determining whether personal information is being collected, used or disclosed for an appropriate purpose; and
- give the Commissioner the authority to include a monetary component with any compliance agreement it enters into with an organisation it believes has contravened the CPPA.

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; and
- 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.

As noted previously, the Canadian government re-introduced proposed legislation to replace PIPEDA's personal information provisions with a new law, the Consumer Privacy Protection Act (CPPA), and this legislative reform remains under consideration by Parliament.

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.

Quebec's privacy law now requires 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. In September 2023, Quebec's privacy regulator released a guide and template on conducting privacy impact assessments in compliance with the new law.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

Artificial Intelligence and Data

AI systems often rely on large datasets. Organisations that develop AI systems using large

datasets in Canada must balance the need to maximise the value of large datasets 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 may use anonymised and 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 outside Quebec (see below). However, the potential for re-identification increases as datasets grow and other datasets 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; though the proposed Consumer Privacy Protection Act being considered by Parliament would introduce such definitions. Revisions to Quebec’s privacy law have introduced 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” and in compliance with regulation on anonymisation (the Quebec government published draft regulations for consultation in December 2023).

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”.

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 and under consideration by the House of Commons at this time (January 2024).

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 for certain unlawful or fraudulent conduct in respect of AI systems. In November 2023, the minister responsible

for AIDA presented a set of proposed amendments to the parliamentary committee studying the new law. Among other things, the proposed amendments would do the following.

- Provide new legal definitions, including formal definitions of “artificial intelligence system”, “general purpose system” and “machine-learning model”.
- Establish seven classes of presumptively high-impact AI systems, including those related to:
 - (a) employment-related decision-making;
 - (b) biometric information-processing and healthcare;
 - (c) content recommendations for online platforms; and
 - (d) systems used to determine the eligibility and price for services offered to individuals.
- Explicitly require the use of accountability frameworks to ensure that organisations involved in the development and deployment of both general-purpose and high-risk AI systems are accountable for their risk-management practice.
- Provide new powers to the Artificial Intelligence and Data Commissioner.
- Align AIDA with the EU Artificial Intelligence Act.

Canadian privacy law requirements regarding consent, openness and transparency are areas of concern with regard to AI and machine learning (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.

Since September 2023, Quebec’s privacy law requires 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 AI 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). In October 2023, the Canadian government launched a consultation related to authorship of AI-generated content and issues related to the use of copyright-protected content in the training of AI services and tools. The government characterised the purpose of the consultation as focusing on “the impacts of recent developments in AI on the creative industries and the economic impacts that these technologies have, or could have, on Canadians, and [looking] at whether change is required to further improve or reinforce copyright policy for a modern, evolving Canadian economy”. The consultation closed for public comment in January 2024.

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 use of personal information to manage the employee-employer relationship, and employers must provide notice to employees of the use of IoT devices that collect employee personal information and of 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.

Since September 2023, Quebec law requires organisations that use technologies that can identify, locate or profile individuals to have this functionality off by default. IoT devices and services must 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 that are indefinite or fixed, and those licences are subject to conditions of service and certain orders and regulations that it deems appropriate for the implementation of Canada's broadcasting policy. Licensees are generally subject to a variety of regulatory obligations, including requirements relating to the exhibition of Canadian content and to programme expenditures and/or contributions.

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.

To be eligible to hold a broadcasting licence, a company must be owned and effectively controlled by Canadians. Broadcasting licensees will also generally be required to pay broadcasting fees under the Broadcasting Fees Regulations, which are expected to become effective on 1 April 2024. The broadcasting fees will be a licensee's pro rata share of the annual cost of the CRTC's operations.

In addition to licensing, the CRTC has the authority to exempt classes of traditional broadcasting undertakings from holding a licence, and it 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 undertakings, and do not require a company to pay any broadcasting fees or to obtain any further authorisations from the CRTC to operate in Canada.

Online Video-Sharing Platform Services

Entities that operate online video-sharing platforms (including those that offer user-generated content) and other online streaming services in Canada are permitted to do so in Canada under the amended Broadcasting Act, and may be subject to regulatory obligations imposed by the CRTC, including:

- financial contributions and/or expenditures that support Canadian artists or programming;
- specific commitments to the promotion, discoverability or prominence of Canadian or Indigenous content;
- the carriage of services in French, Indigenous or other languages; and
- maintaining a certain percentage of Canadian and Indigenous content in an on-demand catalogue.

Certain online undertakings will also be required to pay broadcasting fees under the proposed Broadcasting Fees Regulations. There are, however, no Canadian ownership and control requirements applicable to online undertakings, as operators are not required to hold licences for their online undertakings.

In May 2023, the CRTC initiated three separate proceedings to begin implementing its new mandate under the amended Broadcasting Act. Two of those proceedings have concluded, and resulted in requirements for certain online streaming services to register with the CRTC and provide information about their activities in Canada, and to comply with modest conditions of service, which include a requirement to make content available in a way that is not tied to a specific mobile or internet service.

The third proceeding, which included a three-week hearing beginning in November 2023, considered the contributions online streaming services will need to make to support Canadian and Indigenous content. A decision in that proceeding is expected to be issued in spring 2024, and will be followed by subsequent proceedings considering whether to impose other regulatory obligations – financial and non-financial – for online undertakings.

Among other reforms, the amended Broadcasting Act also provides the CRTC with the authority to impose administrative monetary penalties (AMPs) on all types of broadcasting undertakings (both traditional and online) for violations of certain regulatory obligations imposed under the Act, and provides the CRTC with more explicit information-gathering powers.

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:

- 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 calling 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; as will a BITS licence. 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 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 such as 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, though 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);
- industry-specific regulations, such as requirements governing the use of IT services (and third-party services generally) by federally regulated financial institutions (FRFIs), and

- including requirements that certain records of FRFIs be located in Canada; and
- 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 and Edge 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 elec-

tronic 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 – that impose “know your customer” requirements.

For example, the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, and its underlying regulations, prescribe certain acceptable methods that a reporting entity (eg, a bank, trust and loan company, securities dealer, money service business, etc) can use to identify an individual, corporation or entity other than a corporation. These methods include:

- referring to a 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 ability of a reporting entity to use the government-issued photo identification method when a person is not physically present. This requires the reporting entity to have a process in place to authenticate the government-issued photo identification document. At this time, FINTRAC guidance provides few details with respect to the specifications or technical requirements for such a process, other than that the process must be able to determine that a government-issued photo identification document is authentic, valid and current. The guidance does, however, indicate that it is not enough to only view a person and their government-issued photo identification document through a video conference or another type of virtual application.

CHINA

Law and Practice

Contributed by:

Cloud Li, Joanna Jiang, Zhengwei Yang and Dimitri Phillips
DaHui Lawyers

Contents

1. Metaverse p.82

1.1 Laws and Regulation p.82

2. Digital Economy p.86

2.1 Key Challenges p.86

3. Cloud and Edge Computing p.90

3.1 Highly Regulated Industries and Data Protection p.90

4. Artificial Intelligence p.92

4.1 Liability, Data Protection, IP and Fundamental Rights p.92

5. Internet of Things p.94

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.94

6. Audio-Visual Media Services p.94

6.1 Requirements and Authorisation Procedures p.94

7. Telecommunications p.96

7.1 Scope of Regulation and Pre-marketing Requirements p.96

8. Challenges with Technology Agreements p.97

8.1 Legal Framework Challenges p.97

9. Trust Services and Digital Entities p.98

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.98

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 of 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, and 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. Zhengwei 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. She focuses on the IT and telecommunications, media, entertainment, and healthcare industries. Joanna 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

dahui

1. Metaverse

1.1 Laws and Regulation

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 Catalogue 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 September 2023, the Ministry of Industry and Information Technology (MIIT), in collaboration with four other ministries, released the Three-Year Action Plan for the Innovative Development of the Metaverse Industry (2023–2025), which outlines a policy framework and specific measures aimed at fostering the growth of the metaverse industry. Key strategies involve advancing AI-based tech-

nologies, such as data circulation technology, content generation technology, digital twin technology, perception and interaction technology, and networking and computing technology. The overarching goal is to facilitate the formation of what is referred to as the “industrial metaverse”.

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 Catalogue of Telecommunications Businesses, issued and regularly amended by the 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 services 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.

On 23 November 2023, the State Council approved the Plan on Supporting Beijing to Deepen the Development of the Comprehensive Demonstration Zone of National Service Industry (“Plan”), with the objective of advancing the further opening and reform of various service sectors. The most notable part of the Plan is its relaxing of foreign investment shareholding restrictions in specific sub-categories of value-added telecommunications services (VATS) in Beijing, including the elimination of foreign shareholding limitations in the operation of app stores (under a B25 licence) and internet access services (under a B14 licence).

Under the prevailing regulatory framework, the operation of app stores in China is limited to

50% foreign investment, except for investment in free trade zones (FTZs) and for qualified service providers from Hong Kong or Macau under the Closer Economic Partnership Arrangement (CEPA), while foreign investment in internet access services in China is 100% prohibited, subject to the same exceptions.

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, copying 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, PRC Patent 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.

Data Property Rights and Data Transactions

The Chinese government recognises data as a significant “factor of production” in the digital economy, akin to capital, land, technology, and human resources. On 19 December 2022, the Central Committee of the Chinese Communist Party and the State Council jointly released the Opinion on Building a Data Basic System to Enhance the Utilisation of Data Elements, which introduces 20 measures (“20 Measures”) designed to establish fundamental data systems that will promote the rapidly growing data industry in China. According to these 20 Measures, China plans to develop basic data systems from four key aspects:

- data property rights;
- data circulation and transaction;
- data income distribution to promote fair competition; and
- data security governance.

In alignment with the 20 Measures, several local governments in China, including Jiangsu, Zhejiang, Beijing, and Shenzhen provincial governments, have enacted relevant regulations to define data property rights and establish mechanisms for data transactions. These regulations have instituted a property rights operating mechanism to delineate the right to hold data resources, the right to use data processing, and the right to operate data products. Entities possessing data with “commercial value” can apply for and obtain ownership certificates for such data. These certificates serve as legitimate credentials in data transactions, income distribution from data usage, and dispute resolution, forming the basis for data circulation and the burgeoning data-driven economy.

In March 2023, China further solidified its commitment to data governance by establishing the

National Data Bureau. Tasked with promoting data-related basic systems, this bureau collaborates with other departments to facilitate data sharing and development, as well as to guide the planning and development of the digital economy.

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.

The financial value of virtual property has been increasingly acknowledged by PRC judicial bodies. In a case adjudicated by the Beijing Internet Court and publicised as one of the “10 Typical Cases for China Internet Governance in 2022”, the plaintiff filed a claim against a game company to refund his unused game coins and pay compensation for other game props since the game company shut down the game. The Court upheld the plaintiff’s claim and ruled that the game props have the nature of property and shall be protected as internet virtual property. While the Court determined that the game company was liable in tort for infringing the property rights of the plaintiff, the specific compensation amount depends on the nature and characteristics of the game props. For example, game coins were directly purchased with legal tender, so the game company must refund the amount equivalent to the value of the unused virtual coins.

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.

Metaverse platform providers and participants who (also) engage in operations deemed to fall within “critical information infrastructure” could be deemed Critical Information Infrastructure Operators (CIIOs) and therefore subject to more strict obligations under the cybersecurity regime.

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 so-called “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).

- Under the current data protection regime, the transfer of PI outside of China is subject to the following requirements (“Data Export Requirements”):
- Security Assessment – the following parties must carry out so-called “security assessments” before transferring data offshore:
 - (a) CIOs seeking to transfer PI offshore;
 - (b) data handlers seeking to transfer so-called “important data” offshore;
 - (c) data handlers who process the PI of more than one million individuals and seek to transfer any PI offshore;
 - (d) data handlers who cumulatively transfer offshore, the PI of more than 100,000 individuals in the period since 1 January of the preceding year; and
 - (e) data handlers who cumulatively transfer offshore, the “sensitive personal information” of more than 10,000 individuals in the period since 1 January of the preceding year.
- Standard Contract or PI Protection Certification – if none of the thresholds for the security assessment listed above is triggered, a party wishing to transfer any PI out of China must nevertheless carry out one of the following procedures:
 - (a) executing a standard contract issued by the CAC with the relevant overseas recipient of the PI; or
 - (b) passing “PI protection certification” from a specialised institution designated by the CAC.

On 28 September 2023, the CAC released the Draft Provisions on Regulating and Facilitating Cross-Border Data Transfer (“Draft Regulation”). If the Draft Regulation is ultimately issued sub-

stantially in its current form, many cross-border data transfers involved in various daily operations of multinational companies, will not be subject to Data Export Requirements, including:

- PI exporting that is necessary for the conclusion or performance of a contract to which the PI subject is a party, such as cross-border shopping, payments, ticket and hotel bookings, visa applications, etc;
- exporting PI of employees for purposes of implementing HR management according to employment policies and collective labour contracts;
- exporting PI of no more than 10,000 individuals within one year;
- exporting PI for purposes of protecting individuals’ life, health, or property security in emergency situations;
- exporting of PI that is not collected or generated within mainland China; and
- exporting non-PI data that is collected or generated during international trade, academic co-operation, cross-border manufacturing and marketing, and certain other as-yet unspecified activities, unless such data is recognised as “important data”.

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 Regulation**;
- 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;
- the Advertising Law, most recently revised in 2021, and the Measures for the Administration of Internet Advertising issued by the State Administration for Market Regulation (SAMR) in 2023; 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 CIIOs.

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 as listed and defined in the Classification Catalogue of Telecommunications Services.

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.

Advertisements

To refine the advertising regulatory rules applicable to numerous new types of advertisements over the internet, on 25 February 2023, the SAMR released the Measures for the Administration of Internet Advertising (“Online Advertising Measures”), which came into effect on 1 May 2023. The Online Advertising Measures impose different compliance requirements on various forms of internet advertisements, including advertisements with links, soft advertising in forms of experience sharing or consumer commenting, advertisement pushing to smart devices, pop-up ads and splash ads, and ads on livestreaming, etc. For example, it remains controversial (and is perhaps not legally settled) whether using livestreaming to promote products or services constitutes advertising under PRC law. However, according to the Online Advertising Measures, for some internet livestreaming with essential features of commercial advertisements, the operators and marketers in the livestreaming room must assume the responsibilities of an advertising operator and publisher. Likewise, if any individuals conducting live marketing activities use their own name or image to endorse products, they must abide by the legal responsibilities and obligations of an advertising endorser. For internet advertising that appears in the form of pop-ups or splash screens when launching an internet application, both the advertiser and the advertising publisher

are obligated to prominently display a button to ensure easy closure with just one click.

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, the PIPL and/or the PRC Critical Information Infrastructure Regulations, such as local data hosting and offshore data transfer restrictions (see **1.1 Laws and Regulation**). Ultimately, in some circumstances, businesses that have offshore components (eg, servers hosted outside China, or networks between PRC subsidiaries and foreign parent companies) and are subject to offshore data transfer restrictions 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 Regulation**).

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 stand-

ards 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 CIIO 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 CIIO 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-CIIOs 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 CIIO 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 July 2023, 72 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 or executing the “standard contracts” or obtaining the certification 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 Regulation and 2.1 Key Challenges).

4. Artificial Intelligence

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

Although there had been some quasi-legislation of AI before mid-2023 (eg, the Ethical Norms for New Generation Artificial Intelligence from September 2021), the first major component in the Chinese regulatory framework for AI was issued on 10 July 2023: the Interim Measures for the Administration of Generative Artificial Intelligence Services (“Generative AI Measures”), effective as of 15 August 2023. Any entity, organisation or individual that provides services that generate any text, images, audio recordings, videos or other content to the general public in mainland China using “generative AI technology”, whether through APIs or other means, will be subject to the Generative AI Measures.

The Generative AI Measures require providers of generative AI services to take a number of actions, including executing service agreements with users, labelling videos and other generated content if the service provider offers “deep synthesis” services, and reporting content violations and wrongful activities to PRC regulators, etc. For any generative AI services with “public opinion properties or the capacity for social mobilization”, their providers are required by the Generative AI Measures to conduct security

assessments and algorithm filings via the CAC's designated online platform. As of November 2023, the CAC already accepted filings of 262 applicants.

Further legislative developments on AI are expected in the near term according to the State Council's 2023 legislative agenda, including an "AI law".

At the local government level, from the previous two years, multiple municipal or provincial governments (including Beijing, Shanghai and Shenzhen) have issued guidelines to facilitate the AI industry, aiming at leaving more space and flexibility for AI based technologies in industries spanning healthcare, scientific research, financial, autonomous driving, etc. For example, the Shanghai Provisions on Promoting the Development of the AI Industry ("Shanghai AI Provisions"), effective from 1 October 2022, call for management systems based on grading and "sandbox" supervision. Such management intends to leave space and flexibility for the AI industry to develop. Most notably, 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.

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 Regulation**, **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 cannot be considered entitled to patent rights for its inventions.

Recently, a landmark case marks the first instance in China wherein a user's copyright claim on an AI-generated image has been acknowledged. The case was ruled by the Beijing Internet Court in November 2023. Mr Li, the plaintiff, posted an image created by an AI-based model on his social media account. Subsequently, he filed a copyright infringement claim against the defendant, who had used this image in an article published on a news blog. The Beijing Internet Court supported the plaintiff's claim, asserting that the AI-generated image encapsulates the intelligent efforts and original thinking of Mr Li. Consequently, the image was deemed a work product, and Mr Li has the copyright. It has sparked widespread attention, prompting discussions on the issue of whether users employing AI-based technology should be afforded copyright 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 Regulation, 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 Ministry of Science and Technology (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 Programme Services; and
- the PRC Administrative Regulations on Internet Audio-Visual Programme 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 licenced 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 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 (which was last updated on 21 December 2023) 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.

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 safekeeping of individuals’ PI and the protection of privacy (see **1.1 Laws and Regulation**, **2.1 Key Challenges** and **3.1 Highly Regulated Industries and Data Protection**).

Trends and Developments

Contributed by:

Cloud Li, Joanna Jiang, Zhengwei Yang and Dimitri Phillips
DaHui Lawyers

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 of 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, and compliance and general corporate matters. Cloud has acted for some of the largest and most established participants in China's TMT sector.



Joanna Jiang is a partner in DaHui Lawyers' corporate, TMT, and cybersecurity practice groups. She focuses on the IT and telecommunications, media, entertainment, and healthcare

industries. Joanna 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.



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. Zhengwei is recognised by clients for his strategic thinking and quality of service.



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



Technology, Media and Telecommunication in China in 2024

After years of robust growth, technology, media and telecommunication (TMT) companies in China are encountering evolving regulatory scrutiny and new challenges along with the continued opening-up to foreign investment. Key regulatory developments that affected the TMT industry in 2023 include:

- establishment of detailed mechanisms for cross-border data transfer, followed quickly by indications of potential exemptions;
- promulgation of the first major piece of legislation on artificial intelligence (AI) activities;
- intense regulatory scrutiny and enforcement activities in the field of anti-monopoly/competition; and
- release of the amended Company Law.

While enhanced or refined regulation is a constant reality (in China, as elsewhere), especially in areas such as AI and data protection, perhaps the two most notable developments in 2023 were the lifting of restrictions on foreign shareholding in certain telecommunication businesses and the release of a draft regulation easing cross-border transfer restrictions that entered

into effect only at the end of November 2023. Both are signals that China is keeping its doors open, in some ways opening them more than in 2022, for foreign TMT businesses to tap into the country's still enormous and vibrant market.

Further opening to foreign investment

The trend of foreign-investment liberalisation carried over (and arguably grew) from 2022. The revisions to the Administrative Provisions on Foreign-Invested Telecommunications Enterprises ("FITE Provisions"), which came into effect on 29 March 2022, 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, inter alia, may have 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 even 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, the China Academy of Information and Communications Technology has reported the total number of FITEs with one type of such licences (specifically, a licence for value-added telecommunications business) increased from 1,097 to 1,448 between September 2022 and June 2023.

The above developments were followed by even more significant ones in 2023, especially in the Plan on Supporting Beijing to Deepen the Development of the Comprehensive Demonstration Zone of the National Service Industry (“Plan”), released by the State Council on 23 November 2023. Among other things, the Plan relaxes foreign investment shareholding restrictions in specific sub-categories of value-added telecommunications services (VATS) in Beijing. Notably, this includes the elimination of foreign shareholding limitations in the operation of app stores (under the B25 licence) and internet access services (under the B14 licence).

Under the prevailing regulatory framework, the operation of app stores in China is limited to 50% foreign investment, except for investment in free trade zones (FTZs) and for qualified service providers from Hong Kong or Macau under the Closer Economic Partnership Arrangement (CEPA), while foreign investment in internet access services in China is 100% prohibited, subject to the same exceptions.

This development is significant not only in itself but also in being a signal that the Chinese TMT markets may in the near term open up even more to foreign investment.

Data and privacy protection

In 2023, PRC regulators released several implementing rules concerning data protection and related areas, almost all primarily elaborating on the existing law. 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.

Cross-border data transfers

Though the Cybersecurity Law had emphasised cross-border data transfer controls as far back as 2016, they did not take on concrete form until 2021’s Personal Information Protection Law (PIPL), and only in 2022 and 2023 did the system crystallise with detailed implementing rules.

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 into a “standard contract” with the data transfer recipient; or
- obtaining a “certification” from certain government-designated agencies.

The details of the “security assessment” were largely provided in 2022, while in 2023, specific regulations were promulgated to provide guidance on executing the “standard contract” for cross-border transfer of personal information (PI).

On 24 February 2023, the Cyberspace Administration of China (CAC) released the finalised Measures on Standard Contracts for the Outbound Cross-Border Transfer of PI (“SC Measures”). The SC Measures took effect on 1 June 2023, and allowed a six-month grace period

for full compliance; ie, until 30 November 2023. In addition, on 30 May 2023, the CAC issued guidance for the standard contracts and for the PI protection impact assessment (PIPIA) report that needs to be carried out in tandem therewith. On 2 June 2023, the Beijing branch of the CAC released a set of local filing guidelines for further directions related to the standard contract mechanism.

A data handler who satisfies the following criteria can transfer data outside China by using only a standard contract and PIPIA (instead of a security assessment):

- it is not a critical information infrastructure operator (as specified in the PRC Cybersecurity Law);
- it does not process PI of more than one million individuals;
- it does not provide PI of 100,000 individuals or more to overseas recipients since 1 January of the preceding year; and
- it does not provide sensitive PI of 10,000 individuals or more to overseas recipients since 1 January of the preceding year.

To the amazement of many, just two months before the grace period ended for parties to comply with the SC Measures, the CAC did an apparent about-turn. On 28 September 2023, it released the Draft Provisions on Regulation and Facilitating Cross-Border Data Transfer (“Draft Regulation”), which exempted many cross-border data transfers involved in various daily operations of multinational companies from the most wide-reaching and burdensome cross-border data transfer requirements.

Specifically, if the Draft Regulation is implemented substantially in its current form, many cross-border transfers of PI of China employees,

customers, vendors, and other business associates will not be subject to security assessments, standard contracts, or PI protection certification. Though that is likely the main purpose, and would be the main effect, of the Draft Regulation, it also eases other restrictions and requirements; eg, exempting data handlers in FTZs from requirements related to cross-border transfer of data as long as the data type to be transferred is not included in particular negative lists (which do not exist as of year-end 2023).

As the Draft Regulation was not promulgated as of year-end 2023, and the grace period for complying with the SC Measures expired, many companies already began work to comply with the SC Measures.

Data property rights and data transactions

The Chinese government recognises data as a significant “factor of production” in the digital economy, akin to capital, land, technology, and human resources. On 19 December 2022, the Central Committee of the Chinese Communist Party and the State Council jointly released the Opinion on Building a Data Basic System to Enhance the Utilisation of Data Elements, which introduced 20 measures (“20 Measures”) designed to establish fundamental data systems that will promote the rapidly growing data industry in China. According to these 20 Measures, China plans to develop basic data systems from four key aspects:

- data property rights;
- data circulation and transactions;
- data income distribution to promote fair competition; and
- data security governance.

In alignment with the 20 Measures, several local governments in China (including Beijing, Shen-

zhen, Jiangsu and Zhejiang), have enacted relevant regulations to define data property rights and establish mechanisms for data transactions. These regulations have instituted a property rights operating mechanism to delineate the right to hold data resources, the right to use data processing, and the right to operate data products. Entities possessing data with “commercial value” can apply for and obtain ownership certificates for such data. These certificates serve as legitimate credentials in data transactions, income distribution from data usage, and dispute resolution, forming the basis for data circulation and the burgeoning data-driven economy.

In March 2023, China further solidified its commitment to data governance by establishing the National Data Bureau. Tasked with promoting data-related basic systems, this bureau collaborates with other departments to facilitate data sharing and development, as well as to guide the planning and development of the digital economy.

Artificial intelligence and the emerging trend

As the first major component in the Chinese regulatory framework for AI, the Interim Measures for the Administration of Generative Artificial Intelligence Services (“Generative AI Measures”) was issued on 10 July 2023 by the CAC, alongside six other PRC government departments, and came into effect on 15 August 2023. Any entity, organisation or individual that provides services that generate any text, images, audio recordings, videos or other content to the general public in mainland China using “generative AI technology”, whether through APIs or other means, will be subject to the Generative AI Measures.

The Generative AI Measures require providers of generative AI services to take certain actions,

including executing service agreements with users, labelling videos and other generated content if the service provider offers “deep synthesis” services, and reporting content violations and wrongful activities to PRC regulators. For any generative AI services with “public opinion properties or the capacity for social mobilization”, their providers are required by the Generative AI Measures to conduct security assessments and algorithm filings via the CAC’s designated online platform. As of November 2023, the CAC already accepted filings of 262 applicants.

Further legislative developments on AI are expected in the near term according to the State Council’s 2023 legislative agenda, including an “AI law”.

At the local government level, from the previous two years, multiple provincial governments (including Beijing, Shanghai and Shenzhen) have issued guidelines to facilitate the AI industry, aiming at leaving more space and flexibility for AI-based technologies in industries spanning healthcare, scientific research, finance, autonomous driving, and more.

Anti-monopoly and competition

Following the amendment of the PRC Anti-monopoly Law (“AM Law”) in 2022, the State Administration for Market Regulation (SAMR) has released implementing regulations and more detailed guidelines. On 24 March 2023, SAMR issued:

- Regulations on the Review of Concentration of Undertakings (“Merger Control Regulations”);
- Regulations on the Prohibition of Monopolistic Agreements (“Monopolistic Agreements Regulations”);

- Regulations on the Prohibition of Abusing Dominant Market Positions (“Abusing Dominant Market Positions Regulations”); and
- Regulations on the Prohibition of Abusing Administrative Power to Eliminate or Restrict Competition.

To provide detailed guidance on the above regulations, on 5 September 2023, SAMR issued the Antitrust Compliance Guidelines for Concentrations of Undertakings (“Antitrust Guidelines”). The Antitrust Guidelines serve as an essential reference for parties involved in establishing a compliance management system for transactions.

Some highlights of the Antitrust Guidelines include the following.

- Key factors in determining “control” – the analysis of whether a transaction triggers filing requirements hinges on whether a party has gained control over the target through an M&A transaction. The Antitrust Guidelines stipulate that, even in cases where a buyer acquires a minority stake in the target, it may still be considered as acquiring “control” if it possesses veto rights on strategic decisions such as the annual business plan, budget and appointment of senior management.
- Clarification on filing timing – in the context of a greenfield joint venture project, a common question arises regarding when to seek merger control clearance. The Antitrust Guidelines specify that parties completing business registration for a newly established joint venture before obtaining clearance may be deemed in violation of legal obligations. Additionally, in cases involving multiple interrelated steps designed for the same economic purpose and mutually conditional, it is necessary to

submit notification about such transactions before the first step is implemented.

In June 2023, the SAMR released the Annual Report on China’s Anti-monopoly Law Enforcement (2022) (“2022 Report”). The 2022 Report reflects the enforcement activities of Chinese anti-monopoly and unfair competition policies in 2022. According to the 2022 Report, Chinese regulators concluded 794 cases involving concentrations of business operators, and 187 anti-monopoly cases of other types.

Company Law

On 29 December 2023, China passed certain amendments to the PRC Company Law which will take effect on 1 July 2024. While some amendments do nothing more than codify already existing judicial rules and regulatory practices, others may affect how companies in China are run in the coming years.

The amended Company Law requires shareholders of companies to inject their subscribed registered capital within five years from the company’s establishment date. Companies established before the amendments come into effect must “gradually adjust the payment timeline to be in compliance” (if they are not already in compliance). While this provision is not precise, the amended Company Law provides that PRC company registries (ie, SAMR) may require such companies to adjust their capital payment timelines.

The amended Company Law provides more flexibility in organising the management of a company, although some new requirements are also added. There is no longer a maximum number of directors, though the minimum remains three, except if the company is “relatively small in scale and number of shareholders”, in which case it

can have just one director (called “sole director” instead of the current title, “executive director”). On the other hand, a company with 300 or more employees must have at least one director selected by the employees and acting as their representative.

Instead of a supervisor or board of supervisors, under the amended Company Law, a company can now alternatively set up an audit committee comprised of an unspecified number of directors of the board that is responsible for supervising the company’s financial and accounting matters. The general manager’s powers and functions are no longer specified in the law, but rather are expected to be enumerated in the articles of association of the company or as delegated by the directors. The amended Company Law imposes enhanced liability on directors and officers, calling for the directors and officers to perform their duties and functions more diligently and carefully.

EGYPT

Law and Practice

Contributed by:

Ibrahim Shehata, Tasneem El-Naggar, Dina ElSaiedi and Salah Mohamed
Shehata & Partners



Contents

1. Metaverse p.110

1.1 Laws and Regulation p.110

2. Digital Economy p.112

2.1 Key Challenges p.112

3. Cloud and Edge Computing p.119

3.1 Highly Regulated Industries and Data Protection p.119

4. Artificial Intelligence p.121

4.1 Liability, Data Protection, IP and Fundamental Rights p.121

5. Internet of Things p.122

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.122

6. Audio-Visual Media Services p.124

6.1 Requirements and Authorisation Procedures p.124

7. Telecommunications p.126

7.1 Scope of Regulation and Pre-marketing Requirements p.126

8. Challenges with Technology Agreements p.129

8.1 Legal Framework Challenges p.129

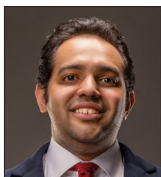
9. Trust Services and Digital Entities p.133

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.133

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



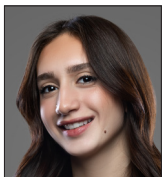
Ibrahim Shehata has accumulated a decade of experience within the Egyptian market. Starting his career with Ibrachy & Dermarkar law firm, followed by Sharkawy & Sarhan

law firm, he then moved to the US to earn a Master's degree in International Arbitration and Venture Capital from New York University. Having focused on corporate law, he successfully advised several multinational companies on doing business in Egypt. Shehata has been recognised in the last few years as one of the key players in the entrepreneurial ecosystem through working with more than 40 start-ups, helping both start-ups and venture capital firms navigate their legal issues and guiding them to be more investment-ready.



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, she has been actively working in the fintech sector by delivering strategic advice to Balad and to other start-ups in this promising sector.



Dina ElSaiedi joined Shehata & Partners in 2022. She has been involved with several key start-ups accounts and has been able to provide a business-mindset approach when

advising Egyptian start-ups. As well as interning in several top-tier law firms in Egypt, she has invested her time in learning how the legal and business fields are intertwined. Dina has proved to be an integral member of Shehata & Partners through having a keen eye for legal developments within Egypt.



Salah Mohamed recently joined Shehata & Partners. Prior to joining, Salah interned at several top-tier law firms. In addition to being the first Egyptian law student chosen by Google LLC

to participate in Google EMEA's LSI's first edition, he also ranked in the top three in the JESSUP competition 2022. Salah is now actively involved in the legal market, serving different sectors.

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



1. Metaverse

1.1 Laws and Regulation

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 of 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 EGP20 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 Ministers' 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 2024.

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 of 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

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 of 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, humid-

ity 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 licens-

ing 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.
- 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;
- 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;

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 sending 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 means 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 (the “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 EGP2 million and EGP5 million in addition to imprisonment for between one and 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 manufacturing, 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 patent; 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 techni-

cal 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 protection 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 termination 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 agree-

ment, 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 of 1968, and the Protection of Intellectual Property Rights Law No 82 of 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 and, in addition to the

Government Electronic Certification Authority (Gov-CA), the following are the licensed companies in the Arab Republic of Egypt:

- The Egyptian Co. For Digital Signature & Information Security SAE (Egypt Trust);
- El Delta Electronic Systems;
- Fixed Misr; and
- Misr for Central Clearing, Depository, and Registry (MCDR).

Moreover, the New Banking Law No 194 of 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 back-up.

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 authorises 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.

FRANCE

Law and Practice

Contributed by:

Bertrand Liard, Clara Hainsdorf, Saam Golshani and Guillaume Vitrich

White & Case LLP



Contents

1. Metaverse p.138

1.1 Laws and Regulation p.138

2. Digital Economy p.139

2.1 Key Challenges p.139

3. Cloud and Edge Computing p.140

3.1 Highly Regulated Industries and Data Protection p.140

4. Artificial Intelligence p.142

4.1 Liability, Data Protection, IP and Fundamental Rights p.142

5. Internet of Things p.145

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.145

6. Audio-Visual Media Services p.147

6.1 Requirements and Authorisation Procedures p.147

7. Telecommunications p.149

7.1 Scope of Regulation and Pre-marketing Requirements p.149

8. Challenges with Technology Agreements p.151

8.1 Legal Framework Challenges p.151

9. Trust Services and Digital Entities p.153

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.153

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 combating 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

1. Metaverse

1.1 Laws and Regulation

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, the EU Digital Services Act and the EU Digital Market 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 mat-

ter is expected to be published in July 2023 and firstly discussed in plenary session.

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, including 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. However, since 25 August 2023, the DSA must

be respected by online platforms and search engines with more than 45 million monthly active users ("very large online platforms" and "very large online search engines") in the European Union (EU).

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 (the "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.

On 6 July 2023, the European Commission published the list of seven companies that have identified themselves as "gatekeepers". Attributed to digital platforms capitalised to more than EUR75 billion on the stock market or with a turnover of more than EUR7.5 billion in Europe, the concerned platforms will then have to comply with the new DMA regulatory framework by 6 March 2024.

Digital Governance Act

Like the Data Act, the Digital Governance Act (DGA) is part of the European Data Strategy, presented by the European Commission in February 2020. This strategy aims to develop a single data market by supporting responsible access,

sharing and reuse, in compliance with EU values and in particular the protection of personal data.

The DGA was adopted in May 2022 and has been applicable since 24 September 2023, with a compliance obligation for entities providing data intermediation services by 24 September 2025 at the latest. The text aims to promote the sharing of personal and non-personal data by setting up intermediation structures and concerns all sectors of activity, public and private, without restriction given the nature of the data. It includes a framework facilitating the reuse of certain categories of protected public sector data (confidential commercial information, intellectual property, personal data); regulates the provision and sharing of data services by imposing notification obligations (private as well as public) and compliance obligations on the operators of these services; and develops a framework for the voluntary registration of entities that collect and process data provided for altruistic purposes.

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.

After the opinion of the French Competition Authority on the potentially anti-competitive practices of 29 June 2023 concerning the cloud computing companies, the French Parliament adopted the bill “Secure and Regulate the Digital Space” on 17 October 2023. This law makes provision for the interoperability of cloud services, the prohibition of data transfer fees and the time limitation of cloud credits, in particular to align with the provisions of the Data Act.

Cybersecurity Implications

Cloud service providers are qualified as “digital service providers” under the EU Directive Network and Information Security (the “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 frame. 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 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.

With the aim of rebalancing competition between the various players and strengthening the control of personal data by the data subjects, the DMA prohibits access controllers for certain practices including the use of cross-linking of personal data from the various services provided by the access controller and the registration of end users to other services of the access controller in order to combine their data, unless the end users consent. The DMA is also intended to condition the access and use of the data provided or generated but also to strengthen the transparency obligations on profiling practices.

Additionally, in order to encourage internet users to know the realities of IT risks on the sites they consult, the French law of 3 March 2022 introduced a cyberscore. Effective since October 2023, the cyberscore will be displayed on web-

sites in order to warn the internet user of the security of the latter and the data hosted. To obtain this cyberscore, companies must carry out audits with providers qualified by the ANSSI.

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.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures to ensure a high common level of cybersecurity throughout the Union,

amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1772, and repealing Directive (EU) 2016/1148 (the “SRI Directive 2”), creates a common regulatory framework to ensure a high level of cybersecurity across the Union, known as the NIS2. The directive requires EU member states to strengthen their cybersecurity capabilities and introduces cybersecurity risk management measures and reporting in critical sectors, as well as rules on co-operation, information sharing, supervision and enforcement. The Directive must be transposed into national law by 17 October 2024.

The rules should apply from 18 October 2024. The Directive applies mainly to medium and large entities operating in high-criticality sectors, which explicitly targets banking and financial infrastructures such as credit institutions, trading platform operators and central counterparties.

4. Artificial Intelligence

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.

On October 2023, in order to clarify the rules applicable in AI, the CNIL published a first set of guidelines for the use of AI that complies with personal data protection requirements. These will be followed by two others, which will supplement them on other issues raised by the AI sector. Finally, in November 2023, the CNIL selected four AI projects aimed at improving public services. These winners will receive personalised support over a period of several months. The CNIL will also be advising four other projects that are also of interest in terms of data protection.

Responsibility/Liability

As AI can take decisions with a degree of autonomy, a key legal issue is responsibility/liability. As far as 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. In a press release published on 9 December 2023, the Council of the European Union claimed to have reached an agreement with the Parliament on the first AI rules in the world. The AI legislation harmonises rules for AI systems, ensuring they are safe and respect EU fundamental rights and values. The final text must now be formally adopted by the Council and the Parliament, as EU co-legislators. Finally, AI legislation is expected to apply from 2026.

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 damage 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 protec-

tion 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 new challenges to consumers as well as 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 (the “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.

On 27 November 2023, the Council of the European Union finally adopted the Data Act, laying down harmonised rules for fair access to and fair use of data. It specifies who can access and use data generated within the EU in all economic sectors. It aims to:

- ensure fairness in the distribution of the value generated by data between players in the digital environment;

- stimulate the development of a competitive data market;
- open up opportunities for data-driven innovation; and
- make data more accessible to all.

Following the formal adoption by the Council, the new Regulation will become applicable 20 months after its effective date. However, the requirements for simplified access to data for new products will only apply to connected products and related services placed on the market 32 months after the date of entry into force of the Regulation.

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 protection legislations) also recommends proceeding to Data Protec-

tion 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 one 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 Commission proposed a regulation aiming to reinforce the security of hardware and software marketed in the European Union, and to protect consumers and businesses who purchase or use products or software with a digital component. This is the Cyber Resilience Act. At the end of November 2023, the Council and Parliament reached a provisional agreement, concerning manufacturers' responsibility in relation to product compliance, the vulnerability treatment process, or obligations in terms of product security transparency. In the same context, ANSSI published its recommendations on the security of connected objects, which, on the one hand, aim 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, provide 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 to 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 Direc-

tive (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 AVMS 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.

On 15 December 2023, the European Parliament and the Council reached a political agreement on the European Media Freedom Act. These new rules will better protect editorial independence, media pluralism, ensure transparency and fairness, and bring better co-operation of media authorities through a new European Media Board. The political agreement is now subject to formal approval by the European Parliament and the Council.

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 the 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 regime 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 down 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. Given 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). On 23 November 2018 (No 15/19053), the Paris

Court of Appeal handed down a decision confirming that, when an IT project involves the integration of software, an obligation of result cannot be imposed on the service provider, unless otherwise stipulated in the contract (in this case, the customer was claiming an obligation of result with regard to the installation of the software proposed by the service provider), since the success of the project largely depends on the active collaboration of the customer at each stage of its implementation.

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.

In relation to 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 (the “eIDAS Regulation”) and the French Civil Code.

Three categories of electronic signatures exist pursuant to the eIDAS Regulation. Advanced electronic signatures are 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 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, including a reference of security requirements of 11 August 2022.

GREECE

Law and Practice

Contributed by:

Nikos Nikolinakos, Dina Kouvelou and Alexis Spyropoulos

Nikolinakos & Partners



Contents

1. Metaverse p.157

1.1 Laws and Regulation p.157

2. Digital Economy p.159

2.1 Key Challenges p.159

3. Cloud and Edge Computing p.161

3.1 Highly Regulated Industries and Data Protection p.161

4. Artificial Intelligence p.163

4.1 Liability, Data Protection, IP and Fundamental Rights p.163

5. Internet of Things p.165

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.165

6. Audio-Visual Media Services p.168

6.1 Requirements and Authorisation Procedures p.168

7. Telecommunications p.170

7.1 Scope of Regulation and Pre-marketing Requirements p.170

8. Challenges with Technology Agreements p.172

8.1 Legal Framework Challenges p.172

9. Trust Services and Digital Entities p.174

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.174

Nikolinakos & Partners is an Athens-based law firm known for its strong foundation in regulatory, transactional and litigation matters. The firm specialises in various practice areas, including TMT, digital business, emerging digital

technologies (eg, artificial intelligence and IoT) and robotics, data privacy and cybersecurity, competition law, corporate compliance, intellectual property, administrative law/public procurement and tech litigation.

Authors



Nikos Nikolinakos is the managing partner of Nikolinakos & Partners, and co-head of the competition law, TMT and digital business practices. He provides regulatory and policy advice in

the TMT sector, and on EU/national competition law, data protection and cybersecurity, emerging digital technologies, robotics, IP rights advocacy and compliance. Nikos was previously the legal and regulatory affairs director for a major telecoms operator and internet provider, and a senior in-house adviser to the Telecoms & Post Commission of Greece. He has held senior consulting roles in various international projects for governments, national regulatory authorities, market players and the European Commission.



Dina Kouvelou is a partner at Nikolinakos & Partners, where she heads the data protection and cybersecurity practice and co-heads the competition law, TMT and digital business

practices. Her professional career has spanned TMT, data protection and cybersecurity, betting and gaming, competition law and corporate/commercial law. She was previously general counsel and head of legal and regulatory affairs in a leading alternative fixed telecoms operator; senior competition law and regulatory policy adviser in the legal department of the Telecoms and Post Commission of Greece; and legal consultant in tech regulatory, competition law and commercial law projects with Greek and international law firms and consultancies.

Contributed by: Nikos Nikolinakos, Dina Kouvelou and Alexis Spyropoulos, **Nikolinakos & Partners**



Alexis Spyropoulos is a partner at Nikolinakos & Partners, and head of the administrative law and public procurement practice. From 2007 to 2015, he acted as head of the legal department of the Greek Telecoms and Post Commission, handling numerous complaints, actions and infringement proceedings. Alexis is experienced in representing undertakings and government bodies in all kinds of proceedings (including competition law and data protection issues) before administrative courts and regulatory authorities. He has extensive experience in the fields of TMT, administrative law, data protection and competition law.

Nikolinakos & Partners Law Firm

182, Mesogeion Avenue
P.C. 15561
Athens
Greece

Tel: +30 2130 020 020
Email: nikolinakos@nllaw.gr
Web: www.nllaw.gr

NIKOLINAKOS
& **PARTNERS** LAW FIRM

TECH

1. Metaverse

1.1 Laws and Regulation

Concept

The metaverse is a term describing a hypothetical enhanced digital environment, which is more immersive, interactive and interconnected than the internet today. It is a shared virtual space where users can create, interact and transact with each other in real time, using advanced technologies such as virtual and augmented reality, blockchain and artificial intelligence.

While this development seems exciting, the metaverse brings several legal and regulatory challenges that have either not been addressed or need to be revisited. Some of these issues relate to the collection of personal data, cybersecurity and intellectual property, but many more are likely to arise in the future.

Laws and Regulations

There is currently no specific legislative framework that applies exclusively to the metaverse in Greece. Nonetheless, the relevant technology is already regulated to some extent by existing laws and regulations both in Greece and in the EU, the main of which include:

- Regulation (EU) 2022/2065 (Digital Services Act);
- Regulation (EU) 2022/1925 (Digital Markets Act);
- “Proposal for a Regulation [...] laying down harmonised rules on artificial intelligence (AI) and amending certain union legislative acts”, COM (2021) 206 final (AI ACT) (if adopted);
- “Proposal for a Directive [...] on adapting non-contractual civil liability rules to artificial intelligence”, COM (2022) 496 final (AI Liability Directive) (if adopted);

- Regulation (EU) 2016/679 (GDPR) and implementing Greek Law 4624/2019; and
- Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification [...] (Cybersecurity Act).

Data Protection

A key legal challenge that arises in the context of the metaverse concerns the processing and protection of personal data. In order to provide the user with an unparalleled immersive experience, a substantial amount of personal information about their habits, behavioural patterns and general communication is collected, with concurrent processing of biometric data. This highlights the essential need for platforms to comply with the GDPR, particularly given that biometric data resides within the special categories of personal data, thereby raising the issue of the legal basis supporting its processing.

An important and simultaneously difficult issue arises with regard to the definition of the roles and responsibilities concerning personal data governance within the metaverse – namely, the roles of data controller and data processor – as in such a multi-layered environment it may not always be clear who actually determines the purpose for the processing of such data.

Moreover, a pivotal concern involves the procurement of user consent and the obligation to notify users comprehensively regarding the protection of their privacy, as well as the point in time at which the information and consent will be given accordingly. On the other hand, excessive effort to comply with the GDPR may result in users being unable to comprehend any complex and obscure terms of use.

Finally, it is important to note that the geographical scope of the GDPR is precise, as outlined in Article 3 thereof, so the applicable law may vary depending on the area of the virtual world used by the user, creating issues regarding the competence of authorities, legal uncertainty and the precariousness of rights.

Cybersecurity

Within the metaverse, prevailing cybersecurity challenges encompassing phenomena such as phishing, malware and hacking will intensify, deviating from contemporary internet-based attacks and threats. Cybersecurity issues may also arise in the main economic pillars of the metaverse, notably cryptocurrencies and non-fungible tokens (NFTs), and the risk of counterfeit or hacked avatars is imminent, posing problems such as deepfakes, identity theft and various challenges to identify virtual crimes.

However, cybersecurity legislation such as Directive (EU) 2022/2555 (NIS 2) has been introduced, which aims, inter alia, to ensure a high level of cybersecurity and cyber-resilience within the EU. Meanwhile, the “Proposal for a Regulation [...] on horizontal cybersecurity requirements for products with digital elements, COM (2022) 454 final (EU Cyber Resilience Act) could also be implemented once adopted, and has the potential to significantly enhance cyberprotection within the metaverse. The NIS 2 Directive replaces Directive (EU) 2016/1148, which was incorporated into Greek law through Law 4577/2018, which remains in force. Within the broader cybersecurity framework, the following laws may also apply:

- Greek Law 5002/2022 regarding the procedure for the lifting of communications secrecy, cybersecurity and data protection; and

- Greek Law 4961/2022 on “Emerging information and communication technologies, strengthening digital governance and other provisions”.

Moreover, essential operations within the metaverse are executed through Virtual Reality (VR) and Augmented Reality (AR) devices, like virtual reality headsets. Therefore, the devices themselves should maintain a robust level of security and be constantly updated for new security patches. These devices are categorised as consumer products and may not fall within the scope of the NIS 2 Directive, but they do fall within the scope of the General Product Safety Regulation (EU) 2023/988, which refers, inter alia, to the existence of appropriate cybersecurity features for product protection.

Intellectual Property

The challenges posed by the metaverse in the field of intellectual and industrial property, such as unauthorised use of registered trade marks, copyright violations, jurisdiction and classification issues, also cannot be ignored. The metaverse provides a variety of virtual goods and services, all of which are either copied from the physical world or created, and are therefore subject to intellectual property laws and/or in need of protection. However, the challenges associated with tracking and enforcing intellectual property rights (IPR) have historically proven difficult and are anticipated to persist in the future.

With the underlying technology itself being subject to extensive patents, together with the introduction of innovative assets like digital collectibles documented via NFTs, new and unique intellectual property issues are emerging. For example, the utilisation and exploitation of previously licensed or acquired IPR, particularly by

licensees, poses challenges regarding the scope of rights acquired under pre-existing contracts in the metaverse.

Legal issues also arise in the area of trade mark registration, and many companies have filed trade mark applications to enter the metaverse and the world of NFTs. As a result, trade mark owners face uncertainty in industrial property law due to the significant barriers to the successful detection of counterfeiting and the enforcement of trade mark rights that exist in the metaverse, such as the difficulty of identifying infringers. In Greece, full authority and responsibility for trade marks is assumed by the Hellenic Industrial Property Organisation according to the provisions of Law 4679/2020, entitled “Trademarks – transposition of Directive (EU) 2015/2436 on the approximation of the laws of the Member States relating to trademarks and Directive 2004/48/EC on the enforcement of IPR and other provisions”.

In addition, there are a number of intellectual property issues related to AI, which can obtain data from copyrighted works and reproduce it in an algorithmically automated way in the metaverse, without compensating the authors. In this context, technologies such as blockchain could be integrated into AI systems, making it possible to identify copyrighted, trade marked or patented content that has been used by AI. At the same time, creators and consumers of the metaverse have an obligation to respect the rights of copyright holders to the exclusive exploitation of their IPR within the metaverse. In Greece, copyright is protected by virtue of Law 2121/1993 on “Copyright, Related Rights and Cultural Matters” and Law 4481/2017 on “Collective management of copyright and related rights, multi-territorial licensing in musical works for online use in the internal market and other

issues falling within the scope of the Ministry of Culture and Sports”.

The Hellenic Copyright Organisation is the national competent authority responsible for safeguarding the rights of authors and right holders in the field of copyright and related rights.

2. Digital Economy

2.1 Key Challenges

Directive 2000/31/EC was incorporated into Greek law by Presidential Decree 131/2003 and establishes rules on a number of issues in the European Union concerning electronic commerce and the provision of information society services. This law includes regulations relating to the establishment of service providers, the information that the provider is obliged to provide to the recipients of the service, commercial communications and advertising, the conclusion of contracts by electronic means, and the liability of providers for illegal content circulated on their platforms.

In December 2020, a proposal for a Digital Services Regulation was published, which essentially updates the E-Commerce Directive. Following the adoption stages, the Digital Services Act (Regulation 2022/2065) was published on 27 October 2022 and is directly applicable in Greek law. The Regulation will progressively enter into application by 17 February 2024, and addresses issues such as:

- measures to deal with illegal content online;
- the traceability of marketers;
- the prohibition of misleading practices and specific types of targeted advertising;
- the liability of online intermediaries for third party content;

- the safety of users online; and
- due diligence obligations for different service providers depending on their size.

In addition, Articles 3b and 3ba of Law 2251/1994 contain provisions regarding the information that the supplier must provide to the consumer prior to the conclusion of a sales contract. Articles 3c and 3d set out the formal requirements for distance contracts.

Directives No 2019/770 on the supply of digital content and services and No 2019/771 on the sale of goods are part of the EU's effort to regulate digital markets from a competition law and consumer protection perspective. Directive 2019/770 was incorporated into Greek law by Law No 4967/2022, while Directive 2019/771, which establishes rules for contracts for the sale of goods with digital elements, has been incorporated into the Civil Code by Law No 4967/2022 and a small part of it in Law 2251/1994.

In the digital economy, the general rules on competition (mergers, acquisitions, abuse of dominant position) apply in the field of competition. In Greek law, EU Regulation 2019/1150 – also known as the P2B Regulation – is directly applicable and seeks to establish transparency and fair treatment for business users who use the platform as a channel for selling or promoting their business and their products, highlighting the obligation for transparent and detailed terms of use. It includes, inter alia, the obligation for platforms to post the ranking and promotion mechanisms of entrepreneurs, etc. Articles 4–8 of Law No 4753/2020 designate the Interdepartmental Market Control Unit at the Ministry of Development and Investment as the competent supervisory authority for the implementation of the Regulation.

Finally, following the initial proposal of the European Commission in December 2020, Regulation (EU) 2022/1925 (DMA) was adopted by the European Parliament and the Council on 14 September 2022, and was published in the Official Journal on 12 October 2022. The DMA entered into force on 1 November 2022 and became applicable on 2 May 2023. It is one of the first regulatory tools to comprehensively regulate the gatekeeper power of the largest digital companies. The DMA complements but does not change EU competition rules, which continue to apply fully.

Digital Services Act

The Digital Services Act (Regulation (EU) 2022/2065) entered into force on 16 November 2022 and will be enforced through a pan-European supervisory architecture. According to the Regulation, member states shall designate one or more competent authorities as being responsible for the supervision of intermediary service providers and the enforcement of this Regulation (“competent authorities”).

Member states shall designate one of the competent authorities as their digital services coordinator, which will be responsible for all matters relating to the supervision and enforcement of this Regulation in that member state, unless the member state concerned has delegated certain specific tasks or areas to other competent authorities. In any case, the digital services coordinator shall be responsible for ensuring coordination at the national level in relation to those issues and for contributing to the effective and consistent supervision and enforcement of this Regulation throughout the EU.

Greece shall designate its digital service coordinators by 17 February 2024. It is therefore expected that a legislative act will be adopted

empowering the competent authority to be responsible for the supervision of intermediary service providers and the enforcement of this Regulation.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Law 4727/2020 on Digital Governance defines cloud computing as a service standard that enables internet access to an expandable and flexible group of shared physical or virtual resources. The provision of the service is based on the needs of the user, and the management of resources by the service provider is done only at the request of the user. Law 4727/2020 references the following models of cloud computing.

- **Public:** services are potentially available to any customer and the resources of the service are controlled by the service provider. A public cloud can be owned, managed and operated by a business, academic or governmental organisation, or by a combination thereof. The computing infrastructure is located on the premises of the service provider.
- **Private:** services are used exclusively by a single organisation and resources are controlled by that organisation. A private cloud can be owned, managed and operated by the organisation itself or by a third party, and the computing infrastructure may be located on-site or off-site. The private cloud service provider may allow access to other parties.
- **Hybrid:** uses at least two different cloud computing service models. The two services remain unique but are interconnected by the appropriate technology that enables interoperability, data and application portability. A hybrid cloud can be owned, managed and

operated by the organisation itself or by a third party, and can be located on-site or off-site.

The Ministry of Digital Governance is responsible for determining the use of cloud computing infrastructure by public sector bodies and for defining criteria for the selection of techniques and methods for the use of cloud services. To promote the use of cloud services by public administration, the Ministry will design and launch a digital marketplace of cloud services and applications where public sector bodies and cloud service providers will be registered, where cloud service providers will post the cloud services they provide, the technical details and the costs of procurement.

Public Administration

With regard to the public administration sector, Law 4623/2019 and Law 4727/2020 contain provisions concerning the acquisition and use of cloud computing services by public administration in Greece.

In particular, the General Secretariat of Public Administration Information Systems (GGPS-DD), the National Network of Technology and Research Infrastructures (EDYTE) and the Digital Governance of Social Insurance (HDIKA) must prioritise the acquisition of cloud computing services for all public sector entities over other technological solutions, for storing data, hosting information systems and other specified activities. Every new information system of public sector entities must be accompanied by a data classification study.

The provision of digital public services by public sector bodies is carried out through:

- the central infrastructure of the Government Cloud of the Public Sector (G-Cloud), managed by GGPSDD;
- the Government Cloud of the Research and Education Sector (RE-Cloud), managed by EDYTE; and
- the Government Cloud of the Health Sector (H-Cloud), managed by HDIKA.

The entities responsible for the management of the government clouds must each retain a digital register of the central electronic applications and the central information systems installed in the respective cloud. The government cloud computing systems may be interconnected to provide optimal public services and to create back-up, business continuity and disaster systems, in compliance with the provisions of the legislation on personal data protection.

All central electronic applications and information systems that relate to transactions between public administration and natural or legal persons or legal entities, and that are maintained by all ministries (except for the Ministry of Health and the Ministry of Education and Religious Affairs), public sector bodies (other than hospitals and health centres), independent authorities and Information Society S.A., must be installed on the G-Cloud by 1 January 2025. By the same date, all electronic applications and central information systems of the Ministry of Education and Religious Affairs and its supervised bodies, as well as those offered by the Ministry to the education and research community, must be installed on the RE-Cloud. The same applies for the applications and central information systems of the Ministry of Health, hospitals and health centres, concerning the processing of medical data and citizens' medical transactions. GGPSDD, EDYTE and HDIKA must provide service level agreements to the above-mentioned entities.

With regard to the financial services sector, specific provisions on the use of cloud services are included in Act 2577/2006 and Act 2597/2007 of the Governor of the Central Bank of Greece on internal control and privacy systems for the banking sector, and also in Law 3431/2006 and Law 2472/1997, to the extent that they do not conflict with the GDPR.

GDPR

In Greece, personal data protection in cloud services is regulated by the GDPR, along with Law 4624/2019 implementing the GDPR, which introduces specific criminal penalties for the illegal processing of personal data, in addition to the administrative penalties provided under the GDPR.

According to the GDPR, the parties involved in the provision of cloud services are obliged to provide transparency on the purposes of data processing, to ensure that data subjects can exercise their rights and can clearly identify the roles of data controllers and data processors. The latter is particularly challenging in cloud computing, with great variations between B2B and B2C cases. In B2C cloud services, the cloud provider is usually the data controller collecting and processing personal data relating to end-customers; in B2B, where businesses act as customers, they are considered data controllers with the cloud providers acting as data processors, even though the business customers do not have full control of the infrastructure used for the processing.

The GDPR also requires cloud providers to use suitable technical solutions to ensure the appropriate level of security depending on the nature of data and to have mechanisms in place for data breach notifications and to prevent them from transferring this data to third parties unless

an adequate level of data protection is proven to be in place.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

Law 4961/2022 on “Emerging Information and Communication Technologies, Strengthening Digital Governance and Other Provisions”

This is the legal instrument regulating AI in Greece. There are also legislative proposals on the EU level regarding AI-related issues (ie, the AI Act), in order to establish harmonised EU-wide rules for AI.

The proposal of the AI Act was published by the EU Commission in 2021 to set a gradual regulatory framework, in which various AI systems are subject to requirements and obligations depending on the risks associated with them. The proposed AI Act contains a classification of regulatory requirements depending on the inherent risk associated with the AI system being used, namely:

- prohibited AI practices;
- high-risk AI systems; and
- low-risk systems.

In December 2023, the EU Parliament reached a provisional agreement with the EU Council on the AI Act. The draft Regulation aims to ensure that AI systems placed on the EU market and used in the EU are safe and respect the fundamental rights and values of the EU.

The main new elements of the provisional agreement can be summarised as follows:

- rules for the general purpose AI models of high impact that may pose a systematic risk in the future;
- a governance system with some enforcement powers at EU level;
- an extension of the list of prohibitions, with the possibility for law enforcement authorities to implement remote biometric identification in public places, subject to safeguards; and
- a wider protection of rights by requiring operators developing high-risk AI systems to carry out an impact assessment regarding fundamental rights before using an AI system.

In Greece, Law 4961/2022 introduced rules and obligations for organisations in both the private and public sectors that use AI systems, as outlined briefly below.

Obligations of public sector bodies

The use of AI systems by public sector bodies in the exercise of their functions, in decisions or actions that affect the rights of a natural or legal person, is permitted only if it is expressly provided for in a specific provision of law containing appropriate safeguards for the protection of those rights.

Before they become operational, public bodies must conduct an algorithmic impact assessment of the AI systems, and also have transparency obligations, consisting of the public provision of information on the exercise of the information rights of natural persons and the provision of information to the natural or legal persons concerned by the decision or the action in an intelligible and easily accessible form.

Each public sector body is required to keep a register of the AI systems it uses, including the information specified by the law. The register is updated annually and in any event when a new

system is put into operation. Each public sector body shall make that register available to the National Transparency Authority upon request.

Obligations of private sector bodies

Before the first use of the AI system related to existing or prospective employees, each undertaking is required to provide said employees with relevant information.

Each medium-sized or large entity is required to establish and maintain an ethical data use policy and to keep a register of the AI systems it uses.

The law also provides for obligations of contractors in public contracts for the design or development of an AI system, regarding the provision of information to public bodies and to affected natural or legal persons, the delivery of the AI system to the operator with specified terms and the adoption of appropriate measures for the compatibility of the system with the legal framework.

Data Protection

Since AI systems analyse vast amounts of data to function and improve their performance, whenever personal data forms part of the large pools of data used in an AI system's algorithmic decision-making process, this activity must abide by Law 4624/2019 and the GDPR.

Data subjects have the right to object to decision-making based solely on automated processing, including profiling. Where such decision-making exists, meaningful information about the logic involved in the process, as well as its significance and its envisaged consequences, should be provided to the data subjects.

According to Law 4961/2022, organisations must comply with all data protection require-

ments arising from the GDPR and this law. Specifically, they must carry out a Data Protection Impact Assessment, inform affected individuals and ensure that all data subjects' rights are respected.

Liability

The Greek Civil Code sets out five conditions that need to be fulfilled for tortious liability to be attributable to a party:

- human behaviour;
- illegal action;
- fault;
- damage;
- causal link between the behaviour and the damage.

Where a system operating in the spectrum of autonomy causes damage, a number of these conditions are challenging to substantiate, particularly determining a party's fault and the causal link between the human behaviour and the damage that occurred. In addition, all AI technologies in Greece should meet the essential health and safety requirements laid down in the EU safety legislation, as it has been transposed into Greek law.

The EU product liability regime is complementary to the product safety regime. It was introduced by the Product Liability Directive (Directive 85/374/EEC) and was implemented by amendments to the Greek Consumer Protection Law 2251/1994. The existing framework is also applicable to new digital technologies. The Greek Consumer Protection Law establishes a strict liability regime under which producers of defective products are held liable when such products cause damage to natural persons or their property, while the injured consumers are not required to prove the fault of the producer.

So far, the current legal framework of extra-contractual liability can be applied to damages caused by AI. However, as the new generation of AI edges closer to operational autonomy and behavioural unpredictability through their capacity to analyse and learn from their environments, assigning legal responsibility for harmful actions is bound to present a point of contention across most jurisdictions, as the natural person at fault for damage caused by an AI system will become increasingly difficult to identify.

In the absence of a specific tortious liability regime covering advanced AI, businesses and organisations that aim to operate in the nascent AI scene in Greece should act in a proactive manner, contractually regulating liability for such systems and investing in insurance coverage.

Intellectual Property

Greek Copyright Law 2121/1993 is human-centric as it is traversed by the “principle of truth”, according to which only a natural person shall be considered as the author of a work.

The copyrightability of computer programs depends on whether they can be considered the “author’s own intellectual creation” – namely, where the author made “free and creative choices” while creating the work. Therefore, devices cannot be recognised as “authors”, and any work they produce cannot qualify as copyright-protected content.

Computer-generated and AI works may only be protected if the prerequisite of “human intervention” is fulfilled (ie, through the selection of the data to be entered into a machine or of the parameters determining the objective of the machine’s activity); inversely, works autonomously and exclusively produced by information technology systems are not copyrightable.

Accordingly, non-humans are not awarded protection. The creation of works by AI systems in whole or in part is expected to pose significant challenges to IPR in the near future. However, it is not yet clear how such copyrights could be enforced or enjoy their own copyright protection.

There are two cases where legal persons are recognised as potential copyright holders over a work: for computer programs and for databases where it is clearly provided that the maker of a database enjoying the *sui generis* right over its content is either the natural or the legal person taking the initiative and bearing the risk of the “substantial investment”. Moreover, computer programs are excluded from patentability according to Law 1733/1987. The legal definition of an invention for which patent protection may be sought (including inventions embodied in software) requires novelty, inventive activity and the susceptibility of industrial application.

For all these reasons, and in the absence of a tailor-made legal framework, issues of ownership and the transfer of rights in such work should be regulated by contract, through appropriate and detailed contractual clauses.

5. Internet of Things

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

In Greece, there is currently no specific legislation solely for governing the internet of things (IoT). However, chapters (B) and (C) of part (B) of Greek Law 4961/2022 on “Emerging information and communication technologies, strengthening digital governance and other provisions” contain definitions and provisions regarding the use of IoT technology.

According to Law 4961/2022, IoT is any technology that:

- enables devices or a group of interconnected or related devices, through their connection to the internet, to perform automatic processing of digital data on a programmed basis, including technology that involves the interconnection of physical things, in particular appliances, vehicles and buildings, with electronic components, software, sensors, actuators, radio links and network connectivity; and
- enables the collection and exchange of digital data in order to offer a variety of services to users, with or without human involvement.

Data Privacy

Law 4961/2022 mandates that the processing of personal data related to the operation of IoT technology devices shall be carried out in accordance with EU and Greek legislation, and in particular in accordance with the GDPR, Law 4624/2019 implementing several provisions of the GDPR and Law 3471/2006 on the protection of personal data and privacy in the sector of electronic communications.

In its annual report for 2021, the Hellenic Data Protection Authority (HDPa) noted that emerging technologies including IoT will affect compliance with the GDPR in the coming years. Cutting-edge issues such as risks from machine learning, facial recognition and profiling are high-priority issues for supervisory authorities.

Furthermore, during a seminar marking European Data Protection Day, the HDPa addressed issues related to personal data within the IoT context. Among the risks to privacy and personal data protection, the highlighted concerns included:

- use for secondary purposes;
- the creation of individual profiles;
- detailed monitoring;
- automated decision-making;
- the lack of the possibility to remain anonymous;
- the lack of security;
- portability; and
- issues of consent.

Cybersecurity

Law 4961/2022 provides that IoT devices shall be designed and developed in such a way as to achieve an appropriate level of cybersecurity throughout their lifecycle and to prevent attempts by unauthorised third parties to alter their use or performance, and shall incorporate measures to ensure an appropriate level of cybersecurity, such as:

- the use of secure passwords;
- timely updates of software from reliable sources;
- the encryption of critical security data in transit, including remote access control and management data;
- identification by the IoT operator of a public contact point to which users can report device security incidents; and
- the provision of a vulnerability or security incident notification policy or procedure.

Law 4961/2022 also imposes legal obligations on manufacturers, importers, distributors and operators of IoT technology devices, as follows.

Manufacturers, importers and distributors

IoT devices intended to be made available to IoT operators must be accompanied by:

- a declaration of conformity by the manufacturer, stating the conformity of the device with the technical safety specifications;
- an instruction and safety information manual in terminology easily understood by end-users – the instructions shall include the information required for the safe installation, configuration and operation, depending on the intended use of the device, as well as a record of possible risks in case of non-compliance; and
- a procedure for the management of cases where an incident or a security vulnerability is identified by users – the management process shall include appropriate documentation from the manufacturer on the nature and likely occurrence of such incidents or vulnerability, detailed instructions for dealing with them, and appropriate measures to mitigate any adverse consequences.

Before making the IoT device available to IoT operators, importers and distributors must verify that the device is accompanied by the declaration of conformity. When they become aware that an IoT device does not conform with the technical safety specifications, importers and distributors shall refrain from making such device further available until it does.

If the National Cybersecurity Authority (NCA) finds that an IoT device presents a risk relating to the security of its operation or to the security of the operator's network and information systems, despite complying with the necessary technical security specifications, it orders the manufacturer, importer and distributor to take all necessary measures to withdraw the device within a reasonable period of time, depending on the nature of the risk, and to ensure that the device will not present a risk when made available again to the IoT operator.

IoT operators

Law 4961/2022 introduces measures for the transparent and safe operation of IoT devices used by essential service operators and digital service providers acting as IoT operators. Such IoT operators are required to use IoT technologies in accordance with the technical security specifications, including cybersecurity measures specified by law, and bear several obligations under this legislation.

- Operators are required to designate an IoT Security Officer to be responsible for monitoring the proper implementation of the technical and organisational measures, and for maintaining the log created by the device for a reasonable period of time, in accordance with the purpose of its use.
- Operators must keep a register of the IoT technology devices they use (the "register of connected devices"), which must be updated on an annual basis and, in any case, when they start using a new IoT device. This register is made available to the NCA or the competent response team when requested.
- Transparent information: IoT operators must ensure that users of IoT devices are provided with information on their secure installation, configuration and operation in a concise, transparent, intelligible and easily accessible form, as well as detailed instructions for checking device security. They must also ensure that users are involved in the installation and operation of the devices as little as possible.
- If the IoT Security Officer suspects that an IoT device presents a risk, they shall make a recommendation to the operator, who shall in turn inform the NCA, the competent response team, the manufacturer, the importer and the distributor of the device and suspend the use of the device to the extent necessary.

- Upon being notified by the NCA, IoT operators must without delay suspend the use of any IoT device that the NCA has found presents a risk relating to the security of its operation or to the security of the operator's network and information systems, despite complying with the necessary technical security specifications.
- IoT operators must carry out an impact assessment of the envisaged processing operations of personal data related to the operation of the IoT device, in accordance with Article 35 paragraph 1 of the GDPR.

National Cybersecurity Authority

The NCA is the competent authority for supervising compliance with the IoT security framework. Its powers include:

- overseeing the compliance of IoT manufacturers, importers, distributors and operators with their obligations and requesting all necessary information;
- assessing the conformity of IoT devices with the technical specifications;
- receiving notifications from IoT operators about incidents or vulnerabilities;
- ordering IoT device manufacturers, importers or distributors to take all necessary corrective action to bring devices into conformity with the applicable legislation; and
- ordering devices presenting risks to be temporarily withdrawn from the market and replaced only after such risks have been removed.

Upon the recommendation of the NCA, the competent body of the Ministry of Digital Governance may impose sanctions on non-compliant manufacturers, importers, distributors and operators – ie, recommendations, reprimands and fines of

up to EUR15,000 or, in case of recurrence, up to EUR100,000.

Ministerial decisions shall specify the technical specifications and technical and organisational security measures of IoT devices, the obligations of manufacturers, importers, suppliers and operators of such products, and sanctions in case of non-compliance.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

The main requirements for providers of audio-visual media services falling within the Greek jurisdiction, pursuant to Articles 7–30 of Greek Law 4779/2021, include the following.

- Ensuring that identification/contact information of the provider is easily, directly and permanently accessible to the recipients of the service.
- Ensuring that the service does not contain any incitement to violence or hatred against a group of persons or a member of a group identified on the basis of race, colour, national or ethnic origin, descent, ancestry, religion, disability, sexual orientation, identity or gender characteristics.
- Ensuring the protection of minors, in terms of providers not making available content that could be harmful for their physical, mental or moral development. Measures may include appropriate age marking, selection of the time of the broadcast and age verification tools. Unjustified violence and pornography shall be subject to stricter measures. Minors' personal data cannot be processed for commercial purposes, such as direct marketing, profiling and behaviourally targeted advertising.

- Gradually making the service accessible to people with a visual or hearing disability (in particular, with the subtitling of programs and the use of sign language, auditory descriptions and spoken subtitling).
- Complying with multiple regulations with regard to audio-visual commercial communications, sponsorships, product placement, television advertising and teleshopping.

Fewer requirements apply to companies with video-sharing platform services falling within the Greek jurisdiction, and some refer to the same issues as for providers of audio-visual media services. In particular, in accordance with Article 32 of Law 4779/2021, companies with video-sharing platform services are required to take appropriate measures to protect minors from content that may have a negative impact on their physical, mental or moral development, a set of which is provided in the legislation. The obligation to protect the general public from content that incites violence or hatred against a group of persons or a member of a group identified on the basis of race, colour, national or ethnic origin, descent, ancestry, religion, disability, sexual orientation, identity or gender characteristics is also provided. Fewer obligations are provided in relation to audio-visual commercial communications.

While not required, both providers of audio-visual media services and companies with video-sharing platform services are encouraged to establish national codes of conduct with the particular aim of further protecting consumers, minors, public health and healthy competition (Article 6 of Law 4779/2021).

Pursuant to Law 4339/2015, licences for digital terrestrial free-to-air TV are granted by way of public auction. This procedure is carried out

by the National Council for Radio and Television (ESR), which issues the relevant notice. The notice specifies the conditions and the procedure for granting licences to content providers.

To qualify for participation in the auction, the applicants shall meet the following conditions set out in Articles 3–10 of Law 4339/2015:

- minimum share capital;
- registered shares;
- legal form;
- non-conviction of shareholders and members of the board for certain crimes;
- not having entered into liquidation or insolvency procedures;
- compliance with tax and insurance obligations;
- the presentation of evidence regarding the source of the financial means available for the operation of the company; and
- not exercising control over another company operating in the same media sector.

There are also some content requirements, mainly of a qualitative nature.

The tender procedure is conducted in accordance with the applicable Frequency Map of terrestrial digital broadcasting of television signals, which sets out in detail the frequencies, the transmission restrictions imposed on network providers and the permitted broadcasting centres, as well as their geographic coverage area and the technical specifications that network providers must satisfy.

The auction is carried out by way of a multi-round procedure with an increasing price on the starting price fixed in accordance with Article 2(4) of Law 4339/2015. The auction ends on the

date of the proclamation of the successful bidders. The relevant notice of the ESR determines:

- the duration of each round;
- the determination of the increase of the bid price per round;
- the obligations of the participants;
- the method of submitting offers by the participants;
- the announcement of the successful bidders;
- the method of payment of the price; and
- any other necessary details for its conduct.

TV services delivered over IP-based broadband networks are regulated by Law No 3592/2007, which is a *lex specialis* in relation to Law 2644/1998. Article 15 paragraph 3 of said law provides that services delivered via broadband networks qualify both as electronic communication services and as radio/TV services. As such, for the provision of those services, not only is approval from the ESR required, but also a General Authorisation from the Hellenic Telecommunications and Post Commission (EETT).

The licensing framework for pay-tv and radio services via satellite, cable or frequencies is outlined in Law 2644/1998, as amended. Licences to provide subscription radio and TV services are held only by *Sociétés Anonymes*. Licences are granted by decision of the ESR and the conclusion of a concession agreement with the Greek State, excluding the provision of linear television services through broadband networks, for which Article 15 of Law 3592/2007 applies. Fees vary according to the number of channels.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Local telecommunications rules that apply to electronic communication networks (ECNs) and electronic communication services (ECSs) include Law 4727/2020 – “Digital Governance (Transposition into Greek Legislation of Directive (EU) 2016/2102 and of Directive (EU) 2019/1024) – Electronic communications (Transposition into Greek Legislation of Directive (EU) 2018/1972) and other provisions” – and relevant decisions of the EETT.

Regardless of the specific technologies used to provide a network or a service, the applicability of the regulatory framework for electronic communications depends on whether the technology falls within the scope of ECNs and/or ECSs. ECNs encompass all transmission systems, whether or not they are based on a permanent infrastructure or a centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements that are not active, used to convey signals, operated for public or private use, including wireless networks (eg, mobile, Wi-Fi), cable (eg, IP broadband network) and electricity cable systems, to the extent that they are used for transmitting signals, networks used for radio and television broadcasting, and cable television networks, regardless of the type of information conveyed.

ECSs encompass any service normally provided for remuneration via ECNs, including the following types of services, with the exception of services providing or exercising editorial control over content transmitted using ECNs and ECSs:

- internet access service;

- interpersonal communications service; and
- services consisting wholly or mainly of the conveyance of signals such as transmission services used for the provision of machine-to-machine services and for broadcasting.

In Law 4727/2020, the definition of “electronic communications service” was expanded to include any interpersonal communications services provided over the internet, including VoIP services, messaging apps and email services that do not use telephone numbers, and number-based interpersonal communications services (interpersonal communications services) that connect with publicly assigned numbering resources (namely, a number or numbers in national or international numbering plans) or that enable communication with a number or numbers in national or international numbering plans.

Activity of any kind relating to the provision of electronic communications networks and/or services within the territory of Greece, with the exception of number-independent interpersonal communications services, shall be subject to a General Authorisation, in the form of a Registration Declaration to the EETT. Electronic communications activities may commence immediately upon filing a complete Registration Declaration and paying the applicable administrative fees. ECN providers pay annual fees for their General Authorisation.

Where the electronic communications activity is subject to the granting of rights to use numbers or radio frequencies, the person concerned must also obtain the required rights to use numbers or radio frequencies, in addition to the General Authorisation, before proceeding with the activity in question. More specifically, the conditions attached to the use of radio frequencies for which no granting of individual rights is required

due to the fact that the risk of harmful interference is negligible are determined in the Regulation on the Terms of Use of Radio Frequencies issued by the EETT. With the exception of free spectrum bands for all wireless services, an individual right to use frequencies is required and is granted by the competent authorities upon a relevant request being made. If there is a limited number of rights of use of frequencies, the EETT usually awards them through auctions. ECN providers pay annual fees for the rights to use spectrum and numbering resources. Spectrum licences and applicable secondary legislation specify the permitted use and the technical characteristics of the equipment that may be used, taking into account the principle of proportionality and technological neutrality.

According to Law 4070/2012 and Law 4727/2020, the EETT is the competent authority for issues concerning conditions of use and the placing on the market of terminal and radio equipment, which is regulated in Greece by Presidential Decree 98/2017, transposing Directive 2014/53/EU RED. Radio equipment includes all electrical or electronic products that deliberately broadcast and/or receive radio waves for radio-communication and/or radio-tracking purposes, or electrical or electronic products that have to be completed with a component (ie, an antenna) so as to broadcast and/or receive radio waves for radio-communication and/or radio-tracking purposes. The provisions of PD 98/2017 are not applicable to radio equipment used exclusively for activities related to public security, defence and state security. Radio equipment has to be labelled according to PD 98/2017 and Directive 2014/53/EU, and must be constructed to meet the following essential requirements:

- the protection of the health and safety of persons and of domestic animals, and the protection of property;
- the adequate level of electromagnetic compatibility; and
- effective support for the efficient use of radio spectrum in order to avoid harmful interference.

Restrictions on putting into service and authorisation of use requirements must be presented according to EU Regulation (EU) 2017/1354. No regulatory fees apply to this procedure.

The electrical, electronic and telecommunication terminal equipment used must comply with the provisions in force (such as the Low-Voltage Directive 2014/35/EU and the Electromagnetic Compatibility Directive 2014/30/EU, which have been incorporated into Greek law with the joint ministerial decisions Oik 51157/DTBN 1129/2016 and Oik 37764/873/F342/2016, respectively).

ECN providers are obliged to use radio equipment that allows for the efficient exploitation of the spectrum allocated in order to avoid harmful interference and to comply with the equipment standards established by the national and European authorities and the European Telecommunications Standards Institute.

Finally, all telecoms operators are obliged to obtain the appropriate licences for every antenna they use. The relevant framework was reviewed with Law 4635/2019 and EETT's Regulation 919/26/2019.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges Licensing Model

In Greece, technology agreements are mainly regulated by the Civil Code and the Commercial Code; as an EU member state, Greece also adheres to EU legislation.

Key Issues

Scope of the agreement

Although technology agreements usually take the form of software licences, some are much more complex. In many cases, the organisation procuring the technology services provides a solution that includes multiple components. This is important to bear in mind when drafting a technology agreement so as to avoid any ambiguity, to explicitly describe the parties' obligations, to include charges covering all the components and to foresee all possible risks that may lead to a breach of contract or exposure to liabilities. Depending on the technology agreement, various chapters of the Civil Code may be applicable (ie, sales contracts, work contracts, service contracts). Due to the rapid development of technology and services provided via the internet, one of the challenges is the impossibility to include these agreements within the categories of Greek legislation.

Customisation

Some companies prefer a customised IT solution not through a licensing model, but through a software development agreement or an SaaS agreement (or PaaS). Other companies prefer the licensing agreement with the customisation it offers; this customisation, alongside the integration that may be required, creates a new set of provisions that need to be included in the agreement, especially referring to timelines, failures,

rectifications and quality controls. In certain regulated industries, such as banking, the entities involved provide a complete set of services that an interested party may outsource to them, including technology services, applicable licences, monitoring, etc (ie, banking as a service). This type of agreement is not yet commonplace among the IT service providers established in Greece. However, due to the development of new technologies, such as AI and cloud computing, technology agreements are expected to be used frequently in the near future.

Recipient of the technology service (B2B and B2C)

A significant factor to consider is whether an IT solution will ultimately be addressed to other businesses (B2B) or to consumers and individuals (B2C). In the first case, contracts between professionals are generally ruled by the parties' freedom of contract. In the second case, however, apart from the applicable Greek law, an elaborate body of consumer laws is in place, primarily driven by EU initiatives and instruments, prohibiting unfair terms, abusive clauses and under-negotiated clauses.

Maintenance

Service level agreements must be carefully drafted to include such items as the availability uptime, back-ups, disaster recovery, schedules of maintenance, and support means and response times, while taking into account business continuity and the possibility of termination of the agreement.

Intellectual property

Software, computer programs and databases are protected by Greek Copyright Law 2121/1993, and are considered works of intellectual creations of speech, art or science. Databases are also protected by a sui generis right by the above

law, which protects the investment of manufacturers of databases. Therefore, the protection of copyright works in technology agreements (ie, software and databases) is also based on specific provisions of Greek legislation, in addition to the Civil Code.

IPR warranty and indemnities

One of the clauses that has traditionally been included in almost all software and IT-related agreements, on the IPR warranty and the provision of indemnity from the original provider, remains a necessity today, even in cloud computing agreements. The risk of a third party claiming ownership of software licensed to the organisation and thus prohibiting use of the licensed software and interrupting the business continuity is still present, and should be taken into account for indemnity provisions.

Data protection

Technology agreements often involve the processing of personal data. In these cases, the data protection legal framework in Greece must be taken into account and the parties must comply with their relevant obligations. Specifically, they shall:

- appoint the contractor as processor (Article 28 of the GDPR);
- define and implement technical and organisational measures;
- define the liability regime of the contracting parties; and
- limit the transfer of personal data outside the EEA, unless adequate safeguards are put in place.

Liabilities

All software and technology services or technology agreements include clauses that limit the liability of the provider. A technology agreement

must therefore include back-to-back provisions that fully cover intermediary parties (in B2B cases) and end-customers (in B2C cases) against the original provider of the service. The clause setting a liability cap for the provider is of major importance – this cap is usually a multiple of the contract value.

From a judicial point of view, in B2C agreements, clauses that extensively limit the liability of the professional against the consumer – especially if they have not been negotiated – are usually considered as abusive and, thus, null and void. On the other hand, in B2B agreements under which the parties usually demonstrate similar bargaining powers, the freedom of the parties supersedes, unless one party has acted maliciously or in a grossly negligent manner, or has acted without previous experience and knowledge in this type of agreement, thus demonstrating a disadvantage in bargaining.

In Greece, it is common practice for the parties that offer IT services to have insurance coverage, in order to safeguard their business in case of breaching events, such as cyber liabilities, data protection (personal data breaches) and network disruptions. The existence of these insurance agreements can increase the cost of the provision of the IT services, but they appear to be necessary in the contemporary international technology landscape. This becomes more significant in cases where the IT services are provided to regulated and supervised entities.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The legal framework regulating the delivery of trust services, the use of electronic signatures and digital identity schemes in Greece consists mainly of the Regulation (EU) 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), which came into direct effect for all EU member states on 1 July 2016, including Greece, and the ninth chapter (Articles 48–58) of Law 4727/2020 and the Regulation of the EETT on the provision of Trust Services (Decision No 837/1B/2017), which complement the provisions of the eIDAS Regulation. Also, Law 4727/2020 provides that the Ministry of Digital Governance is responsible for determining the necessary institutional and regulatory framework for trust services.

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security for electronic identification means and trust services, Regulation (EU) 910/2014 lays down the conditions under which member states recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another member state. It also lays down rules for trust services, particularly for electronic transactions, and establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services and certificate services for website authentication.

The Regulation defines “trust services” as the electronic services normally provided for remuneration and 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.

Moreover, the Regulation refers to qualified trust services – ie, trust services meeting the applicable requirements laid down in this Regulation.

Trust services are provided by a “trust service provider” – ie, a natural or legal person who provides one or more trust services either as a qualified or non-qualified trust service provider. A “qualified trust service provider” is a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body. In Greece, the supervisory body is the EETT, which also maintains an electronic record of trust service providers established in Greece.

Regulation (EU) 910/2014 and EETT decisions provide specific security requirements for trust service providers, which must take the appropriate technical and organisational measures for the security of their trust services and inform the EETT of any breach of security or loss of integrity that has a significant impact, within 24 hours of the incident.

Both the Regulation and the national law provide that trust service providers shall be liable for damage caused intentionally or negligently

to any natural or legal person due to a failure to comply with their obligations. The burden of proving the intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage, while the intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage occurred without their intention or negligence.

Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations. According to the Regulation, a qualified trust service provider providing qualified trust services must maintain sufficient financial resources and/or obtain appropriate liability insurance.

The processing of personal data shall be carried out in accordance with the GDPR and Law 4624/2019. Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.

In case of violation of the legislation regarding trust services, the EETT, after hearing the interested parties, may impose one or more of the following sanctions, depending on the gravity of the violation:

- recommendation;
- a fine up to EUR100,000; and/or
- the suspension or revocation of the rights deriving from the relevant EETT decisions for serious and repeated violations.

Electronic Signatures

An electronic signature is defined as data in an electronic form that is attached to or logically associated with other data in electronic form, and that is used by the signatory to sign. The Regulation provides for two particular types of electronic signatures:

- advanced electronic signatures – ie, electronic signatures that are:
 - (a) uniquely linked to the signatory;
 - (b) capable of identifying the signatory;
 - (c) created using electronic signature creation data that the signatory can, with a high level of confidence, use under their sole control; and
 - (d) linked to the data signed therewith in such a way that any subsequent change in the data is detectable; and
- qualified electronic signatures – ie, advanced electronic signatures that are created by a qualified electronic signature creation device, and that are based on a qualified certificate for electronic signatures.

A qualified electronic signature has the equivalent legal effect of a handwritten signature. This means that where the law or the agreement of the parties provides for the use of written form, the document with the electronic signature has the status of a private document within the meaning of Article 160 of the Civil Code and is considered, by law, as a private document according to Article 443 of the Civil Procedure Code.

The legal effect and admissibility of the simple electronic signature as evidence in legal proceedings shall not be denied under the Regulation. However, a simple electronic signature cannot be considered equivalent to a handwritten signature, since that would be contrary to Article 25, Section 2 of the Regulation, and

therefore it cannot be used as a substitute for the electronic signature in legal transactions where using the written form is mandatory. In this context, Article 16 of Law 4727/2020 expressly states that an electronic document bearing a simple or advanced electronic signature or an advanced electronic seal of its issuer constitutes a mechanical representation, within the meaning of Article 444 of the Civil Code – ie, a medium used by a computer or a computer's peripheral memory, to record, store, produce or reproduce, by electronic, magnetic or other means, information that is not directly readable, as well as any magnetic, electronic or other material on which information, images, symbols or sound are recorded, provided that these materials are intended or suitable to provide proof on facts of legal significance.

However, in cases where the use of written form is required and therefore a private document must have the handwritten signature of its issuer in order to produce evidence, a qualified electronic signature or a qualified electronic seal is required. Electronic documents with a simple or advanced electronic signature are freely evaluated as legal evidence, based on the applicable procedural provisions.

Digital Identity

Following the European Commission's proposal for the creation of a framework for a European digital identity, the European Parliament and the Council of the EU have reached a final agreement on the Regulation introducing European Digital Identity Wallets, which is now subject to formal approval by the European Parliament and the Council. The Regulation to be issued will amend the eIDAS Regulation.

The European Digital Identity will be available to EU citizens, residents and businesses that want

to identify themselves or provide confirmation of certain personal information. It can be used for both online and offline public and private services across the EU. Every EU citizen and resident in the EU will be able to use a personal digital wallet. Member states will have to provide EU Digital Identity Wallets to their citizens 24 months after the adoption of the Implementing Acts setting out the technical specifications for the EU Digital Identity Wallet and the technical specifications for certification.

In Greece, Gov.gr Wallet enables the creation, storage and control of citizens' digital documents. Digital ID cards, digital driving licences, digital disability cards, digital employment agency cards and digital ring cards are already supported. The digital documents issued through Gov.gr are fully equivalent to the paper documents, for any legal use within the Greek territory. They are not international travel documents. To create these documents, citizens connect with their personal TaxisNet codes, and a confirmed mobile phone number is required.

INDIA

Law and Practice

Contributed by:

Dhruv Singh, Shivalik Chandan, Arjun Khurana and Srijoy Das
G&W Legal



Contents

1. Metaverse p.181

1.1 Laws and Regulation p.181

2. Digital Economy p.182

2.1 Key Challenges p.182

3. Cloud and Edge Computing p.183

3.1 Highly Regulated Industries and Data Protection p.183

4. Artificial Intelligence p.185

4.1 Liability, Data Protection, IP and Fundamental Rights p.185

5. Internet of Things p.187

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.187

6. Audio-Visual Media Services p.188

6.1 Requirements and Authorisation Procedures p.188

7. Telecommunications p.189

7.1 Scope of Regulation and Pre-marketing Requirements p.189

8. Challenges with Technology Agreements p.190

8.1 Legal Framework Challenges p.190

9. Trust Services and Digital Entities p.192

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.192

G&W Legal is a full-service business law firm that assists its clients at the intersection of law and pragmatism by combining the experience of big-law with the expertise of a boutique. The firm's attorneys advise and assist clients across intersecting areas such as corporate law, intellectual property, franchising and distribution, advertising and marketing, privacy and data protection, product liability and consumer protection, international trade, foreign investment, antitrust/competition, regulatory affairs,

and dispute resolution. G&W Legal's TMT practice team has extensive experience in handling cross-border technology transactions, intricate licensing agreements, delicate data protection issues, fintech, platforms and intermediary regulations/liability, trust and safety, internet and social media, e-sports, and online gaming. The team handles all facets of data protection and privacy, traditional and new media, and digital business.

Authors



Dhruv Singh is counsel and head of G&W Legal's regulatory practice. With a wealth of experience working in-house with some of the biggest brands in the world, such as ByteDance

(TikTok), Walmart-Flipkart and Penguin RandomHouse, Dhruv uses his business-side experience as well as legal subject-matter expertise to counsel large multinationals as well as individuals and non-profits on the ever-changing privacy and data protection regulations in India, digital media and intermediary regulations, technology transactions, AI products, content moderation and a host of other issues. Dhruv holds a CIPP-E certification from the International Association of Privacy Professionals and is a certified DPO.



Shivalik Chandan is an associate at G&W Legal. He has a particular interest in tech and media law, including on issues of freedom of speech. He regularly advises on issues of intermediary safe harbour, privacy, and data protection, as well as franchising matters.



Arjun Khurana is a partner at G&W Legal. He chairs the Tech, Media and IP practice, leading on emerging issues and dispute resolution. His practice traverses privacy and data protection, emerging issues, advertising and marketing, and digital businesses, with an additional focus on dispute resolution. Arjun is a member of the International Association of Privacy Professionals and INTA's Data Protection Committee.

Contributed by: Dhruv Singh, Shivalik Chandan, Arjun Khurana and Srijoy Das, **G&W Legal**



Srijoy Das is counsel and an integral part of G&W Legal's TMT practice. He has over 27 years of experience advising multinationals expanding to and doing business in India. He is primarily responsible for the firm's Technology Transactions practice and has led teams for over 100 acquisitions in the technology sector. Srijoy has been appointed as a director by several Indian subsidiaries of large multinationals, including Bunnings Technologies India Private Limited (subsidiary of Wesfarmers Group, Australia), Fischer Systems India Private Limited (subsidiary of Fischer International, US) and Digi-Key Electronics & Automation Trading Private Limited (subsidiary of Digi-Key Corporation, US).

G & W Legal

C-9 / 9624,
Vasant Kunj
New Delhi
110070
India

Tel: +91 124 4402666
Email: srijoydas@gnwlegal.com
Web: www.gnwlegal.com



1. Metaverse

1.1 Laws and Regulation

As is the case with the laws of most other countries, there are no specific Indian laws designed to deal with the metaverse. In fact, the metaverse finds no mention and has not been defined under any Indian statute. The following regulations stand out as some of the most important from an Indian perspective.

Intellectual Property

- **Trade marks** – Trade marks may be used to protect branding and logos of brand owners from unauthorised use over the metaverse. While no cases of note have been reported in India, this is a topic that is currently getting a lot of attention. Brand-owners may consider it advisable to ensure that their interests in the virtual world are protected by way of their trade mark registrations.
- **Copyright and personality rights** – Indian copyright law potentially has the capacity to be enforced for infringements in the metaverse, as well as to protect programmes.

In an interesting case before the Honourable High Court of Delhi in 2023 (*Digital Collectibles Pte Ltd. and Ors. v Galactus Funware Technology*), the issue of the use of personality/image rights of sports players on NFTs without authorisation was dealt with in an attempt to obtain an injunction on the grounds of passing off, unfair competition, breach of personality rights, unjust enrichment and tortious interference with economic interests. In this instance, the prayer for an injunction was refused, citing it as unjust, and against the balance of convenience in the circumstances of the case.

Privacy

Pursuant to 2017's landmark judgment of the Supreme Court in *Justice K.S. Puttaswamy v Union of India*, the right to privacy has been guaranteed under the Indian Constitution. This means it may be enforced against the state. However, when it comes to private parties, it is still governed by statutes such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "SPDI Rules"), which are set to be replaced soon by the Digital Personal Data Protection Act, 2023 (DPDPA).

While the SPDI rules only require consent for the purposes of processing sensitive personal data such as sexual orientation, health data, biometrics, financial information and passwords, the DPDPA allows the processing of all personal data (not merely sensitive personal data) only on the receipt of consent of the data subject, or without consent in the event of a very limited range of legitimate purposes – such as for the purposes of responding to a medical emergency, or for the purposes of the state's performance of its obligations in furtherance of protecting sovereignty and integrity. Exactly how this is expected to play out will only become clear after subordinate legislation is published by the Indian government, which is expected later in 2024.

Intermediary Guidelines

Under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (the "Intermediary Guidelines"), intermediaries, such as app service providers, are required to comply with its provisions to be able to use their status as an intermediary as a shield against being held personally liable for illegalities perpetrated by users on their platforms. The Intermediary Guidelines place a number of diligence obligations on the intermediary,

including the need to publish user agreements and the platforms' rules and privacy policies in a comprehensible and easily accessible manner, appoint a grievance officer, put together a grievance redressal mechanism, etc.

Free Speech

As with any other form of mass communication, the metaverse is also subject to the same Indian laws as applicable to more conventional means of communication. Where it doesn't act as an intermediary, the platform would be subject to the same laws on obscenity, defamation, sedition, and hurting of religious sentiment as a normal conventional platform, such as a news channel or a magazine.

2. Digital Economy

2.1 Key Challenges

The primary areas of legislation applicable to the digital economy in India are those of data protection and consumer protection, as well as the regulatory framework for digital payments. Additionally, as discussed below, the digital economy space has seen increased scrutiny by India's antitrust regulator in the past few years.

The SPDI Rules and requirements thereunder will be applicable on all aspects of the digital economy pertaining to personal data, such as the requirement of publishing a privacy policy, consent for "sensitive" personal data, purpose limitation and data minimisation. Similarly, the DPDPA, once put into force, will also apply to all entities (whether Indian or foreign) if they are processing personal data in India or if they are pursuing personal data of Indian data subjects with an intent of offering goods/services to them.

In 2019, India's primary consumer protection legislation, the Consumer Protection Act (CPA) was amended to explicitly include e-commerce consumers within its ambit. In furtherance of extending consumer protections to the digital economy, India has also put in place specific rules which are applicable to e-commerce sellers, which has placed obligations such as a specific restriction on utilising unfair trade practices, putting in place a grievance redressal mechanism, labelling and information obligations on the website, and a restriction on cancellation charges. These rules, in addition to being applicable on e-commerce entities incorporated in India, are also applicable on foreign entities which "systematically" offer goods/services to consumers in India.

In addition to the above, the Indian government has also issued guidelines regarding the restriction of false or misleading advertisements. These guidelines regarding advertisements place specific restrictions on advertisers and advertising agencies as well as manufacturers, sellers, and traders – specific conditions have been prescribed for an advertisement to be considered non-misleading. Additionally, conditions to be met for a "bait" advertisement to be valid have also been prescribed, and surrogate advertising has been prohibited.

In 2023, a set of guidelines was published by the government which restricted e-commerce entities from using dark patterns on their website. These guidelines prescribe 13 specific "dark patterns" and prohibit all platforms which systematically offer goods/services in India, advertisers, and sellers from engaging in any of these specified dark patterns. The dark patterns listed under the guidelines include false urgency, basket sneaking, forced action, bait and switch, and drip pricing.

Entities functioning as payment systems are bound to comply with a host of regulations issued by the RBI. The Payment and Settlement Systems Act (the “PSS Act”) is the primary legislation governing payment systems in the country and prescribes that any payment system must be approved by the RBI prior to operating in India. The RBI is also empowered to issue regulations which payment systems are bound to comply with.

Additional guidelines relevant to payment systems include the Guidelines on Regulation of Payment Aggregators and Payment Gateways, the Master Direction on Credit Card and Debit Card – Issuance and Conduct Directions, and the circular on Tokenisation of Card Transactions. These guidelines and directions govern various disparate aspects of the digital payment economy in India and their relevance must be considered on a case-to-case basis, depending upon the nature of business of the entity.

Large e-commerce entities have been subject to increased scrutiny in terms of antitrust issues over the past few years. In 2020, the Competition Commission of India (CCI), the country’s antitrust regulator, initiated a probe into Amazon and Flipkart, the two largest e-commerce platforms in the country, for alleged contraventions of the Competition Act, 2002 (the “Competition Act”), India’s primary antitrust legislation. These actions were challenged by both Amazon and Flipkart in courts, but these challenges were struck down. It remains to be seen what the findings of the CCI’s investigation are, and whether any penalties or corrective actions are imposed upon these e-commerce platforms.

The space of mobile OS and app ecosystems has also seen scrutiny from antitrust regulators. As an illustration, the CCI in 2022 passed an

order imposing substantial fines on Google. In its order, the CCI found that Google’s practices regarding the Android OS and the Android app ecosystem amounted to a violation of the Competition Act. The mandatory installation of the Google suite of apps (including Gmail, Google Maps, etc) and the denial of access to competing web search service providers, among other things, were held to be violative of the Competition Act by the CCI. Additionally, in a separate order, the CCI held Google’s practice of mandating that app developers use Google’s billing system to carry out in-app purchases also violates the Competition Act.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

No specific laws regulate cloud or edge computing in India. No specific regulatory licences need to be obtained from service providers. As with the response in **1. Metaverse**, a similar range of broad laws will be applicable.

Privacy

The SPDI rules will apply to the parties. Wherever sensitive personal data is being processed, this may only be done with consent that is obtained at the front end by the data controller (this is a practical observation, as no distinction between a data processor and data controller exists in the SPDI Rules). Under the DPDPA, such processing may only be justified as a result of consent obtained from the data subject, or through a reliance on a narrow band of other legitimate purposes. It is important to note here that the SPDI rules prescribe that the processor needs to have the same level of data protection standards as the party transferring the data to it. Under the DPDPA, there are no obvious restrictions on

cross-border data transfers, save the fact that the central government may notify a list of countries to which such transfers shall be restricted.

CERT-In Rules

On 28 April 2022, the Indian government notified a requirement for all service providers, intermediaries, data centres, body corporates and the government itself to report all cybersecurity incidents to the Indian Computer Emergency Response Team (the “CERT-In”) within six hours of these incidents being noticed. Such cybersecurity incidents include a wide variety of occurrences, such as the unauthorised access of IT systems, identity theft, data breaches and data leaks.

Intermediary Guidelines

As is the case in the response to **1. Metaverse**, cloud service providers may well fall within the purview of an “Intermediary” as has been defined under Indian law. It is, however, important to note that in order to be able to successfully claim intermediary safe harbour, the other compliance obligations that are placed on the intermediary by way of statutes like the Intermediary Guidelines should be met.

Interception, Monitoring and Blocking

The Indian government, and in some instances, certain state governments, have powers to demand access to information, decryption and monitoring of information – for the purposes of public order, crime prevention/investigation and in the interest of national security. A failure to abide by a valid direction may lead to imprisonment and a fine. The Indian government may also issue blocking orders under similar provisions included within the IT Act and through subordinate legislation called the Information Technology (Procedure and Safeguard for Moni-

toring and Collecting Traffic Data or Information) Rules, 2009.

India’s banking regulator, the Reserve Bank of India (RBI), imposes a number of obligations on Indian banks. When it comes to storage of payment information, on 6 April 2018, the RBI issued a direction to all banks and Payment System Operators to store all payment data in systems located in India only, except in the case of cross-border transactions where a copy of the payment data, including the domestic component, may also be stored abroad.

Additionally, the Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015, require that all insurers are to maintain records of their issued policies and claims, and these records, whether maintained electronically or otherwise, are to be maintained in India only.

The following aspects, in the context of the Indian legal landscape, may present challenges to the utilisation and functioning of cloud and edge computing services.

Breach notification

As stated above, cybersecurity incidents are to be reported to CERT-In within six hours of becoming aware of the incident, and a contravention of this directive carries with it penal provisions – imprisonment of up to one year, a fine of up to INR10,000,000 (approximately USD120,000), or both. Even though CERT-In has clarified that penalties for contravention will only be imposed in extraordinary cases for wilful non-compliance, practically speaking, this has led to a lot of friction between cloud service providers and their customers, which consist of corporations providing services to Indian customers and processing their personal informa-

tion, and has greatly complicated the negotiation of any such agreements. This issue is exacerbated by the fact that the global standard for data breach notifications (including as set out in the General Data Protection Regulation) requires data breaches to be reported within 72 hours of becoming aware of the breach.

Jurisdiction

As is the case with all internet-enabled technologies, the question of jurisdiction also poses a challenge in contravention by cloud and edge computing services. Even though the IT Act has been granted extraterritorial jurisdiction, actual enforcement against foreign entities who have no tangible presence in India is highly unlikely, and such entities may simply claim that the IT Act has no jurisdiction over them and refuse to comply with any requirements provided under the IT Act or rules framed thereunder while dealing with Indian consumers or business entities.

Cross-border data transfers

The Indian government may choose to restrict or block data transfers to countries which it feels are a threat to its national security. The DPDPA also has a specific provision which allows the Indian government to notify countries to which data transfers may be blocked. In 2022, the Indian government banned over a hundred apps with Chinese links, including major global players such as TikTok. This also presents a potential challenge to foreign cloud computing services operating in India, as a chance of being restricted or banned by the Indian government exists. As may be expected, the degree of this risk is contingent on India's geopolitical stances.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

There is no single Indian law that governs the use of AI in the country. A host of more general statutes, such as the IT Act, privacy law (currently through the SPDI Rules and in the near future, the DPDPA), and copyright law would be relevant in this space. Some of the things that stand out when considering laws that would govern AI apps, particularly those relevant for AI-generated content (AIGC) applications, are the following.

Web Scraping

The potential access to computer resources without permission of the owner has the potential to fall foul of various provisions of the IT Act. The scraping of information through automated means from websites that prohibit this under their terms of service may well also be considered a violation of contract. Clickwrap agreements have been held to be enforceable if they meet the other requirements of the Indian Contract Act, 1872, and a breach would open the door to remedies available under the law. Additionally, scraping may entail storing of copyright-protected works and their reproduction, which may give rise to claims of infringement. Each such scenario will need to be considered based on possible defences available under the law.

Intermediary Guidelines

It is possible, dependent on the use of AI made in each instance, that a platform may be considered to be an intermediary. In order to qualify thus, it would need to meet the test laid down in Section 79 of the IT Act – namely, that it does not initiate a transmission, select a receiver or exercise any editorial control. In the instance of AIGC specifically, it is unlikely that the third of these

tests would be met. Additionally, even if this test is met, the intermediary claiming safe harbour shall be required to comply with the obligations placed upon it by way of the law, including specifically under the Intermediary Guidelines.

Free Speech

Any content-generation AI will be subject to laws applicable to conventional forms of media, such as those prohibiting the hurting of religious sentiment, sedition and defamation.

Privacy

Even after being recognised as a fundamental right, the right to privacy is only guaranteed against the state, whereas its enforcement against private entities is dependent on statutes passed by parliament (such as the DPDPA) or subordinate legislation (such as the SPDI Rules). While the SPDI Rules continue to be applicable until rules that bring the DPDPA into effect are in force, the following considerations need to be borne in mind:

- the processing of any sensitive personal data will need specific consent; and
- data subjects will need to be provided the right to withdraw from further processing, as well as the right to correct their information.

The following points are of particular note under the DPDPA:

- consent, or other legitimate justifications permitted under the DPDPA, shall be required in each instance where personal data is processed (and not merely for sensitive personal data) as under the SPDI Rules;
- the definition of personal data under the DPDPA expressly excludes publicly available information;

- personal data of a data subject that has withdrawn consent is required to be erased unless reasonably required under any law;
- there are specific provisions under the law with regard to the processing of a minor's data which include the prohibition of behavioural monitoring; and
- there are other specific provisions that would be applicable to any AI app provider in the event it meets the threshold to be classified as a Significant Data Fiduciary – the threshold for which is yet to be notified. These shall include the need to carry out a data protection impact assessment, data audits, and the appointment of a Data Protection Officer.

Reports/Advisories/Best Practices and Guides

In 2018, the Ministry of Electronics and Information Technology, Government of India (MeitY), formulated multiple committees to work on different areas on AI to promote technology and develop a policy framework. These committees submitted multiple reports, including one on the Cyber Security, Safety, Legal and Ethical Issues associated with AI (the “MeitY Report”). It covers the new opportunities and challenges AI presents in the field of cybersecurity, including its potential use in combating cyberwarfare, the safety and privacy implications associated with such use of AI in the cybersecurity field, and the weaponisation of AI.

The MeitY Report also prescribes a comprehensive set of guidelines for the establishment of an accountability framework regarding AI technology.

In addition to the above, the apex public-sector think tank, NITI Aayog, in 2018 published a strategy document titled the National Strategy for Artificial Intelligence (the “NITI Report”),

based on the premise that India is in a position to emerge as one of the world's leaders in the AI space, focusing on the principles India can adopt to achieve social and inclusive growth "in line with the development philosophy of the government".

The NITI Report covers five major topics – global developments in AI, AI and India, focus areas for AI intervention, key challenges to AI adoption in India, and the way forward to harness AI (including research, re-skilling, accelerating adoption, and ethics, privacy, and security concerns).

It is important to note that neither the MeitY Report, nor NITI Report are in any manner legally binding.

5. Internet of Things

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

There are no bespoke Indian laws that govern machine-to-machine (M2M) communication or IoT. The more general laws on privacy, interception, monitoring, blocking and breach reporting requirements would continue to apply.

It is important to point out here that there will be additional requirements that will be brought forth by the soon to come into force DPDPA, which would include a parallel data breach reporting requirement as well as greatly enhanced penalties for failures to ensure compliance.

Other than the above, the following may be of particular note.

- The government of India, in December 2016, approved 13-digit numbers for the purposes

of M2M communication. Pursuant to this, allocations of 13-digit numbers to telecom service providers was carried out in 2018.

- In 2018, the Indian government issued a directive that issuers of SIM cards to be utilised for the purposes of M2M communications were to follow verification norms prescribed under the unified licence regime for telecom operators (as discussed in **7. Telecommunications**). The directive also prescribed a number of restrictive features to be implemented on such SIMs for M2M communication. The restrictive features were relaxed somewhat in 2019 further to representations by industry.
- In January 2022, the government issued a directive stating that a no objection certificate (NOC) would need to be issued by the Department of Telecommunication (DoT) for the sale or rent of International Roaming SIMs/global calling cards of foreign operators – including for the purpose of M2M communications. Only companies registered under the Indian Companies Act may make applications for the NOC, and in case of companies with foreign investment, they must be compliant with the extant foreign direct investment regulations of India. The directive also stated that where innovative app-based solutions were to be offered through the use of such SIMs, they would be approved by the DoT on a case-to-case basis pursuant to presentations and other requested information being submitted. NOCs are valid for a period of three years, with further renewal for up to three years at a time.
- In 2022, the government of India issued guidelines for the grant of a unified licence (as discussed in **7. Telecommunications**) which included authorisation for three categories of M2M services. Additional guidelines were also issued by the DoT in 2022 which inter

alia required the registration of M2M service providers.

In addition to the above, on 24 December 2023, the Indian Parliament passed the Telecommunications Act 2023 (the “Telecom Act”), which is aimed to replace the archaic Telegraph Act, 1885 (the “Telegraph Act”) and the Wireless Telegraphy Act, 1933 (the “Wireless Telegraphy Act”). The new law will also be applicable to the M2M space, and will require holders of existing licences, registrations and permissions to eventually seek authorisation from the government. Provisions of the Telecom Act have been discussed in more detail in 7. **Telecommunications**.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Currently, a number of pieces of legislation govern the provision of audio-visual media services in India. However, this legislation was put in place prior to the advent of the internet as a medium for audio-visual media, and as such, most do not include internet-based services within their ambit.

The Cable Television Networks (Regulation) Act, 1995 (the “Cable Television Act”) governs the operation of cable television networks in the country, defined specifically as systems which are designed to provide cable services for reception by multiple subscribers. This legislation is restricted to terrestrial broadcasting mediums and does not include satellite television within its scope. The Cable Television Act requires all entities intending to operate as a cable operator to register themselves with the relevant authority. All cable operators are required to comply with the prescribed programme code and advertise-

ment code, and not broadcast any programmes or advertisements which contravene the requirements of the respective codes. The Cable Television Act also imposes certain other obligations on cable operators, such as the requirement to mandatorily broadcast “Doordarshan” channels (TV channels operated by the Indian government), maintain certain registers, and transmit certain programmes/channels as prescribed by the Indian government.

Applications for approval to function as a cable operator are to be accompanied by the prescribed fee. Only individuals who are citizens of India, or companies incorporated under the laws of India, are permitted to register as cable operators.

Satellite television saw widespread adoption in India since the Indian government permitted its utilisation in 2000. In 2022, The Guidelines for Uplinking and Downlinking of Television Channels (the “Television Channel Guidelines”) in India were issued by the Indian government to update and consolidate the regulations regarding operation of TV channels over satellite television. Different fees are prescribed for uplinking and downlinking of TV channels from within and outside India. Permission forms for a TV channel are to be accompanied by a prescribed fee. Annual permission fees as prescribed by the Television Channel Guidelines are to be paid for uplinking/downlinking TV channels in India as well. Additionally, the Television Channel Guidelines prescribe minimum net worth requirements to carry out these activities. The Television Channel Guidelines have also made the programme and advertisement codes prescribed under the Cable Television Act applicable on the TV channels being broadcast using satellite television, with penal actions ranging from an advisory

being communicated to the entity to suspension or revocation of permission.

With regard to internet streaming of audio-visual media, no specific legislation has been instituted yet. No specific registration or approval is required to operate an Over-The-Top (OTT) platform in the country. However, the provisions of the IT Act and the subordinate legislation framed thereunder, specifically the Intermediary Guidelines are applicable on such OTT platforms, as they fall under the definition of “intermediary” prescribed in the IT Act.

The Intermediary Guidelines require all intermediaries (including social media intermediaries – which would include hosts of user generated audio-visual content such as YouTube and Instagram) to abide by certain due diligence provisions in order to be beneficiaries of the “safe harbour” protection granted by the IT Act.

Obligations imposed by the Intermediary Guidelines (as discussed earlier) include the publication of the terms of use and privacy policy of the platform on its website or mobile app and provide an annual notice of these to users as well, and the obligation to inform users annually that in case of non-compliance with the platform’s terms of use or privacy policy, their right to use the platform may be restricted. Additionally, intermediaries are required to make “reasonable efforts” to ensure that content hosted on the platform is compliant with certain conditions, such as those regarding obscenity, infringing upon intellectual property rights, content being deceptive as to its origin or information, or content which threatens the unity, integrity, defence, security or sovereignty of India, among other conditions. Intermediaries are also required to put in place a grievance redressal mechanism through instituting a Grievance Officer, who is

required to acknowledge any complaint within 24 hours of receipt and resolve it within 15 days of receipt.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Various legislation and policies govern the telecommunications space in India. These include the Telegraph Act, the Wireless Telegraphy Act, and the Telecom Regulatory Authority of India Act, 1997.

The DoT, a department set up under the Ministry of Communications, government of India, has been granted the power to issue telecom licences under the Telegraph Act and Wireless Telegraphy Act. Further to the National Telecom Policy 2012 issued by the Indian government, unified licences are now granted by the DoT covering multiple telecommunications services, including access services, internet services, and national and international long-distance services.

Only companies registered under the Indian Companies Act may apply for the grant of a unified licence. Minimum net worth and equity requirements have been prescribed to apply for a unified licence, along with requirements for an entry fee and a bank guarantee. The extant foreign direct investment (FDI) policy of India allows for up to 100% FDI into entities engaging in the telecommunications space, however, security clearance from the Ministry of Home Affairs, government of India, is required to be obtained prior to such investments.

Upon the grant of the licence, licensees are required to pay an annual licence fee for each service area and each authorised service, cal-

culated as a percentage of the Adjusted Gross Revenue of the company. Licences are issued for a term of 20 years and may be renewed for ten years at a time upon payment of a renewal fee.

In addition to the licence, the DoT conducts periodic auctions to provide telecom companies with access to the radio spectrums for operating telecom networks. This process is separate and independent from the licence acquisition process.

In 2023, the Indian legislature passed the Telecom Act to overhaul and replace the existing telecom regime in the country. Although the Telecom Act has been passed by the Indian legislature, it will come into force at a later date to be notified by the government. This is expected later in 2024.

The Telecom Act updates and streamlines the currently disparate regulations which pertain to entering and operating in the Indian telecom industry. It retains the requirement for obtaining a licence from the government to operate a telecom business and clarifies that licences obtained prior to its institution under the Telegraph Act or Wireless Telegraphy Act shall continue until their date of validity after which they may be migrated to the fresh authorisation. Specific details as to the requirements of the licence under the Telecom Act will be put in place by delegated legislation (referred to as “Rules”), which have not been published yet. The Telecom Act has also been granted extraterritorial jurisdiction, and its provisions will apply to contraventions outside India if the contravention involves telecom services, equipment, or networks located in India.

Assignment of spectrums under the Telecom Act shall be conducted through auctions (except for

certain specific purposes as listed for which the assignment shall be done through an administrative process). Similar to the licensing requirements, the requirements for being eligible to receive a spectrum assignment will be prescribed by the Rules.

The Telecom Act also grants the government the power to issue Rules regarding the protection of users, including on topics such as obtaining user consent before sending certain classes of messages, the institution of “Do-not-disturb” registers, a mechanism for users to report contravention of these measures, and the requirement for authorised telecom service providers to put in place a grievance redressal mechanism.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Essentially, while it may be viewed as an oversimplification, a technology transfer agreement is a contract that enables the movement of data, know-how and intellectual property from one organisation to another. The considerations discussed herein are of note while engaging in technology transfer agreements in India.

Foreign Exchange Regulation

Previously under the FEMA (Current Account Transaction) Rules, 2000, remittances for technical collaboration above a particular threshold required government approval, however, through a series of moves aimed towards easing business, these rules were relaxed.

Foreign licensors should, however, be conscious of the fact that the Foreign Exchange Management (Guarantees) Regulations, 2000, framed under the Foreign Exchange Management Act,

1999, do not automatically permit an Indian licensee or its owners to provide a personal or corporate guarantee to a non-resident without seeking permission of the regulator – ie, the RBI. There will be serious hurdles in the enforcement of such a guarantee.

Taxation

The Indian government has recently increased the quantum of withholding tax payable on royalties and fees for technical services of foreign entities by Indian parties.

A withholding tax will be required to be deducted by an Indian licensee from a foreign licensor of intellectual property. Licensors/transferors are advised to specify obligations in this regard in any agreement, including appropriate tax certificates proving payment.

The prevailing tax rate on royalties and fees for technical services is 20% plus applicable surcharge, but foreign licensors of intellectual property would be best advised to take advantage of various double taxation avoidance arrangements (DTAAs) that India has with most other nations.

In order to take advantage of DTAAAs, the licensor will require a Tax Residency Certificate from its home country, register with the web portal of the Indian Income Tax Department, and provide a declaration that it does not have a permanent establishment in India.

Applicable Law and Jurisdiction

Usually, a party in the stronger bargaining position would look to ensure that the laws of its home jurisdiction would be the governing laws of the contract. As far as technology transfer agreements are concerned, this would usually be the licensor that would have the upper hand. As a

consequence, courts of the home jurisdiction of the licensor would also ordinarily be provided exclusive jurisdiction over adjudicating disputes arising from the licence agreement.

The above having been said, licensors could face challenges enforcing foreign judicial awards, as Indian courts recognise the enforceability of only some foreign courts. Parties should consider this aspect before determining foreign jurisdiction in any agreements which would potentially require enforcement actions by Indian courts. Additionally, licensors would be well advised to retain the power in the agreement to approach courts in the licensee's jurisdiction to seek injunctive relief, should the relationship between the parties sour.

Adjudicating disputes in Indian courts also carries several challenges, not least the significant backlog of cases in the Indian judicial systems. Resolving disputes in Indian courts may take five to ten years (and possibly even longer).

If parties intend to adjudicate disputes through arbitration, care must be taken to ensure that the arbitration is held in a country that is notified as a reciprocating territory by the Indian government and is a signatory to the New York or Geneva Convention.

Stamp Duty

This is often a stumbling block from the point of view of foreign entities. For an agreement to be entered as evidence before Indian courts of law, it is necessary that the requisite stamp duty under the Indian Stamp Act, 1899, needs to have been paid. Until such requisite duties have been paid, the agreement may not be validly enforced or placed in evidence before an Indian court, which would then be bound to impound such an agreement and insist that the parties

pay the applicable penalties. Licensors should be conscious to insist that such obligations are completed by the Indian party from the get-go, and that the licence agreement itself carries a specific obligation in this regard.

Competition

Often, technology transfers are riddled with restrictive covenants, as well as minimum pricing directions upon the licensee. Licensors would be best served seeking specific legal assistance from local counsel on antitrust issues, such as restrictions on owners of the licensees to ever engage in competing businesses in the future, or deal with other parties that may be seen as competitors of the licensor. Provisions in agreements that have the propensity to be violative of Indian antitrust laws may be held to be void.

Similarly, provisions within these agreements that are overly restrictive on the business activities of the licensee as well as the owners of such licensee may be seen as agreements in restraint of trade and, as a result, unenforceable.

Intellectual Property

Under Indian law, patent licences are only valid if made by written agreement. Such licence needs to be registered with the Controller of Patents by way of the submission of a prescribed form with requisite fee.

Similarly, copyright licences are required to be in writing and duly executed in accordance with applicable law. However, there is no express requirement in the law for such licences to be registered with the Copyright Office.

Confidentiality

Strong confidentiality provisions in an agreement where information is the most important asset are a must. Even prior to the execution

of the actual agreement, discussions between the parties should be subject to an NDA. The licensor should make it a point to mark information that is not for outside eyes as confidential specifically, to remove all doubt from the mind of a licensee's representative. The confidentiality provisions within the agreement should specify the requirement for access control measures, as well as the technological measures that the parties should put in place. Agreements should also specify the period after the termination and/or expiry of the licence agreement pursuant to which the confidentiality obligations shall continue to be applicable.

Various provisions of law may classify the unauthorised sharing of confidential information as a "breach of trust", while the IT Act also provides remedies against breaches of confidentiality as they relate to electronic records.

Indemnity and Related Provisions

Complications with regard to seeking guarantees from owners of the licensee have already been highlighted above in the heading titled "Foreign Exchange Regulation".

In addition, foreign licensors should be cognisant of the fact that liquidated damages according to Indian law may not be permitted to be unreasonable, and may not be inserted with the intent of penalising the breaching party.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Regulation of trust services in India is limited to legislation governing electronic signatures. Electronic signatures, their issue, use and legal

validity are governed by the provisions of the IT Act and rules issued thereunder. The IT Act grants legal recognition to electronic records and allows for the authentication of electronic records by way of digital signatures or electronic authentication techniques, which are considered reliable and are specified in the provisions. Conditions for reliability include the signature/authentication data being linked to the signatory, being under control of the signatory at the time of affixing, and any alterations to the signature/authentication or to the information after it is signed/authenticated being detectable.

Certifying Authorities are defined as those persons/entities who have been granted licences to issue Digital Signature Certificates (DSC) to end users under the provisions of the IT Act. Eligibility requirements for obtaining this licence include prescribed minimum paid-up capital and net worth requirements, as well as an FDI cap of 49%. Applications for licences are to be accompanied with a fee and a bank guarantee of the prescribed amounts.

Licences are valid for a period of five years from date of issue and may be renewed upon applications for such renewal. Certain obligations regarding reliability, security procedures, publishing of information, etc, are also imposed on Certifying Authorities by the IT Act.

End users may apply to a licenced Certifying Authority for obtaining a DSC and pay the prescribed fees for obtaining a DSC with a validity of two years.

India has adopted a digital identity system called *Aadhar*, which was initially launched in 2009. The *Aadhar* ecosystem is administered by the Unique Identification Authority of India, a statutory body set up by the Indian government. *Aadhar* numbers are unique 12-digit identity numbers which may be obtained by Indian residents. The assignment of the *Aadhar* number is linked to biometric and demographic data. *Aadhar* numbers are a mandatory requirement for availing of many government-provided services, subsidies and benefits.

As part of a challenge raised in courts against the constitutionality of mandatorily requiring *Aadhar* numbers for statutory benefits, the Supreme Court of India, in Justice KS Puttaswamy v Union of India, held that the right to privacy is enshrined with the fundamental right to life and liberty granted by the Indian Constitution (as discussed above). Via this judgment, the Supreme Court also struck down the provisions of the *Aadhar* legislation which allowed private entities to use *Aadhar* authentication. Such authentication is now only permitted when it is made permissible by a law in force.

INDONESIA



Law and Practice

Contributed by:

Agus Ahadi Deradjat, Mahiswara Timur and Natasya Amalia

ABNR Counsellors at Law

Contents

1. Metaverse p.197

1.1 Laws and Regulation p.197

2. Digital Economy p.198

2.1 Key Challenges p.198

3. Cloud and Edge Computing p.200

3.1 Highly Regulated Industries and Data Protection p.200

4. Artificial Intelligence p.202

4.1 Liability, Data Protection, IP and Fundamental Rights p.202

5. Internet of Things p.203

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.203

6. Audio-Visual Media Services p.204

6.1 Requirements and Authorisation Procedures p.204

7. Telecommunications p.205

7.1 Scope of Regulation and Pre-marketing Requirements p.205

8. Challenges with Technology Agreements p.208

8.1 Legal Framework Challenges p.208

9. Trust Services and Digital Entities p.209

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.209

ABNR Counsellors at Law was founded in 1967 and is Indonesia's longest-established law firm. ABNR pioneered the development of international commercial law in the country following the reopening of its economy to foreign investment after a period of isolationism in the early 1960s. With more than 100 partners and lawyers (including two foreign counsel), ABNR is the largest independent full-service law firm

in Indonesia and one of the country's top three law firms by number of fee earners, giving it the scale needed to simultaneously handle large and complex transnational deals across a range of practice areas. The firm also has global reach as the exclusive Lex Mundi member firm for Indonesia since 1991. Lex Mundi is the world's leading network of independent law firms, with members in more than 100 countries.

Authors



Agus Ahadi Deradjat (Agung) is a partner at ABNR Counsellors at Law and a former member of the firm's management board, Agung focuses his practice on corporate/M&A, foreign direct

investment (FDI), and TMT. He advises leading domestic and multinational corporations across all leading industries and sectors, but offers particular expertise and experience in life sciences, technology and telecommunications, e-commerce and automotive. Agung recently worked on a number of major M&A and FDI transactions for high-end multinational clients, as well as significant FDI transactions in the technology, pharma industry, manufacturing, chemicals, and the natural-resources sectors. Agung is ranked for TMT (Band 1) and corporate and M&A by Chambers Asia-Pacific.



Mahiswara Timur joined ABNR Counsellors at Law as an associate in June 2015. Timur has focused on IT-related assignments such as telecommunications networks

(including for submarine cables and satellites) and services, cybersecurity, privacy and personal data protection, digital content compliance, cloud computing, e-commerce, broadcasting, over-the-top services, data centre operation, digital platforms and services in Indonesia, the internet of things, and online games. He has advised start-up clients and leading multinational technology, social media and streaming companies. His extensive understanding of the regulatory, technical and practical aspects of TMT business has enabled Timur to provide precise, comprehensive advice as well as practical solutions well-tailored to client needs and business operations.



Natasya Amalia focuses her practice on TMT. Prior to joining ABNR Counsellors at Law, she was employed at a prominent international law firm where she worked on fintech, M&A, and general corporate matters. Her TMT work includes data privacy and protection, e-commerce, digital content compliance, cybersecurity, advertising, online gaming, and general advice on technology services and compliance in Indonesia. In fintech, Natasya has assisted a long list of local and international fintech players amid Indonesia's online lending boom, including a well-known Indonesian e-commerce entity, which she advised on the structuring and establishment of its peer-to-peer lending business.

ABNR Counsellors at Law

Graha CIMB Niaga
24th Floor
JI Jenderal Sudirman Kav 58
Jakarta 12190
Indonesia

Tel: +62 21 250 5125/5136
Fax: +62 21 250 5001
Email: info@abnrlaw.com
Web: www.abnrlaw.com



COUNSELLORS AT LAW

1. Metaverse

1.1 Laws and Regulation

In an increasingly digital world, countries such as Indonesia have been trying to adapt their regulatory environments to embrace this, including the metaverse – a digital space using virtual reality and augmented reality, which emerged owing to market dependency on social media (particularly during the COVID-19 pandemic). The nation is also a big player in the adoption of other digital products – for example, non-fungible tokens (NFTs) and crypto-assets (digital assets depending primarily on cryptography and distributed ledger technology).

However, Indonesia has yet to introduce a law/regulation that specifically addresses the metaverse. Nevertheless, it is subject to general laws and regulations, as follows.

General Operation of Electronic Systems

The operation of electronic systems in Indonesia is regulated under the following laws and regulations:

- Law No 11 of 2008 as lastly amended by Law No 1 of 2024 on Electronic Information and Transactions (the “EIT Law”);
- Government Regulation No 71 of 2019 on the Provision of Electronic Systems and Transactions (“GR 71”);
- Minister of Communications and Information Technology (MCIT) Regulation No 20 of 2016 on Personal Data Protection in Electronic Systems (“MR 20”); and
- MCIT Regulation No 5 of 2020 on Private Electronic Systems Operators, as amended by MCIT Regulation No 10 of 2021 (“MR 5”).

Operation of the metaverse would be subject to the obligations on an electronic system operator (ESO), such as:

- obtaining an ESO registration certificate – the operator of the metaverse must register themselves with the MCIT if they provide their platforms within the Indonesian territory, carry out business in Indonesia, or their electronic systems are used or offered within Indonesian territory;
- applying content moderation – the ESO must ensure that its electronic system does not contain prohibited electronic information and/or electronic documents and does not facilitate the distribution of prohibited electronic information and/or electronic documents (prohibited contents include pornography, gambling, slander, scam, hate speech based on ethnicity, religion, race, and inter-group relations (SARA), violence/violence against children, trading of regulated goods, terrorism radicalism, separatism/dangerous organisation, IP rights, information security breach, negative content based on sectoral institutions’ recommendation, content that causes public disturbance, content that violates social and cultural value, hoax/fake news, and extortion);
- using secure and compatible hardware and secure and reliable software;
- maintaining security measures for the components of the electronic systems; and
- complying with the minimum requirements for the operation of electronic systems, which are:
 - (a) being capable of displaying electronic information in its entirety;
 - (b) protecting the availability, integrity, authenticity, confidentiality, and accessibility of the electronic information;
 - (c) being capable of operating in accordance

- with the prescribed procedure;
- (d) providing operation guidelines in the Indonesian language; and
- (e) updating the operation guidelines.

Personal Data Protection

Law No 27 of 2022 on Personal Data Protection (the “PDP Law”) is the main regulation governing personal data protection and applies generally to any personal data processing, including in the metaverse. One of the concerns raised in the context of the metaverse is identity theft, in respect of which the PDP Law provides criminal sanctions towards any person that illegally obtains, collects, displays, uses or falsifies other individuals’ personal data.

Digital Assets

The metaverse is closely tied to digital assets such as NFTs, which are not yet specifically covered and acknowledged by Indonesian law. However, an NFT would still be considered “property” under the Indonesian Civil Code (specifically, as intangible, movable property).

It is also noteworthy that – under Commodity Futures Trading Regulatory Agency (Bappebti) Regulation No 8 of 2021 on Guidelines for the Implementation of Physical Crypto-Assets Market Trading in the Futures Exchange, as amended by Bappebti Regulation No 13 of 2022 – crypto-assets are defined as “intangible, digital commodities that rely on cryptography, an IT network and distributed ledger technology to create new units, and verify and secure transactions without the involvement of other parties”. As such, NFTs may fall under such definition. However, Bappebti previously clarified that NFTs have yet to be regulated, meaning they are currently unregulated.

Given the rapid growth of NFT transactions (many aspects of which may raise concerns), it is expected that the Indonesian government will establish clear NFT regulations.

2. Digital Economy

2.1 Key Challenges

As in other parts of the world, the digital economy plays a pivotal role in shaping Indonesia, particularly as a developing country that is heavily reliant on various types of inbound investment. The Indonesian government has been quite aggressive in introducing new regulations (or, in some cases, updates to current regulatory regimes) in order to accommodate digital economy-related trends.

The Indonesian digital economy is mainly regulated under the following laws and regulations.

E-Commerce

Government Regulation No 80 of 2019 on E-Commerce (“GR 80”) serves as the umbrella law for e-commerce transactions. GR 80 governs the main aspects of e-commerce, including licensing requirements, obligations for e-commerce providers, content liability, consumer protection, and data protection.

GR 80 generally defines “e-commerce” as a form of commerce in which transactions are conducted using electronic equipment and procedures, whereas an “e-commerce undertaking” is “an individual or undertaking, whether incorporated or unincorporated and whether domestic or non-domestic, that engages in commercial operations in the e-commerce field”. Considering the broad definition of e-commerce, many electronic platforms would qualify as an

e-commerce undertaking and should comply with e-commerce regulations provisions.

E-commerce undertakings are further classified into three categories:

- e-commerce providers – providers of electronic communication facilities used for trading transactions;
- merchants – business undertakings engaged in e-commerce, either by using e-commerce facilities created and managed directly by themselves or through a facility owned by an e-commerce provider (or through other electronic systems that provide an e-facilities platform); and
- Intermediary Services Providers (ISPs) – domestic or foreign business actors (other than telecommunications operators) that provide an electronic communications platform, which only functions as an intermediary in electronic communications between a sender and recipient.

E-commerce undertakings are required to obtain the relevant licences via the Online Single Submission system. The exceptions are ISPs that do not directly benefit from e-commerce transactions and are not a party to contracts between parties conducting e-commerce transactions.

Recently, in an attempt to regulate the aggressive foreign e-commerce platforms, the Indonesian government issued Ministry of Trade (MOT) Regulation No 31 of 2023 on Licensing, Advertising, Development and Supervision of Business Undertakings in the E-Commerce Sector (“MR 31”) as an amendment to the previous implementing regulation of GR 80.

Notable provisions governing the obligations of e-commerce undertakings under GR 80 and MR 31 include the following.

- Content moderation – e-commerce providers shall be held liable for legal consequences/impacts due to illegal electronic information content within their platform. However, GR 80 provides a safe harbour if the e-commerce provider takes immediate action to delete a link to illegal electronic content once aware of its nature.
- Product compliance for foreign merchants – foreign merchants are required to verify their identity and provide specified documentation and information to an e-commerce provider, which indicate:
 - (a) details on identity;
 - (b) a copy of business licence that has been apostilled by an authorised institution or legalised by an Indonesian Embassy overseas;
 - (c) evidence of compliance with the relevant compulsory standards and technical requirements for the goods/services being sold;
 - (d) bank account numbers used for transaction payments; and
 - (e) a certificate or report confirming the veracity of the merchant’s identity particulars and business licence from an independent surveyor in the merchant’s country of origin.

The newly issued MR 31 tries to capture platforms that provide both social media and e-commerce within the same application by introducing the term “social commerce”, which is defined as a “social media operator that provides certain features, menus or facilities that enable merchants to offer goods or services”. The regulation imposes an e-commerce licens-

ing obligation on an undertaking that falls within the definition of social commerce, which was previously not clear. Social commerce platforms are also prohibited from acting as a manufacturer and facilitating payment transactions.

Other than social commerce, MR 31 also provides for specific business models that are subject to the e-commerce regulations – namely, online retail, marketplace, online classified advertising, price comparison platforms, and daily deals.

Payment Service Providers

The payment system industry is also a major contributor to the growth of Indonesia's digital economy. However, this industry is considered a highly regulated sector under the authority of Indonesia's central bank, Bank Indonesia (BI). The two regulatory frameworks regulating payment services activities are BI Regulation No 22/23/PBI/2020 on Payment Systems and BI Regulation No 23/6/PBI/2021 on Payment Service Providers ("PBI 23").

Under PBI 23, the main activities of payment service providers (PSPs) include account issuance services, account information services, payment initiation and/or acquiring services and money remittance services. PSPs may be required to obtain different licences depending on the types of business activities they provide, which are categorised into three types under PBI 23:

- Category 1 – account issuance services, account information services, payment initiation and/or acquiring services and money remittance services (eg, issuer);
- Category 2 – account information services and payment initiation and/or acquiring services (eg, acquirer, payment gateway provider, e-wallet provider);

- Category 3 – money remittance services and/or other services determined by BI.

The categorisation is designated to compartmentalise various types of payments services, relative to the degree of their involvement in payment processing and attributed risks. A business model with inherently greater risk would be subject to higher scrutiny and licensing requirements.

The ever-evolving digital payment ecosystem poses a practical challenge. Business undertakings often find it quite difficult to determine the appropriate licences under PBI 23 for their business models.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Business undertakings have learnt that efficiency is key. This necessarily involves the adoption of cloud services. By using cloud storage and cloud computing, advanced technology is now more accessible and cost-effective. However, there is a possible security downside when using cloud technology, as business undertakings often collaborate with third-party cloud computing providers and share their data with them.

In Indonesia, a specific set of regulations on cloud and edge computing does not yet exist. However, some general compliance related to the EIT Law, the PDP Law, and consumer protection law is applicable to the use of cloud computing – with greater restrictions applying to certain industries, such as the financial sector and healthcare.

Financial Sector

Banks are generally allowed to co-operate with third-party IT providers in implementing their IT (including the use of cloud computing). However, the co-operation must comply with the requirements under OJK Regulation No 11/POJK.03/2022 on Implementation of Information Technology by Commercial Bank (“POJK 11”), such as:

- having supervision over the implementation of the third party provider services;
- the procurement of the third-party provider must consider the matters provided under POJK 11; and
- having co-operation agreement with minimum provisions as set out in POJK 11.

If a bank intends to co-operate with a foreign IT service provider for any IT-based transaction processing, it must obtain approval from the Financial Services Authority (*Otoritas Jasa Keuangan*, or OJK). The regulation also requires banks to place their data centre and/or disaster recovery centres in Indonesia, unless the OJK grants an approval to place their data centers offshore.

Similar to banks, Non-Bank Financial Institutions (NBFIs) are also subject to data localisation requirements under OJK Regulation No 4/POJK.05/2021 on the Implementation of Risk Management in Using Information Technology by Non-Bank Financial Services Institutions, as partially revoked by OJK Regulation No 10/POJK.05/2022 on Peer-to-Peer Lending (“POJK 4”). They may place their data centres and/or disaster recovery centres offshore only upon obtaining an approval from the OJK.

Healthcare

Under Ministry of Health (MOH) Regulation No 24 of 2022 on Medical Records, medical records can be stored on digital-based storage media at health service facilities, which includes server, certified cloud computing and any other certified digital-based storage media. The health-care facilities can co-operate with an ESO that has onshore data storage facilities and the ESO must obtain recommendation from the relevant MOH department. The co-operation itself must be based on an integrity pact or non-disclosure agreement.

Processing of Personal Data in the Context of Cloud Computing

In many instances, cloud computing services would be procured from a third-party provider. In such case, the third-party provider must confirm their role in the personal data processing (eg, whether they act as the data processor of the data controller). This is crucial for the third-party cloud computing provider, as the PDP Law differentiates between the liability of a data controller and data processor. A data controller is fully accountable and liable to the data subject for the processing of their personal data, whereas the liability of the data processor is limited – ie, they should only be independently liable if they are processing personal data in a manner that deviates from the data controller’s instruction, order or purpose. Thus, the third-party cloud computing provider and the user should establish a set of clear provisions on the role, obligations and liability of each party in the context of personal data processing.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

Artificial Intelligence (AI) has also reached Indonesia. The popularity of generative AI (eg, Chat-GPT) has led to its rapid increase in usage and integration in a variety of sectors. This has resulted in concerns about compliance, as Indonesian regulations do not yet specifically encompass this particular technology. However, AI is still subject to sectoral regulations such as the EIT Law, the PDP Law, copyright law, and consumer protection law.

As a response to the rapid utilisation of AI, the MCIT issued Circular Letter No 9 of 2023 on Ethics of Artificial Intelligence (“CL 9”) on 19 December 2023. CL 9 is essentially a guideline, rather than a binding regulation per se. The measures taken are focused more on supervision and governance in order to reduce potential risks. CL 9 is intended as a pointer to ethical values for business actors that use AI-based software.

Some of the noteworthy provisions of CL 9 shall be examined here.

The scope of CL 9 includes general definitions and general guidelines for values, ethics, and control of consulting, analysis and programming activities with an AI basis by business actors and electronic systems operators. This circular letter applies to the following parties:

- business actors operating under Indonesian Standard Business Classification (*Klasifikasi Baku Lapangan Usaha Indonesia*, or KBLI) 62015 – AI-Based Programming Activities;
- public ESOs; and
- private ESOs.

Ethical values of AI introduced under CL 9 are – among others – inclusivity, humanity, safety, accessibility, transparency, credibility and accountability, personal data protection, sustainable development and environment, and IP rights.

There are three ways for the business actors, public ESOs and private ESOs to honour their ethical responsibilities when it comes to AI – namely, by:

- ensuring AI is not implemented as a policymaker and/or decision-maker regarding humanity;
- providing information about the development of AI-based technology by developers to prevent negative impacts and losses from the resulting technology; and
- taking into account risk management and crisis management in AI development.

In addition to the CL 9, the OJK has set a Code of Ethics for Responsible and Trustworthy AI in the Financial Technology Industry (the “OJK Code of Ethics”). The basic principles set under this Code of Ethics are that, among other things, AI should be:

- based on *Pancasila* (the official, foundational philosophical theory of Indonesia);
- beneficial;
- fair and accountable;
- transparent and explicable; and
- robust and secure.

The current government’s approach allows for flexibility in the development of AI-based technology in Indonesia, while allowing it to take a “wait and see” approach to determining the appropriate measures to govern this technology.

5. Internet of Things

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

Internet of things (IoT) applications continue to rapidly evolve in this increasingly technology-reliant era. From smart homes that optimise energy consumption to industrial applications that streamline production processes, IoT offers substantial transformation and increased operational efficiency.

In Indonesia, IoT is starting to be acknowledged, as indicated by the inclusion of KBLI 62024 – IoT Consultation and Design Activities as an Indonesian Standard Business Classification, along with the following description.

“This group includes consulting service activities, designing and manufacturing integrated system solutions based on orders (not ready-to-use) by modifying existing hardware, such as sensors, micro-controllers and other hardware. These modifications are made to the IoT hardware and/or software embedded in it. This group excludes chip manufacturing activities (26120) and IoT software publishing/development activities (58200 and 62019).”

In addition to the foregoing, the elements that can be relevant to the operation of IoT have been included in several laws and regulations, as follows.

Provision of IoT Services

The provision of IoT services heavily relies on stable and adequate telecommunications connectivity, as one of the main elements of IoT services. MR 5 stipulates that the provider of IoT services must either:

- obtain a business licence for the operation of telecommunications services (*Perizinan Berusaha Penyelenggaraan Jasa Telekomunikasi*) of a data communication system service from the MCIT; or
- co-operate with a telecommunications provider of a data communications system service.

Connectivity providers are also required to implement a unique addressing system, including (but not limited to):

- using a local Mobile Station Integrated Services Digital Network (MSISDN);
- device end user ID; or
- protocol internet (PI) number.

Electronic Agent

Although not being specifically regulated, the characteristics of IoT in automating information processing render it comparable to an “electronic agent” under Indonesian law. The EIT Law essentially defines an electronic agent as “a device of an electronic system that is made to perform an action on certain electronic information automatically by a person”. The phrase “automatically by a person” refers to natural persons or legal entities (both Indonesian citizens and foreign nationals).

In addition, electronic agents are required to provide features that allow users to make changes to an existing information transaction process.

Data Protection

Many of the data processing activities involved in the operation of IoT will fall within the material scope of the PDP Law, given that IoT devices may involve the processing of personal data. The key challenges of data protection that can be relevant to the use of IoT are as follows.

Difficulty in determining the responsibility upon failure to protect personal data

IoT services typically involve more parties than simply mobile operators – for example, device manufacturers, telecommunications services operators, online platforms, third-party applications, and software licensing. Given the multitude of components involved, it is essential to conduct an assessment of the data processing activities in order to determine the applicable data protection roles (ie, data controller or data processor) and the obligations that follow. Under the PDP Law, the data controller determines the purpose and controls the personal data processing. Meanwhile, the data processor is the party who processes the personal data on behalf of the data controller.

Obligation to protect the continuously recorded data

As IoT devices continuously record and process user data, the use of IoT must comply with the data storing, collection and processing provisions under the PDP Law. Further, in the event that the IoT devices handle vast amounts of specific personal data (eg, data and information on health, children's data, biometric data) will lead to the obligation to implement a Data Protection Impact Assessment (DPIA) and appoint Data Protection Officer (DPO) should the main operations of the data controller involve large-scale processing of sensitive personal data.

Abuse of data collection purposes

Private entities that provide IoT devices or services that can access IoT data may use or disclose personal information for additional purposes, such as for profiling, targeted advertising or sale of the data-to-data brokers. The PDP Law requires that the collection of personal data should be limited and specific, legally valid, appropriate, and transparent. Furthermore, the

processing of personal data must be conducted in accordance with its purposes. Thus, the data controller must inform the data subject regarding the purpose of processing.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

The audio-visual media industry has witnessed unprecedented growth during the past few years, followed by technological advancements and an increasing demand for enhanced user experiences. The regulatory frameworks for audio-visual media services and video-sharing platform services in Indonesia would depend on whether they are broadcasting companies or internet-based video-sharing platforms.

Broadcasting Companies

Broadcasting companies are generally subject to Law No 32 of 2022 on Broadcasting as amended by Law No 6 of 2023 on Ratification of Government Regulation in Lieu of Law No 2 of 2022 on Job Creation as a Law (the “Broadcasting Law”) and its implementing regulations. The Broadcasting Law applies to the activity of broadcasting through transmitting facilities and/or transmission facilities using the radio frequency spectrum; this covers radio and television broadcasts.

Prior to conducting broadcasting activities, the broadcasting companies must obtain a broadcasting operational licence (*Izin Penyelenggaraan Penyiaran*) from the MCIT.

As regards broadcast content, the Indonesian Broadcasting Commission (*Komisi Penyiaran Indonesia*, or KPI) – an independent state institution – has the authority to regulate and super-

vide broadcasting matters. In practice, the KPI actively monitors broadcasting content and enforces against non-compliance.

Aside from the Broadcasting Law, broadcasting companies must also comply with the content-related provisions under Law No 33 of 2009 on Film, as amended by Law No 11 of 2020 on Job Creation (eg, on censorship), as well as with the EIT Law (eg, on distribution or transmission of prohibited electronic information/electronic documents).

Internet-Based Video-Sharing Platforms

Business undertakings that provide video-sharing platform services are deemed ESOs under the supervision of the MCIT and hence are subject to the laws and regulations on electronic systems (ie, the EIT Law, GR 71, MR 20 and MR 5). The providers of internet-based video-sharing platforms must comply with the obligations of an ESO, including the mandatory requirement to obtain an ESO registration certificate.

Takedown Requests

One of the most substantial issues related to video-sharing platforms concerns content compliance, particularly on how this business model should be governed. There were several attempts to bring online video-sharing platforms within the ambit of the Broadcasting Law, meaning they would be subject to the KPI. However, the Constitutional Court has clearly established that internet-based video-sharing platforms are beyond the scope of the Broadcasting Law. Accordingly, the operation of video-sharing platforms remains independent of the Broadcasting Law.

Nevertheless, the operation of internet-based video-sharing platforms is still subject to regulations on ESO, including MR 5, GR 71 and the

EIT Law, under the authority of the MCIT. In an effort to regulate internet-based video-sharing platforms, these regulations require platform operators to ensure that their platforms do not contain or facilitate the distribution of prohibited content. Further, these operators are also required to comply with takedown requests (TDRs) issued by the MCIT.

The MCIT usually issues a TDR after receiving a report flagging allegedly unlawful content from the public, ministries and government institutions, or law enforcement/judiciary institutions. Intermediaries must delete or block prohibited content within 24 hours of receiving a report of the unlawful content and, if deemed to be urgent prohibited content, the intermediary must delete or block such content within four hours of receiving a report of the unlawful content.

The MCIT tries to establish strict compliance by platform operators through establishing a mechanism that allows the MCIT to impose a monetary fine for non-compliance with TDR, which is calculated based on a certain formula. The calculation variable would be determined by several variables, including business scale, types of content, severity of violation, compliance level, etc.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Telecommunications is a highly regulated industry in Indonesia and is under strict supervision by the MCIT. Specifically, the MCIT scrutinise the operation of telecommunications networks (including those that are based on copper cable, fibre optics, satellite, and radio frequency spectrum) and telecommunications services (such as

mobile services, internet, data communication systems, VoIP, and network access points). Further, as a response to the emerging of telecommunications services alternatives, the MCIT has been increasing their focus on Mobile Virtual Network Operators (MVNOs) and over-the-top (OTT) services providers.

The telecommunications industry is governed under the following regulations:

- Law No 36 of 1999 on Telecommunications as amended by Law No 6 of 2023 on Job Creation (the “Telco Law”);
- Government Regulation No 52 of 2000 on the Operation of Telecommunications, partially revoked by Government Regulation No 46 of 2021 on Posts, Telecommunications, and Broadcasting;
- MCIT Regulation No 01/PER/M.KOMINFO/01/2010 on the Operation of Telecommunications Networks, amended several times, last by MCIT Regulation No 5 of 2021 on the Operation of Telecommunications;
- MCIT Regulation No 12 of 2018 on Provision of Special Telecommunications for the Needs of Government Agencies or Legal Entities;
- MCIT Regulation No 13 of 2019 on the Operation of Telecommunications Services, amended several times, last by MCIT Regulation No 14 of 2021;
- MCIT Regulation No 5 of 2021 on the Operation of Telecommunications (MR 5/2021); and
- Government Regulation No 46 of 2021 on Posts, Telecommunications, and Broadcasting (GR 46/2021).

Pursuant to the Telco Law, telecommunication is defined as “the transmission, delivery, and/or receipt of information in the form of signs, signals, text, images, sounds, or noises through

wire, optical, radio, or other electromagnetic systems”.

Telecommunications Services

Under the Telco Law, telecommunications services are divided into three implementing services, as follows.

- Implementation of telecommunications network – the provision and/or service of a telecommunications network that enables the implementation of telecommunications;
- Implementation of telecommunications services – the activity of providing and/or providing services of telecommunications services that enable the implementation of telecommunications; and
- Implementation of special telecommunications services – telecommunications operations of a special nature, designation and operation (ie, for research or government agencies).

The operation of telecommunications in Indonesia may only be performed by a licensed Indonesian legal entity.

While the government acknowledge that the MVNO business model is inevitable, it is imperative for them to protect conventional telecommunications operators that have spent resources to build the infrastructure. As a response to this development, the MCIT tries to frame MVNO businesses as re-sellers of telecommunications services.

Radio Frequency Spectrum Use

Radio frequency spectrum is considered a finite resource in Indonesia. Its use in telecommunications services is therefore regulated under MCIT Regulation No 7 of 2021 on the Use of Radio Frequency Spectrum, as partially revoked by

MCIT Regulation No 9 of 2023 (“MR 7”), which stipulates three licences that must be obtained by businesses:

- Radio Frequency Band License (*Izin Pita Frekuensi Radio*, or IPFR) – a licence to use a radio frequency spectrum in the form of a radio frequency band based on specific requirements.
- Radio Station Licence (*Izin Stasiun Radio*, or ISR) – a licence to use a radio frequency spectrum in the form of a radio frequency channel based on specific requirements.
- Class Licence – a licence for the use of radio frequency spectrum attached to a telecommunications tool and/or telecommunications equipment in compliance with technical standards and used based on certain requirements.

MR 7 stipulates a number of obligations to be fulfilled by business undertakings intending to use radio frequency spectrum in Indonesia for the purpose of obtaining the above-mentioned licences. Further, as an effort to boost the development of telecommunications technology in Indonesia, the government allows a spectrum-sharing arrangement, which is subject to contractual agreement between telecommunications operators.

Certification of Telecommunications Equipment and/or Device

Pursuant to MCIT Regulation No 16 of 2018 on Operational Provisions for the Certification of Telecommunications Equipment and/or Devices, telecommunications devices must be certified in order to prove they are up to the technical specification and/or standards set out in the regulation. The regulation specifies that all telecommunications equipment or devices manufactured,

assembled or imported to be traded and/or used in Indonesia must be certified.

Internet Business Undertaking

GR 46/2021 refers to OTT services as business activities via the internet in the form of telecommunications services substitutes, audio and/or visual content services platforms, and/or other services as determined by the MCIT. Further, GR 46/2021 defines a telecommunications services substitute as “a service that can replace telecommunications services, including communications in the form of short messages, voice calls, video calls, video conferences, online conversations, and/or sending and receiving data”.

While this business model is not prohibited, business undertakings that carry out activities through the internet to users in Indonesia (ie, OTT services providers) must co-operate with local telecommunications operators, pursuant to GR 46/2021 and MR 5/2021. The obligation is set for business undertakings that fulfil the following criterion in relation to significant usage:

- the percentage of domestic traffic used;
- active daily users in Indonesia within a certain period up to a certain amount; and/or
- other criteria stipulated by the MCIT.

Although the regulations do not provide sanctions for non-compliance with the co-operation requirement, GR 46/2021 and MR 5/2021 authorise local telecommunications operators to enforce traffic management so as to limit connectivity to a certain service. This could be broadly interpreted to include bandwidth throttling.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

The advance of technology has continued to break down barriers and diminish physical jurisdictional borders. However, this has proved to be a challenge, owing to the State's interest in safeguarding the nation's cybersovereignty. This highlights a need for a balance between upholding national interests in relation to cybersecurity while also maintaining the principle of technological neutrality in order to promote innovation and advancements.

In navigating this complex landscape, it has become imperative to carefully weigh the need for sovereignty with the need to facilitate technological advancement. Thus, the Indonesian government has attempted to do so by allowing freedom of use of foreign data centres as stipulated in GR 71, provided that there is a guarantee of data accessibility to facilitate supervision and law enforcement.

When entering into a technology agreement with a local organisation, the "freedom of contract" and data protection principle from the PDP Law apply. However, should a technology agreement include cross-border data transfer, the parties may be subject to greater restrictions in certain industries such as the financial and health sectors.

Cross-Border Data Transfer Requirements

The PDP Law and the MCIT regulations stipulate certain obligations in relation to cross-border data transfer and/or in relation to data localisation. Cross-border data transfer obligations include establishing a basis for the transfer of personal data, as follows.

- Adequacy of protection – the country of domicile of the receiving party has a personal data protection level that is equal or higher than the provisions in the PDP Law.
- Appropriate safeguard – there is adequate and binding personal data protection in place.
- Consent from data subject – the data subject must have provided their consent to the data transfer.

Further to establishing at least one basis, cross-border data transfers must be reported to the MCIT pursuant to MR 20. The obligations mentioned apply in a general sense to any organisations engaging in data transfer outside of Indonesia.

Restrictions for Financial and Health Sectors

There are greater restrictions and obligations in relation to data localisation for the financial and health sectors. Pursuant to POJK 11, POJK 4 and MOH Regulation No 24 of 2022, there is an obligation for data localisation. In order to store data offshore or engage in activities that require cross-border data transfer, the organisation must obtain approval from certain governmental authorities such as the OJK or Ministry of Health (as applicable) if they engage with organisations in the financial and health sectors.

Restrictions Under EIT Law

There are further restrictions on entering into technology agreements with local organisations under the EIT Law. It stipulates that parties to an international electronic transaction that contains standardised clauses made by an ESO must be governed by Indonesian law, in event of the following:

- the user of the ESO's services as one of the parties in the electronic transaction originates

- from Indonesia and issues their approval from or within the jurisdiction of Indonesia;
- the implementation of the contract takes place in the Indonesian territory; and/or
- the ESO has a place of business or carries out business activities in the Indonesian territory.

Based on the language of this provision, the criteria provided are not cumulative and therefore may cause restriction in the freedom of contract for the parties to a technology agreement that fulfils one of the above-mentioned criterions.

9. Trust Services and Digital Entities

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

Under Indonesian laws and regulations, trust services are managed by Certification Authorities. The EIT Law stipulates that a Certification Authority may provide the following:

- electronic signatures (e-signatures);
- electronic seal – electronic data attached to, associated with, or related to electronic information and/or electronic documents so as to guarantee the origin, integrity and completeness of electronic information and/or electronic documents used by business entities or agencies;
- electronic time stamps – binding markers between time/date and electronic information and/or electronic documents, using a reliable method;
- registered electronic delivery service – a service that provides delivery of electronic information and/or electronic documents, provides evidence related to the delivery of

electronic information and/or electronic documents, and protects the delivered electronic information and/or electronic documents from the risk of loss, theft, damage or unauthorised addition;

- website authentication – a service that identifies the owner of a website and associates the website with the person or business entity receiving the website's electronic certificate using a reliable method;
- preservation of electronic signature and electronic seal – a service that ensures the legal force of electronic signatures and/or electronic seals in electronic information and/or electronic documents can still be validated even if the validity period of the electronic certificate expires;
- digital identity – electronic information containing the unique identity of a legal subject, the utilisation of which is under the control of the legal subject associated with the identity; and/or
- other services that use electronic certificates.

The EIT Law and MCIT Regulation No 11 of 2022 on Implementation of Electronic Certification Governance require Certification Authorities offering electronic certification and providing services that use electronic certificates in Indonesia to be Indonesian legal entities domiciled in Indonesia. The EIT Law further provides that a foreign Certification Authority may provide electronic certification services only if the services are not available in Indonesia. Although this requirement is mainly intended to promote local Certification Authorities, this would raise a question as to the validity of certificates issued by foreign Certification Authorities, which could be a substantial legal issue in cross-border transactions.

Electronic Signatures/Digital Identity Schemes

E-signatures are regulated under the EIT Law and GR 71. They are considered a form of electronic certification and must be issued by a Certification Authority. The Certification Authority for electronic certification may either be an Indonesian Certification Authority or a foreign Certification Authority.

However, the classification of e-signatures produced by the two differ in evidentiary value before the Indonesian court. An Indonesian Certification Authority is able to produce a “certified e-signature”, whereas a foreign Certification Authority is only able to produce a “non-certified e-signature”. (A non-certified e-signature has lesser evidentiary value in court.)

Currently, several Certification Authorities have been registered with the MCIT, which indicates the MCIT’s efforts in promoting the use of e-signatures in Indonesia.

ITALY MEDIA



Trends and Developments

Contributed by:

Marzia Amiconi and Mauro Amiconi
Amiconi Studio Legale

Amiconi Studio Legale is a boutique firm specialising in the TMT media sector, covering media law and new media law, electronic communications law, IP law and corporate law. It assists mainly media service providers, content providers, digital network operators and Internet Service Providers, on matters such as legal opinions, contractual Law, administrative procedures for obtaining licences and authorisations, litigation (both judicial and administrative), communication to the public and the dis-

tribution of audio-visual content, including live concerts and events. Activity focuses on corporate and commercial matters. The team also assists clients in matters connected to environmental law, including criminal litigation issues. The firm's penetration in the Italian media market has grown during the last decade, attracting top clients producing all kinds of content and cross media companies providing specialised services.

Authors



Marzia Amiconi provides legal advice in all TMT areas, notably in radio/television and new media at national and international levels, including smartphone applications,

network operators and suppliers, AVOD/SVOD and Smart TV. She assists companies in the audio-visual media service area on legal issues related to licensing, authorisations and public tender procedures, in addition to the administrative law elements of corporate matters. Marzia represents clients at the Authority for Communication Standards and the Ministry of the Enterprises at all levels of civil and administrative procedure, and is also an expert in multimedia content, helping companies and/or authors in the copyright area and exploitation of media content.



Mauro Amiconi provides legal advice in civil, bankruptcy and banking law, and is also expert in broadcasting law and new media, representing the industry's customers even

before the higher jurisdictions. He also provides assistance in environmental and energy law when related to media law. Mauro is a consultant for financial companies, construction companies and housing co-operatives, dealing with contracts and ordinary and administrative litigation. He deals with civil liability litigation in the field of banking contracts and the recovery of ordinary and land credits for primary banking institutions.

AMICONI STUDIO LEGALE ASSOCIATO

Viale G. Mazzini, 88
00195 Roma
Italy

Tel: +39 06 373 51 931
Fax: +39 06 3724 424
Email: marzia@amiconi.eu
Web: www.amiconi.eu



Radio is Cross-Media in Italy

The rapid evolution and convergence towards new media (ie, its digitalisation) has been the main factor allowing radio to maintain a prominent role during the radical transformation of the media sector.

The first phase of the digitalisation process, the technological one, began in the 1990s with the development of Digital Audio Broadcasting (DAB) technology. The system enables the simultaneous transmission of content by fragmenting it into small numeric packages, based on a binary code transmitted by carrier wave signal, which can easily be duplicated and replicated over the network. Due to the quality of the system, the sound is higher and the signal is received without interruptions or “signal noise”, even in remote areas.

In Europe, the UK’s BBC and Germany’s ARD began delivering their services using DAB technology in 1995. During the following decade, the BBC and ARD expanded the service and implemented this new technology to achieve national network coverage in the UK and Germany, respectively.

In the US, the spread of the digital radio system took place even faster, through the use of a different standard (“HD radio”), which allows a digital signal to be transmitted over traditional radio frequencies. In practice, this allowed the various broadcasters to use the frequencies already in use.

The integration of radio into the universe of new media, particularly the internet, has gone beyond the purely technological aspect, giving rise to the phenomenon of web radio. It is therefore no surprise that radio was the medium that first developed the fundamental characteristic of digital communication: interactivity. The tendency towards interaction and the increased involvement of the listener allowed radio to overcome its traditional role, by generating direct interaction with users.

In summary, radio has transformed into a social tool, serving as an instrument for cultural growth, fostering inclusion and participation, and providing a model for economic development.

European Digital Agenda

The European Digital Agenda for 2020–2030 addresses the widespread, rapid and large-scale development of digital service platforms to:

- create secure spaces and services;
- foster the development of a level playing field in those markets with large platforms;
- strengthen Europe's digital sovereignty; and
- contribute to the European goal of climate neutrality by 2050.

The European Digital Agenda plans to address the technological challenges brought by the use of new technologies, artificial intelligence, access to information available online, and the different ways of purchasing goods and services. Among those themes, the creation and implementation of 5G, mobile HD and digital terrestrial radio DAB+ are key priorities for the European Union.

The introduction of 5G will generate significant benefits in various economic sectors, such as healthcare, manufacturing, logistics and telemedicine. In Italy, the government intends to expand broadband and ultra-wideband connections to 100% of the national territory by 2026. Fewer resources are allocated to the improvement of the DAB+ network than to other strategic areas, but they are still sufficient to foster the development of the digital radio market in the entire national territory.

Regulatory Changes

In line with the Digital Agenda for Europe, Italy has initiated a process to adapt the relevant legislation, which has led to major regulatory changes in the TMT sector. Law No 205 of 27 December 2017 (Budget Law 2018) and Law No 145 of 30 December 2018 (Budget Law 2019)

introduced structural changes to the regulatory framework for radio broadcasting.

In particular, under the Budget Law 2018, it became mandatory for all radio devices sold as of 1 January 2020 to be equipped with the capability to receive digital radio signals. This requirement impacts all devices, including portable radio devices and car stereo systems.

Subsequently, the Budget Law 2019 established that the 174–230 MHz frequency band, previously allocated in shared use to television and radio broadcasting, should be allocated primarily to audio broadcasting and only partially to television broadcasting. This made it possible to identify the spectrum resources designated to radio broadcasting services, which is a necessary first step before the allocation of the frequencies to both national and local broadcasters.

More specifically, the Provisional National Plan for the Assignment of Frequencies in VHF III band allocated the following to DAB+ digital radio broadcasting services:

- three national networks;
- 54 local networks with regional coverage (27 of which can be sub-divided); and
- 36 local networks with multi-provincial or provincial coverage.

The plan is “provisional” insofar as it remains formally open under the co-ordination of the Ministry of Enterprise and Made in Italy. It also established an international negotiating table with neighbouring states, to plan the allocation of frequencies across the Adriatic Sea. The outcome of such negotiations might impact the current allocation of radio frequencies and, therefore, it might be necessary to revise the plan in the coming years.

The regulatory framework for digital radio broadcasting is outlined within the Regulation on the new discipline for the launch phase of terrestrial radio broadcasting in digital technology, under Resolution No 664/09/CONS of the AGCOM – the Italian Communications Authority. The regulation provides specific rules and procedures for market access and conditions for independent content providers in order to promote the enrichment of the offer of programmes available to users, and to ensure the development of the terrestrial digital radio broadcasting market in an open, balanced and pluralist sense.

More than ten years ago, Italy completed the television switch-off by definitively discontinuing analogue transmissions in favour of digital ones. As for radio broadcasting, digital transmissions (DAB+) will operate in parallel with analogue transmissions, since no real switch-off is planned. However, it is likely that technological transition will lead to a series of switch-overs in the next few years.

Licences

In 2023, after a long preparation phase, the Ministry of Enterprise and Made in Italy started assigning 20-year licences for digital terrestrial radio broadcasting services. In Italy, there is a distinction between radio broadcasters that air signal nationally (covering more than 70% of the territory) and radio broadcasters that air signal locally (covering less than 50% of the national territory), as they are assigned different types of licences.

From a regulatory perspective, the only entities authorised to broadcast radio content are those that are entitled to establish systems and business clusters to build the infrastructure dedicated to DAB+ transmission, as these entities

operate in the market under a different type of licence.

National radio broadcasters are already well advanced with the construction of the network infrastructures for territorial coverage. In contrast, local broadcasters will begin to receive the necessary licences to build the networks from February 2024. The market is open to foreign companies, provided they comply with the obligations of audio-visual media service providers included in the AGCOM Regulation.

When fully operational, the market will comprise about 60 national digital radio networks and about 1,000 local digital radio networks, including private and public broadcasters (ie, the state-owned *Radiotelevisione Italiana S.p.A.*).

Italy is divided into 20 regions. The current process for requesting authorisations for both the realisation of the digital network and the broadcasting of content will be handled at both national and regional levels. Therefore, the Italian government intends to establish two tiers of network infrastructure utilising DAB+ technology. The first tier comprises network operators covering the entire national territory, while the second tier consists of networks managed by local operators, catering to either micro or macro areas exclusively.

Considering these points, it can be affirmed that the principles of fairness, transparency and non-discrimination derived from the EU directives and domestic legislation on electronic communication networks and services have been fully respected. Consequently, the framework established by the Italian government ensures equal conditions for market entry for all radio broadcasters, fostering a level playing field for both

private and public operators, including foreign companies.

In light of the above, 2024 represents a year of significant activity for the TMT sector and a turning point for radio media services in digital technology, from both a regulatory and authorisation perspective.

Which Improvements Will DAB+ Technology Bring to Users?

Implementing DAB+ technology across the entire national territory will improve the diffusion and quality of outdoor signals, with an expected coverage of no less than 95% for outdoor signals and no less than 70% for indoor signals. Users will continue to listen to the radio through analog devices, satellite (through TV devices) or the internet (through PCs or smartphones) with an improved signal and high-quality sound. In addition, signal reception will be uninterrupted, especially for users listening from cars or mobile devices, with perfect sound for both music and radio programmes.

Analog radio broadcasting has historically been impacted by interference, causing interruptions and reducing the quality of the signal, especially when the user was listening to the radio while driving. DAB+ transmissions generate a clean, high-quality and uninterrupted signal, thus mitigating this problem.

By becoming interactive and multimedia, radio broadcasting is changing its role within the media sector. Unlike traditional television broadcasting, which has suffered a steady, non-reversible decline over the past decade due to streaming TV platforms and OTT services, radio broadcasting will be able to maintain a position in the market (or even improve it) by offering new products, information, entertainment and music at reasonable costs. All these elements considered together can help radio broadcasters change and develop their targeted audience and compete with on-demand streaming services, especially those aimed at young people.

JAPAN

Law and Practice

Contributed by:

Hiromi Hayashi, Masaki Yukawa and Daisuke Tsuta
Mori Hamada & Matsumoto



Contents

1. Metaverse p.219

1.1 Laws and Regulation p.219

2. Digital Economy p.220

2.1 Key Challenges p.220

3. Cloud and Edge Computing p.222

3.1 Highly Regulated Industries and Data Protection p.222

4. Artificial Intelligence p.223

4.1 Liability, Data Protection, IP and Fundamental Rights p.223

5. Internet of Things p.225

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.225

6. Audio-Visual Media Services p.226

6.1 Requirements and Authorisation Procedures p.226

7. Telecommunications p.227

7.1 Scope of Regulation and Pre-marketing Requirements p.227

8. Challenges with Technology Agreements p.228

8.1 Legal Framework Challenges p.228

9. Trust Services and Digital Entities p.229

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.229

Mori Hamada & Matsumoto is a full-service international law firm based in Tokyo, with offices in Fukuoka, Nagoya, Osaka, Takamatsu, Sapporo, Beijing, Shanghai, Singapore, Yangoon, Bangkok, Ho Chi Minh City, Hanoi, Jakarta (ATD Law), and New York. The firm has over 700 attorneys and a support staff of approximately 600, including legal assistants, translators and secretaries. It 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, bank-

ruptcy, 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.



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

1. Metaverse

1.1 Laws and Regulation

The metaverse has been attracting attention from businesses and government, and there have been considerable developments in related legal discussions and legislation. In November 2022, the government convened a council consisting of businesses, legal experts and government officials, which discussed legal issues related to the metaverse, and released a final report in May 2023. Two laws were amended in 2023 relating to the metaverse. One extends a protection for product design from the real world to the metaverse, and the other introduces a more expedited and simplified state licensing scheme for secondary use of user-generated contents (UGC).

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.

In the metaverse, users often engage in creative activities and copyright for their creative works may be granted to them depending on the terms of use of the metaverse. If so granted, a third party who wants a secondary use of such user-generated contents must obtain a licence from the user holding the copyright. To facilitate such secondary use, even if the copyright owner does not timely respond to a licensing request, the Copyright Act was amended in May 2023 to allow a more expedited and simplified state licensing scheme for the secondary use of user-generated contents within three years from May 2023.

Design imitation

Under the current laws, a design owner usually cannot block a third party from replicating a product from the real world to the metaverse even if it is protected by a design right. To protect the design owner's interest, the Unfair Competition Prevention Act was amended in 2023 to prohibit the provision via telecommunications of data which imitates another's product, from April 2024.

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-own-

ing 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 February 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 is 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. 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. Further legislation for fair competition and user protection is also currently under discussion.

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 provid-

ers 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.

Fair Competition in the Digital Market

The Digital Market Competition Study Group administered by the Cabinet Secretariat released a report and called for public comments in June 2023. The report proposes to introduce new regulations on large-scale mobile OS providers, app stores, browser providers, and search engines. The proposed regulations include:

- prohibiting large-scale app stores from forcing in-app payment;
- obligating large-scale mobile OS providers to allow alternative app stores;
- obligating large-scale mobile OS providers and browser providers to allow users to easily change default settings;
- obligating large-scale mobile OS providers to provide an opportunity for users to elect pre-installed apps;
- obligating large-scale search engines to treat third-party services on a non-discriminatory basis vis-à-vis in-house services;
- prohibiting large-scale mobile OS providers, app stores, and browser providers from using non-public data for other services;
- obligating large-scale mobile OS providers, browser providers, and app stores to provide data portability;
- prohibiting large-scale app stores from forcing social login; and
- obligating large-scale mobile OS providers to allow third parties to equally access OS functions.

Although the report has generally taken a strict attitude, it also seems to agree that seemingly

problematic acts may be justified if necessary for security or privacy. A bill is expected to be submitted to the Diet in 2024.

User Protection of Digital Platforms

The Platform Service Study Group administered by the MIC published their third report in January 2024. The report recommends that the government require providers of large-size digital platforms where unspecified users can distribute contents to take measures to protect defamed people, including having a complaint window, procedure for accepting a complaint, and a staff member familiar with Japanese culture and society, completing the investigation within one week, and notifying the complainant of the results of investigation. The report also recommends that such providers be required to publicly disclose their policies, notify contributors of the ground for banning, and publicly disclose how measures are implemented.

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 infor-

mation 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.

Cloud use by private-sector essential infrastructure

New legislation titled the Act on the Promotion of National Security through Integrated Economic Measures, which was promulgated in May 2022, imposes an additional requirement on essential infrastructure providers designated by the government from 14 essential infrastructure areas, namely, electric power, gas supply, petroleum, water, railways, motor freight, ocean freight, aviation, airports, telecommunications, broadcasting, postal services, financial services, and credit cards. Designated providers will be required to submit a written plan to the competent government ministry for review before they install certain essential facilities or outsource the

maintenance or management of certain essential facilities, which include cloud services. In relation to the plan to use a cloud service, certain parts of the plan may be omitted if the provider is registered with the ISMAP steering committee.

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 services 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

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 AI themselves will not be subject to the PL Act. Rather, it is the producers of movable goods into which big data, machine learning or AI 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 AI.

Producers of big data, machine learning or AI 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 AI, 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.

In June 2023, PPC issued guidance to users and providers of generative AI. Users were advised not to input personal data to generative AI unless the use of AI is within the purposes of use notified to data subjects and there is assurance that the input data will not be used for machine learning. The guidance suggested that providers not collect sensitive data, which collection requires data subjects’ consent, and disclose purposes of use to data subjects.

Copyrights Consideration

In the process of machine learning, copyrighted works may be copied or adapted, which may cause an infringement of copyrights. To pro-

more 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.

In light of the recent increased use of generative AI, copyright holders have concerns about free riding, and the Agency for Cultural Affairs is expected to issue new guidelines regarding AI and copyrights in 2024. The guidelines are expected to clarify cases which will not allow the use of copyrighted works for AI. AI developers should pay attention to this development.

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 was previously excluded from protection even if the foregoing conditions were met, but under a 2023 amendment, from April 2024, that information will also be protected as long as it is not protected as a trade secret. 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 Act.

5. Internet of Things

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

Under the Radio Waves Act (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, the UK 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.

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:

- 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.

- can be used by connecting to a smartphone;

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

As described in **5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection**, 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 $\frac{1}{3}$ 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 telecommunications 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

Under the Act on the Promotion of National Security through Integrated Economic Measures, essential infrastructure businesses 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 essential infrastructure providers were designated in November 2023 and the requirements are expected to be implemented in May 2024. After the implementation, when contracting with designated essential infrastructure providers in Japan, this Act should be taken into consideration. Contractual risk management measures, including those related to cybersecurity, will be required.

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, nine electronic signature service providers received confirmation that they satisfy the requirements of enabling “electronic signatures” from the Digital Agency in accordance with Article 4, paragraph 1 of the Electronic Signatures Act.

The Legal Affairs Bureau, which operates the real property and 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, except where substitute measures designated by the ordinance of the Electronic Book Preservation Act are taken. 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 time stamp in compliance with the Electronic Book Preservation Act must be provided by service providers that obtain an

accreditation from MIC. To obtain the accreditation, the time stamps must meet certain requirements under the Public Notice issued by MIC. The Japan Data Communications Association, a private association, investigates whether or not the requirements are met. As of August 2023, three time stamp service providers were accredited by MIC.

Electronic Seal

In June 2023, the Cabinet approved the “Strategic Plan for Realising Digital Society”. According to the plan, the government will promote standards to evaluate the credibility and conformity of services which provide electronic seals. MIC established a study group to discuss how to promote electronic seals in line with the plan and called for public comments on the draft of its final report in March 2024. The draft proposes that MIC accredit providers of electronic seals that meet certain requirements, which is similar to accreditation given to providers of time stamps.

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). From May 2023, the certificate can also be embedded into Android smartphones. 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 use 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. In June 2023, the government issued a policy plan to abandon KYC using drivers’ licences or other identification and only allow KYC by JPKI in the future.

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 card 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.

Trends and Developments

Contributed by:

Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Yuki Matsumiya
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 telecoms 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 a counsel 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 Yuki Matsumiya,
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 in 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.



Yuki Matsumiya is an associate at Nagashima Ohno & Tsunematsu. Her practice focuses on HR tech, healthtech, AI, data protection/security matters and cross-border and

domestic M&A transactions involving tech companies. She worked at Mitsui Fudosan Co. Ltd. from 2021–2023. She was admitted to the Bar in Japan (Tokyo Dai-ichi Bar Association) in 2013 and in New York in 2019.

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

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Yuki Matsumiya,
Nagashima Ohno & Tsunematsu

Ride-Hailing

In Japan, due to the shortage of taxis, discussions on the use of private cars and ordinary drivers are rapidly advancing. In December 2023, the Japanese government announced that it would allow taxi companies to provide transportation services in areas where there is a shortage of taxis from April 2024, by using an app to dispatch local private cars and ordinary drivers and collect fares. Until now, there has been significant debate about releasing ride-hailing services using private cars, and to date, in Japan it has only been allowed in very limited cases. Therefore, this new service is attracting attention as a potential sign of broader implementation of ride-hailing services in Japan.

However, this new service may only be offered by taxi companies. In this regard, in parallel with the development of this new service, the Japanese government announced that it would proceed with discussions on the establishment of a new legal system allowing non-taxi companies to operate ride-hailing businesses. The result of discussion will be made public around June 2024. Those who are interested in the ride-hailing business in Japan should pay attention to the Japanese government's actions in 2024.

AI

Government trends concerning AI

"AI White Paper"

In April 2023, the Liberal Democratic Party, the ruling party in Japan, announced the "AI White Paper". This paper notes that Japanese society has not adequately responded to the advancements of AI that may have a major social impact, including the emergence of large-scale language models such as Chat GPT, and makes several recommendations. The essence of these recommendations can be classified into the following four categories.

- Fostering and strengthening the foundations for domestic AI development – strengthening support for the accumulation of domestic knowledge on AI and for human resource development in the AI area.
- Promotion of usage of AI in public administration – utilisation of government-owned data and support for smart cities.
- Policies to encourage and support the utilisation of AI in the private sector – measures to encourage private businesses to take on the challenge of AI, including formulation of guidelines, etc.
- New approach to AI control – given the possibility of the risk posed by the misuse of AI with regard to important social values such as human rights, security, and democracy, moving from the soft law-centred regulation to implementation of the necessary hard law.

Hiroshima AI Process

Following the G7 summit held in Hiroshima in May 2023, the Hiroshima AI Process was launched also in May 2023, with the participation of G7-member countries and relevant international organisations to discuss the opportunities and risks of the technology, including generative AI, that has been developing rapidly in recent years. The study lasted for six months and at the G7 Digital & Tech Ministers' Meeting in December 2023, "the Hiroshima AI Process Comprehensive Policy Framework" consisting of the following four elements was announced as the first international framework aiming at promoting the safe, secure and trustworthy advancement of AI systems.

- The "OECD's Report" towards a G7 Common Understanding on Generative AI – as far as high-priority challenges and risks are shared by the G7 countries, this report raises issues of lack of transparency, misinformation/

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Yuki Matsumiya,
Nagashima Ohno & Tsunematsu

disinformation, intellectual property rights, protection of privacy and personal information, fairness, security and safeguards. On the other hand, as far as opportunities for AI technologies are concerned, the report highlights the drive for productivity gains, innovation, healthcare improvement, helping to solve the climate crisis, and support for progress toward achieving the Sustainable Development Goals (SDGs).

- International guiding principles – specifically, the “Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems” and the “Hiroshima AI Process International Guiding Principles for All AI Actors” were formulated.
- International code of conduct – based on the aforementioned “Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems”, the “Hiroshima Process International Code of Conduct for Organizations Developing Advanced AI Systems” was formulated. This code of conduct lists specific actions and recommendations in response to the recent developments in advanced AI systems.
- Project-based co-operation on AI – the meeting declared the importance of project-based co-operation, including projects on generative AI which will contribute to supporting the implementation of the Hiroshima AI Process.

Artificial Intelligence Strategy Council

Following the Hiroshima AI Summit in May 2023, the Cabinet Office took the lead in launching the Artificial Intelligence Strategy Council, an advisory council to discuss policies on AI. The purpose of the council is to “maximize the potential and address risks”; this means the promotion of usage of AI and improvements in industrial competitiveness, and formulating necessary regulations to mitigate risks. In carrying out the above

purposes, the council has announced proposals on the directionality of AI-related measures and a summary of the issues on generative AI.

AI guidelines for business operators

The Artificial Intelligence Strategy Council decided to develop guidelines for business operators that are more uniform and easy to understand. These guidelines are based on the preliminary summary of issues discussed by the council and compile existing guidelines on AI (“Governance Guidelines for Implementation of AI Principles”, “AI R&D guidelines for international discussions”, and “AI Utilization Guidelines”). An outline of the proposed guidelines was discussed in September 2023 and a draft was published in December 2023, following a review by experts. These guidelines aim to promote the safe use of AI by providing uniform guidelines for Japanese AI governance.

The guidelines are not legally binding. Business operators involved in AI are expected to voluntarily promote specific initiatives, such as establishing appropriate AI governance. In addition, the Liberal Democratic Party has declared it will move toward enacting legislation in order to ensure compliance with the guidelines.

The guidelines (including an appendix) total approximately 200 pages. An outline of the guidelines is as follows.

- The entities covered by the guidelines are broadly classified into three categories: “AI Developer” (including entities that study AI), “AI Supplier” (entities that provide services incorporating AI), and “AI User” (entities that use AI systems or AI services).
- The guidelines present ten principles that are common to the target entities, and points of emphasis in AI activities are specified by

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Yuki Matsumiya,
Nagashima Ohno & Tsunematsu

category of the target entities. In addition, the above-mentioned International Guiding Principles introduced through the Hiroshima AI Process (“Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems” and the “Hiroshima AI Process International Guiding Principles for All AI Actors”) are incorporated into the guidelines as the policies that should be complied with, and the requirements for the developers of advanced AI systems (referring to the most sophisticated AI systems, including state-of-the-art infrastructure models and generative AI systems).

- The ten principles are: (i) human-centric, (ii) safety, (iii) fairness, (iv) protection of privacy, (v) security, (vi) transparency, (vii) accountability, (viii) education and literacy, (ix) fair competition, and (x) innovation. Principles (viii) to (x) are expected to be addressed by each entity in co-operation with society.
- Examples of specific guidelines are as follows.
 - (a) In relation to “safety” (principle (ii)), AI developers should set the scope of safe use of AI in order to prevent issues. Also, AI suppliers should remind AI users about the possibility of inappropriate learning by AI models, and AI users should use AI systems/services keeping in mind the precautions set forth by AI suppliers and within the scope of use anticipated by the AI supplier.
 - (b) In relation to “fairness” (principle (iii)), AI developers should be aware of the fact that bias cannot be completely eliminated from AI models, and they should develop AI by implementing a variety of methods to mitigate bias. AI suppliers should monitor bias in AI models and encourage AI developers to improve the AI model as necessary. AI users should use AI out-

put responsibly, keeping in mind that AI prompts may be biased.

- The appendix to the guidelines includes the following:
 - (a) examples of AI services (including relationships among entities);
 - (b) AI benefits and possibilities, specific examples of risks;
 - (c) practical points for developing AI governance and practical examples;
 - (d) commentaries based on the three categories (AI developer, AI supplier, and AI user), examples of specific methods for implementing the guidelines, and easy-to-understand references; and
 - (e) checklist for business operators for compliance with the guidelines.
- The guidelines were published for public comment in January 2024. A finalised version will be announced in March 2024. It will be amended as necessary, such as to reflect the latest trends, going forward.

Examining key legal issues related to generative AI

The Japanese government, led by the Agency for Cultural Affairs and the Cabinet Office, is facilitating discussions on issues related to intellectual property rights, particularly copyright, in the development and use of generative AI. In terms of copyright, discussions are taking place separately for the two phases of generative AI: (i) the learning and development phase; and (ii) the generation and use phase. Although Japan’s Copyright Act does not have a general provision on fair use, the Act provides that copyrighted works may be used without the consent of the copyright holder in the following cases (among other cases).

- Non-enjoyment use – use of existing copyrighted works that is not intended for the

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Yuki Matsumiya,
Nagashima Ohno & Tsunematsu

enjoyment of the thoughts or sentiments expressed in the works (Article 30-4 of the Copyright Act).

- Minor use – minor use of existing copyrighted works that is incidental to computerised data processing or the provision of the results thereof, or preparatory acts for such minor use (Article 47-5 of the Copyright Act).

At the learning and development phase, the use of existing copyrighted works as training data for generative AI is generally considered to fall under non-enjoyment use or minor use and may be conducted without the consent of the copyright holder. However, given the growing concern from creators and performers about the unlimited use of their works in AI learning and development, active discussions are underway about the scope of non-enjoyment use by which copyrighted works can be used without the copyright holder's consent.

At the use phase, the issues being discussed include the following.

- Whether the input of existing copyrighted work as a prompt to a generative AI constitutes copyright infringement.
- The requirements for AI-generated materials to be copyrighted works.
- Whether AI-generated materials that are similar to existing copyrighted works constitute copyright infringement.

The Agency for Cultural Affairs' position on these issues is as follows.

- The requirements for the private replication or non-enjoyment use can be met in many cases of existing works being used as a prompt, in which case it is possible to use existing copyrighted works.

- If the generated materials are not autonomously created by the generative AI but the user of the generative AI creatively contributes to the final material, it may become the user's copyrighted work.
- The general rule is that if the creative expression of the generated material is the same as or similar to an existing copyrighted work, infringement will be found if the generation relies on that existing work. Such reliance will be found if the user is aware of the existing work. Further discussion is needed as to whether reliance will be found even if the user is not aware of the existing works but the generative AI's training data includes the existing copyrighted work.

Web3 and the Metaverse

Web3

The Japanese government has been looking to “web3” and “start-ups” as engines of growth of the Japanese economy. The Japanese government began to promote various government policies in 2022. In 2022, the Project Team 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” illustrating the challenges and presenting proposals regarding NFTs. The Project Team has continued to have various discussions, and in April 2023, announced “The web3 White Paper: Towards an era of mass adoption of Digital Assets” (the “web3 White Paper”).

The web3 White Paper details challenges and provides recommendations for the following two issues:

- issues to be addressed immediately for promoting web3; and

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Yuki Matsumiya,
Nagashima Ohno & Tsunematsu

- issues that should be further explored for the further development of web3.

Issue 1 – “Issues to be addressed immediately for promoting web3” refers to the following topics:

- Japan’s contribution to the establishment of international rules;
- tax reform;
- ensuring opportunities for accounting audits of crypto-asset issuing companies and others;
- establishment of special laws for LLC-type DAOs;
- screening, issuance, and trading of various tokens;
- measures against unlicensed NFTs and consumer protection;
- clarification of criteria for financial institutions’ entry into web3 business and appropriate operations of regulations;
- NFT business; and
- diversification of investment vehicle schemes for blockchain-related businesses.

Issue 2 – “Issues that should be further explored for the further development of web3” refers to the following topics:

- clarification of the treatment of digital asset transactions under private law;
- supporting the overseas expansion of Japan’s content industry using web3;
- licensing of web3 businesses;
- safe and secure use environment;
- clarification of issues related to the use of unhosted wallets;
- utilisation of web3 in revitalising local communities;

- further promotion of measures against money laundering and terrorist financing in collaboration with the international community;
- establishment of a legal framework for investment DAOs; and
- organising the issues on utilising the metaverse for diversifying workforce participation.

In December 2023, the Liberal Democratic Party announced that, in 2024 tax reform, the taxation on crypto-assets would be changed in response to the web3 White Paper. Also, discussion about establishment of special laws for DAOs has been continued. As seen above, the Japanese government will promote various government policies in response to the web3 White Paper. In addition, it is expected in 2024 that issuance of stable coins under the Payment Services Act will be issued. Close attention should be paid to the Japanese market of web3 business.

Metaverse

The metaverse is also mentioned under Issue 2 of the web3 White Paper. The Japanese government has continued to discuss legal issues in relation to the metaverse as well as web3. In November 2022, the Public-Private Co-operative Council for New Legal Issues Concerning Contents in the metaverse was established in the Intellectual Property Strategy Headquarters of the Japanese government and various legal issues have been discussed by the Council. In May 2023, the Intellectual Property Strategy Headquarters published the “Summary of Arguments for Responding to New Legal Issues Concerning Contents, etc, in Metaverse” (the “Summary of Arguments”) as a result of the discussions in the Public-Private Co-operative Council.

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Yuki Matsumiya,
Nagashima Ohno & Tsunematsu

The topics of the Summary of Arguments are divided into the following four categories:

- use and protection of intellectual property rights;
- rights of publicity of avatars;
- regulation on user behaviour in the metaverse; and
- international jurisdiction and governing law.

In each category, legal issues and interpretation of the existing laws are introduced. The Summary of Arguments covers various topics, which are highly important for those considering launching a metaverse business in Japan.

Although the Summary of Arguments does not provide a new interpretation of laws, there are some discussions of amendments to laws. Close attention should be paid to future discussion of amendments. Separately from the discussion in the Summary of Arguments, the Unfair Competition Prevention Law was amended in June 2023, to include imitations in the metaverse. It is an important amendment for relevant players in the metaverse to enable them to make claims for imitation in the metaverse. In addition, the Summary of Arguments contains a suggestion that the Summary of Arguments itself be reorganised for each stakeholder. Attention should be paid on the process of such reorganisation.

Start-Ups

In the TMT area, start-ups play an important role in accelerating innovation. In addition, collaboration between start-ups and major companies will be vital to realise innovation and DX. The amount of funds raised by start-ups is increasing year by year, and in 2022, the amount raised by domestic start-ups, which was JPY87.7 billion in 2012, was JPY877.4 billion, roughly ten times higher.

As seen above, the Japanese government has been looking to start-ups as well as web3 as engines of growth of the Japanese economy. At the end of 2022, the Japanese government formulated the “Start-up Development Five-Year Plan”, which aims to further increase investment in start-ups by a factor of ten (at a scale of JPY10 trillion) and create 100 unicorn companies and 100,000 new start-ups. Continuing from last year, the Japanese government’s “Basic Policy” for 2023 confirmed its existing policies for promoting start-ups. In addition, the Outline of the 2024 Tax Reform Proposals contains a proposal where the special tax system for angel investors would cover a convertible equity in order to promote start-up investment. In this way, the Japanese government is actively working to expand start-up investment and expand the market.

The Japanese government initiative on expanding start-ups also covers legal issues. Regarding collaboration between big companies and start-ups, there were concerns that start-ups had to conclude disadvantageous contracts due to their relatively weak bargaining power. In this regard, the Ministry of Economy, Trade and Industry and the Japan Fair Trade Commission (JFTC) jointly published the “Guidelines on Business Partnership Contracts with Startups” in 2021 and, as an amendment, the “Guidelines on Business Partnership Contracts with Startups and Investment in Startups” (the “Guidelines”) in 2022. The Guidelines are intended to protect start-ups from requests by business partners or investors which would violate competition law.

The Guidelines can be divided into two parts: (i) issues regarding business partnership contracts with start-ups; and (ii) issues regarding investment in start-ups. The discussion of issues regarding business partnership contracts

Contributed by: Keiji Tonomura, Minh Thi Cao Koike, Akira Komatsu and Yuki Matsumiya,
Nagashima Ohno & Tsunematsu

illustrates potential issues in the following agreements:

- NDA (eg, forcing disclosure of trade secrets);
- PoC agreements (eg, additional work free of charge);
- joint research agreements (eg, unfair transfer of intellectual property rights);
- licence agreements (eg, grant of licences free of charge); and
- other contractual clauses (eg, restrictions on selecting suppliers).

The discussion of issues regarding investments illustrates potential issues in various clauses of investment agreements. For example:

- disclosure of trade secrets;
- appraisal rights (significantly high price, founder's obligation to purchase); and
- most favoured nation clause.

After the publication of the Guidelines, the JFTC has conducted a survey on the status of compliance with the Guidelines and warned some companies that they may be in violation of competition law. When co-operating with or investing in start-ups in Japan, these Guidelines and Japanese practice must be taken into consideration.

Legal Tech

In Japan, legal tech services are being developed in various fields including contract and project management, contract drafting, due diligence, and legal research. In 2022, there was some uncertainty about the legality of AI contract review services in particular. This was highlighted when the Ministry of Justice responded

to inquiries from legal tech service providers about the legality of such services, suggesting that their contemplated services may constitute the unauthorised practice of law. However, in August 2023, the Ministry of Justice issued guidelines clarifying that the following types of contract drafting, review and management services do not constitute the unauthorised practice of law.

- Services that assist in the drafting of contracts and review of legal issues in the ordinary course of business regarding corporate legal matters that do not involve litigation or disputes.
- Services in which, if the language or clauses of the contracts being reviewed are the same as or similar to those pre-registered in the system, such as contract templates or checklists, the said same or similar language or clauses are displayed without individual modification (as opposed to the services that involve the legal processing of the content of the contract based on the specific factual background or instructions regarding the content and the generation of detailed, case-specific drafting or modification of the contract accordingly).
- Services used by lawyers who individually review the material generated by the AI and make necessary changes themselves.

The guidelines have made it clear that the scope of legality for AI contract review services is quite broad. As a result, competition has accelerated among legal tech service providers to develop services, and services using LLM models, such as GPT, are also beginning to be offered.

MACAU, SAR CHINA

Law and Practice

Contributed by:

Pedro Cortés and Luís Rêlo

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

Contents

1. Metaverse p.242

1.1 Laws and Regulation p.242

2. Digital Economy p.242

2.1 Key Challenges p.242

3. Cloud and Edge Computing p.243

3.1 Highly Regulated Industries and Data Protection p.243

4. Artificial Intelligence p.244

4.1 Liability, Data Protection, IP and Fundamental Rights p.244

5. Internet of Things p.245

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.245

6. Audio-Visual Media Services p.246

6.1 Requirements and Authorisation Procedures p.246

7. Telecommunications p.248

7.1 Scope of Regulation and Pre-marketing Requirements p.248

8. Challenges with Technology Agreements p.250

8.1 Legal Framework Challenges p.250

9. Trust Services and Digital Entities p.252

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.252

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 (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.



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 Commission Against Corruption (2010–14) and a jurist at the Office for Personal Data Protection (2014–18).

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



1. Metaverse

1.1 Laws and Regulation

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 Personal Data Protection Bureau (PDPB) 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 Personal Data Protection Bureau (PDPB)

From 1 February 2024, the former Office for Personal Data Protection was replaced by the Personal Data Protection Bureau, pursuant to Administrative Regulation No 42/2023.

Directly under the Chief Executive of the Special Administrative Region of Macau, the PDPB is vested with the same powers and took over the functions and operations of the former 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 PDPB.

The transfer to a legal system which does not ensure an adequate level of protection can be made by notification to the PDPB 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 PDPB 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 (Law No 13/2023 – RJFS) stipulates that the members of the governing bodies of credit institutions, their senior management officers, 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

4.1 Liability, Data Protection, IP and Fundamental Rights

There is currently no specific legislation on artificial intelligence (AI) in the MSAR. However, the challenges presented by the processing of 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 AI tools necessarily include the processing of 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 121/2023, there are 139 such operators, 76 of which belong to the financial sector. As previously indicated, there is currently no specific legislation regarding 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 generally subject to notification to the PDPB, 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 PDPB.

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 PDPB. However, the transfer to a legal system which does not ensure an adequate level of protection can be made by notification to the PDPB 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. Television 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 Government Information Bureau (*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, lastly amended by Administrative Regulation No 40/2022.

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 million, 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 subjects 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 qualifica-

tion, 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 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 Dispatch 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 cyber-

security 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.

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.

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.

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.

MALAYSIA

Law and Practice

Contributed by:

Charmayne Ong, Jillian Chia and Natalie Lim
Skrine



Contents

1. Metaverse p.257

1.1 Laws and Regulation p.257

2. Digital Economy p.259

2.1 Key Challenges p.259

3. Cloud and Edge Computing p.260

3.1 Highly Regulated Industries and Data Protection p.260

4. Artificial Intelligence p.262

4.1 Liability, Data Protection, IP and Fundamental Rights p.262

5. Internet of Things p.266

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.266

6. Audio-Visual Media Services p.267

6.1 Requirements and Authorisation Procedures p.267

7. Telecommunications p.269

7.1 Scope of Regulation and Pre-marketing Requirements p.269

8. Challenges with Technology Agreements p.270

8.1 Legal Framework Challenges p.270

9. Trust Services and Digital Entities p.271

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.271

Skrine is a leading legal firm in Malaysia with a global reputation and a wide range of highly regarded practice groups to cater to the diverse needs of its clients. As one of Malaysia's largest legal firms, **Skrine** prioritises the development of legal minds and the improvement of the community. In an increasingly borderless and competitive world, where the law is challenged in new ways daily, **Skrine** remains steadfast in its founding principles: wisdom, fortitude and ingenuity. The TMT practice currently consists

of six lawyers and has vast experience in providing regulatory advice on various trending telecommunications issues, such as over-the-top (OTT) service offerings, the establishment of data centres for cloud computing services, and the leasing of sub-sea and terrestrial fibres. It also advises clients on regulatory compliance queries and assists them in obtaining regulatory approvals and licences, such as spectrum assignments and telecommunications licences.

Authors



Charmayne Ong heads **Skrine's** IP and TMT practice and is a leading figure in IP and TMT legal advisory and compliance. She has extensive experience and has worked with regulators,

public institutions and companies of all sizes. Charmayne manages the registration of, and general advisory and drafting work relating to, the classic forms of IP rights. She regularly deals with regulators and advises clients on complex regulatory compliance and licensing matters. She is the Malaysian member of the Global Leaders Forum (TMT practice) and a member of the Federation of Malaysian Manufacturers (for IP and TMT).



Jillian Chia is the head of **Skrine's** privacy and data protection practice, and focuses on advising local and multinational companies on data protection and privacy issues.

She reviews and drafts relevant documentation, such as privacy policies, data processor agreements and data transfer agreements, ensuring her clients' internal practices are in line with the requirements of privacy and data protection laws. Jillian's expertise extends to the TMT industry, where she advises global telecommunications and technology companies on their investments and service offerings in Malaysia. She also handles the registration of industrial designs and general advisory work relating to IP rights.

Contributed by: Charmayne Ong, Jillian Chia and Natalie Lim, **Skrine**



Natalie Lim is a partner in Skrine's IP practice, specialising in TMT and data protection. She regularly advises domestic and international clients in the TMT sector on various regulatory matters concerning their infrastructure and services, such as satellite communications, fibre and terrestrial wireless connectivity, cloud services, OTT service, and encryption. Natalie

also advises multinational and local companies on data protection issues, including compliance with data protection laws, drafting the necessary documents and assisting with registration. Her expertise includes advising on, drafting and negotiating IP licence and assignment agreements as well as technology agreements for outsourcing, licensing, development and systems integration.

Skrine

Level 8
Wisma Uoa Damansara
50 Jalan Dungun
Damansara Heights
50490 Kuala Lumpur
Malaysia

Tel: +603 2081 3999
Fax: +603 2094 3211
Web: www.skrine.com

SKRINE

1. Metaverse

1.1 Laws and Regulation

To date, there is no specific or standalone legislation that governs the metaverse. Instead, existing laws govern activities within this evolving digital realm, and their applicability depends on the technologies used and the functionalities they enable.

Contracts and Digital Assets

The metaverse is increasingly becoming a platform for complex interactions and transactions. These transactions often involve digital assets, which can include cryptocurrencies, non-fungible tokens (NFTs) and other virtual property. Understanding the relationship between contracts and digital assets in the metaverse is crucial, as it defines the legal framework for how these assets are traded, owned and managed.

Under the Malaysian Contracts Act 1950 (Contracts Act), transactions within the metaverse, including those concerning digital assets, would be enforceable as long as the essential contractual elements like offer, acceptance, consideration and intention to create legal relations are satisfied without specific documentary requirements. The Electronic Commerce Act 2006 (ECA) (see **9.1 Trust Services and Electronic Signatures/Digital Identity Schemes**) further recognises the validity of electronic messages for contract formation, which could extend to transactions in the metaverse due to the broad definition given under the ECA.

Digital assets in the metaverse may also fall under financial and securities regulations. For instance, in the Malaysian capital markets and securities sector, blockchain-based digital assets could qualify as a “digital currency” or “digital token” as defined under the Capital

Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019 (Prescription Order), and be deemed as securities under the Malaysian Capital Markets and Services Act 2007. This classification subjects them to the oversight of the Securities Commission of Malaysia (SC), and the offering and trade of these digital assets, along with the operation of the platform that hosts these digital assets, will be subject to the approval and registration requirements of the SC. They may also be subject to anti-money laundering/counter-financing of terrorism (AML/CFT) controls. However, the decentralised and often borderless nature of the metaverse poses challenges in regulation enforcement and transaction monitoring.

Intellectual Property

Malaysian intellectual property law may also protect digital creations and innovations within the metaverse. In this context, end-user licence agreements or terms of service serve as a vital mechanism for defining and protecting intellectual property rights. Clear and enforceable terms in these agreements lay the groundwork for safeguarding digital creations. For instance, trade mark rights, copyright protections and other intellectual property considerations can be expressly outlined, guiding users on the lawful usage, reproduction or distribution of virtual assets.

However, the metaverse's unique nature also introduces complex jurisdictional challenges, particularly when addressing infringement claims. The metaverse operates with a degree of anonymity, allowing users to interact with greater privacy than in the physical world, making it challenging to identify infringers and establish concrete jurisdiction.

Data Protection and Cybersecurity

The Personal Data Protection Act 2010 (PDPA) regulates the processing of personal data in commercial transactions, which can extend to the processing of personal data within the metaverse where vast amounts of personal data will be processed. Data users in the metaverse must comply with the PDPA's data protection principles but the metaverse's borderless nature introduces complexities in applying and enforcing data protection laws, including the PDPA.

The seven data protection principles are set out below:

- General Principle – prohibits a data user from processing a data subject's personal data unless consent (or "explicit consent", for sensitive personal data) has been obtained from the data subject or where an exception applies. The General Principle also sets out certain parameters for the processing of personal data. It provides that personal data shall not be processed unless:
 - (a) it is for a lawful purpose directly related to the activity of the data user;
 - (b) it is necessary for or directly related to that purpose; and
 - (c) the data is adequate and not excessive for that purpose.
- Notice and Choice Principle – the PDPA requires a data user to inform a data subject by written notice of certain prescribed matters. It is also mandatory under the PDPA that the written notice (usually issued in the form of a data protection notice or privacy policy) is provided in both English and the national language (Malay).
- Disclosure Principle – prohibits the disclosure, without the data subject's consent, of personal data:
 - (a) for any purpose other than that for which the data was disclosed at the time of collection, or a purpose directly related to it; and
 - (b) to any party other than a third party of the class notified by the data user.
- Security Principle – the PDPA imposes obligations on the data user to take steps to protect the personal data during its processing from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.
- Retention Principle – personal data must not be kept longer than is necessary for the fulfilment of the purpose for which it is processed. The data user has a duty to take reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was processed.
- Data Integrity Principle – the data user must take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date, having regard to the purpose (and any directly related purpose) for which it was collected and processed.
- Access Principle – the data subject must be given the right to access their own data and to correct it where the personal data is inaccurate, incomplete, misleading or outdated. The PDPA provides grounds on which the data user may refuse to comply with a data access or data correction request from the data subject.

Each of these principles is subject to certain exceptions and conditions. Furthermore, there are specific standards set out in the Personal Data Protection Standard 2015 (PDP Standard) for the security, retention and data integrity principles.

The PDPA generally prohibits the transfer of personal data out of Malaysia, except where it is to a permitted place (although no permitted place has been gazetted at the time of writing), or where certain exceptions apply – eg, where data subjects have consented to the transfer.

Consumer Laws

Consumer protection laws remain applicable, safeguarding consumer rights in the context of digital transactions and services. Again, however, there will be difficulties in determining which jurisdiction's laws apply to activities in the metaverse, which is inherently decentralised.

2. Digital Economy

2.1 Key Challenges

The digital economy lacks a singular legislative framework explicitly governing its operations but businesses must comply with various laws, regulations, guidelines and industry codes of conduct that are broadly applicable, as follows.

Consumer Protection

The Consumer Protection Act 1999 (CPA) extends to any trade transaction conducted through electronic means, and the Consumer Protection (Electronic Trade Transactions) Regulations 2012 also mandate the disclosure of specific information by any person who operates a business for the purpose of supplying goods or services through a website or in an online marketplace on the website where the business is conducted.

The Price Control and Anti-Profiteering Act 2011, along with its subsidiary legislation, aims to control the prices of goods and charges for services, and to prohibit profiteering, regardless of the method of supply. It applies to the supply

of goods and services, including through electronic methods.

Electronic Commerce Act

The ECA legally recognises contracts formed through electronic communications, facilitating online business relationships.

Data Protection

Inevitably, the digital economy involves the processing of personal data, which is governed by the PDPA – see **1.1 Laws and Regulation** (Data Protection and Cybersecurity).

Content

Online content is primarily under the purview of the Malaysian Communications and Multimedia Commission (MCMC), which regulates the communications and multimedia industry in Malaysia. Depending on the type of content, it can be subject to a host of laws, including the Communications and Multimedia Act 1998 (CMA), which inter alia prohibits offensive content.

The Malaysian Communications and Multimedia Content Code (Content Code) issued pursuant to the CMA also applies to content made available in the networked medium, including advertisements and marketing, and is administered by the Communications and Multimedia Content Forum of Malaysia (CMCF). Compliance with the Content Code is voluntary unless the content provider is a member of the Content Forum, has voluntarily agreed to be bound by the Content Code, or is specifically directed by MCMC. However, the CMCF may impose sanctions on those subject to the Content Code following a complaint, and compliance is a defence against any prosecution, action or proceeding of any nature.

In aiming to facilitate self-governance for online curated content, the CMCF introduced its inau-

gural supplementary guidelines in December 2023: the Guidelines for Online Curated Content (OCC) Service Providers, which cover recommendations and best practices for OCC service providers. The Guidelines encompass the overarching principles of public and national interest, racial and religious sensitivities, and improvement of accessibility standards for disabled persons.

Payment

Electronic money (e-money) is governed by the Financial Services Act 2013 and the Islamic Financial Services Act 2013, and is recognised as a payment instrument under said Acts. E-money issuers must be approved by the Central Bank of Malaysia (BNM) and must adhere to the Policy Document on Electronic Money issued by BNM. For digital currencies and digital tokens, see **1.1 Laws and Regulation**.

Key Legal Challenges

While offering numerous opportunities for innovation and growth, the digital economy presents several key legal challenges. One of the biggest challenges is ensuring privacy and data protection, given the vast amounts of personal data collected and processed. Laws like the GDPR set stringent standards but compliance and enforcement can be complex, especially for global businesses. In Malaysia, while there are laws on data protection, there are plans to strengthen the regulatory framework, including by amending the PDPA and introducing a new cybersecurity law. Balancing the regulation of digital content to prevent the spread of offensive and harmful content while respecting freedom of expression also poses a significant challenge for regulators.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Industry Codes of Conduct

In Malaysia, cloud and edge computing services are regulated through various legislative provisions, technical codes and guidelines. The primary legislation is the CMA, enforced by the MCMC.

CMA

Under the CMA, providers of cloud and edge computing services may require the following types of licences, depending on the exact service offerings, technical set up and network topology, as the requirement for a licence depends on whether the activities fall within a “licensable activity”.

- Applications Service Provider (ASP) Licence: for providing end-user services through network services, including cloud services and internet access services. Notably, cloud services have been regulated as a licensable activity requiring an ASP licence since 1 January 2022.
- Network Facilities Provider (NFP) Licence: for the ownership and provision (including maintenance, installation, operation and establishment) of network facilities or physical infrastructure – eg, fixed links and cables.
- Network Service Provider (NSP) Licence: for providing network services for basic connectivity and bandwidth supporting various applications – eg, bandwidth services, switching services, access applications service and gateway services.

These licences are available to local entities and are issued as either individual or class licences (ASP licences are only issued as class licences).

If a CMA licence is required, the CMA imposes a host of obligations, including mandatory contributions to the universal service provision fund and compliance with the access regime.

Whilst not specific to companies providing cloud or edge computing services, any company intending to import, use or offer communications equipment for sale must ensure that such equipment has been certified in accordance with the relevant technical standards/codes.

Technical codes and guidelines set out additional standards for specific types of equipment and service offerings. For instance, the Technical Code on Information and Network Security – Cloud Service Provider Selection provides selection criteria for cloud service providers based on risk assessment, industry standards and certification capabilities.

PDPA

The PDPA is the main framework for personal data protection in Malaysia, imposing obligations on data users (those who either alone or jointly, or in common with other persons, process any personal data or have control over or authorise the processing of any personal data) when using cloud and edge services. Key requirements include:

- ensuring – for the purpose of protecting personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction – that data processors (eg, a cloud and edge computing service provider) who process personal data on their behalf provide sufficient guarantees in respect of the technical and organisational security measures governing the processing of such personal data, and that the data processor takes reason-

able steps to ensure compliance with those measures;

- prohibitions on transferring personal data outside Malaysia, subject to certain exceptions; and
- adherence to the PDP Standard, which imposes obligations on data users to ensure that, inter alia, transfers of personal data through cloud and edge computing services are recorded and that the written consent of an officer authorised by the top management of the data user organisation is obtained before such a transfer is made. Personal data transferred through a cloud and edge computing service must comply not only with the personal data protection principles in Malaysia but also with the personal data protection laws of other countries.

CMA licensees must register as data users with the Personal Data Protection Commissioner and comply with a specific code of practice for personal data protection.

Currently, the PDPA does not contain direct obligations for data processors and does not provide for a general data localisation requirement, although there has been a public consultation paper suggesting that these might be introduced in the future.

Greater Restrictions for Certain Industries

Financial services laws

Certain regulated industries, like banking and insurance, face stricter regulations when utilising data processing and other technological services from third parties, including cloud and edge computing services.

BNM has issued policy documents on risk management, outsourcing and customer information management. Among other stipulations, finan-

cial institutions (FIs) must consult with BNM before using a public cloud for critical systems, and must notify BNM prior to the use of cloud services for non-critical systems. In respect of outsourcing arrangements, which includes outsourcing arrangements with cloud and edge service providers, the Policy Document on Outsourcing requires, among other things, that FIs obtain BNM's approval before entering into an outsourcing arrangement, and that FIs that use cloud services maintain a register containing additional particulars of the arrangement – ie, the nature of the data held and the locations where it is stored.

The Policy Document on Management of Customer Information and Permitted Disclosures outlines requirements for FIs regarding measures and controls in handling customer information throughout the information life cycle, covering the collection, storage, use, transmission, sharing, disclosure and disposal of customer information. Among other things, FIs must ensure that the service-level agreement between them and the provider adequately reflects the FI's obligation to safeguard customer information.

Specifically on cloud services, the Policy Document on Risk Management in Technology requires FIs to conduct comprehensive risk assessments prior to utilising cloud services and to implement safeguards to protect customer information. The Policy Document also includes specific guidance for assessing the key risks and control measures when utilising cloud services.

Government entities

Where cloud and edge computing services are provided to government entities, policy documents may mandate specific security measures, such as infrastructure and traffic segregation when handling official secrets, as well as access

controls. Although there is no overarching mandate for data centres to be designated as “protected areas” or “protected places”, facilities and data centres of cloud and edge service providers that handle or store official secrets are subject to stricter regulations. These facilities may need to be classified areas, potentially being designated as prohibited areas to which access is heavily restricted.

Healthcare laws

Government approval may be required for the use and provision of cloud computing services in public hospitals and institutions. Healthcare providers may also be subject to separate data localisation requirements or requirements to maintain patient data within the healthcare facilities.

Others

Data localisation requirements may also vary by industry – eg, e-money licences may impose this requirement as a licence condition.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

While there is growing acceptance of the implications of artificial intelligence (AI), Malaysia has not yet established specific legislation or guidelines dedicated exclusively to regulating AI. The Ministry of Science, Technology and Innovation (MOSTI) is exploring the regulation of AI applications and a proposed ethics and governance code for AI, which aims to address issues such as data privacy, public awareness of AI, transparency, accountability and cybersecurity. The code may also incorporate guidelines for educating the public about AI and promoting research in the field, and is being drafted

based on the Recommendation on the Ethics of AI adopted by the United Nations Educational, Scientific and Cultural Organisation (UNESCO) in November 2021.

The Minister of Economy has also referred to the Malaysian government's plan to transform Malaysia into a regional AI hub by implementing new strategies and improvements of the AI ecosystem that will be contained in the Kuala Lumpur (KL20) action plan.

Complementing these initiatives, the Malaysian Standards Department has formed a National Mirror Committee to draft national AI standards. This committee, chaired by MIMOS Berhad (a research and development centre under MOS-TI), comprises representatives from the industry, academia and government ministries and agencies, ensuring a comprehensive approach to AI standardisation.

The Malaysia National AI Roadmap 2021–2025 (AIRmap) further outlines the government's vision for AI development, proposing to establish an AI Coordination and Implementation Unit (AI-CIU) to be responsible for institutionalising existing cybersecurity policies and best practices for AI incorporation and establishing clear guidelines for data sharing within government to enable AI implementation.

It was reported in June 2023 that ministers from the ASEAN nation members agreed in February 2023 to develop an "ASEAN Guide on AI Governance and Ethics", although details on what this guide would entail are not available at the time of writing.

Some of the key issues which could be relevant are discussed below.

Liability and insurance

In the absence of specific legislation, liability resulting from AI-enabled technologies would have to be addressed under the existing legal framework. This includes the CPA and the Sale of Goods Act 1957 (SOGA) (although AI or its output may not be classified as "goods"), along with established principles of contract and tort law.

Contract law, particularly the Contracts Act, would be relevant in evaluating liability for defective AI. Contractual provisions specific to AI usage may be incorporated to apportion liability for AI defects, but the effectiveness of such clauses has not been tested and, in the absence of case law, claimants may argue breaches of the implied terms under statutes such as the CPA and SOGA, which contain implied terms (eg, guarantees and conditions regarding title, quality, fitness for purpose, price and repairs) that cannot be contractually excluded. The manufacturer or supplier of AI technologies may be liable for malfunctions that breach these implied terms, depending on the extent of non-compliance with representations and guarantees made by the supplier regarding the technology. Product liability claims for AI under the CPA may, however, be particularly challenging due to the difficulties in pinpointing when defects occur and, unlike some jurisdictions like the European Union, there is no specific framework for AI liability in Malaysia.

Claims for damages in the context of AI-related incidents may also be framed in negligence. Central to the law of negligence is the concept of the foreseeability of loss, requiring a claimant to establish a direct chain of causation between their loss and the actions of the defendant. However, there are distinct challenges in applying traditional negligence principles (such as fore-

seeability and causation), given the unique characteristics of AI, particularly its ability to evolve and learn over time through machine learning. Similarly, vicarious liability – a legal principle governing accountability for one person's actions by another in a legal relationship – becomes complex when applied to AI. Associated with the relationship between a principal and an agent, such as employer and employee, vicarious liability may be argued in instances where AI, operating within designated tasks, causes harm. Here, the AI may be viewed as an intellectual agent whose actions are assigned to a principal but not recognised as a full legal person.

Nevertheless, vicarious liability comes with constraints, dictated by the scope of the agent's activity. Not every action of AI may be ascribed to its owner or operator, and deviations from defined responsibilities can introduce a responsibility gap, disrupting the chain of causation.

Evidently, each case will need to be meticulously examined on its individual merits, factoring in the complex interplay between AI's autonomous capabilities and the responsibilities of those who create and deploy these systems.

Data protection

There are challenges in safeguarding sensitive and confidential information in the process of using AI, since input data can serve as ongoing training material for the AI model. The machine learning aspect of AI would require large amounts of data for AI training and operation, which can trigger the applicability of the PDPA where personal data is involved. Organisations must ensure that all data and information processed by AI is compliant with applicable data protection laws, including the PDPA. There are no specific rules under the PDPA on AI but, in general, data users must ensure they are trans-

parent about the use of AI and how data subjects' personal data is being collected, used and processed.

Organisations must ensure that they have obtained the necessary consent from individuals for the processing of their personal data for the specific purposes for which it is being collected, and must make sure that such data is processed securely and safely. This becomes a challenge where "data scraping" is utilised to extract large datasets which are then used to "train" AI models – ensuring that each data subject whose personal data was "scraped" has consented to the use of their personal data in this way would be practically impossible.

Future legal developments, such as the forthcoming Profiling and Automated Decision-Making Guideline announced by the Minister of Digital, may introduce additional requirements and restrictions relevant to the processing of personal data in AI applications, so it is crucial for organisations to stay abreast of these developments as AI regulation evolves.

Intellectual property (IP)

The current IP statutory regime in Malaysia presents ambiguities when it comes to extending protection to AI-generated IP. This uncertainty arises due to the lack of specific provisions addressing AI's role in IP creation under existing laws.

In essence, AI can be conceptualised as a compilation of software algorithms operating on computer systems. These algorithms execute mathematical methods to emulate the problem-solving and decision-making abilities of humans. However, seeking patent protection for AI becomes challenging, as it may infringe upon what is traditionally deemed non-patentable or

excluded subject matter in many jurisdictions, including Malaysia. This contention is exemplified in Section 13(1) of the Patents Act 1983 (PA), which expressly deems mathematical methods per se as being non-patentable.

When assessing the existing patent framework, particularly in the PA and the Patents Regulations 1986, the lack of an explicit definition of an “inventor” and the absence of provisions addressing AI involvement in the invention process leave room for ambiguity. The inclination in the language of these statutes suggests that AI may be excluded from coverage thereunder, and that inventors are expected to be natural persons. This expectation is notably reinforced by Section 18 of the PA, which vests the right to apply for a patentable invention in the inventor. Furthermore, according to the Patents Regulations, patent applications must include personal identification of the inventors, or signed written declarations where anonymity is sought.

Similar perspectives have emerged internationally. In the United Kingdom, both the High Court and the Court of Appeal have agreed that an inventor must be a natural person and cannot include an AI system. In addition, the Federal Court in Australia overturned its previous decision, stating that the “inventor” listed in an application for a patent under the Patents Act must be a natural person. However, it is crucial to note that the Federal Court in Australia clarified that its ruling does not preclude the possibility of granting a patent to an invention created by an AI system. Instead, it underscores the necessity to identify a human “inventor” for the patent application, such as the developer of the AI system. Therefore, an invention devised by an AI system may still receive patent protection, provided a human “inventor” is identified.

The situation is similarly unclear under the Copyright Act 1987 concerning AI-created works. The ongoing discussion as to whether AI-generated work is protected by the Copyright Act revolves around its language, which primarily focuses on the rights of individuals and legal entities. For instance, Section 10 of the Copyright Act grants copyright to works eligible for protection, requiring the author to be a qualified person at the time of creation. A “qualified person” is defined as follows:

- in relation to an individual, a person who is a citizen of, or a permanent resident in, Malaysia; and
- in relation to a body corporate, a body corporate established in Malaysia and constituted or vested with legal personality under the laws of Malaysia.

While untested in Malaysian courts, the existing legal framework suggests that AI-created works may not qualify for copyright protection. The argument stems from the notion that AI-created works are essentially computer-generated, and the AI creator does not neatly fit the definition of a “qualified person” under the law.

Examining the current UK legislative framework reveals that a natural person would be the author for copyright ownership for the purposes of computer-generated works; this would therefore exclude an AI system. This position has recently been affirmed by the UK Supreme Court in *Thaler (Appellant) v Comptroller-General of Patents, Designs and Trade Marks (Respondent)* 2023 UKSC 49. The UK courts have consistently held that it is likely necessary for a human to have at least exercised some degree of control over the creative process that resulted in the work in question to attract copyright protection. This approach aligns with the principle that copyright

should be tied to human agency in the creative process, raising similar questions about the attribution of authorship and copyright eligibility in AI-generated works. Malaysia has yet to provide explicit guidance on these matters, but the UK decision sets a precedent that could influence future rulings in common law jurisdictions such as Malaysia.

Another consideration would be when a user edits AI-generated output, transforming it into their independent creation. This action may arguably meet the criteria set forth in Section 7 of the Copyright Act, requiring sufficient effort to render the work original and reducing it to material form. Such a transformation raises questions about the eligibility of this modified creation for copyright protection. This scenario prompts inquiries into the interplay between AI and human creativity, potentially signalling the need for copyright law to evolve and adapt to these emerging dynamics. Other key considerations include the duration of copyright in AI-created works, moral rights related to AI, and the enforcement of copyright for such works.

The above highlights the need for clear regulatory guidelines and legal frameworks to address the intricacies of AI involvement in IP creation. As AI technology continues to evolve, establishing clear parameters and legal clarity becomes essential to navigate the intricate intersections of AI and intellectual property rights.

5. Internet of Things

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

At present, Malaysia lacks a dedicated statute specifically addressing the internet of things

(IoT). However, regulation is achieved through existing sector-specific guidelines and a suite of laws that possess sufficient breadth to encompass IoT projects. Key examples of such encompassing laws, regulations and guidelines are outlined below.

Telecommunications Regulations

In the implementation of IoT initiatives, adherence to the licensing and regulatory framework of the CMA is mandatory. This framework, inclusive of spectrum usage requirements, is particularly pertinent when engaging in licensable activities specified in the CMA and its subsidiary legislation; see **7.1 Scope of Regulation and Pre-marketing Requirements**. Procuring the necessary licence is obligatory, accompanied by compliance with diverse obligations stipulated in the CMA. Notably, projects involving spectrum usage must align with assignments by MCMC, in harmony with the Spectrum Plan and relevant Standard Radio System Plans. In addition, communications equipment, integral to IoT, must obtain certification from the certifying body designated by MCMC, namely SIRIM QAS International Sdn Bhd, ensuring adherence to safety and technical standards, including the Technical Code on Short Range Devices.

Various technical codes also contribute to the regulatory framework for IoT, covering areas such as application security requirements, high-level functional architecture, security management and short-range device specifications.

Cybersecurity

Despite the absence of a dedicated cybersecurity law, Malaysia has adopted a proactive stance in addressing emerging threats. The Minister of Communications, Fahmi Fadzil, disclosed plans for an upcoming Cybersecurity Bill, spearheaded by the National Cyber Security Agency (NACSA).

This initiative signifies a critical step in reinforcing Malaysia's digital resilience, and underscores Malaysia's commitment to swift adaptation to evolving cyber threats. The bill aims to establish a legal structure promoting proactive governance, effective response mechanisms and continuous improvement in cybersecurity.

Organisations undertaking IoT projects are advised to consider existing legislation with potential relevance to cybersecurity, including laws such as the Computer Crimes Act 1997, the Penal Code, the Copyright Act, the Digital Signature Act 1997, the Strategic Trade Act 2010 and the Official Secrets Act 1972. Furthermore, the Guidelines for Secure Internet of Things, released in 2020 by CyberSecurity Malaysia (an agency under the purview of MCMC), offer valuable yet non-binding insights. These guidelines serve as a practical resource, outlining security requirements and controls for stakeholders, with the objective of establishing a robust IoT security framework and enhancing awareness of existing threats and vulnerabilities.

Data Protection

As IoT initiatives extend into machine-to-machine communications, the relevance of data protection and communications secrecy comes to the forefront. Cross-border data flows between IoT devices necessitate a nuanced approach, considering compliance requirements, especially regarding the consent of data subjects for cross-border transfers of personal data via IoT devices. This entails a commitment to key data protection principles under the PDPA.

The IoT Guidelines provide a comprehensive set of security controls, facilitating the development of secure IoT systems. These controls include risk mitigation measures related to communications encryption, cloud security, authentication,

access control, data protection and privacy, operation and maintenance, among others. This holistic approach aims to navigate the complexities of data protection and communications security in the evolving landscape of IoT projects in Malaysia.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Regulation of the Media Sector

In Malaysia, content is governed by a host of laws, depending on the type of content. Online content/content in the networked medium, which would include video channels, is primarily under the purview of MCMC, which also regulates licensing requirements for the provision of content in general. Specifically on censorship, the Film Censorship Board (FCB) regulates traditional media outlets and content on TV and in cinemas. The National Film Development Corporation Malaysia (FINAS) has prerogative over film production, distribution and exhibition activities in Malaysia. Note that the likelihood of enforcement by FINAS and FCB may differ for over-the-top content, including video-sharing platform services.

Licensing Requirements – CMA

Under the CMA, providers of content applications services are required to obtain a Content Applications Service Provider (CASP) licence, unless specifically exempted under the CMA. The CMA provides exemptions from licensing requirements for providers of “closed” content applications services (ie, services that are not accessible to the general public) and “incidental” content applications services (ie, services that provide content in a manner entirely incidental to the service provided). Internet content appli-

cations services (such as over-the-top services and online video-sharing platforms) are also exempted under the Communications and Multimedia (Licensing) (Exemption) Order 2000.

CASP licences may be issued as either individual licences or class licences (see **7.1 Scope of Regulation and Pre-marketing Requirements**). CASPs that meet the following criteria are likely to require an individual licence, on the basis that the content:

- is made available to the general public and is likely to be of broad appeal; and
- can be received by commonly available consumer equipment or is likely to exert a high degree of influence in shaping community views in Malaysia.

CASP individual licences are typically required for entities involved in the traditional broadcasting industry, such as terrestrial radio broadcasting, satellite broadcasting, terrestrial free-to-air TV and subscription broadcasting. On the other hand, CASPs providing limited content applications services are not required to hold an individual licence and are exempted from the requirement to be licensed, unless a class licence is applicable. A CASP of a limited content applications service is regulated by a class licence if it falls within the following categories:

- a content applications service of limited appeal or one that is targeted at a special interest group and available through subscription by persons using equipment specifically designed for receiving said service;
- a content applications service restricted to a particular geographic area;
- a content applications service for distance-learning purposes; or

- a content applications service specifically linked to or associated with a sporting, cultural or other one-off event.

As an industry regulated under the CMA, licences for the provision of content applications services are subject to the same fees and eligibility requirements as telecommunications services, and the applicable fees and eligibility requirements would depend on whether the licence is an individual licence or class licence (see **7.1 Scope of Regulation and Pre-marketing Requirements**). Applications for licences are to be made to MCMC in the prescribed forms.

Other Licences/Approvals

Depending on the facts, additional licensing requirements may apply. For example, the production, distribution or exhibition of films may require a licence from FINAS. Such films may also require the approval of the FCB.

Content Requirements and Restrictions

As set out above, content is subject to a host of laws, depending on the type of content, with the main laws being:

- the CMA;
- the Printing Presses and Publications Act 1984;
- the Sedition Act 1948;
- the Penal Code;
- Sharia; and
- advertisement laws, codes and guidelines.

For example, the CMA generally prohibits the provision of content that is indecent, obscene, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass any person via a content applications service, and content that is deemed seditious will contravene the Sedition Act. Additional laws may also

apply, depending on the specific facts, such as the Copyright Act for content that infringes copyright.

To aid the regulation of the content industry, the CMCF issued the Content Code, which contains obligations and restrictions relating to content, and guidelines for a variety of different content platforms, including advertising guidelines, specific broadcasting guidelines and specific online guidelines.

Of relevance to providers of video-sharing platform services, the Content Code stipulates that providers of access to content that have neither control over the composition of such content nor any knowledge of such content are deemed innocent carriers, and are not responsible for the content provided, although there is also case law suggesting that an online intermediary platform may still be liable for third-party content.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The regulatory and licensing framework under the CMA is sufficiently extensive to cover a wide range of technologies and services, even in the absence of specific references to individual technologies and services. Specific technologies and services may also be addressed through various regulations, guidelines, technical codes and other voluntary codes issued by MCMC and/or other industry forums.

Licensing

Under the current telecommunications regime, there are four categories of licensable activities.

- NFP for the provision of network facilities such as infrastructure – eg, satellite earth stations, fixed links and cables.
- NSP for the provision of network services for basic connectivity and bandwidth to support a variety of applications – eg, switching services, bandwidth services, access applications service, gateway services and cellular mobile services.
- ASP for the provision of particular functions, such as voice services, data services, content-based services, electronic commerce and other transmission services. Applications services are essentially the functions or capabilities that are delivered to end-users. Examples include PSTN telephony, public cellular services, IP telephony, public switched data services, directory services, internet access services and messaging services.
- CASP for the provision of application services that provide content, such as satellite and subscription broadcasting.

Spectrum

Aside from telecommunications licences, the use of spectrum is regulated and an assignment of spectrum is required in order to use any part of the spectrum. The use of the spectrum is prohibited without one of the following:

- a spectrum assignment, which confers rights on a person to use one or more specified frequency bands for any purpose consistent with the assignment conditions set by MCMC;
- an apparatus assignment, which confers rights on a person to use the spectrum to operate a network facility of a specified kind at a specified frequency at a specified frequency band or bands; or
- a class assignment (CA), which confers rights on any person to use the frequency(ies) for

a list of devices. The usage of devices under a CA is subject to conditions provided in the CA issued under Section 169 of the CMA. A CA is valid until it is cancelled by MCMC.

If the technology or device falls under any of the Schedules under the latest CA document, and use thereof complies with the requirements (including any conditions attached to the CA), no fees or application will be required. The use of device and frequency/frequency band for any purpose other than specified in the Schedules requires approval from MCMC.

The devices must also be certified by MCMC or its registered certifying agency (ie, SIRIM) either with a compliance approval, which is granted to a specific model of a device that has been certified as compliant with the specified standards or technical codes, or by way of a special approval. Special approvals are only granted to equipment that is used exclusively by the applicant for specific purposes.

Other Issues

Aside from the licensing and spectrum requirements outlined above, there may potentially be other issues, like numbering requirements, technical standards, etc, depending on the specific facts and services.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

A variety of challenges that apply generally to contracts will also apply to technology agreements, but there may be unique challenges posed, especially when contracting with Malaysian government or customers from highly regulated industries such as finance and healthcare.

Some of the key challenges that organisations may face when entering into a technology agreement are outlined below.

IP Rights

One of the critical aspects of technology agreements is the handling of IP rights, and common challenges include ambiguity as to the ownership of IP rights and joint ownership issues (note that in the absence of an agreement, joint ownership may also arise by operation of law when the IP is jointly developed or created by two or more persons). If IP is jointly owned, there are certain risks (eg, in relation to granting a licence) and, in certain circumstances, a joint decision by both parties is required, depending on the type of IP involved. Therefore, it is advisable to expressly stipulate the rights and obligations of the respective parties under the agreement, as well as whether there are restrictions imposed on the parties. Furthermore, parties should negotiate and define who bears the responsibility for enforcing the IP rights against an infringer, who will pay for and control the enforcement process, and how costs and expenses are allocated among the parties.

Scope of Work

Aside from ownership of the technology in question and IP licensing, disputes also typically revolve around the scope of work and non-payment. A well-defined scope of work and clear deliverables are crucial to prevent such disputes, which includes detailing project timelines, performance criteria and service level obligations, milestones, change of control and project governance.

Confidentiality, Data Protection and Cybersecurity

With the increasing importance of data in the digital economy, technology agreements must

sufficiently address confidentiality, data protection and cybersecurity. The role of confidential information is especially critical where IP law does not offer adequate safeguards. Agreements must also ensure compliance with applicable laws like the PDPA. Furthermore, in highly regulated sectors, there tend to be stricter requirements on data protection and cybersecurity, which must be catered for in the agreement. For instance, health data that is categorised as “sensitive personal data” under the PDPA may be subject to localisation requirements, particularly in the private healthcare sector.

Sector-Specific Requirements

Where the technology agreement is with an organisation in a regulated industry, the organisation should be aware that it may also be subject to other regulations or guidelines.

For instance, FIs in Malaysia are subject to guidelines issued by BNM and some of BNM’s Guidelines – in particular, the Risk Management in Technology Guidelines – set out certain requirements concerning engaging third-party service providers. For example, where an FI’s IT system is managed by third-party service providers, the FI is required to ensure, including by way of contractual obligations, that the relevant third-party service providers give sufficient notice before any changes that may impact the IT system are undertaken. Furthermore, an FI or financial service provider may be required to include specific provisions in its contract with the organisation and certain contracts/arrangements may require approval from BNM, pursuant to the requirements under the relevant BNM Guidelines.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Overview

In Malaysia, contracts formed electronically are recognised pursuant to the ECA. The ECA provides for legal recognition of electronic messages in commercial transactions and the use of electronic messages to fulfil legal requirements, and enables and facilitates commercial transactions through the use of electronic means.

As long as there is compliance with the requirements for an “electronic signature” or “digital signature”, as set out below, the general rule is that acceptance by electronic means will be legally recognised and enforceable, unless the document is subject to a specific statutory form requirement.

Note that there is a distinction between electronic signatures and digital signatures under Malaysian laws, whereby the latter is a sub-set of the former and uses certificate-based digital IDs to authenticate each signer’s identity. There are two separate statutes governing both types of signatures, namely the ECA and the Digital Signature Act 1997 (DSA). The legal requirements under both statutes are set out below.

Electronic Signatures

The ECA recognises the use of an electronic signature (defined 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”), provided that certain conditions are met, as follows:

- it is attached to or is logically associated with the electronic message;

- it adequately identifies the person and adequately indicates the person's approval of the information to which the signature relates; and
- it is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.

An electronic signature will be considered "as reliable as is appropriate" if it can be shown that the means of creating the electronic signature is linked to and under the control of that person only, and that any alteration made to the electronic signature or document after the time of signing is detectable.

There has not been much guidance as to the exact measures that must be taken to ensure that an electronic signature complies with these requirements. The case of *Yam Kong Seng & Anor v Yee Weng Kai* [2014] 4 MLJ 478 provides some guidance, wherein an SMS was deemed to have fulfilled the requirements of an electronic signature under the ECA as the sender was adequately identified with the telephone number representing the caller or the sender of the electronic message. However, as this case appears to apply a very liberal interpretation, it remains to be seen whether this would continue to be upheld.

The following types of documents cannot be signed or executed electronically if they are intended to be legally binding:

- power of attorney;
- the creation of wills and codicils;
- the creation of trusts; and
- negotiable instruments.

Depending on the documents to be executed, other laws may come into play when determin-

ing whether an electronic signature would be legally binding – eg, certain types of documentation may be required to be notarised (statutory declarations, money lending agreements, etc) and therefore having the document electronically signed may not be sufficient. Furthermore, where any law requires a seal to be affixed to a document, an electronic signature will not suffice as the ECA states that the requirement of the law would only be fulfilled, if the document is in the form of an electronic message, by a digital signature as defined under the DSA.

The ECA is complemented by the Electronic Government Activities Act 2007, which provides for legal recognition of electronic messages in dealings between the Malaysian government and the public.

Digital Signatures

Under the DSA, "digital signature" is defined as "a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine –

- whether the transformation was created using the private key that corresponds to the signer's public key; and
- whether the message had been altered since the transformation was made."

Furthermore, under the DSA, where a rule of law requires a signature or provides for certain consequences in the absence of a signature, that rule shall be satisfied by a digital signature where:

- that digital signature is verified by reference to the public key listed in a valid certificate issued by a licensed certification authority;

- that digital signature was affixed by the signer with the intention of signing the message; and
- the recipient has no knowledge or notice that the signer:
 - (a) has breached a duty as a subscriber; or
 - (b) does not rightfully hold the private key used to affix the digital signature.

The DSA further provides that a document signed with a digital signature that meets these requirements for validity is as legally binding as a document signed with a handwritten signature, or an affixed thumbprint or any other mark.

Digital Identity Scheme

In pursuit of enhancing Malaysia's digital service and economy, the Malaysian government has unveiled the National Digital Identity Initiative as a verifiable platform of trust to verify internet identities or individual virtual identities in the cyber realm. Following this, Prime Minister Datuk Seri Anwar Ibrahim announced in August 2023 that the development of the National Digital Identity (IDN) will be fast-tracked to boost digital transformation in the public sector.

The Prime Minister added that the government will further implement initiatives to strengthen the ecosystem and boost involvement for start-up companies.

Trends and Developments

Contributed by:

Charmayne Ong, Jillian Chia and Natalie Lim
Skrine

Skrine is a leading legal firm in Malaysia with a global reputation and a wide range of highly regarded practice groups to cater to the diverse needs of its clients. As one of Malaysia's largest legal firms, Skrine prioritises the development of legal minds and the improvement of the community. In an increasingly borderless and competitive world, where the law is challenged in new ways daily, Skrine remains steadfast in its founding principles: wisdom, fortitude and ingenuity. The TMT practice currently consists

of six lawyers and has vast experience in providing regulatory advice on various trending telecommunications issues, such as over-the-top (OTT) service offerings, the establishment of data centres for cloud computing services, and the leasing of sub-sea and terrestrial fibres. It also advises clients on regulatory compliance queries and assists them in obtaining regulatory approvals and licences, such as spectrum assignments and telecommunications licences.

Authors



Charmayne Ong heads Skrine's IP and TMT practice and is a leading figure in IP and TMT legal advisory and compliance. She has extensive experience and has worked with regulators,

public institutions and companies of all sizes. Charmayne manages the registration of, and general advisory and drafting work relating to, the classic forms of IP rights. She regularly deals with regulators and advises clients on complex regulatory compliance and licensing matters. She is the Malaysian member of the Global Leaders Forum (TMT practice) and a member of the Federation of Malaysian Manufacturers (for IP and TMT).



Jillian Chia is the head of Skrine's privacy and data protection practice, and focuses on advising local and multinational companies on data protection and privacy issues.

She reviews and drafts relevant documentation, such as privacy policies, data processor agreements and data transfer agreements, ensuring her clients' internal practices are in line with the requirements of privacy and data protection laws. Jillian's expertise extends to the TMT industry, where she advises global telecommunications and technology companies on their investments and service offerings in Malaysia. She also handles the registration of industrial designs and general advisory work relating to IP rights.

Contributed by: Charmayne Ong, Jillian Chia and Natalie Lim, **Skrine**



Natalie Lim is a partner in Skrine's IP practice, specialising in TMT and data protection. She regularly advises domestic and international clients in the TMT sector on various regulatory matters concerning their infrastructure and services, such as satellite communications, fibre and terrestrial wireless connectivity, cloud services, OTT service, and encryption. Natalie

also advises multinational and local companies on data protection issues, including compliance with data protection laws, drafting the necessary documents and assisting with registration. Her expertise includes advising on, drafting and negotiating IP licence and assignment agreements as well as technology agreements for outsourcing, licensing, development and systems integration.

Skrine

Level 8
Wisma Uoa Damansara
50 Jalan Dungun
Damansara Heights
50490 Kuala Lumpur
Malaysia

Tel: +603 2081 3999
Fax: +603 2094 3211
Web: www.skrine.com

SKRINE

TMT in Malasia: An Introduction

In a year marked by pivotal advancements, the TMT sector has witnessed significant regulatory shifts that signal a clear intent by the government to strengthen oversight in the TMT sector. These changes, driven by the need to balance innovation with responsible governance, have garnered considerable attention in Malaysia. This article will spotlight the key regulatory developments that have dominated the headlines in the TMT sector throughout the year.

Content regulation

With the ever-increasing popularity of content-driven social media platforms and online content, the Malaysian government has been increasingly active in its regulation of content, with reports indicating that it has issued a record number of requests to certain popular social media platforms to remove or restrict content deemed divisive or provocative. Legal and regulatory developments in this space also indicate the government's increasing scrutiny of content.

In November 2023, it was reported that the government is considering mandatory registration for all social media platform service providers with the Malaysian Communications and Multimedia Commission (MCMC). The Minister of Communications, Fahmi Fadzil, said this move is deemed appropriate to ensure all such providers understand and comply with the country's legislation.

Furthermore, the Malaysian Media Council Bill aims to regulate Malaysia's media industry and will, inter alia, address issues related to advertising revenue for media organisations and include a grievance mechanism to enable any party to lodge complaints to the council on their dissatisfaction about any news. Deputy Minister of Communications, Teo Nie Ching, emphasised

the bill's role in promoting responsible media practices and stated that the council will serve as an authoritative body to decide whether a news report has violated journalistic ethics (eg, whether the contents of an article are ethical or unethical) or whether the article is using click-bait headlines to invoke emotional reactions in readers. At the time of writing, the bill's content is under scrutiny, with discussions reportedly focused on definitions, enforcement powers and other key issues, with the aim of reaching a consensus among all stakeholders.

In December 2023, the Communications and Multimedia Content Forum of Malaysia (Content Forum) published the Guidelines for Online Curated Content (OCC) Service Providers, which set out recommendations and best practices for OCC service providers. The guidelines encompass overarching principles of public and national interest, racial and religious sensitivities, and the improvement of accessibility standards for disabled persons. They also address other key points, such as:

- content classifications;
- consumer safeguards;
- content advertising and promotion;
- news and other factual content; and
- consumer protection and feedback mechanisms.

Developments in Malaysia's 5G landscape

In recent years, Malaysia has taken proactive measures to adequately integrate 5G technology. The roll-out began in late 2021 through a Single Wholesale Network (SWN) model led by Digital Nasional Berhad (DNB), the special-purpose vehicle established by the Malaysian government to drive the development of 5G infrastructure in Malaysia, in which the government was initially the sole shareholder. Since

then, there have been notable developments in Malaysia's 5G landscape.

Shortly after its formation, equity stakes in DNB were offered to major Malaysian mobile network operators (MNOs); as of 1 December 2023, five major MNOs have each signed share subscription agreements (SSA) with DNB. Under their respective SSAs, the MNOs will each subscribe for 100,000 shares in DNB and make an advance of MYR233,333,333 to DNB as prepayment for 5G products and services. The SSAs give effect to the MNOs' total subscription of 70% equity in DNB, with each MNO obtaining a 14% stake. The remaining 30% of DNB's share capital will be held by the Minister of Finance Inc. of Malaysia, which will, in addition, hold a "special share" that confers certain rights involving national interests, as well as the right to appoint a director to DNB's board of directors to represent the Malaysian government's interests. The five MNOs are CelcomDigi Berhad (via its wholly-owned subsidiary, Infranation Sdn Bhd), Maxis Berhad (via its wholly-owned subsidiary, Maxis Broadband Sdn Bhd), U Mobile Sdn Bhd, Telekom Malaysia Berhad and YTL Power International Bhd (the holding company of YTL Communications Sdn. Bhd.).

In May 2023, after a five-month review, the government decided to transition from the SWN model to a Dual Wholesale Network (DWN) model, where a new entity (Entity B) will be selected to build Malaysia's second 5G network. This decision was reportedly made by the government considering the sustainability of Malaysia's telecommunications industry ecosystem and the benefits of a competitive 5G landscape. The Minister of Communications has stated that the transition to the DWN model would take place once 5G network coverage in populated areas reaches 80%, which has reportedly been

achieved as of 31 December 2023, with coverage reaching 80.2%. According to news reports, a mutual agreement will have to be reached among the MNOs as to which will make a jump to Entity B, with the MCMC having the discretion to make a final decision if no deal is reached.

Communications and Digital Ministry split to meet growing demands of portfolio

To address the growing demands in the communications and digital sectors, the Malaysian government restructured the Communications and Digital Ministry, dividing it into the Ministry of Communications and the Ministry of Digital. The new Ministry of Digital is primarily dedicated to spearheading the country's digital transformation, particularly in response to the increase in demand for data centres and artificial intelligence.

It was reported in mid-December 2023 that the Minister of Digital, Gobind Singh Deo, will take over several agencies that were previously under the now-defunct Ministry of Communications and Digital, such as the Malaysia Digital Economy Corporation (MDEC), MYNIC and the Personal Data Protection Department; it was further announced in early January 2024 that DNB, CyberSecurity Malaysia and the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) are also among the other agencies placed under the new Ministry of Digital. The MCMC will remain under the Ministry of Communications.

Developments in Malaysia's AI landscape

The Malaysian government has previously made known its intention to transform Malaysia into one of the top AI infrastructure and technology hubs in the region, and is actively looking to cultivate the use of AI in the country and to implement appropriate instruments to regulate

use thereof. Key recent developments on AI in Malaysia include the following.

- The Minister of Science, Technology and Innovation has previously stated that the Malaysian government is working on drafting legislation to regulate the use of AI in Malaysia, which will include requiring that material produced by AI applications be appropriately labelled. In the interim, the Ministry of Science, Technology and Innovation will develop a code of ethics and governance for AI.
- Malaysia is actively cultivating an AI-skilled workforce, as outlined in the National Artificial Intelligence Roadmap. This roadmap outlines various initiatives that aim to create a thriving and sustainable AI innovation ecosystem for national competitiveness and economic growth.
- During Malaysia's Budget 2024 announcement in Parliament, the Prime Minister revealed the establishment of an AI learning centre in the University of Technology Malaysia, supported by an initial allocation of MYR20 million.
- The Minister of Digital has announced that one of the guidelines that will be developed is the Profiling and Automated Decision-Making Guideline, which may introduce requirements and restrictions relevant to the processing of personal data in AI applications.

Malaysia Digital Status – an initiative for the digital economy

In a significant stride towards advancing Malaysia's digital landscape, the Malaysia Digital (MD) initiative was launched on 4 July 2022, replacing the longstanding Multimedia Super Corridor initiative. The MD initiative aims to fortify Malaysia's digital capabilities and propel the national digital economy to new heights towards accomplishing its goal of becoming a regional data centre hub.

The MD initiative concentrates on nine key growth sectors:

- digital tourism;
- Islamic digital economy;
- digital trade;
- digital agriculture;
- digital services;
- digital cities;
- digital health;
- digital finance; and
- digital content.

The Guidelines on Malaysia Digital Status, issued on 30 June 2022, delineate crucial aspects of MD Status, including eligibility criteria, conditions, benefits, application processes and ongoing obligations. To be eligible for MD Status, a company must be incorporated under the Companies Act 2016, must be resident in Malaysia, and must carry out, or propose to carry out, one or more of the MD Approved Activities. The MD Approved Activities encompass a spectrum of technologies, including big data analytics, artificial intelligence, financial technology, internet of things, advance telecommunications technology, data centre and cloud.

MD Status companies are obliged to comply with certain conditions as set out in the Guidelines on Malaysia Digital Status within 12 months, including requirements to:

- commence the operation and undertaking of the MD Approved Activity(ies) for which MD Status was granted;
- employ a minimum number of knowledge workers;
- meet operating expenditure requirements; and
- maintain a minimum paid-up capital.

MD Status companies enjoy an array of incentives, rights and privileges outlined in the Malaysia Digital Bill of Guarantees. These include access to world-class infrastructure, employment flexibility, freedom from local ownership requirements (subject to the requirements and discretion of the relevant regulatory authority), global capital sourcing and competitive financial incentives.

The application process involves assessment by MDEC and approval by a committee of government representatives. Successful applicants receive an MD Status Digital Certificate, with the status being perpetual and contingent on continued compliance with the conditions attached to the MD Status. MD Status companies can apply to add new MD Approved Activities under their MD Status, subject to meeting the original conditions. MD Status companies must notify MDEC of certain changes to the company, such as changes in the paid-up capital and name of the company; they are also required to submit annual reports, verified by an independent auditor, detailing the progress of the company in carrying out the relevant MD Approved Activity(ies) and compliance with the conditions attached to the MD Status. MDEC may also request additional information for monitoring purposes.

MD Status may be revoked in case of non-compliance with any of the conditions attached to the MD Status, leading to the withdrawal of granted incentives. Surrender requests are accepted if the company has complied with the conditions attached to its MD Status, with the surrender taking effect upon approval by the Approval Committee. Notably, companies with Multimedia Super Corridor status will automatically transition to MD Status without reapplication, with benefits continuing, subject to compliance with the applicable conditions.

The introduction of MD Status marks a pivotal moment in Malaysia's digital journey, offering enhanced privileges and incentives. The successful transition of this rebranding from the Multimedia Super Corridor demonstrates Malaysia's commitment to furthering its position in the global digital economy.

MEXICO



Law and Practice

Contributed by:

Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco
and Mauricio Fernández Villarreal

Galicia Abogados

Contents

1. Metaverse p.283

1.1 Laws and Regulation p.283

2. Digital Economy p.284

2.1 Key Challenges p.284

3. Cloud and Edge Computing p.285

3.1 Highly Regulated Industries and Data Protection p.285

4. Artificial Intelligence p.286

4.1 Liability, Data Protection, IP and Fundamental Rights p.286

5. Internet of Things p.287

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.287

6. Audio-Visual Media Services p.289

6.1 Requirements and Authorisation Procedures p.289

7. Telecommunications p.289

7.1 Scope of Regulation and Pre-marketing Requirements p.289

8. Challenges with Technology Agreements p.290

8.1 Legal Framework Challenges p.290

9. Trust Services and Digital Entities p.291

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.291

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**

Galicia Abogados has a TMT practice integrated by a multidisciplinary group of expert practitioners. Partner Ricardo García Giorgana acts as lead attorney and co-ordinator of all the team's efforts. Furthermore, Galicia recently retained Xavier Careaga Franco as counsel of the firm, to focus exclusively on the development of its TMT practice. Together with a team of ten partners, two counsel, more than ten associates and other team members, they regularly participate in the rendering of TMT services. The above-mentioned co-ordination is required

in order to address holistically technology as an industry that demands legal services from different practice areas, such as regulatory, private equity, health/life sciences, competition, data privacy, e-commerce, education, tax, and intellectual property, among others. This multidisciplinary approach has allowed the firm to offer clients better advice on topics such as IoT, distributed ledger technology, remote (app-based/web-based) contracting, cryptocurrencies and fintech, among others.

Authors



Ricardo García Giorgana is head partner of Galicia's technology practice. He has become a trailblazer in rendering legal services dealing with the intersection of technology and

e-commerce, web- and app-based contracting, and tech-related consumer protection. Ricardo's strategic acumen and dedication to staying ahead of industry trends have earned him a reputation as a trusted adviser to both tech-driven businesses and businesses that are exploring technology applications to boost and expand their growth. His leadership extends beyond legal prowess, recently enriching his specialised education with advanced programs by the Massachusetts Institute of Technology and ESADE business school.



Carlos Chavez Alanis stands out in the realm of competition and antitrust law in the legal landscape. He consistently provides Galicia's clients with advice on the regulatory

framework, positioning himself as a trusted advocate for telecommunications carriers embroiled in regulatory and antitrust proceedings. Carlos's expertise not only underscores his proficiency in legal intricacies but also solidifies his reputation as a go-to authority in the dynamic intersection of technology and law. Carlos's influence extends beyond individual cases, as he actively contributes to shaping the future of legal practices and policies. His dedication is exemplified by his role as a member of Galicia's Innovation and Technology Committee.

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**



Xavier Careaga Franco is a seasoned lawyer in internet matters, having dedicated his entire professional career to technology law and to helping technology companies create, develop and implement their products and features within safe legal margins. He designs extensive multi-jurisdictional and multidisciplinary strategic defences to protect companies' business models, reinforcing the social benefits of technologies involved while mitigating any unintended negative externalities. Prior to joining Galicia, Xavier oversaw a broad spectrum of Meta's legal defence for 35 LATAM, including litigation and regulatory, IP, privacy, competition, e-commerce, consumer protection, product regulatory compliance, content self-regulation, free speech, legislative and international treaty negotiations.



Mauricio Fernández Villarreal plays a pivotal role in supporting Galicia's TMT endeavours. His responsibilities include conducting legal research on technology-related cases and topics, drafting documents, and providing crucial administrative support to the legal team. Mauricio's commitment to excellence and his ability to adapt swiftly to the fast-paced world of technology law make him an indispensable asset. He contributes significantly to the success of the firm's TMT practice.

Galicia Abogados

Bldv Manuel Avila Camacho 24-7
Col. Lomas de Chapultepec
11000 Mexico City
Mexico

Tel: +52 55 5540 9200
Fax: +52 55 5540 9200
Email: galicia@galicia.com.mx
Web: www.galicia.com.mx

Galicia

1. Metaverse

1.1 Laws and Regulation

Within current Mexican regulation, the existence of the metaverse or of facts or legal acts, including advertising or economic transactions explicitly covered in the metaverse or through the use of mixed virtual reality devices, is not regulated per se. Thus, any promotions and advertisements made in the metaverse would be subject to the applicable provisions of the Consumer Protection Act, as well as any relevant legal provisions pertaining to specific categories such as food, beverages, health and others. If, within the metaverse, banking services are offered, specific financial regulations apply, depending on which service is being offered or carried out. While Mexico has put in place an Act to Regulate Financial Technology Institutions (the “Fintech Act”), the act regulates specific models that may or may not exist in the metaverse, such as cryptocurrencies, and, therefore, while not specifically regulated, the scope of the act as drafted is broad enough to regulate the activities that take place in the metaverse, rather than regulate the Metaverse itself.

However, not all Mexican laws and legal provisions would apply in this way. For example, when talking about the sale of spaces that can be purchased within the metaverse, one might think that the specific law that regulates the same activity in the physical world would apply. However, one would be wrong to make this assumption because certain laws exist that speak exclusively of physical spaces. This topic has been widely commented upon in forums discussing the legal nature of such activity and the general consensus is that what would be purchased would not be any land or space or any title that entitles a person to any type of property right as such, but a licence to use a space within

a software would be purchased and, therefore, it would be regulated by the Mexican copyright statutes.

Additionally, there is general concern about security in the metaverse. The metaverse, being essentially a space that allows and encourages interaction between users, allows freedom of behaviour and, therefore, certain crimes such as sexual harassment can be committed. Despite the fact that, within the Federal Criminal Code, such crime is typified in a way that implies that it is physical (such as obscene touching or groping), certain acts that simulate it can be performed in the metaverse. Therefore, it does not directly fall within the aforementioned definition and so it is not considered a crime. However, from the psychological and social point of view, it can have negative and harmful effects on the victim, and yet, under the current legislation, the victim will not be protected. The current legislation needs to be reformed in order to protect possible victims from this type of interaction that can occur in the metaverse.

As the regulations continue to evolve, responsibility still currently falls on the platforms that facilitate access to the metaverse. From a social perspective, these platforms will be required to efficiently moderate content, promptly address and respond to reports of aggressive and dangerous behaviour, with the ultimate goal of safeguarding users. Additionally, there are emerging technologies that enable users to record the final minutes of an incident, such as acts of violence or harassment, and submit these reports directly to the platform for further action.

This brings conflicts, mainly the fact that the biggest sanction that the platform can issue, not being an authority, is the banning of the user to prevent them from continuing to perform such

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**

acts in that same platform, which allows them to switch to another platform and continue with such violent acts.

Additionally, the aforementioned measure brings serious privacy concerns as it is constantly recording every interaction and/or any action performed in said metaverse. This is of concern mainly due to the fact that it collects information from users, which in certain occasions can become personal data. Given its primarily social nature, there is a possibility of sharing sensitive information like sexual preferences, religious beliefs, and other personal data. It is crucial to analyse the underlying purposes (beyond the obvious) of the platforms through which one accesses the metaverse. Additionally, current technologies used for creating digital avatars that graphically represent users in the metaverse may require a photo or a scan of the user, thus capturing biometric data.

This is made worse when considering the potential cybersecurity risks that may be involved, particularly considering the collection of various personal data on such platforms. The current data privacy laws in Mexico have relatively limited protection and would require a pro-human rights interpretation in order to effectively protect users who may be at risk when entering the metaverse.

2. Digital Economy

2.1 Key Challenges

To regulate e-commerce, the Mexican Secretariat of Economy issued the NMX-COE-001-SCFI in 2018, which provides guidelines for individuals and entities offering, marketing, or selling goods, products, or services through digital platforms. This standard specifically targets those

who regularly or professionally promote, market or distribute goods, products or services using electronic, optical or other technologies. Its application is exclusively for consumer transactions between suppliers, intermediary suppliers or third-party providers, and the consumers of these goods, products or services. This regulation establishes a set of practices and standards for e-commerce in Mexico, focusing particularly on consumer protection and rights. It addresses issues ranging from transparency in advertising and terms of sale to security in online transactions, including the protection of personal data. It also covers the specifics of cross-border e-commerce, setting clear guidelines for payment methods and delivery processes. The primary goal is to create a secure, reliable and equitable e-commerce environment, where both consumers and businesses are protected, and transactions are conducted fairly and transparently.

Legislatively, there have been attempts to incorporate the provisions of the NMX into the Consumer Protection Act and even into the Commercial Code. However, these reforms have not been approved.

Additionally, the United States-Mexico-Canada Agreement (USMCA) dedicates an entire chapter to regulating e-commerce, representing a legislative effort to adapt and modernise the legal framework in the face of the challenges and opportunities of e-commerce. With clear and detailed definitions, it lays the foundation for understanding and regulating the complexities of digital commerce, including aspects like algorithms, electronic authentication, and digital products. It aims not only to protect consumers in electronic transactions but also to ensure the privacy and security of their personal data. At the same time, it prohibits practices such as impos-

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**

ing tariffs on digital products and promotes fair and non-discriminatory treatment in digital trade.

The USMCA emphasises the importance of international co-operation on these issues, recognising that digital commerce transcends borders. This implies a joint effort to address challenges such as cybersecurity and source code management, crucial for maintaining integrity and trust in the digital space.

It is also important to refer again to the Fintech Act, which primarily regulates five types of institutions. The first and most utilised are Electronic Payment Fund Institutions (EPFIs), requiring authorisation from the National Banking and Securities Commission to perform activities like opening and managing electronic payment fund accounts for clients, transferring electronic payment funds, and handling national and foreign currency and virtual assets.

The second institution regulated under this act is Collective Funding Institutions (CFIs). These institutions act as intermediaries between investors and funding applicants, facilitating debt financing, equity financing, and co-ownership or royalty financing.

Additionally, the act begins to regulate cryptocurrencies, specifically the operations conducted with these virtual assets, understood as electronically registered value representations used as a means of payment for various legal acts and transferable through electronic means.

Moreover, the act attempts to regulate companies authorised to operate with innovative models, also known as the Sandbox. These are startups that, on a temporary basis, can provide a novel financial service using technology. Despite its promising nature and apparent encourage-

ment of financial market innovation, this model has not yet been utilised by any company.

The fifth and last institution regulated by the Fintech Act are the Application Programming Interfaces (APIs), which are defined as programming methods that allow communication and information sharing between two or more sites or applications. The Fintech Act specifically aims for financial intermediaries to share information uniformly. Consequently, it imposes an obligation on certain financial entities to implement APIs that facilitate connectivity and access to other APIs developed by other entities, for sharing open financial data, aggregated information, and transactional data of users.

The Fintech Act's approach is to create a more integrated and efficient financial services landscape, enhancing the capacity for innovation and adaptation in the rapidly evolving digital finance sector. This regulatory framework is crucial in establishing a solid foundation for the growth and development of financial technology in Mexico, ensuring that it remains competitive, transparent and secure.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

In Mexico, there is currently no specific regulation on cloud and edge computing. However, Article 52 of the Regulations for the Federal Act on the Protection of Personal Data Held by Private Parties (PDPL) provides a definition for cloud computing as “the model for the external provision of on-demand computer services, entailing the supply of infrastructure, platforms or software, which is flexibly distributed through

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**

virtualization processes on dynamically shared resources”.

Furthermore, the PDPL allows for regulatory departments, along with the National Institute of Transparency, Access to Information and Personal Data Protection (INAI), to issue criteria for the proper processing of personal data using cloud computing services. The INAI has, accordingly, issued guidelines for “Minimal Suggested Criteria for the Hiring of Cloud Computing Services Involving the Processing of Personal Data”.

Given the fact that the PDPL and its regulations are mandatory, and that there are currently no specific acts in Mexico regulating cloud and edge computing, there are no specific restrictions for industries regarding the processing of personal data via cloud and edge computing services. Relationships with third-party vendors providing cloud and edge computing services are subject to compliance with-, and hence governed exclusively by traditional rules on third-party data processing (with cloud vendors being regarded as data processors acting on behalf of a data controller).

The cloud service providers must have personal data protection policies that comply with the principles and obligations set forth by the act and its regulations. It is crucial that they disclose any subcontracting that affects the managed information, and it is prohibited for them to assume ownership or control of such information. Moreover, they are required to maintain the confidentiality of personal data at all times.

Additionally, providers must implement mechanisms to inform about changes in their privacy policies or service conditions. It is important that they allow the data controller to limit the processing of personal data and that they establish

adequate security measures for its protection. Upon termination of the service, they must guarantee the deletion of personal data and ensure that the data controller can recover it. Providers are also required to restrict access to the data to unauthorised persons and, in the event of access by a competent authority, to inform the data controller about it.

The lack of further regulation has allowed data controllers to process data unrestrictedly in the context of cloud and edge computing. However, the increased use of these technologies may result in the enactment of specific regulations or legislation, which passing should, accordingly, be closely monitored.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

Currently, there are no specific acts or statutes regulating Artificial Intelligence (AI) in Mexico. However, the parliamentary group of one political party has introduced an initiative to enact the Act on Ethical Regulation of Artificial Intelligence and Robotics.

Under the Federal Copyright Act (FCL) only natural persons (who have created literary or artistic works susceptible to being disclosed or reproduced) can be considered authors. Therefore, the operation of AI paves the way for certain discussions, with one key focus being the attribution of authorship. Given that AI cannot be considered as author under applicable acts in Mexico, the work-product resulting from the use of AI cannot be considered as a creation of the authorship and, thus, under the ownership of AI directly. A notable aspect under consideration is whether creators of AI should be acknowledged

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**

as authors for the works produced by their AI systems, or if the AI itself can be regarded as an independent authorial entity separate from its human creators. Additionally, further discussion arises regarding whether AI, while learning from copyrighted information, inadvertently infringes upon the copyrights of other authors. This regard gives place to an additional discussion: whether AI, in its autonomous learning processes (which virtually do not fall under a fair use doctrine), might unintentionally violate the intellectual property rights of original creators whose works contribute to its knowledge base.

By the same token, under the Federal Act on the Protection of Industrial Property, AI cannot be deemed an inventor, as it expressly establishes that inventions are “human creations”.

The absence of regulations on AI in Mexico poses certain difficulties to the determination of rights and obligations concerning the works generated by AI, which will likely result in the enactment of specific regulations or legislation.

5. Internet of Things

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

In Mexico, as of publication of this guide (February 2024), there is no specific regulation regarding cybersecurity. However, on 25 April 2023, a draft federal cybersecurity act was introduced, which has not yet been approved. This proposed act was motivated by various attacks on different systems since 2018, including, but not limited to, the following:

- the May 2018 attack on the Interbank Electronic Payment System (SPEI), where

Advanced Persistent Threat groups (APT) stole approximately MXN300 million;

- the February 2020 Ransomware Doppel Paymer attack on Petróleos Mexicanos, affecting 60 areas and 5% of the company's computers;
- the July 2020 attack on the National Commission for the Protection and Defense of Financial Services Users (Condusef) by the Anonymous hacker group, which threatened to disconnect the systems of the Bank of Mexico and took down Condusef's website; and
- the February 2023 information theft from the Credit Bureau, compromising the credit history of tens of thousands of individuals, among other cases.

The purpose of this bill is as follows:

- to define which institutions will be responsible for cybersecurity;
- to establish principles and general guidelines for the national cybersecurity policy;
- to set the basis for the prevention and prosecution of cybercrimes;
- to define the rights and obligations of cyberspace users (understood as a global intangible environment supported by information and communication technologies, where public, private entities and society in general communicate and interact); and
- to establish the basis for sanctioning illicit activities in cybersecurity, among other objectives.

Additionally, this bill begins to regulate not only cybersecurity but also brings definitions of important concepts for any type of regulation of interactions between individuals, companies, and/or government institutions.

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**

It also aims to create an Intersecretarial Commission of Information and Communication Technologies and Information Security, which could act as a co-ordinating body among authorities responsible for implementing and developing actions in the field of information and communication technologies, as well as computer security in the federal public administration.

In Mexico, Normalización y Certificación NYCE, S.C. (NYCE) currently standardises communication between electronic devices to facilitate and improve such communication. This is achieved through specific norms and standards that devices must comply with, including aspects of security, quality and compatibility, among others.

Furthermore, Mexican regulations include the Guidelines for the Standardisation of Products, Equipment, Devices or Apparatus for Telecommunications or Broadcasting (the “Devices”), issued by the Plenum of the Federal Telecommunications Institute (the “Institute”), which came into force on 27 June 2022. These guidelines are mandatory as they were issued in compliance with Article 15, Section I of the Federal Telecommunications and Broadcasting Act, which empowers the Institute to issue general administrative provisions.

These guidelines involve the standardisation of Devices through Homologation Certificates granted by the Institute through a procedure supervised and determined by the Institute’s Unit of Concessions and Services. Among the conditions to be met to obtain the certificate, the following stand out:

- having an address in Mexico;
- starting the procedure through the Institute’s Electronic Window with a personal username and password; and
- being processed by a physical or legal person.

There are different types of standardisation, Type A, Type B and Type C, which follow different procedures but share the following steps.

- They begin with an application by the interested party at the Institute’s Electronic Window, following the requirements published within that window.
- After receiving documents, technical evaluation is carried out by the Unit of Concessions and Services.
- Obtaining the Homologation Certificate or the resolution that denies it.

This certificate, being of a mandatory nature, is necessary to connect, install, operate or use the Devices, which would be considered duly standardised.

Internationally, there is the Budapest Convention on Cybercrime, to which the member countries of the Council of Europe are parties, primarily regulating aspects of criminal law, specifically computer crimes related to content, intellectual property, and procedural aspects. However, it is important to mention that Mexico has not ratified this convention and therefore it is not applicable within its national territory, even though it could be very helpful in regulating these aspects at a national level.

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Under the Federal Telecommunications and Broadcasting Act (FTBA), a licence is required to provide telecommunications and/or broadcasting public services. Such licence can be granted for a term of up to 30 years and may be extended.

In addition to the foregoing, free-to-air TV, broadcasted radio and providers of any other services which require to use spectrum frequencies, must either lease such spectrum for licensed holders or secure their own spectrum licences (which are auctioned and require the payment of annual duties).

Likewise, the provision of satellite telecommunications services requires a separate orbital slot concession, which is also granted subject to availability to Mexico of such slots per international treaties and through public tender proceedings.

While traditional audio-visual media services such as paid TV or free-to-air TV require a licence, online audio-visual platforms and over-the-top services (OTTs) are not considered telecommunications services nor broadcast and therefore do not require a licence to operate in Mexico.

In order to obtain a telecommunications or broadcasting licence, an application must be filed before the Federal Telecommunications Institute (IFT), along with the technical plans that support the telecommunications and/or broadcasting services for which a licence is sought, and documents and information that establish the administrative, legal and economic capacity

of the applicant to render such services according to applicable laws and regulations. The IFT has 60 calendar days to analyse and assess the documents submitted and may request additional information when necessary. Once such term has expired and all requirements have been met, the IFT shall grant the licence.

Governmental duties payable to secure the aforementioned licence amount to approximately USD1,200.

On the other hand, spectrum licences are granted through a public tender process (in the case of commercial services) and upon payment of an upfront consideration and an annual royalty. This type of licence can be granted for a term of up to 20 years and may be extended up to equal terms. To grant such licence IFT will take into consideration the economic proposal, coverage, quality and innovation, lower prices to the end user, prevention of concentration, and entry of new competitors into the market.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The FTBA regulates telecommunications and broadcasting services. The Federal Telecommunications Institute, the agency vested with applying the FTBA and the Federal Competition Act in the telecommunications and broadcasting industries, has defined, among others, paid-TV, fixed and wireless broadband access, fixed and wireless voice. Along the same lines, satellite communications are also considered telecommunications services. Hence, audio-visual streaming, instant messaging or video/audio calls do not fall within the scope of local telecommunications rules.

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicia Abogados**

On the infrastructure side, while no licence is required to own or commercialise telecommunications infrastructure (towers, antennas, fibre optic), only licensed carriers may provide services on such infrastructure. The use thereof, however, is subject to telecommunications rules as it forms an integral part of the telecommunications network.

Other cases where authorisation from the IFT is required are:

- to incorporate and operate or exploit a telecommunications service provider without licensee status (resale of services);
- installing, operating or exploiting earth stations to transmit satellite signals;
- to install telecommunications equipment that crosses national borders;
- to exploit the rights of emission and reception of signals and frequency bands associated with foreign satellite systems that cover and can provide services within Mexico (landing rights); and
- temporarily use spectrum bands for diplomatic visits.

The IFT may exempt authorisation to those transmitting earth stations which, by complying with established standards, do not cause harmful interference to other telecommunications systems.

These authorisations shall be valid for a term of up to ten years and may be extended for up to equal terms; the process to obtain such authorisations shall be resolved within 30 business days after submitting the application. Once this period expires, with no resolution from the IFT, the authorisation shall be considered granted.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Currently, one of the most relevant challenges that organisations face when entering into a technology agreement is the lack of standardisation of contracts in the sector. This is a general rule, as there are some specific sectors that have managed to standardise to a certain extent; however, this is the exception to the rule and it is not an absolute standardisation.

This lack of standardisation means that, at the time of contract negotiation, it becomes extremely technical and complex, which may lead to the fact that, in the event of a controversy and/or litigation, the judge may have problems in correctly understanding the essence of such contracts and, therefore, may not judge correctly in such lawsuits. This could even cause the parties to actively seek arbitration as a method of dispute resolution in order to have a judge who has the technical knowledge of the issues since, unfortunately, current judges do not have sufficient technological knowledge.

Additionally, due to the lack of standardisation, technology agreements can also suffer from the opposite issue and not be technical enough, which could leave a lot of room for interpretation by either the parties or a judge and therefore not be an ideal contract for the specific transaction and/or operation. This is often reflected in definitions being invented specifically for a contract and, in the absence of specific regulation, these can be erroneous because the process requires a lawyer who fully understands the operation, as well as the functioning, of the technology involved, in order to properly tailor a certain contract to that operation.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The Commercial Code distinguishes between three categories of electronic signatures: simple electronic signature, advanced or reliable electronic signature (FEA), and certified advanced electronic signature. Each is defined as follows.

- Simple Electronic Signature – consists of electronic data linked or associated with a message, serving to identify the signatory and demonstrate their approval of the message's content. This signature has the same legal validity as a handwritten signature and is acceptable as evidence in court.
- Advanced or Reliable Electronic Signature – not only identifies the signatory and shows their approval of the message but also meets additional requirements such as being unique to the signatory and under their exclusive control at the time of signing; allowing the detection of any changes to the signature after signing; and ensuring that any alteration to the message's content can be detected after the signature.
- Certified FEA – an FEA that has been verified and certified by a Certification Service Provider (PSC), accredited by the Secretariat of Economy. These signatures meet the same requirements as uncertified FEAs, but with the added assurance of having been validated by a PSC.

The legal effects of the FIEL (Advanced Electronic Signature) are regulated within the Advanced Electronic Signature Act, which establishes that electronic documents and data messages signed through such means have the same probative value as applicable provisions grant them.

Among these provisions, those of the fiscal sector stand out, as they have enabled means like the taxpayers' tax mailbox, allowing both individuals and legal entities to present annual or supplementary declarations, defence mechanisms such as revocation appeals, notices provided within Annex 1-A of the Miscellaneous Fiscal Resolution (such as the appointment of a legal representative by foreign companies), and even consultations to the Tax Administration Service. The aforementioned documents enjoy full probative value in accordance with applicable fiscal provisions.

By defining the electronic signature, it is established that it has the same legal validity and is accepted as evidence in court just like a handwritten signature. In this context, the Federal Code of Civil Procedures as well as the Commercial Code recognise the validity of electronically generated information as evidence. Both codes consider the reliability of the method used to generate, communicate, receive or store that information when assessing its probative force.

Moreover, the Commercial Code indicates that electronic signatures created abroad are equally valid and have the same probative value as those issued in Mexico, as long as they align with internationally recognised standards.

Although there are few judicial precedents regarding the use of electronic signatures, most recognise their validity. However, it is important to note that electronic information can be altered. Therefore, any electronic signature, regardless of its type, can be questioned in litigation or arbitration proceedings. In such cases, it would be necessary to present additional technological evidence, which may pose procedural challenges.

Contributed by: Ricardo García Giorgana, Carlos Chavez Alanis, Xavier Careaga Franco and Mauricio Fernández Villarreal, **Galicía Abogados**

For this reason, use of an electronic signature that offers the highest possible probative value in case of dispute, such as an FEA or a certified FEA, is recommended. In dispute situations, the responsibility of proving the reliability of the electronic signature falls on the signatory, who must provide the necessary evidence to support its authenticity.

Section 19.6 of the USMCA (United States-Mexico-Canada Agreement) states that the legal validity of an electronic signature should not be denied simply because it is electronic,

except under specific circumstances. It also prohibits legal entities from adopting measures that limit the choice of electronic authentication methods or electronic signatures in electronic transactions, or that prevent parties from demonstrating their legal compliance in judicial or administrative processes. Thirdly, it allows for certain categories of transactions to require specific performance standards or certification by accredited authorities for electronic signatures or authentication methods. Lastly, it encourages the promotion of interoperable electronic authentication use among the parties.

NETHERLANDS



Trends and Developments

Contributed by:

Herald Jongen, Radboud Ribbert, Robert Hardy and Wouter van Wengen
Greenberg Traurig, LLP

Greenberg Traurig, LLP is an international law firm with approximately 2,300 attorneys serving clients from 40 offices in the USA, Latin America, Europe, Asia and the Middle East. The firm's dedicated TMT team consists of more than 100 lawyers, seven of which are in Amsterdam. The Amsterdam team is well versed in representing clients around the world in domestic, national

and international policy and legislative initiatives, and in guiding them through the business growth cycle for a variety of technologies. As a result, it provides forward-thinking and innovative legal services to companies producing or using leading-edge technologies to transform and grow their businesses.

Authors



Herald Jongen is a shareholder at Greenberg Traurig, and 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. Herald is known for his efficient pressure-cooker negotiations. Before joining Greenberg Traurig, he was a partner in the corporate team of Allen & Overy for 20 years.



Radboud Ribbert is an experienced entertainment and media lawyer, and a well-known expert on media law, copyright law and neighbouring rights law, with more than 25 years'

experience. He advises clients on the creation of television and radio stations, and on the distribution of the signals of these stations. Radboud has litigated copyright issues with respect to the satellite transmission of music in television signals with copyright societies, and was involved in the auction of the FM radio frequencies for commercial radio broadcasters.

NETHERLANDS TRENDS AND DEVELOPMENTS

Contributed by: Herald Jongen, Radboud Ribbert, Robert Hardy and Wouter van Wengen, **Greenberg Traurig, LLP**



Robert Hardy has over 13 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. Robert also represents clients before the Dutch civil law courts on issues relating to standard-essential patents and FRAND licensing disputes. His sector focus includes technology and telecommunications. He holds an LLM from Harvard.



Wouter van Wengen is an associate at Greenberg Traurig, and focuses his practice on intellectual property law, IT contracts and data protection law. He is admitted to practise

law in the Netherlands and New York. Combined with his experience in various complementary (tech-related) disciplines of law, he can identify and address client's needs from a transatlantic angle. Wouter represents national and international clients in the creative sector, the technology industry and a variety of other companies, in both EU and US law matters.

Greenberg Traurig, LLP

Beethovenstraat 545
1083 HK Amsterdam
The Netherlands

Tel: +31 651 289 224
Fax: +31 20 301 7300
Email: herald.jongen@gtlaw.com
Web: www.gtlaw.com



Introduction

The Dutch business community and the government have a positive view on technology and the chances and benefits it offers. Cloud and AI are embraced, but of course with caution and an open eye for the risks. However, in general such risks are deemed to be low and acceptable. This differs from a number of other EU countries.

2023 witnessed remarkable strides in the dynamic realm of TMT, setting the stage for transformative trends that will shape the near future. From the surge in Generative AI adoption and the imperative to curtail algorithmic biases to the convergence of Augmented Reality (AR), Virtual Reality (VR) and Artificial Intelligence (AI) signalling an era of unparalleled customisation, this article explores the key developments driving innovation across industries, with an emphasis on the developments in relation to AI.

Delving into the realm of robotics, the integration of machine learning algorithms and sensor technologies brings us closer to the realisation of collaborative human-robot ventures. As the digital landscape braces for an increase in cyber threats, a unified defence against sophisticated AI-powered attacks becomes paramount, emphasising the need for standardised cybersecurity frameworks and collaborative efforts between industries and governments to safeguard data and privacy. An instrumental role to curtail these threats is foreseen in the EU Artificial Intelligence Act (AI Act).

This article will also discuss the latest TMT trends regarding competition law, the various inbound legislations on the use of data, an update on the 5G and FM frequency auctions, and important developments in light of personal data protection and taxes.

EU AI Act

On 9 December 2023, the European Parliament reached a provisional agreement on the text of the AI Act, which is likely to be the world's first comprehensive law regulating the use of AI. The agreement must still be approved by all EU member states and the entire European Parliament; the law will enter into force two years after such approval. The AI Act is risk-based, which means that the obligations of providers and users of AI systems depend on the level of risk that the respective AI technology may create and/or generate, and that AI systems with a higher risk of affecting society will be subject to stricter requirements.

The AI Act attempts to establish guidelines to navigate the complexities of AI-generated content and authorship. The legislation recognises the importance of human creativity and addresses concerns surrounding ownership and attribution in instances where AI autonomously produces content. Furthermore, the AI Act integrates provisions for digital rights management tailored to AI-generated media, safeguarding against the unauthorised use and potential misuse of copyrighted material.

Prohibited uses

The proposal bans AI systems that violate EU values such as through violation of fundamental rights. This applies, for example, to “social scoring” by governments or companies, or the classifying or profiling of people based on their social behaviour or personal characteristics. The banned systems include:

- “real-time” biometric identification systems in public places;
- biometric categorisation based on sensitive characteristics, such as gender, race, ethnicity, citizenship, religion and political affiliation;

- predictive detection systems, based on profiling, location or previous criminal behaviour; and
- emotion recognition in law enforcement and workplace settings (among others).

High-risk AI

High-risk systems, such as AI systems that may cause significant harm to human health, safety and/or fundamental rights, are subject to more restrictions under the AI Act. For instance, AI used in controlling critical infrastructure in the fields of water, gas and electricity or medical devices will be subject to more scrutiny. Biometric identification, categorisation and emotion recognition systems are also considered high-risk.

Minimal risk

Minimal risk AI systems are those that can be developed and used according to existing legislation – ie, there are no additional requirements for them in the proposed regulation. Such systems include spam filters and search engines.

Specific transparency risk

Users should be made aware that they are interacting with a chatbot when employing such an AI system – eg, ChatGPT. There will also be a requirement for registration in a central European database before the application can be marketed in Europe. In addition, it is mandatory to record all copyrighted data used to train AI systems and to disclose its use in a detailed overview. Deep-fakes and other AI-generated content need to be labelled as such. When biometric categorisation or emotion recognition systems are used, users need to be informed. Last but not least, providers need to make the content detectable as having been artificially generated or manipulated, by designing the system in a way that artificially

generated or manipulated audio, video, text and images are marked in machine-readable format.

Innovation

To support innovation in AI, the AI Act inserted exemptions for research activities and for AI components provided under open-source licences. The AI Act promotes so-called test environments (sandboxes) set up by government agencies to test AI before it is brought to market.

Position of citizens

The European Parliament wants to strengthen citizens' rights. Think, for example, of being able to file complaints and get explanations about decisions using AI systems.

Next steps

On 9 December 2023, the European Parliament and the Council of the EU reached a preliminary political agreement on the AI regulation; they are still working on the formal legal text before the regulation is adopted by both bodies. Once the AI regulation is adopted, member states will begin implementing the regulation domestically. Most standards will take effect two years after the effective date, which is expected to be in mid-2026.

Furthermore on AI, on 11 December 2023, the Dutch government announced by way of a letter from the Minister of Digitalisation that it is currently in the process of creating guidance on safe and responsible use of generative AI within the government. In addition, the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*) announced in its yearly plan for 2024 that algorithms and AI will be a specific area of focus.

Technology Trends in Competition Law

The EU Digital Markets Act (DMA) became applicable in May 2023, and intends to ensure fair and contestable digital markets. In September 2023, the European Commission designated six companies as so-called “gatekeepers” under the DMA for the first time – Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft.

Being designated as a gatekeeper comes with various obligations to maintain fair and effective competition. By March 2024, gatekeepers must have adjusted their businesses to comply with the DMA. Apple, ByteDance and Meta have all appealed their designations. More gatekeepers may be designated by the Commission in 2024. The case law resulting from the different proceedings will likely shape the Commission’s DMA enforcement in 2024 and the years to come.

The EU Digital Services Act (DSA) intends to create a safer digital space where the fundamental rights of users are protected, and to establish a level playing field for businesses. It already applies to designated online platforms and search engines, and will apply to all regulated companies as of February 2024. In December 2023, the Commission adopted a second set of designation decisions under the DSA, designating three very large online platforms: Pornhub, Stripchat and XVideos.

These designations follow a first set of designation decisions of 19 very large online platforms and search engines in April 2023. Amazon and Zalando have already challenged their designation by the Commission. Separately, in December 2023, the Commission opened formal proceedings against X to assess whether it may have breached the DSA in areas linked to risk management, content moderation, dark pat-

terns, advertising transparency and data access for researchers. Again, the outcome of the different proceedings will likely guide the Commission’s DSA enforcement in future. Amazon, in particular, has put forward wide-ranging arguments against the Commission’s designation, including challenges to the scope of the DSA itself.

In 2024, the Dutch Authority for Consumers and Markets (ACM) will likely continue to pay particular attention to companies’ use of algorithms and AI.

The focus in relation to antitrust damages cases before the Dutch civil law courts will likely continue to shift from follow-on cartel damages cases to abuse of dominance damages cases, specifically in relation to Big Tech. In 2024, the Dutch litigation landscape is expected to change even further in relation to Big Tech companies that have been designated under the DMA/DSA. A new wave of private enforcement actions may therefore be forthcoming in the Netherlands shortly.

Reporting Obligations for Platform Companies in Respect of Tax

EU rules were introduced in 2023 (under Directive 2021/514, also known as DAC-7) that extended EU tax transparency requirements to digital “platforms”. The aim of DAC-7 is to improve administrative tax co-operation – and counter tax fraud/tax evasion – and to address the challenges posed by the digital platform economy. Accordingly, an obligation was introduced for “platform operators” to provide information on income derived by sellers through those platforms.

An entity qualifies as a platform operator if it contracts with sellers in order to provide access

and use of an online “marketplace” platform to those sellers. A platform operator falls under the scope of DAC-7 rules if, in brief, it is tax resident, has been incorporated under the laws of or is operationally active in an EU member state. 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 of 1 January 2023 and platform operators had to file their first DAC-7 reporting, with regard to 2023, in January 2024.

Delayed Introduction of Digital Services Tax

The Dutch political parties that formed the 2021–2023 government (which collapsed in the fall of 2023) agreed to the introduction of a digital services tax in the Netherlands. However, unlike several other EU member states, they did not progress this topic, and no such tax has yet been introduced. The political parties that won the elections on 22 November 2023 did not include any significant notes related to the introduction of a digital services tax in their campaign plans.

Accordingly, it remains most 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 based not on where they are located or are otherwise

active, but on where their consumers are located (also known as “Pillar 1”).

5G Auction to be Held

The 5G frequency auction that was originally scheduled to be held in 2023 has been postponed to early 2024, due to a conflict with Dutch maritime company Inmarsat. Now that this auction is likely to finally take place this year, media and telecommunications companies can brace themselves for an important year.

(Upcoming) Data-Related Legislation

In an attempt to keep up with the fast-evolving landscape of digital governance and the accumulation of a significant quantity of data in the digital space, the EU has undertaken significant legislative initiatives to fortify its financial, cybersecurity and data management frameworks, including the Digital Operational Resilience Act (DORA), the NIS2 Directive, the EU Data Act and the EU Data Governance Act.

Digital Operational Resilience Act

DORA is a ground-breaking legislative move in the EU, reshaping the way financial institutions manage operational risks in an increasingly digital era. Addressing the escalating reliance on digital infrastructure and the severe consequences of operational disruptions, DORA introduces a comprehensive framework to counteract cyber threats and enhance operational resilience.

Under DORA, outsourcing service providers in the EU face heightened requirements, compelling them to invest significantly in robust cybersecurity measures, compliance frameworks and incident response capabilities. This shift is expected to fuel demand for specialised cybersecurity services within the outsourcing industry.

DORA mandates financial institutions to identify and manage cyber risks through regular risk assessments, resilience testing and incident reporting to competent authorities. The regulation aims to ensure the stability and security of the financial sector, safeguard consumers and strengthen the overall economy. Virtually all financial entities in the EU fall under DORA's purview, including key third parties providing ICT-related services.

Outsourcing is central to DORA, with financial institutions facing stringent responsibilities regarding cybersecurity assessments and monitoring of third-party service providers. Key requirements include addressing ICT third-party risks through rigorous contractual arrangements, location indications for data processing, service descriptions, access guarantees, exit strategies, audits and performance targets.

DORA has been in effect since 14 December 2022 and requires in-scope companies to achieve compliance by 17 January 2025. As a binding regulation applicable across all EU member states, ongoing outsourcing agreements should already integrate DORA's requirements, emphasising the need for prompt adherence. Within the Netherlands, the Dutch Authority for the Financial Markets (*Autoriteit Financiële Markten*) will be responsible for supervising compliance with DORA.

NIS2 Directive

The EU Directive on measures for a high common level of cybersecurity across the Union ("NIS2 Directive") signifies a monumental step towards harmonising cybersecurity standards across EU member states. Replacing the previous NIS Directive, the NIS2 Directive broadens its scope to cover medium-to-large enterprises

and public organisations performing vital functions for the economy or society.

The NIS2 Directive introduces measures for elevating the cybersecurity posture of critical infrastructure operators and digital service providers, focusing on risk management, incident reporting and security certification schemes. Compliance with the NIS2 Directive is essential for outsourcing service providers, necessitating investments in advanced cybersecurity technologies, workforce training and robust incident-response capabilities.

Notably, the relationship between DORA and the NIS2 Directive is critical, with both pieces of legislation sharing significant requirements. As a regulation, DORA applies directly to all EU member states, while the NIS2 Directive is a directive requiring implementation into national law. The NIS2 Directive provides an exemption to ensure overlapping DORA provisions take precedence.

The implementation of NIS2 in 2023 requires EU member states to adopt it into national legislation by 17 January 2025. As organisations seek expert guidance for cybersecurity compliance, there is likely to be an increased demand for cybersecurity consulting services, offering a competitive advantage to outsourcing providers with robust security measures.

Furthermore, the Dutch legislature expects to publish the proposal for the Dutch implementation of the NIS2 Directive for public consultation in the first quarter of 2024.

Data Act

In addition to DORA and the NIS2 Directive, the proposed EU Data Act promises to have a profound impact on the technology and outsourcing landscape, particularly concerning the vast

amounts of data processed through internet of things (IoT) services. Aimed at establishing a unified data governance framework across the EU, the EU Data Act emphasises data sharing and management practices, prioritising data protection and privacy.

The EU Data Act introduces new rules regarding data governance, access and sharing, enhancing data portability and interoperability. For outsourcing providers, compliance requires robust data management practices, stringent privacy measures and secure data-sharing protocols. Organisations aligned with the principles of the General Data Protection Regulation (GDPR) will find themselves well-prepared for the EU Data Act, while non-compliance may pose challenges in serving European clients or processing EU citizens' data.

The Data Act was adopted by the European Council on 27 November 2023 and entered into force on 11 January 2024. It will apply 20 months later, on 12 September 2025, prompting outsourcing providers to closely monitor developments and proactively ensure adherence to its provisions. In the Netherlands, it is not yet clear which supervisory authority will be responsible for monitoring adherence with this regulation.

EU Data Governance Act

Finally, 2023 marked the enactment of the EU Data Governance Act. This regulation on data governance seeks to improve the development of trustworthy data-sharing systems by regulating the re-use of data held by the public sector. In order to achieve this purpose, the EU Data Governance Act provides for four broad sets of measures:

- member states must facilitate the re-use of certain public sector data that cannot

be made available as open data – eg, certain health data can be re-used to advance research to find cures for rare or chronic diseases;

- it includes measures to install data intermediaries that will function as trustworthy organisers of data sharing or pooling within the common European data spaces;
- there are measures to assist citizens and businesses in the process of making their data available for the benefit of society; and
- there are measures to facilitate data sharing by making it possible for data to be used across sectors and borders, and to ensure that the right data can be re-used for the right purpose.

The EU Data Governance Act applies to both personal and non-personal data, whereas the GDPR only applies to personal data. Where personal data is in scope, the GDPR will apply alongside the EU Data Governance Act.

The EU Data Governance Act entered into force on 23 June 2022 and has been applicable since September 2023. Within the Netherlands, the Netherlands Authority for Consumers and Markets (*Autoriteit Consument en Markt*) is responsible for supervising compliance with the EU Data Governance Act.

Data Protection – Transferring Personal Data to the US

Perhaps the most impactful trend with respect to data protection was the adoption of the adequacy decision for the EU-U.S. Data Privacy Framework (EU-US DPF), succeeding the Privacy Shield. This decision reinstates the possibility of data transfers between EU organisations and those in the US that have self-certified compliance with the principles of the EU-US DPF. Following the EU, the UK and Switzerland have also

adopted their respective transfer mechanisms: the UK Extension to the EU-US DPF and the Swiss-U.S. DPF.

Given the previous invalidation of predecessors such as the “Safe Harbour” agreement and the “Privacy Shield” by the Court of Justice of the European Union (CJEU), the sustainability of the EU-US DPF is yet to be seen. One attempt from a member of the French Parliament, Philip Latombe, to challenge this decision – through an application for interim relief – has already been recorded, but ultimately failed because the CJEU held that he failed to establish the presence of serious and irreparable harm. Therefore, the CJEU has not (yet) reviewed this transfer mechanism on the merits. However, with a declaration of intention to initiate a legal action against the EU-US DPF by the person responsible for the invalidation of its two predecessors, this is still likely to occur in the next couple of years.

This and other data protection-related trends will be discussed in more detail in the [Netherlands Trends & Development chapter in Chambers Data Protection & Privacy 2024](#).

Cloud

Although the Netherlands has a relatively high adaptation of cloud solutions, many enterprises have a major roadmap to bring applications to the cloud. These projects can be challenging, especially if it is not recognised early on that applications will need to be replaced by applications with slightly different functionality. This nears the risk of failure.

The Dutch government has a positive view on technology and on the cloud, and has adopted a new cloud policy that allows broad use of cloud applications. US cloud providers are not seen as

suspicious and the risks of the [US CLOUD Act](#) are usually deemed acceptable.

Conclusion

In conclusion, the continuously evolving TMT landscape witnessed transformative developments in 2023 that set the stage for the future. The adoption of Generative AI, the convergence of AR/VR and AI, and the advancements in robotics signal a paradigm shift in innovation. As the digital landscape faces escalating cyber threats, the EU AI Act and collaborative defence mechanisms take centre stage, emphasising the importance of standardised cybersecurity frameworks.

The EU AI Act, with its risk-based approach, is poised to become the world’s first comprehensive law regulating AI use. It addresses concerns surrounding AI-generated content, emphasising human creativity, ownership and attribution. The Act’s focus on prohibited uses and the regulation of high-risk AI systems demonstrates a commitment to safeguarding fundamental rights and societal well-being.

In the realm of competition law, the DMA and DSA are reshaping digital markets by designating gatekeepers and establishing a safer online space. These designations, along with ongoing legal proceedings, will significantly influence DMA and DSA enforcement in the coming years.

In the realm of taxation, the extension of EU tax transparency requirements to digital platforms (DAC-7) and the upcoming reporting obligations for platform operators mark a significant step in countering tax fraud in the digital platform economy.

The delay in the introduction of a digital services tax in the Netherlands reflects a cautious

approach, possibly awaiting global acceptance of the OECD's initiative. Furthermore, the 5G and FM frequency auctions, initially scheduled for 2023, are anticipated in early 2024, bringing substantial developments for media and telecommunications companies in the Netherlands.

The legislative initiatives on data management – including the Digital DORA, the NIS2 Directive, the EU Data Act and the EU Data Governance Act – underline the EU's commitment to fortifying digital governance. DORA's impact on financial institutions and outsourcing providers is evident, emphasising the need for robust cybersecurity measures.

The EU Data Governance Act, enacted in 2023, focuses on trustworthy data-sharing systems, setting measures for re-using public sector data and facilitating cross-sector and cross-border data sharing. This legislation, alongside the EU Data Act, strengthens data protection and privacy, aligning with GDPR principles.

Furthermore, the adequacy decision for the EU-US DPF reinstates data transfers, marking a pivotal trend in data protection. However, the sustainability of the EU-US DPF, given past invalidations, remains a crucial aspect to monitor.

As we move forward, TMT will continue to be an area deserving of close legislative attention, as it remains subject to technological advancements and instrumental in balancing innovation with societal well-being. The next phase will require adaptability and collaboration across industries to navigate the complexities of the rapidly changing digital environment.

NORWAY

Law and Practice

Contributed by:

Leif Eirik Thrane and Arne Byberg
Advokatfirmaet Haavind AS



Contents

1. Metaverse p.305

1.1 Laws and Regulation p.305

2. Digital Economy p.306

2.1 Key Challenges p.306

3. Cloud and Edge Computing p.307

3.1 Highly Regulated Industries and Data Protection p.307

4. Artificial Intelligence p.309

4.1 Liability, Data Protection, IP and Fundamental Rights p.309

5. Internet of Things p.310

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.310

6. Audio-Visual Media Services p.311

6.1 Requirements and Authorisation Procedures p.311

7. Telecommunications p.312

7.1 Scope of Regulation and Pre-marketing Requirements p.312

8. Challenges with Technology Agreements p.313

8.1 Legal Framework Challenges p.313

9. Trust Services and Digital Entities p.314

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.314

Advokatfirmaet Haavind AS 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 to provide dovetailing support for 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 adviser to the software industry and a key contributor to market practice for tech M&A in Norway and beyond. He is also experienced in negotiating large outsourcing agreements, supporting dispute resolution, advising on regulatory and compliance issues, and handling complex licensing matters.



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 EVRY 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. His 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



1. Metaverse

1.1 Laws and Regulation

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, which is 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 in terms of applicable jurisdiction, tax regulation and contract law, for example.

In recent years, the matter of human rights in the metaverse has become an increasingly debated topic, with the Norwegian National Human Rights Institution (NIM) publishing a report on the subject in early 2023. The report highlights issues concerning jurisdiction, accountability, segregation between realities, and the applicability of certain human rights provisions.

New regulations covering the metaverse may be expected in the future. In July 2023, the European Commission adopted a strategy on actions concerning Web 4.0 and virtual worlds. Although it envisages supportive tools to encourage innovation and ensure fundamental rights, the strategy might be a stepping stone for legislative acts. Thus, any future legislation under the strategy might be binding on Norway if the legal acts are incorporated in the EEA Agreement.

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 of 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, as 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 no common code or practice is yet applied across banks in Norway.

The Norwegian Act on Digital Content and Services entered into force in October 2023 and implements EU Directive 2019/770. The Act applies to agreements concerning the supply of digital services or content against payment in consumer relations. It imposes objective and subjective requirements for conformity and equips the consumer with remedies in case of contract breach. In short, the Act can be understood as a consumer sales law in the digital world.

New EU acts covering the digital economy that are deemed relevant for the EEA, such as the proposal for a Cyber Resilience Act, are also likely to be implemented in Norway.

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 GDPR, which requires the data controller to have a legal basis for the processing of personal data, including the transfer of the data to the service provider, and for any transfer of data to countries outside the EU and EEA.

Article 32 of the GDPR requires the controller and the data processor to ensure the safety and integrity of the data processed through technical and organisational security measures. Appropriate measures may be encryption and the 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 the transfer of personal data to third countries and are therefore relevant for cloud computing. The 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 trans-

fer 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. On 10 July 2023, the EU Commission adopted an adequacy decision for US businesses, which came into effect immediately and replaced the Privacy Shield. In brief, this means that the EU Commission has assessed that businesses certified under the new framework (www.dataprivacyframework.gov) ensure a level of protection for personal data equivalent to European standards.

In July, the DPA declared that Meta's surveillance of Facebook and Instagram users for behaviour-based marketing is illegal, and imposed a temporary ban on the practice in Norway. The European Data Protection Board has decided that the Norwegian ban on behaviour-based marketing on Facebook and Instagram should be made permanent and extended to cover the entire EU/EEA.

The Financial Sector

The Bookkeeping Act generally requires that accounting material that is 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; only the Nordic countries are currently covered by the exemption, but the bookkeeping authorities may

grant exemptions for other countries in the EU/EEA on a case-by-case basis. Subsequently, 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 the use of information communication technology (ICT) in the finance sector will also affect the use of cloud computing services in this business segment. It sets out the 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 from European authorities (the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority).

National Security

The Security Act applies to all public bodies, and to 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 the 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 the use of cloud and edge com-

puting 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, and 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 the energy infrastructure in Europe, illustrate the risk and are particularly relevant as Europe's reliance on the Norwegian energy sector has increased. Both events played a part when Norwegian oil and energy company Equinor became subject to the Norwegian Security Act in 2022.

The Norwegian Act on Cybersecurity was adopted in December 2023, implementing EU Directive 2016/1148 (NIS1) and facilitating the implementation of the Cybersecurity Regulation. The Act applies to providers of respectively essential and digital services, which must fulfil minimum cybersecurity requirements, such as regularly conducting IT risk assessments and notifying public authorities of events that could have a significant impact on service delivery. EU Directive 2022/2555 (NIS2) has not yet been incorporated into the EEA Agreement, and is therefore not binding for Norway as of January 2024.

The Council adopted a preliminary position on 20 December 2023, with a press release on the Cybersecurity Regulation. The EU Cyber Solidarity Act will enhance solidarity at EU level for improved detection, preparation and response to significant or large-scale cybersecurity incidents. This will be achieved by establishing a

European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism.

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 incorporated into the EEA Agreement, so 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 public entities to carry out risk assessments of the storage systems to be used and examine whether these fulfil their archiving obligations.

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 the documentation of healthcare, right of access, access control and the deletion of data. In addition, most healthcare providers in Norway are bound by the sector-specific standard “Normen”, a compilation of information security requirements that 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

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, IPR and discrimination in relation to fundamental rights are examples of relevant regulations that will apply to the use of artificial intelligence.

A compromise on the AI Regulation was negotiated by the Council, the Commission and the European Parliament on 9 December 2023. The goal is to make the EU the leading entity in terms of the development and use of secure, reliable and human-centred AI.

EU positions on civil liability – adapting liability rules to the digital age and artificial intelligence – are also likely to have an impact on Norway via the EEA as they materialise and mature at the European level.

Data Protection

Big data, machine learning and artificial intelligence projects will involve the processing of 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 that 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, meaning 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 IPR as regards the results generated by intelligent machines has been resolved by the European Patent Office, which also impacts Norway, so 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.

Furthermore, it is worth noting that the implementation of the Data Act may affect the current regulation of IPR (see **5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection**).

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 automatisisation 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. There have already been 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 is necessary for the purpose of processing (data minimisation) and not processing data in a manner that is incompatible with the initial purposes of processing (purpose limitation).

When IoT technology is applied for non-personal data, the contracts will remain key, although the area is 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 information security, privacy and anti-fraud, based on local implementation of EU cybersecurity laws.

In November 2023, the EU Data Act was adopted in the EU Parliament, with the stated purpose of enhancing innovation within the EU by providing increased access to, as well as greater opportunities for the re-use of, data originating from affiliated entities. The text is considered relevant to the EEA. The process of evaluating whether the text should be included in the EEA Agreement, and subsequently implemented into Norwegian law, traditionally takes significantly longer than the time it takes for the legal act to take effect in EU countries. Nevertheless, the legal act will have implications for Norwegian businesses operating in the EU from the point at which it takes effect there.

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 criterion 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 – eg, 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 services “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 criterion of editorial control will generally exclude media services that distribute user-generated content without interference from the service provider. However, Norwegian authorities are currently considering a proposed amendment to the Norwegian Broadcasting Act, suggesting implementing the rules from Directive 2018/1808, which amends Directive 2010/13/EU (Audiovisual Media Services Directive) concerning 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, and rules on reporting to the authorities and protection measures for younger viewers.

Upcoming EU Acts Relevant for Norway

The European Commission has made proposals covering Audio-Visual Media Services, and many of them are of relevance to the EEA. Not all

of them can be discussed in this paper, but two significant proposals will be highlighted.

The European Media Freedom Act seeks to secure the independence of the media, as well as media pluralism. The proposal also includes rules regarding the editorial responsibility of very large internet platforms – eg, an obligation to state the reasons for removing or blocking content published by media service providers. Norwegian authorities will consider the appropriate measures for implementing the act once the proposal is adopted in the EU.

In addition, the Commission has proposed a regulation to prevent and combat child sexual abuse on the internet (Child Sexual Abuse Regulation, or CSAM). The relevant service providers must assess the risk of their service being used to spread child abuse content and assess the risk of “grooming”. Furthermore, the service providers must establish measures to minimise identified risks. National authorities may require the service provider to track the existence of such content. Norwegian authorities held a hearing about the proposal in February 2023, and are considering proposing a Norwegian act similar to CSAM.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The Electronic Communications Act currently 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, a new electronic communication act is likely to be presented to parliament in 2024. The final result of such new act is not yet known, but it is implied that the scope of the telecommunication rules might be adjusted and may, among other things, include rules concerning data centres.

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) in order to operate legally. The obligation to register applies to:

- providers that install, operate and give access to electronic communications networks that 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 include 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 that use other providers' physical networks, will therefore not need to register.

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.

The 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

The use of frequencies in Norway is not permitted without a licence. General licences are granted in the General Authorisations Regulation and apply to anyone using the specific equipment or service, therefore allowing free use of the specific usage. Section 9 of the Regulation 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 an 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 the 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 considered well in advance, and that the agreement regulates the placement of risk between the parties.

The Norwegian Act relating to the Sale of Goods applies directly to the sale of goods, but 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 a 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 common challenge is compliance 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 part of the EEA, Norway has implemented Regulation (EU) 910/2014 (eIDAS) through the Norwegian Electronic Trust Services Act.

Electronic signatures and electronic ID confirmation and signatures are commonly used in Norway in both the public and private sector. Most governmental online platforms require log ins with an electronic ID, including 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, which 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 include 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 con-

cluded that the electronic identification and signature providers carry a larger part of the liability than previously assumed. Consequently, the new Norwegian Financial Contracts Act was adopted in 2020, with effect from 1 January 2023. The purpose of the new act is to strengthen consumer protection, with more responsibility being placed on the banks and financial institutions in cases of BankID fraud. The deductible has also been significantly reduced in favour of the consumer.

The Commission Proposal amending the eIDAS Regulation is still being discussed in the EU. The Norwegian government considers the amendments to be relevant to the EEA so the act may be incorporated into the EEA Agreement when the proposal is adopted in the EU, which would prompt an amendment to the existing Norwegian legislation.

POLAND



Trends and Developments

Contributed by:

Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk
Softysiński Kawecki & Szlęzak

Softysiński Kawecki & Szlęzak 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 well reputed for the quality of its work and for its innovative approach to complex legal problems. Since the 1990s, SK&S has been closely associated with the ever-changing technology sector, especially the dynamically developing IT industry. The firm

provides high-quality legal services to both individuals and companies, covering the full scope of TMT issues. The team works alongside the firm's fintech, IP/IT, privacy and tax teams to provide an innovative interdisciplinary service, and to help businesses use state-of-the-art technologies in a safe, cost- and time-effective manner. SK&S was the founding member of the New Technologies Association.

Authors



Agata Szeliga joined SK&S in 1998 and has been a partner since 2009. She specialises in new technologies and personal data protection, and in state aid and public procurement. Agata

has advised on cloud computing for many years, especially on its deployment in the financial sector. She also advises on AI and the sharing of data generated by devices or applications, and helps in reviewing IT solutions from the privacy perspective, handling sensitive data protection requests, and complaints. Agata is a member of the European Commission's Expert Group on B2B data sharing and cloud computing contracts.



Sylwia Macura-Targosz is a senior associate at SK&S, specialising in IT, new technologies and e-commerce law. She is experienced in the field of IT system

implementation projects and licensing issues, and also has expertise in personal data protection and privacy matters. Sylwia has advised in a number of IT and employment projects in which personal data was 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 at the Warsaw Bar Association. She specialises in intellectual property cases (copyright,

industrial property, combating unfair competition, IT system implementation contracts) and regulatory issues in telecommunications law and broadcasting law.

Aleksandra supports entrepreneurs in proceedings conducted by Polish regulatory authorities (President of the Office of Electronic Communications, National Broadcasting Council).

Sołtysiński Kawecki & Szlęzak

Jasna 26
00-054 Warsaw
Poland

Tel: +48 22 608 70 00
Fax: +48 22 608 70 01
Email: office@skslegal.pl
Web: www.skslegal.pl



SOŁTYSIŃSKI
KAWECKI
SZLĘZAK

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

TMT in Poland: An Introduction

One of the most important events in Poland in 2023 was the parliamentary elections in October, which established a new parliament and with it new authorities in the various ministries. 2024 will see significant legislative changes in Poland, which will likely cover, in part, those bills that had not been successfully adopted in the previous year. Such projects include the draft Electronic Communications Law (implementing the European Electronic Communications Code), amendments to the Copyright and Related Rights Act (implementing the Copyright Directive) and an act implementing the Digital Services Act. Telecommunications entrepreneurs and email providers will also face new obligations to combat abuse of electronic communications under the new regulations. 2024 will also be a crucial year for cybersecurity and for further empowering consumers in their e-commerce and media activities.

Priorities of the New Minister of Digitisation

A new Minister of Digitisation and deputy ministers were appointed in December 2023, following Poland's parliamentary elections. At a press conference, the new minister presented the priorities of the Ministry of Digitisation for the coming months.

It plans to prepare a strategy for the digital development of the country, which is expected to indicate directions for further development. Legislative activities include the amendment of the law on the National Cyber Security System, which has been discussed for a long time. The last bill, prepared by the previous government, introduced additional obligations for electronic communication entrepreneurs (a new category of entities) regarding the handling of telecommunications incidents, among other changes.

The second legislative project indicated by the new minister is the adoption of the Electronic Communications Law – ie, a law implementing the European Electronic Communications Code. In other areas, the minister mentioned that programmes for the development of digital competencies for schoolchildren are to be continued.

Appointment of New Data Protection Authority

The newly appointed President of the Polish Data Protection Office (*Prezes Urzędu Ochrony Danych Osobowych*) took office on 26 January 2024. The leaving President was often criticised for limited involvement in data protection matters. The Committee of the Lower Chamber of the Polish Parliament met on 15 January 2024 to evaluate four remaining candidates to this post and provide recommendations.

In a unique development, the selection process included a public debate with the candidates for the post, which was held in mid-December 2023. Everyone agreed that the new President has to rebuild public trust in the office. The candidates also stressed that the Data Protection Office should be reorganised and that some procedural changes are needed, particularly to speed up the review of complaints, improve competences in new technologies and enhance open co-operation with other stakeholders. It also follows from the debate that there is a lack of independent supervision over the processing of personal data by the law enforcement agencies, and that this issue should be resolved urgently.

Finally, the Parliament appointed Mr Mirosław Wróblewski, a lawyer and author of many publications, who recently worked for the Polish Ombudsman, as the new President at the end of January 2024.

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

Cybersecurity Remains Crucial

2023 saw a continued increase in the scale of cyber-attacks. At the same time, however, the level of awareness and the effectiveness of security measures among companies and other organisations were also increasing. Subsidy programmes for public organisations that raise the level of digital protection provided additional resources to increase resilience against cyber-attacks.

In 2024, further digital development will be enhanced by the obligations imposed on public and private entities by the EU NIS 2 Directive and the EU CER Directive, which should be implemented into Polish national law by 17 October 2024.

NIS 2 Directive and CER Directive

The EU NIS 2 Directive and the EU CER Directive create a harmonised legal framework for ensuring the continuity of state-critical services and the resilience (both physical and in cyberspace) of the entities providing them. These directives will stimulate additional digital development and increase the level of security in Polish (and European) companies.

The NIS 2 Directive introduces, among other things, obligations to report incidents and to train employees in cybersecurity. One of the key challenges of the NIS 2 Directive will be to ensure that incidents are handled and reported appropriately, and that plans and procedures are in place to restore business operations and to restore data and infrastructure.

The CER Directive establishes a framework for the resilience of critical entities, including resilience strategies, risk assessments by EU member states or mechanisms for identifying critical entities.

National Cybersecurity System

Work on the National Cybersecurity System Act (“Polish Cyber Act”) – aimed at ensuring cybersecurity at the national level, particularly the uninterrupted provision of essential services and digital services, and the achievement of a sufficiently high level of security among the ICT systems used to provide these services – was not completed in 2023, due to the parliamentary elections and the principle of the discontinuity of parliamentary work (when a parliament ends its mandate, it closes all the projects it has worked on and does not pass them on to the new parliament).

At the beginning of January 2024, the Ministry of Digitalisation announced the commencement of work on the Polish Cyber Act and its completion during 2024. The content of the new draft of the Polish Cyber Act is not yet known – ie, whether it will be broader than the current one and include the implementation of the NIS 2 Directive (and the CER Directive) or whether a new law (or laws) will be passed to implement these directives.

Cyber-resistance of the internet of things (IoT)

Complementary to the EU cybersecurity framework referred to above, the Cyber Resilience Act (CRA) regulation is intended to cover the security of internet-connected devices (especially IoT). The CRA will apply to all products that are directly or indirectly connected to another device or network. Exceptions apply to products for which cybersecurity requirements have already been introduced in EU legislation, such as medical devices, aircraft or vehicles.

In addition, the proposed regulation allows consumers to take cybersecurity into account when selecting and using products with digital elements – users will be able to make a conscious

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

choice of equipment and software with appropriate cybersecurity features.

The CRA is expected to come into force in early 2024, and manufacturers will have to apply the regulations 36 months after they come into force.

Empowering Consumers in E-Commerce and Media Activities

Additional obligations for Polish entrepreneurs when trading with consumers

The Omnibus Directive was implemented into the Polish legal system in 2023, imposing new obligations on entrepreneurs entering into contracts with consumers and aiming to increase the protection of consumers, primarily those operating in the digital world, from unfair marketing practices of entrepreneurs.

In order to facilitate the interpretation of the new rules, in May 2023 the Polish President of the Office of Competition and Consumer Protection (*Prezes Urzędu Ochrony Konkurencji i Konsumentów* – OCCP) published extensive explanations on the rules for the presentation of price reductions (“Explanations”). These Explanations provide guidance on the interpretation of the rules regarding the presentation of discounts by, inter alia, shopping platforms and price comparison sites, when using discount codes, and for participants in loyalty programmes.

However, the Explanations appear to go beyond the mere interpretation of the rules and impose new obligations on entrepreneurs that do not stem from the Omnibus Directive. However, the Explanations do not constitute a source of law and entrepreneurs are not obliged to comply with them, according to the OCCP representatives’ declarations.

Prior consent for changing the terms of service subscription

The President of the OCCP recently examined the subscription terms and conditions of various services, looking first at the subscription terms and conditions of the services available as part of the Amazon Prime and Amazon Prime Video packages. In their contracts, Amazon EU and Amazon Digital UK used, among other things, procedures that allowed unilateral price changes from the new subscription period. This type of condition is particularly detrimental to customers in a situation where a payment card (debit or credit) has been assigned to the account and the operator grants itself the right to automatically charge the new amount for the next subscription period.

The President of the OCCP opined that, in such cases, material terms and conditions – including above all the changed price of the service – should not bind consumers if they do not give their informed consent to extend the subscription on new terms, and that the new price or other new material terms of the contract may be introduced from the next subscription period only with the consumer’s prior consent. Amazon EU and Amazon Digital UK have complied with the OCCP’s position and amended their contractual terms.

The OCCP is currently investigating subscription services offered by Apple, Disney+, Google (with YouTube Premium), HBO Max, Microsoft (with GamePass), Netflix and Sony (with PlayStation Plus), and any price changes made by them.

Increased regulatory control over dark patterns

The President of the OCCP began to combat the use of “dark patterns” (ie, the practice of taking unfair advantage of knowledge about

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

consumers' online behaviour to influence their purchasing decisions) by entrepreneurs, and has imposed financial penalties on entrepreneurs who engage in such prohibited market practices. The President of the OCCP recognised, inter alia, the following practices as examples of dark patterns:

- the automatic addition of a product to the shopping cart without the consumer's knowledge so that, when placing an order, the consumer may overlook excess items and make unplanned purchases;
- inducing customers to subscribe for a paid subscription without their knowledge through appropriate use of the website interface (the button for online ordering was improperly labelled); and
- use (next to the offer) of a countdown timer that counts down the hours until the end of the discount; each day the countdown resumes for the next alleged promotion. The countdown timer encouraged quick purchases, which persuaded consumers to take advantage of the same offers each day.

Further action by the President of the OCCP in this area can be expected in 2024.

Influencer marketing – Polish regulator says “check”

Since the end of 2021, the OCCP has been drawing attention to the need to strengthen social media control in the area of advertising content presented by influencers, particularly in the area of medical products, dietary supplements, medicines, gambling or alcohol, the advertising and promotion of which is restricted by law or completely prohibited in Poland. The “Recommendations pertaining to the tagging of advertising content by influencers in social media” announced at the end of 2022 by the

President of the OCCP, indicating good practices in this area, and the large-scale educational campaigns carried out by the OCCP have contributed to raising awareness of influencers and consumers in this area.

However, the scale of influencer marketing and the mislabelling of advertising collaborations by influencers in social media is still very high. Consequently, after two years of informing and building awareness about the rules of advertising co-operation between entrepreneurs and influencers, the President of the OCCP is moving to enforcement, imposing fines of more than PLN5 million in 2023 on a dietary supplement manufacturer and three influencers co-operating with it for using improperly labelled influencer advertising in social media. On behalf of the manufacturer and in accordance with its instructions, the influencers were to post on their profiles posts and accounts in which, under the guise of neutral information, they recommended certain products without sufficiently disclosing that it was an advertisement – such crypto-advertising became the reason for the OCCP's intervention.

Proceedings have also been initiated against three well-known celebrity influencers, and there have been several procedural penalties (for the lack of co-operation with the authority during the proceedings). However, the President of the OCCP has not yet had the last word, and further actions against mislabelled influencer advertising on social media can be expected in 2024.

A further step towards cleaning up the social media advertising market is the so-called round table meeting initiated by the OCCP, which brought together representatives of social media platforms (Meta, Google and TikTok), the advertising industry and universities to discuss faster and more effective elimination of unlawful adver-

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

tising and improved procedures for the supervision of advertising content that may infringe the law.

Development of e-services in public administration

The field of electronic administrative services will clearly develop in 2024. At the end of the year, Poland will face the launch of the e-Delivery system, which will make it easier for citizens to contact the administration. The National e-Invoice System, which was also due to be launched this year, will probably not be launched until 2025.

With the development of e-government, investments in cloud solutions in public administration are also likely to increase.

New Electronic Communications Law

The long-awaited implementation into the Polish legal system of the European Electronic Communications Code (Directive (EU) 2018/1972 of 11 December 2018) was not completed in 2023. The proposed Electronic Communications Law and the Law Introducing the Electronic Communications Law have passed the stage of government work and have been referred to the *Sejm* (lower house of parliament) for further proceedings. However, due to a number of controversies and reported amendments, both bills were withdrawn from the *Sejm* in April 2023.

Critical comments included provisions on “Must carry must offer” (MCMO) regulations (MCMO is the obligation put on certain broadcasters to make their channels available (must offer) to operators that distribute TV channels; the operators, in turn, are obliged (must carry) to distribute these channels or pay a fine) and the obligation of instant messaging providers to store their users’ data (Messenger, WhatsApp) to the same extent as telecommunications entrepreneurs do.

Since the withdrawal of the bills from the *Sejm*, no new projects have been published.

According to announcements made by the new Minister of Digitisation in January 2024, a draft bill – the Electronic Communications Law – will be prepared by the Ministry of Digitisation in the first quarter of 2024. No information is yet available on the extent to which the new bill will coincide with the previous version from last year.

Implementation of the Copyright Directive

The implementation of the Copyright Directive (Directive (EU) 2017/790 of 17 April 2019 on copyright and related rights in the Digital Single Market) was also not completed in 2023. Due to the principle of the discontinuation of parliamentary work when a parliament ends its term of office, the bill implementing the Copyright Directive, which was to significantly amend the Act of 4 February 1994 on Copyright and Related Rights, is unlikely to be further processed following the election of the new parliament in Q4 2023.

No information has yet been provided on when the new draft law implementing the Copyright Directive will be published, nor on the extent to which the draft will differ from the most recent version from last year. An issue that continues to stir up a lot of controversy in the Polish market is the planned regulation of the payment of royalties to creators from online streaming.

The DSA and Changes in the Provision of Electronic Services

In January 2024, the Minister of Digitisation published an invitation to participate in consultations on the assumptions of the bill amending the law on the provision of electronic services and some other laws that implement the DSA – ie, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Sin-

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

gle Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). The bill itself has not yet been published; only the scope of issues that the bill is expected to regulate has been announced. The co-ordinator for digital services in Poland is to be the President of the Office of Electronic Communications (President of the OEC), and part of the duties related to the enforcement of the DSA will be carried out by the competent authorities – namely, the President of the OCCP.

The bill is to address issues delegated to member states for regulation at the national level, including:

- defining the scope of competence of the President of the OEC and the President of the OCCP in connection with the performance of their tasks;
- the conduct of investigations, inspections and proceedings before the competent authorities related to the violation by providers of intermediary services of their obligations under the DSA;
- the procedural aspects of imposing penalties on providers of intermediary services (with the maximum amount of the penalties themselves resulting directly from Article 52 of the DSA);
- the procedural aspects of filing complaints against providers of intermediary services, referred to in Article 53 of the DSA;
- the granting of “vetted researcher” status as referred to in Article 40(8) of the DSA;
- the granting of trusted whistle-blower status (“trusted flaggers”) as referred to in Article 22 of the DSA;
- the certification of out-of-court dispute resolution bodies;
- the adaptation of the requirements for orders to take action against illegal content and orders to provide information; and

- rules on civil liability and proceedings before the courts, in the event of a claim for damages for violation of the DSA.

A number of entities (including chambers of commerce, NGOs and regulatory authorities) participated in the consultations. The Ministry of Digitisation has not yet indicated specifically when the bill will be drafted and published.

New Law: Combatting Abuse in Electronic Communications

Most of the provisions of the Act of 28 July 2023 on Combating Abuse in Electronic Communications came into force in September 2023. The law implements Article 97 (2) of the European Electronic Communications Code into the national legal order, according to which member states should ensure that national regulatory authorities may, in justified cases, require providers of public electronic communications networks or publicly available electronic communications services to block access to numbers or services on a case-by-case basis. The purpose of the new legislation is to increase user protection against harmful activities carried out through communication technologies, including phishing, smishing distribution, email spoofing or CLI spoofing (caller ID spoofing). The law imposes new obligations on telecommunications entrepreneurs and email service providers, and also on CSIRT NASK (the Computer Security Incident Response Team at National Research Institute) and public entities.

New definition: abuse in electronic communications

According to the Act, abuse in electronic communication is the provision or use of a telecommunications service or the use of telecommunications devices contrary to their purpose or the law. The purpose or effect of such action is to

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

cause harm to the telecommunications entrepreneur or end user, or to achieve undue benefits for the abuser of electronic communications or another person/entity. Examples of such abuses (phishing, etc) are indicated above, with this being an open catalogue.

New obligations for telecommunications entrepreneurs and email service providers

Telecommunications entrepreneurs are obliged to block SMS messages containing content with a message pattern that CSIRT NASK deems to be smishing. They may also block SMS or MMS messages other than those matching the template developed by CSIRT NASK, using a system that allows the automatic identification of such messages for smishing. When it comes to combating CLI spoofing, the President of the Office of Electronic Communications will publish a list of numbers of institutions (eg, banks, insurance companies) that are used exclusively to receive calls. The numbers concerned are hotline numbers from which the institutions themselves generally do not make calls, but at the same time these numbers are easy to find online and are often used by fraudsters to impersonate these institutions. Telecommunications entrepreneurs are required to either conceal number identification or block voice calls that are intended to impersonate another person or institution. In terms of protection against fraudulent websites, CSIRT NASK is to maintain a list of warnings against fraudulent websites. The telecommunications entrepreneur will be able to block users from accessing websites that are included on the warning list.

Email service providers that provide services to at least 500,000 users or public entities are required to use the following mechanisms, which are designed to prevent the use of a domain to

impersonate its owner or modify messages sent from it:

- SPF (Sender Policy Framework);
- DMARC (Domain-based Message Authentication Reporting and Conformance); and
- DKIM (DomainKeys Identified Mail).

Implementation of the Data Act

EU Regulation 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) was finally published on 22 December 2023 and entered into force on 11 January 2024. It will become applicable from 12 September 2025.

The Data Act will include rules on:

- the mandatory sharing to users or third parties of non-personal data generated by products connected to the internet and related services;
- facilitating switching between cloud service providers;
- data holders making data available to public sector bodies, the Commission, the European Central Bank and Union bodies where such data is needed in exceptional cases for the performance of a specific task carried out in the public interest; and
- introducing safeguards against unlawful third-party access to non-personal data and the development of interoperability standards.

Before the Data Act starts to apply, the European Commission and member states should implement certain steps. For member states, these steps include the following:

Contributed by: Agata Szeliga, Sylwia Macura-Targosz and Aleksandra Krześniak-Sałajczyk, Sołtysiński Kawecki & Szlęzak

- Designating competent authorities to be responsible for the application and enforcement of the Data Act. In Poland, this authority is most likely to be the current telecommunication and postal regulator (*Prezes Urzędu Komunikacji Elektronicznej*), provided that the monitoring of the application of the Data Act with respect to personal data will be performed by the current personal data regulator (*Prezes Urzędu Ochrony Danych Osobowych*).
- Ensuring that the competent authorities have the appropriate tasks and powers listed in Article 37 Section 5 of the Data Act. Therefore, as in the case of the GDPR or the Data Services Act, the Polish authorities would adopt the local implementing legislation. The draft of such legislation has not yet been proposed.

PORTUGAL



Law and Practice

Contributed by:

Jorge Silva Martins, João Carminho and Inês Coré
CS'Associados

Contents

1. Metaverse p.329

1.1 Laws and Regulation p.329

2. Digital Economy p.330

2.1 Key Challenges p.330

3. Cloud and Edge Computing p.332

3.1 Highly Regulated Industries and Data Protection p.332

4. Artificial Intelligence p.334

4.1 Liability, Data Protection, IP and Fundamental Rights p.334

5. Internet of Things p.336

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.336

6. Audio-Visual Media Services p.338

6.1 Requirements and Authorisation Procedures p.338

7. Telecommunications p.340

7.1 Scope of Regulation and Pre-marketing Requirements p.340

8. Challenges with Technology Agreements p.343

8.1 Legal Framework Challenges p.343

9. Trust Services and Digital Entities p.344

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.344

CS'Associados is a full-service law firm based in Lisbon, serving national and international clients across the different sectors and industries. Through its technology, data and digital innovation practice area, the firm has been actively engaged with numerous companies within the highly dynamic TMT landscape, with a particular focus on electronic communications (including telco operators and towercos), e-commerce, internet law, media law, data protection, and intellectual property. Jorge Silva Martins leads the practice area, which also comprises three

associates. Recent highlights include providing detailed advice for towercos in Portugal, conducting extensive regulatory assessments for product launches for one of the largest global technology companies, and offering legal and regulatory counsel to companies venturing into the realms of Web3 and the metaverse. Additionally, the firm has undertaken significant work involving the drafting and negotiation of agreements related to the development and implementation of software products for road infrastructures.

Authors



Jorge Silva Martins joined CS'Associados in January 2021 and leads the technology, data and digital innovation practice area. With nearly 20 years of experience, primarily in highly

regulated sectors, Jorge offers counsel to both national and international companies across sectors. His areas of focus span electronic communications, e-commerce, internet law, media law, and intellectual property. Over the past few years, Jorge has expanded his expertise to encompass emerging technologies such as blockchain, the metaverse, and artificial intelligence. Additionally, he has authored several articles in the field of technology and is a regular speaker at industry and academic conferences.



João Carminho is a senior associate at CS'Associados in the technology, data and digital innovation practice area. He holds expertise in a range of sectors, such as electronic

communications, e-commerce, privacy and data protection, and consumer law. João not only provides legal counsel to clients in these domains but also offers expert guidance in handling pre-litigation scenarios and facilitating dispute resolution before the relevant authorities. Through his comprehensive legal support, João actively contributes to clients' strategic decision-making within the dynamic landscape of technology, data and digital innovation.

Contributed by: Jorge Silva Martins, João Carminho and Inês Coré, **CS'Associados**



Inês Coré is an associate at CS'Associados in the technology, data and digital innovation practice area. She offers legal assistance, focusing on matters related to data

protection, intellectual property, and information technologies. Inês guides clients through the legal complexities associated with technology and innovation, providing continuous legal support to ensure compliance with ever-evolving regulations. As a member of the Portuguese Bar Association and the International Association for the Protection of Intellectual Property (AIPPI), Inês actively participates in a global network of professionals, which enables her to stay well-informed about international trends and best practices in the field of intellectual property.

CS'Associados

Avenida da Liberdade, No 249 – 8º
1250-143 Lisboa
Portugal

Tel: +351 211 926 800
Email: mailroom@csassociados.pt
Web: www.csassociados.pt

CS'ASSOCIADOS

1. Metaverse

1.1 Laws and Regulation

Metaverses, Web3 (and Web 4.0)

Metaverses, also known as virtual worlds, are immersive technological environments that utilise 3D and extended reality (XR) to integrate physical and digital realms in real-time. They serve various purposes such as social interaction, transactions, and gaming. It is widely acknowledged that metaverses encompass three fundamental elements:

- persistence and real-time operation;
- immersive user experiences; and
- a generalised economic system.

Metaverses, or virtual worlds, are also part of a broader, long-term technological shift: the transition towards Web3 and Web 4.0 (the third and fourth iterations of the World Wide Web). These advancements aim to seamlessly merge physical and digital domains, fostering more intuitive and immersive experiences. This convergence is anticipated through the evolution of diverse technologies, including artificial intelligence (AI), the internet of things (IoT), secure blockchain transactions, as well as the continuous improvement in infrastructure connectivity.

State of Play

Similar to the situation in the vast majority of countries, Portugal currently lacks specific domestic legislation governing the metaverse. However, as a member state of the EU, Portugal aligns with the European approach to the metaverse, which is worth highlighting.

While previous documents, such as the European Commission Communication dated 16 March 2023, and the European Council conclusions dated 23 March 2023, have made refer-

ences to Web 4.0 (as a digital tool to enhance the EU's long-term competitiveness), it is in the Communication dated 11 July 2023, that the European Commission (EC) outlines its strategy and proposed actions regarding Web 4.0 and virtual worlds, aimed at guiding the forthcoming technological transition while ensuring an open, secure, trustworthy, fair and inclusive digital environment for EU citizens, businesses and public administrations.

To this end, the EU has already in place a robust, future-oriented legal framework that addresses various aspects of virtual worlds development, including:

- With regard to the protection of intellectual property rights (including industrial rights), the following legislative frameworks generally apply:
 - (a) Directive on Copyright in the Digital Single Market (Directive (EU) 2019/790, transposed into Portuguese law by Decree-Law No 47/2023);
 - (b) Regulation on the EU Trademark (Regulation (EU) 2017/1001); and
 - (c) Directive on the Protection of Trade Secrets (Directive (EU) 2016/943, transposed into Portuguese law by Decree-Law No 11/2018).
- With regard to the protection and enforcement of rights of EU citizens and companies operating in the metaverse, the following regimes generally apply:
 - (a) Digital Services Act or DSA (Regulation (EU) 2022/2065);
 - (b) Digital Markets Act or DMA (Regulation (EU) 2022/1925);
 - (c) Data Governance Act (Regulation (EU) 2022/868);
 - (d) Data Act (Regulation (EU) 2023/2854);
 - (e) AI Act (pending EU-level approval);

- (f) GDPR (Regulation (EU) 2016/679);
- (g) General Product Safety Regulation (Regulation (EU) 2023/988);
- (h) Markets in Crypto-Assets (MiCA) Regulation (EU) 2023/1114);
- (i) Unfair Commercial Practices Directive (Directive (EU) 2005/29, transposed into Portuguese Law by Decree-Law No 57/2008);
- (j) Accessibility Act (Directive (EU) 2019/882, transposed into Portuguese Law by Decree-Law No 82/2022); and
- (k) Web Accessibility Directive (Directive (EU) 2016/2102, transposed into Portuguese law by Decree-Law No 83/2018).

Additionally, standardisation will also play a pivotal role in achieving trustworthy, secure and interoperable metaverses within the EU. In that regard, the EC has closely engaged with relevant industry stakeholders to develop standards that ensure openness and interoperability across all layers of the metaverse.

Key Legal Challenges

Although the legal landscape on metaverse is still evolving, there are several legal challenges to consider, namely with regard to the following.

- Intellectual property – safeguarding virtual assets within the metaverse (eg, virtual real estate, digital goods, and in-game currencies); addressing copyright concerns related to user-generated content within the metaverse; and determining platform operator's liability for copyright infringement.
- Data protection – addressing privacy concerns related to user data generated within the metaverse and the processing of special categories of data (eg, biometric data); and clarifying ownership and control of personal data in virtual environments.

- Cybersecurity – ensuring secure identity verification and authentication mechanisms to prevent unauthorised access to virtual spaces; protecting user accounts; and securing financial transactions within the metaverse.

2. Digital Economy

2.1 Key Challenges

Introduction

The digital economy is the economic activity stemming from billions of daily online interactions among individuals, businesses, devices, data and processes. At its core, the digital economy thrives on hyperconnectivity, characterised by the increasing interconnection of people, organisations and machines facilitated by the internet, mobile technology, and the IoT.

A growing variety of mobile devices, such as smartphones, tablets, smartwatches and wearables, empower billions worldwide to participate in the digital economy, accessing goods and services on a global scale, at any time and from any location. While this connectivity offers numerous benefits, it also requires intense regulation.

Advantages of the Digital Economy

The digital economy is positioned to wield even greater influence in the future, propelled by advancements in technologies such as the IoT, AI, virtual reality, blockchain, self-driving cars and other ground-breaking developments. Among its many advantages are:

- information accessibility – consumers have access to a wealth of information to inform their purchasing decisions;
- proximity – direct customer service channels enable customers to resolve queries and

issues with a manufacturer or service provider more quickly;

- global reach – businesses can expand their market presence as goods and services become accessible worldwide; and
- security – digital technologies, including robust authentication for online transactions, bolster security measures.

European Union

The digital economy is playing an ever-increasing role in our lives, revolutionising the way we conduct business, communicate and access information.

As this transformation accelerates, effective regulation becomes paramount to ensure fair competition, protect citizens' rights, and address emerging challenges.

Governments worldwide are grappling with the task of formulating comprehensive regulatory frameworks that set a balance between fostering innovation and mitigating potential risks. Key areas of focus include data privacy, cybersecurity, antitrust, consumer protection and intellectual property rights. Policymakers are challenged to keep pace with the rapid evolution of technology, adapt regulations to address novel issues, such as AI and blockchain, and foster international cooperation to create a harmonised approach to the global digital economy.

To achieve this equilibrium, the EU has implemented a comprehensive framework of digital legislation, primarily through the Digital Agenda and the Digital Single Market (DSM) initiatives. Recent legislative efforts, such as the Digital Markets Act (DMA), the Digital Services Act (DSA), the Data Act, the (forthcoming) Artificial Intelligence Act (AI Act), the Data Governance Act (DGA), the (forthcoming) European Health

Data Space (EHDS), and the NIS2 Directive (imposing stricter cybersecurity obligations on entities operating critical infrastructures and essential services), along with the upcoming eIDAS 2.0, emphasise the EU's commitment to digital governance.

As a member of the EU, Portugal aligns its national policies with the Union's overarching digital strategies.

Portugal

On 5 March 2020, the Presidency of the Council of Ministers approved Portugal's Action Plan for Digital Transition, outlining the government's vision in this regard. This Plan revolves around three primary pillars:

- Pillar I – Capacity building and digital inclusion;
- Pillar II – Businesses' digital transformation; and
- Pillar III – Public services' digitalisation.

In this context, reference should also be made to the following legislation passed in recent years:

- Law No 46/2018, which establishes the legal framework for cyberspace security, implementing Directive (EU) 2016/1148, concerning measures for a high common level of security of network and information systems across the EU;
- Law No 58/2019, implementing the General Data Protection Regulation;
- Decree-Law No 12/2021, implementing Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market;
- Law No 27/2021, which approves the Portuguese Charter on Human Rights in the Digital Age;

- Decree-Law No 65/2021, which regulates the legal framework for cyberspace security and defines cybersecurity certification obligations implementing Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification;
- Decree-Law No 84/2021, which regulates consumer rights in the purchase and sale of digital goods, content and services, transposing Directives (EU) 2019/771 on certain aspects concerning contracts for the sale of goods, and (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services, both of 20 May 2019; and
- Law No 16/2022, which approves the new electronic communications law.

Main Challenges

Despite of the benefits resulting from the digital economy, several challenges persist, including the need for further investment in digital infrastructure, addressing the digital skills gap, and ensuring equitable distribution of its benefits across regions.

Portugal's policymakers are actively shaping a regulatory environment to support the digital economy's growth while confronting emerging issues. However, challenges remain, such as the following.

- Data utilisation – access to big data can create disparities in competitiveness.
- Platform practices – concerns exist regarding competition restrictions and opaque data processing models.
- Regulatory adaptation – in sectors regulated by rapid technological innovation, adapting

regulations to keep up with these changes can be a complex undertaking.

- Stakeholder collaboration – the proper implementation of EU regulations often requires the collaboration of various sectors, including governments, companies, non-governmental organisations and other stakeholders. Co-ordination and support from all these entities can take time, especially when there are different interests and perspectives that need to be reconciled.
- Implementation hurdles – complex regulations and resource constraints may impede timely implementation. Also, some regulations may require significant changes to existing systems and infrastructure, both in the public and private sectors. This can require substantial investments in terms of time and financial resources.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Introduction

Cloud computing involves the delivery of computing services, such as storage, processing power and applications over the internet. It allows businesses to access and utilise shared resources, without the need for on-site infrastructure, offering flexibility and cost-effectiveness. In contrast, edge computing involves processing data closer to the source of data generation, reducing latency and enhancing real-time capabilities. It often involves decentralised infrastructure, enabling data processing at the edge of the network, closer to end-users or devices.

These technologies have revolutionised the way businesses operate, offering unprecedented scalability, efficiency and accessibility. However,

in addition to these benefits, they also present risks that need to be addressed, in particular in terms of data protection, privacy and security.

EU

At European level, the regulation of these technologies is essentially ensured by the GDPR, which lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data, with special emphasis on:

- security of the processing;
- processing by processors; and
- data transfers to third countries.

In accordance with the GDPR:

- Controllers and processors must implement appropriate technical and organisational measures, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, to ensure a level of security appropriate to the risk.
- When processing is conducted on behalf of a controller, the controller must engage processors who offer adequate guarantees to meet the Regulation's requirements and safeguard the rights of data subjects. This processing shall be governed by a binding contract or other legal act under Union or member state law, specifying the processing's subject-matter, duration, nature, purpose, types of personal data, and categories of data subjects. This contract must also contain the minimum content provided for in Article 28(3) of the GDPR.

- Transfers of personal data to third countries of international organisations must adhere to Chapter V of the GDPR. Key conditions include (i) the existence of an adequacy decision by the European Commission; (ii) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2) of the GDPR; and (iii) binding corporate rules in accordance with Article 47 of the GDPR.

It should also be noted that:

- industries dealing with significant amounts of personal data or sensitive data (eg, health-care, banking and finance, telecommunications and insurance) face stricter processing security standards;
- providers of these technologies are typically classified as processors under the GDPR; and
- additional safeguards may be required for transferring personal data to the US.

Portugal

In Portugal, alongside EU Regulations, the following legislation must also be taken into account:

- Law No 46/2018, which establishes the legal framework for cyberspace security, transposing Directive (EU) 2016/1148, concerning measures for a high common level of security of network and information systems across the Union;
- Law No 58/2019, which ensures the implementation, in the national legal system, of the GDPR; and
- Portuguese Data Protection Authority (CNPD) Guideline No 2023/1, on organisational and security measures applicable to the processing of personal data.

As cloud and edge computing continue to evolve, the aforementioned legislation should be adapted and updated to address emerging challenges and promote innovation, while maintaining a balance between technological advancement and the rights, freedoms and guarantees of data subjects.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

Legal Concept of AI

An AI system is defined by law (as per the Artificial Intelligence Act) as a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments.

AI systems are thus a “family” of technologies with virtually limitless applications, offering substantial benefits to individuals, companies and society as a whole.

Nonetheless, while many AI systems are harmless and contribute to solve many societal challenges, others might pose risks to individuals and jeopardise their health, safety or fundamental rights.

Portugal

For the time being, there is no specific law on AI in Portugal. However, there are references to the use of AI (especially with regard to the limits of its use) in several national regimes, namely:

- Portuguese Charter on Human Rights in the Digital Age (Law No 27/2021); and
- Portuguese Labour Code (Law No 7/2009).

The respect for fundamental rights, both with regard to the design and use of AI and robots is enshrined in Article 9 of the Portuguese Charter on Human Rights in the Digital Age, which foresees that AI should comply with several ethical principles, including transparency, accountability and non-discrimination.

Similarly, the Portuguese Labour Code sets limits to the use of AI whenever it results in decision-making that jeopardises the exercise of employee's rights provided for by law (such as the right to equal opportunities in the access to the labour market). On the other hand, it establishes information duties with regard to the criteria on which AI algorithms are based for the decision-making process.

Moreover, the Portuguese government has also published several legislative initiatives and strategies which make reference to AI technologies and their development and impact within the Portuguese society.

Anyhow, a comprehensive AI legal framework is mainly being shaped at an EU level, which is understood to be in the forefront of AI regulation.

EU

As Portugal is a member state of the EU, the regulation proposal on AI (Artificial Intelligence Act), expected to be approved next April, will soon be part of the Portuguese legal system.

The Artificial Intelligence Act, proposed by the European Commission (EC) on 21 April 2021 (regarded as the world's first comprehensive AI law) aims primarily to establish a robust internal

market for AI systems within the EU. Its objectives are two-fold: to ensure that the EU remains at the cutting edge of technological advancement, and to safeguard the rights of EU citizens. The Artificial Intelligence Act will thus establish different obligations for providers and users depending on the level of risk posed by the AI system (minimal risk, high risk, unacceptable risk, and specific transparency risk), and will apply to both public and private actors inside and outside the EU, provided that the AI system is placed on the EU market or its use affects people located in the EU.

Moreover, AI will also be regulated under the following legal frameworks within the EU:

- AI Liability Directive; and
- Product Liability Directive.

Both the AI Liability Directive and the Product Liability Directive (which have not yet been adopted) were proposed by the EC on 28 September 2022, and aim to adapt liability rules to the digital age amongst the member states.

On the one hand, the Product Liability Directive intends to update the existing rules on non-fault (strict) civil liability of manufacturers for defective products (including AI systems which are also regarded as products), while the AI Liability Directive targets harmonisation of national non-contractual fault-based civil liability rules for AI in specific. The idea is to facilitate compensation to victims of unsafe products and AI-related damage, respectively.

In short, AI Liability Directive simplifies the legal procedure for victims seeking compensation by facilitating proof that someone's fault led to damage under the following legal mechanisms.

- Presumption of causality – where a relevant fault has been established and a causal link to the AI performance seems likely there is a presumption of a causal link between such non-compliance and the output produced by the AI system.
- Evidence disclosure – where damage is caused by high-risk AI systems, victims have a right of access to evidence from providers or users pursuant to the Artificial Intelligence Act.

AI Liability Directive will thus apply to claims against any person which, due to wrongful behaviour, influenced AI systems in causing damage (any type of damage covered under national law) to either natural or legal persons (ie, individuals or businesses), whereas the Product Liability Directive will apply to claims against manufacturers of defective products for the compensation of personal injury, damage to property or data loss caused by unsafe products, and it is limited to claims made by natural persons (ie, individuals).

Once adopted, all these regimes will certainly bring significant changes to national liability and consumer protection rules.

Moreover, as AI systems process vast quantities of data, the following legal frameworks may have implications for data sharing and data usage under this context:

- General Data Protection Regulation or GDPR (Regulation (EU) 2016/679);
- Data Act (Regulation (EU) 2023/2854);
- Data Governance Act (Regulation (EU) 2022/868); and
- Digital Services Act or DSA (Regulation (EU) 2022/2065).

Specifically with regards to data protection, key requirements for the development of AI technologies will have to be taken into consideration, such as data minimisation (Article 5(1)(c) of the GDPR) or privacy by design and by default (Article 25 of the GDPR).

Codes of Conduct

Furthermore, concerning codes of conduct, the European AI Alliance has devised an AI Impact Assessment (AIIA) which, in essence, is a practical tool that aims to help organisations to design, employ and audit AI.

The starting point of the AIIA is the Code of Conduct for AI, which forms the basis of the AIIA framework. The Artificial Intelligence Code of Conduct thus consists of two parts:

- common European ethical and constitutional values (ie, 1791 liberty, equality, fraternity), legal principles (eg, fairness, proportionality, rule of law) and democratic preconditions; and
- practical rules and codes of conduct for, inter alia, AI applications, the training data corpora, inference systems, deep learning algorithms, neural networks and autonomous systems.

5. Internet of Things

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection IoT at a Glance

The internet of things (IoT) has been defined in a variety of ways, but it is commonly understood as referring to a global distributed network of physical objects which are capable of interacting with their environment and communicating with

each other (including other machines or computers), and are thus regarded as “smart objects”.

The value of these objects (which can either be household appliances and small wearables or even cars and industrial robots) lies in the large amount of data they collect and process in order to communicate with each other. As IoT results in the merging between both the physical and digital worlds, it enables the creation of “smart environments”, giving rise to specific realities, including “smart homes” (ie, IoT applied to the management and control of buildings, such as lighting or heating) or “smart cities” (ie, IoT applied to the management and control of city infrastructures, such as traffic or public transport).

Portugal

For the time being, Portugal does not have specific laws pertaining to IoT. However, the Portuguese government has introduced legislative initiatives and strategies that address IoT’s development and its impact on Portuguese society.

EU

As Portugal is a member state of the EU, IoT regulation at a EU level is worth highlighting. In that regard, the EU is currently actively co-operating with the industry, market players and academia to support research, innovation and development of IoT technologies.

A number of supporting policy actions have thus been adopted by the EC to enhance development of IoT, particularly through funding research and large-scale pilot projects. However, there are no EU regulatory frameworks specifically targeting IoT technologies, apart from the references made below.

Data Protection and IoT

As IoT largely relies on the processing of data to enable Machine-to-Machine Communications, its regulation will necessarily fall under the applicable data protection legal framework, namely:

- General Data Protection Regulation or GDPR (Regulation (EU) 2016/679);
- Data Act (Regulation (EU) 2023/2854); and
- Data Governance Act (Regulation (EU) 2022/868).

The development and usage of IoT will thus have to respect the fundamental right to data protection enshrined in Article 8 of the Charter of Fundamental Rights of the European Union.

IoT technologies may indeed pose threats to personal data protection, since “smart objects” (such as wearables) might often collect personal data, including, special categories of personal data revealing, for instance, data concerning health (Article 9 of the GDPR). It is precisely through the collection of the said data, as well as its combination with other sets of data that it is possible to establish patterns and further enhance the “smart object” performance for the benefit of the user. On the other hand, security risks might give rise to a “personal data breach” (Article 4(12) of the GDPR) and compromise the integrity of the personal data through unlawful access.

The Data Act (which entered into force on 11 January 2024) regulates data generated by a user's product connected to a publicly available electronic communications network, and aims at harmonising rules on the fair access to and use of such data. In other words, it clarifies who can create value from data and under which conditions. This is indeed relevant for IoT technologies

since “smart products” rely immensely on data gathered from its users.

The Data Act will become applicable from 12 September 2025 and creates measures to, namely:

- give access to businesses and consumers of IoT technologies to the data generated by these devices;
- protect businesses from unfair contractual terms that hinder fair data sharing;
- allow public sector bodies to access and use data held by the private sector that is necessary for the pursuit of public interest purposes; and
- allow customers to seamlessly switch between different cloud providers of data-processing services.

The aforementioned measures complement the Data Governance Act (that became applicable from 24 September 2023), which together with the Data Act embody the EU Strategy for Data.

The Data Governance Act focus on data-sharing, regulating processes and structures to facilitate such exchange, namely through the following measures:

- facilitate the reuse of public sector data that cannot be made available as open data;
- ensure that data intermediaries function as trustworthy organisers of data sharing or pooling within the EU data spaces;
- make it easier for citizens and businesses to make their data available for the benefit of society; and
- facilitate data sharing, in order to enable data use across sectors and borders.

Overall, both the Data Act and the Data Governance Act complement existing rights on personal data protection. This applies in particular to the right to data portability (Article 20 of the GDPR) that allows data subjects to move their data between controllers who offer competing services.

Communications Secrecy

Communications secrecy within the context of IoT technologies falls under broader regulations mainly related to data protection, cybersecurity and consumer rights.

Apart from GDPR applicability, which was already addressed, the ePrivacy Directive (Directive 2002/58/EC) regulates the protection of personal data and privacy in electronic communications. While the ePrivacy Directive is currently in force, a new ePrivacy Regulation is under discussion and is expected to update and strengthen privacy rules for electronic communications, including IoT devices.

On the other hand, NIS2 Directive (Directive (EU) 2022/2555) which entered into force on 16 January 2023 replacing its predecessor NIS Directive, is considered the EU-wide legislation on cybersecurity and although it does not specifically target IoT, it has implications for the overall cybersecurity of systems, which indirectly influences communication secrecy within IoT deployments.

Moreover, considering the security risks that products with digital elements may entail (including, IoT technologies), the EC adopted a proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).

Codes of Conduct

With regard to codes of conduct and standards, the European Telecommunications Standards Institute (ETSI) has developed standards and technical specifications pertaining to IoT security and privacy. These standards encompass requirements, architecture, Application Programming Interface (API) specifications, security solutions and interoperability for Machine-to-Machine (M2M) communications. Additionally, the International Organization for Standardization (ISO) has published ISO/IEC 27400:2022, providing guidelines on risks, principles and controls for the security and privacy of IoT solutions.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Provision of Audio-Visual Media Services in Portugal

Audio-visual media services (AVMS) in Portugal are mainly regulated under the following legislation:

- Decree-Law No 46/2023 (implementing Directive (UE) 2019/789 on Copyright and Related Rights applicable to certain Online Transmissions of Broadcasting Organisations and Retransmissions of Television and Radio Programmes);
- Decree-Law No 47/2023 (implementing Directive (UE) 2019/790 on Copyright and Related Rights in the Digital Single Market or DSM Directive);
- Decree-Law No 82/2022 (implementing Directive (UE) 2019/882 on Accessibility Requirements for Products and Services);

- Law No 74/2020 (implementing Directive (UE) 2018/1808 or Audiovisual Media Services Directive);
- Law 54/2010 (Radio Act);
- Law No 27/2007 (TV and On-demand Audio-Visual Services or AVMS Law implementing Directive (EU) 2010/13 on Audiovisual Media Services); and
- Decree-Law No 63/85 (Copyright and Related Rights Code).

As pursuant to the applicable law, AVMS in Portugal may be provided by the following operators:

- television services broadcasters;
- providers of on-demand audio-visual services; and
- video-sharing platform services made available by video-sharing platform providers.

The aforementioned legislation stipulates several requirements that must be met by AVMS providers. Namely, all audiovisual media services are required to adhere to the following obligations:

- identification of media service providers;
- prohibition of incitement to hatred;
- accessibility for people with disabilities;
- qualitative requirements for commercial communications;
- sponsoring; and
- product placement.

More stringent rules in the areas of advertising and protection of minors are foreseen for television broadcasts, due to their significant societal impact, as elaborated below.

In accordance with the Portuguese AVMS Law, AVMS are thus obliged to respect fundamental rights within their programming content, and

may not (i) provoke or incite any violence or hatred towards a particular group of people (eg, minorities); and (ii) provoke or incite the commitment of terrorist offences.

Moreover, television service broadcasters are subject to specific restrictions not only concerning content but also regarding the applicable timeframes for making such content available. This particularly applies to content that is likely to be harmful to minors and could adversely affect the development of their personality. Such content can only be made available during times when minors are unlikely to view them (ie, between 10pm and 6am), and must be identified by the presence of a visual symbol throughout its duration.

The same applies to on-demand audio-visual service providers, who are also obliged to identify such content through a visual symbol. Furthermore, they are required to implement technical functionalities that enable individuals responsible for parental oversight to block minors' access to such content.

Nonetheless, on-demand audio-visual media services are different from television broadcasting (namely, with regard to the choice and control of the user or the impact they have within society) which has justified the imposition of lighter regulation.

With regard to advertising, television commercials and teleshopping aired from 6am to 6pm, as well as from 6pm to midnight, must not surpass 10% or 20%, depending on whether they pertain to conditional access television programme services or free/conditional access television programme services with a subscription.

Video-Sharing Platforms

Regarding video-sharing platform services, some of the aforementioned requirements will also be applicable. The obligations primarily focus on protecting minors and the general public from hate speech, and well as prohibiting the incitement of violence and other forms of hateful content, including criminal and child pornographic material. Therefore, video-sharing platforms are mandated to moderate user-generated content to a certain extent to ensure compliance with these obligations.

Moreover, following the entry into force of the Regulation (EU) 2022/2065 (Digital Services Act or DSA), video-sharing platforms are also required to comply with several measures aimed at combating illegal content online.

Authorisation Procedure

Pursuant to Article 13 of the AVMS Law, television activities are subject to licensing through a public tender, initiated by the government's decision, when utilising terrestrial radio spectrum for broadcasting. The licensed activities encompass (i) organising unconditional access television programme services, and (ii) selecting and aggregating television programme services with conditional access or non-conditional access with subscription.

When television activities involve organising programme services that (i) do not utilise the terrestrial radio spectrum designated for broadcasting, and (ii) are intended to be included in the offerings of a distribution operator previously licensed for television activities, an authorisation is required upon the request of interested parties. Moreover, providers of on-demand audiovisual services are obliged to electronically notify ERC of the commencement and conclusion of each service's activity. *Entidade Reguladora*

para a Comunicação Social (ERC) – Portuguese Regulatory Authority for the Media – holds the responsibility for granting, renewing, amending, or revoking licences and authorisations for television activities.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements Regulatory Framework

In Portugal, the regulation of electronic communications networks and services is governed by numerous legislative acts and regulations, including:

- Electronic Communications Law (Law No 16/2022);
- Communications Infrastructures Law (Decree-Law No 123/2009);
- Privacy in electronic communications Law (Law No 41/2004); and
- Portuguese Cybersecurity Law (Law No 46/2018).

ANACOM serves as the sector-specific regulatory authority, as outlined in its Statutes (Decree-Law No 39/2015).

Moreover, the Portuguese Competition Authority is responsible for monitoring post-market conditions in the electronic communications sector. Oversight of social media platforms may fall within the jurisdiction of the Portuguese Regulatory Authority for the Media (ERC – *Entidade Reguladora para a Comunicação Social*), especially when these platforms operate as broadcasting outlets or are supervised by ANACOM regarding the provision of information society services. Regarding privacy matters, social media platforms fall under the supervision of the

Portuguese Data Protection Authority (CNPD), as stipulated in Law No 58/2019.

The Portuguese Electronic Communications Law

Following a protracted period marked by stagnation and procedural delays, the European Electronic Communications Code (EECC) was finally transposed into national law in Portugal.

Published in the official gazette, Law No 16/2022, marks the enactment of the new Electronic Communications Law (referred to as the “New ECL”). This law heralds a modernised, forward-looking regulatory framework that requires familiarity from all stakeholders, including operators and end-users.

The New ECL represents a comprehensive, intricate regime that closely mirrors the objectives and verbiage of the EECC. Notably, deviations from the EECC’s text are most apparent in the realm of end-users’ rights, which is not unexpected, given the focal point these rights held in parliamentary deliberations throughout the domestic legislative process.

Comparatively, the New ECL introduces noteworthy alterations from the existing regulatory framework, including the following.

- Broader definition of Electronic Communications Services – the New ECL broadens the definition of electronic communications services to include OTT services, which are services delivered over the internet, such as messaging apps and VoIP calling. This expansion reflects the evolving landscape of communication technologies and ensures that regulatory frameworks remain updated and comprehensive.
- Lighter regulations for OTT Services – while OTT services fall within the scope of the New ECL, they are subject to a more lenient regulatory regime compared to traditional electronic communication services. For instance, they may not require general authorisation for provision (depending on their nature) and are exempt from certain general conditions applicable to traditional services.
- Spectrum management powers – ANACOM gains enhanced powers in managing radio spectrum. This includes promoting spectrum sharing among operators to maximise efficiency and ensuring fair competition. ANACOM is also empowered to adjust the duration of frequency rights to prevent distortions in the market.
- Market power obligations – undertakings with significant market power face reinforced obligations, including providing access to infrastructure and commitments to invest in high-capacity networks. These measures aim to foster competition and encourage investment in critical telecommunications infrastructure.
- Consumer protections – the New ECL strengthens consumer protections in various ways. It mandates transparency regarding setup costs and service quality, provides consumers with tools to compare prices and conditions across different services, and offers safeguards in cases of service unavailability or non-compliance with service level agreements (SLAs). Additionally, it regulates minimum contractual commitment periods, ensuring fairness and flexibility for consumers.
- Social regulation challenges – despite advancements in regulatory frameworks, challenges remain in social regulation, particularly concerning universal service provisions. The reliance on the internet social tariff rather than the New ECL’s provisions raises

questions about the effectiveness of achieving social objectives in the digital age.

- Implementation and enforcement – contractual commitments under the new law apply to both existing and future contracts, ensuring continuity and consistency in consumer rights and obligations.

These changes reflect Portugal's efforts to modernise its telecommunications regulatory framework, aligning with European standards, while addressing evolving technologies and consumer needs.

Requirements

The aforementioned legislation outlines the applicable general authorisation requirements in this regard. According to these requirements, individuals or companies planning to offer publicly accessible or private electronic communications networks and services are obligated to inform ANACOM before introducing these services in the market.

The notification submitted to ANACOM should include a concise written description of the network or service and the anticipated launch date for market offerings. More details on the notification process to ANACOM are further specified under the applicable regulation, which addresses the registration of entities providing electronic communications networks and services, as well as outlines information responsibilities to fall upon entities governed by the regulation.

Within the framework of general authorisation rules, any entity engaged in offering electronic communications networks and/or services has the permission to deploy telecommunications infrastructure. However, specific licences, such as administrative authorisations mandated by municipalities may still be necessary.

Therefore, and in accordance with the general authorisation rules, companies are required to provide the following information.

- Comprehensive company identification, encompassing the company's website linked to the provision of publicly available electronic communications networks and services.
- Communication and notification contacts, inclusive of a mandatory email address.
- A concise overview of the network or service they intend to deliver, specifying the network or service type, target market (wholesale or retail), support network for the service, information on the network's characteristics and purpose, the necessity for numbering or frequency resources, and a specification of said resources. Additionally, a general description of the service offer is required.
- The anticipated commencement date for operations.

A noteworthy change brought about by the New ECL pertains to the utilisation of harmonised spectrum for accessing public electronic communications networks through radio, specifically via local networks (such as WiFi networks deployed using LANs in end-users' premises). This particular usage is exclusively governed by the general authorisation framework.

The New ECL explicitly states that the provision of number-independent interpersonal communications services and local networks via radio, when not constituting an economic activity or carried out as an ancillary function to an economic activity or public service not reliant on the conveyance of signals over that network, is exempt from the general authorisation framework, regardless of the entity – be it a company, public authority, or end-user.

Individual licences are granted for the utilisation of numbering and frequency resources.

The provision of electronic communications services for self-use is categorised as non-publicly available.

Main Challenges

The challenges within Portugal's electronic communications regulatory framework primarily centre on securing fair access to communication services, bridging the digital divide and adapting to the swift evolution of technology and business models. There is a pressing need to effectively implement universal service provisions, especially in underserved communities, while grappling with complexities such as digital inclusion, privacy concerns, and cybersecurity threats. Balancing innovation and investment with regulatory oversight, ensuring compliance with evolving EU legislation and fostering collaboration between stakeholders are crucial for maintaining a robust and responsive regulatory framework in an increasingly digital landscape.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Introduction

A technology agreement can be defined as an agreement focusing on technological products and/or services, or those incorporating a technological component. This can apply to various types of agreements, including:

- Software licence agreements.
- Technology transfer agreements.
- Service level agreements.
- Research and development agreements.
- Non-disclosure agreements.

- Joint-venture agreements.
- Outsourcing agreements.
- Hardware purchase agreements.

These agreements generally contain clauses on the rights and obligations of both parties, price, terms of invoicing and payment, intellectual property rights, confidentiality, processing of personal data, duration, termination, liability, assignment of the contractual position and subcontracting, audits, communications, applicable law and jurisdiction, among others.

Challenges

In addition to the challenges associated with drafting clauses on the aforementioned topics – which are common to contracts of any nature – these agreements pose specific challenges, linked to the swift evolution of technology and related legislation. This evolution can result in outdated terms and conditions that may not adequately address emerging technologies and associated risks. Some of these challenges include the following.

- Data privacy and security concerns – with the heightened emphasis on data privacy and security, technology agreements must address these concerns. This is especially crucial in regulated sectors and industries handling significant amounts of personal data (eg, healthcare, banking and finance, telecommunications and insurance), where stringent security standards apply.
- Global operations and jurisdictional complexities – technology agreements involving parties from different jurisdictions often encounter challenges due to legal and regulatory disparities. Determining the applicable laws and jurisdictions for dispute resolution can be intricate and requires careful consideration.

- Performance and service level challenges – defining and measuring performance metrics in service level agreements can be challenging. Ensuring that technology services adhere to agreed-upon standards may require ongoing monitoring and adjustment to maintain satisfactory levels of performance.
- Contractual interpretation – ambiguities in language within technology agreements can lead to misunderstandings and disputes. It is imperative to provide clear definitions, specifications, and obligations to minimise the risk of misinterpretation and ensure smooth contractual execution.
- Cybersecurity vulnerabilities – as technological interconnectedness grows, so does the likelihood of cybersecurity threats. Technology agreements must incorporate robust cybersecurity measures and response protocols to mitigate potential risks.

Addressing these challenges requires thorough due diligence, seeking legal counsel, and consistently reviewing and updating technology agreements. This ensures their ongoing relevance and effectiveness in the ever evolving technology landscape.

Moreover, integrating flexibility into agreements to accommodate changes and unforeseen circumstances can facilitate in mitigating some of these challenges.

Portugal

In Portugal, there is no specific regulation applying to technology agreements. Consequently, these agreements are typically governed by overarching legal principles and rules of private law, in particular, the Civil Code and Commercial Code.

In addition to these two fundamental regimes, there are also some specific frameworks that deserve to be highlighted in this context.

- Law No 58/2019, which ensures the implementation, in the national legal order, of the GDPR.
- Decree-Law No 63/85, which approves the copyright and related rights code.
- Decree-Law No 252/94, concerning the legal protection of computer programs, transposing Council Directive 91/250/EEC. This Directive was repealed by Directive 2009/24/EC, of the European Parliament and of the Council, of 23 April 2009, addressing the same subject.
- Decree-Law No 122/2000, on the legal protection of databases, transposing Directive 96/9/EC, of the European Parliament and of the Council, of 11 March 1996.
- Decree-Law No 446/85, which approves the Standard Contractual Clauses Regime.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes Introduction

According to the 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 (“eIDAS Regulation”):

- “Electronic signature” means 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.

- “Advanced electronic signature” means an electronic signature which 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 his 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.
- “Qualified electronic signature” means 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.
- “Trust service” means an electronic service normally provided for remuneration which consists of:
 - (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services;
 - (b) the creation, verification and validation of certificates for website authentication; or
 - (c) the preservation of electronic signatures, seals or certificates related to those services.
- “Qualified trust service” means a trust service that meets the applicable requirements laid down in this Regulation.

In accordance with this 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;

- a qualified electronic signature shall have the equivalent legal effect of a handwritten signature; and
- a qualified electronic signature based on a qualified certificate issued in one member state shall be recognised as a qualified electronic signature in all other member states.

Importance and Advantages of Trust Services and Electronic Signatures

Trust services and electronic signatures offer essential advantages for companies in the digital era. One key benefit is the significant time and cost savings achieved by streamlining document workflows and eliminating the need for physical signatures. Electronic signatures expedite approval cycles, reduce administrative overheads and enhance overall operational efficiency.

Security emerges as another critical factor. Trust services provide advanced security measures such as encryption and authentication, safeguarding the integrity and confidentiality of digital transactions. Supported by secure authentication protocols, electronic signatures offer a reliable alternative to traditional handwritten signatures, thereby reducing the risk of unauthorised access or tampering.

Moreover, trust services contribute to legal compliance, given the widespread recognition of electronic signatures across many jurisdictions. This not only simplifies the compliance process for companies, but also reduces the risk of disputes related to the authenticity of documents.

Furthermore, these technologies facilitate seamless collaboration in today's globalised business landscape, allowing secure digital document exchange across diverse geographical boundaries.

Portugal

In Portugal, this topic is governed by Decree-Law No 12/2021, which:

- ensures the implementation within the Portuguese legal order of the eIDAS Regulation;
- regulates the validity, effectiveness and probative value of electronic documents;
- establishes the recognition and acceptance of electronic identification means for both natural and legal persons; and
- provides guidelines for the State Electronic Certification System – Public Key Infrastructure (SECS).

According to this Decree-Law, and in line with the provisions of the eIDAS Regulation, affixing a qualified electronic signature to an electronic document holds the same legal weight as a handwritten signature on paper and establishes the presumption that:

- the person who affixed the qualified electronic signature is either its rightful holder or a representative authorised with adequate powers on behalf of the relevant legal person;
- the qualified electronic signature was affixed with the explicit intention of signing the electronic document; and
- the electronic document has remained unaltered since the qualified electronic signature was affixed.

Trusted List

In accordance with the eIDAS Regulation, each member state shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

This information is published in so-called “trusted lists” and Commission Implementing Decision (EU) 2015/1505 defines the technical specifications of these lists.

The trusted list of Portugal comprises information concerning qualified trust service providers who are under the supervision of the National Security Cabinet of Portugal. This list also includes details regarding the qualified trusted services offered by these providers, in accordance with the relevant provisions outlined in the eIDAS Regulation.

The trusted list of Portugal includes the following currently active trust service providers:

- ACIN iCloud Solutions, Lda.;
- AMA – *Agência para a Modernização Administrativa, I.P.*;
- CEGER – *Centro de Gestão da Rede Informática do Governo*;
- DigitalSign – *Certificadora Digital*
- *Instituto dos Registos e do Notariado I.P.*;
- MULTICERT – *Serviços de Certificação Eletrónica S.A.*; and
- NOS Comunicações, S.A.

The Portugal Digital Identity System

Portugal embarked on the development of its digital identity system in 2007, positioning itself as a pioneering nation in aggregating into a single card five different identification numbers and implementing digital certificates with its eID “Citizen Card”. Since then, the Portuguese government has consistently invested in enhancing its eID scheme, introducing various secure and easy-to-use mechanisms.

In 2014, Portugal introduced the “Digital Mobile Key”, a mobile solution that expanded its usage into the private sector. Subsequently, the eID

schemes were broadened to include professional attributes (with the introduction of “SCAP”, 2018). More recently, in 2019, Portugal launched the ID.gov app, a mobile application enabling citizens to securely store, access and share their personal document data at any time, with full legal validity.

SINGAPORE



Law and Practice

Contributed by:

Lim Chong Kin
Drew & Napier LLC

Contents

1. Metaverse p.350

1.1 Laws and Regulation p.350

2. Digital Economy p.353

2.1 Key Challenges p.353

3. Cloud and Edge Computing p.354

3.1 Highly Regulated Industries and Data Protection p.354

4. Artificial Intelligence p.356

4.1 Liability, Data Protection, IP and Fundamental Rights p.356

5. Internet of Things p.358

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.358

6. Audio-Visual Media Services p.360

6.1 Requirements and Authorisation Procedures p.360

7. Telecommunications p.362

7.1 Scope of Regulation and Pre-marketing Requirements p.362

8. Challenges with Technology Agreements p.364

8.1 Legal Framework Challenges p.364

9. Trust Services and Digital Entities p.365

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.365

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 with cybersecurity 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 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,

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 has assisted regulators in conceptualising and drafting "first-of-its-kind" sectoral competition legislation and frameworks.

Drew & Napier LLC

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



1. Metaverse

1.1 Laws and Regulation

A patchwork of legislation is available to tackle issues relating to data protection, the 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 are:

- formed or recognised under the law of Singapore; or
- resident, or have an office or a place of business, in Singapore.

The PDPA does not generally apply to:

- individuals acting in a personal or domestic capacity;
- employees acting in the course of their employment with an organisation; or
- any public agency in relation to the collection, use or disclosure of personal data.

Therefore, in the virtual world, organisations have to comply with the obligations set out in the PDPA. 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 the Personal Data Protection Commission (PDPC) is empowered to impose the following financial penalties if an organisation fails to comply with its obligations under the PDPA:

- in the case of a contravention by an organisation whose annual turnover in Singapore exceeds SGD10 million, the PDPC may impose financial penalties of up to 10% of the annual turnover in Singapore of the organisation; and
- in any other case, the PDPC may impose financial penalties of 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
- safeguard against the use of online accounts for such communication and for information manipulation.

Furthermore, the Foreign Interference (Countermeasures) 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.

The Online Safety (Miscellaneous Amendments) Act 2022 (the “Online Safety Act”) came into operation on 1 February 2023, and the Broadcasting Act 1994 (BA) was 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 Online Safety Act introduced new provisions to the BA to regulate Online Communication Services (OCS) accessible by Singapore end-users. Currently, social media services are the only regulated OCS. OCS are an electronic services (or parts of an electronic service) that have the characteristics of a social media service, which may be provided in or from Singapore, or from outside Singapore. OCS enable end-users to access or communicate content on the internet, or to deliver content to end-users. Under the amended BA, OCS with significant reach and impact in Singapore may be designated as Regulated Online Communication Services. The providers of such Regulated Online Communication Services have the duty to take all reasonably practicable steps to comply with the applicable Codes of Practice, to implement measures to mitigate the risks of danger to Singapore users from exposure to harmful content and to provide accountability to their users on such measures.

Under the new Part 10A of the BA, the Infocomm Media Development Authority (IMDA) is empowered to issue directions to deal with egregious content that can be accessed by Singapore users on 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 BA 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.

On 18 July 2023, the Code of Practice for Online Safety (Online Safety Code) took effect. It seeks to minimise Singapore users’ exposure to harmful content, with additional protection for children, by requiring designated social media services to put systems and processes in place to curb the spread of harmful content on their services, among other measures. The categories of harmful content covered by the Online Safety Code are:

- sexual content;
- violent content;
- suicide and self-harm content;
- cyberbullying content;
- content endangering public health; and
- content facilitating vice and organised crime.

In light of the proliferation of scams and malicious cyber-activities, the Singapore government introduced the Online Criminal Harms Bill, which targets online content that is criminal in nature or that is used to facilitate or abet crimes. Once enacted, the Online Criminal Harms Act will allow the Singapore government to issue directions to any online service provider through which criminal activities could be conducted to remove or block access to content that is suspected of being used to commit crimes such as scams.

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 that fall within the scope of digital payment tokens (DPTs) are subject to the regulatory regime under the PSA, which 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 therein, 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 (SPI) licence or a major payment institution (MPI) licence.

On top of compliance with the PSA, licence holders must also take note of 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 on 23 November 2023 announced the finalised measures relating to business conduct, consumer access and managing technology and cyber-risks for DPT service providers. MAS' regulatory measures on DPT services will be implemented through regulations and guidelines, which will take effect in phases from mid-2024.

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 that specifically targets NFTs, issues such as ownership continue to be governed by the principles of intellectual property and contract law. A contract for the purchase of NFTs usually contains three distinct subject matters that 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 usually 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 must 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 **9.1 Trust Services and Electronic Signatures/Digital Identity Schemes** for more details on the ETA.

Furthermore, the law in relation to NFTs is evolving rapidly. Most notably, in 2022 the Singapore High Court held that the NFTs being considered in that case satisfied the legal criteria to be considered as property and could 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

A patchwork of legislation is currently available, including in relation to consumer protection, the 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 an SPI licence or an MPI licence – see **1.1 Laws and Regulations (Digital Assets)** – if they offer the following services:

- account issuance services that involve issuing a payment account, or any service relating to any operation required for operating a payment account;
- domestic money transfer services that involve providing a local fund transfer service;
- merchant acquisition services that involve accepting and processing payment transactions and payment receipts for and on behalf of a merchant; or
- e-money issuance services that involve the 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 MPI licensees to protect customers by limiting a customer's potential loss from the customer's account. Personal payment accounts issued by an MPI are subject to a load capacity of SGD20,000 and an annual transaction flow cap of SGD100,000.

E-Commerce

E-marketplaces and e-retailers should ensure that they conform with the Consumer Protection (Fair Trading) Act 2003 (CPFTA), which 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 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. In addition, 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. The TR 76 was recently revised to include additional anti-

scam guidelines for e-retailers and e-commerce marketplaces, in order 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, which are particularly relevant in digital markets that feature multi-sided platforms. Notably, the CCCS has defined 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 consumers’ 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, which may be useful to e-commerce providers. For example, the business improvement exception under the PDPA allows organisations to use personal data, without consent, 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

Limitations are 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, which defines “personal data” 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 given 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, BCRs and contracts must specify the countries and territories to which the personal data will be transferred under said 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 clarify 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 indus-

try 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.

Under the PDPC’s Cloud Services Guidelines, MTCS Level 3 certification could give 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 that assist CSCs in identifying, evaluating and negotiating protection needs with CSPs to incorporate into their service-level agreements, and the 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), setting 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 to which the personal data is transferred comply with these standards.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

There is currently 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 give organisations practical recommendations on 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 provide 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 Governance 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:

- 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 the data used, as well as the transparency of the algorithms chosen; and
- 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.

In 25 May 2022, the IMDA and PDPC launched AI 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. AI Verify packages together a set of open-source testing solutions,

including a set of process checks, into a toolkit for convenient self-assessment. The toolkit will generate reports for developers, management and business partners, covering major areas affecting AI performance.

On 7 June 2023, IMDA set up the AI Verify Foundation (the Foundation) to harness the collective power and contributions of the global open source community to develop AI Verify. The Foundation seeks to boost AI testing capabilities and assurance to meet the needs of companies and regulators globally. It has more than 60 general members, with seven premier members – Aicadium, Google, IBM, IMDA, Microsoft, Red Hat and Salesforce – that will set strategic directions and a development roadmap for AI Verify.

Singapore's second National AI Strategy (NAIS 2.0) was officially launched on 4 December 2023 and outlines Singapore's vision to be a place where AI serves as a force for good, where AI is harnessed to uplift Singapore's collective economic and social potential over the next three to five years.

Autonomous Vehicles

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 use such vehicles 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

POFMA was enacted to prevent the electronic communication in Singapore of false statements

of fact, amongst other things. Notably, Section 8 of POFA 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.

Data Protection

The collection and use of large datasets for big data analytics, machine learning and AI may trigger data protection concerns, especially where such data sets involve personal data (see **3.1 Highly Regulated Industries and Data Protection** 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 individual affected.

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

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.

However, AI-related inventions may 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. In addi-

tion, 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 CA, 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 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

Singapore has not enacted any laws that specifically govern the internet of things (IoT), but certain existing laws and regulations may apply to various aspects of IoT projects or applications. In addition, 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 the telecommunications sector in Singapore, amongst others, 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 that have been granted by the IMDA (see **7.1 Scope of Regulation and Pre-marketing Requirements** 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, which sets out a framework for the designation and monitoring of criti-

cal 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 Cybersecurity Act, 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 Cybersecurity Act, including reporting cybersecurity incidents, conducting regular cybersecurity audits and risk assessments, and furnishing relevant information.

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 covers cybersecurity service providers providing penetration testing services and managed security operations centre monitoring services, and aims to improve the standard of cybersecurity service providers and address the information asymmetry between consumers and service providers.

On 15 December 2023, the Cyber Security Agency of Singapore (CSA) launched a public consultation to seek feedback on the Cybersecurity (Amendment) Bill. In light of the adoption of new technological tools and business models,

such as cloud computing, the CSA is proposing amendments to the Cybersecurity Act to ensure that Singapore's cybersecurity laws remain fit-for-purpose to address the emerging challenges in cyberspace. Among other matters, the proposed amendments seek to widen the oversight of the Commissioner of Cybersecurity beyond CII owners to also include major foundational digital infrastructure service providers, entities of special cybersecurity interest and owners of systems of temporary cybersecurity concern.

With the increasing adoption of IoT solutions amongst various stakeholder groups – including consumers, enterprises and governments – organisations that 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 Cybersecurity Act.

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 sector (including broadcasting and film). "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 online 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 online services;
- computer online 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) that 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 the IMDA has deemed to be against the public interest, public order or national harmony or to offend against good taste or decency.

Furthermore, as of 1 February 2023, the amended BA contains 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 **1.1 Laws and Regulations** 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 broadcasts that are capable of being received in 50,000 dwelling houses or more.

Different types of broadcasting licences may come with different licence fees, as follows:

- 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 guarantee 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 online services by internet access service providers – SGD1,000;
- computer online services by non-localised internet service resellers – SGD100 (if fewer than 500 user accounts) or SGD1,000 (for 500 accounts or more); and
- computer online services by localised internet service resellers – SGD100 for each premise at which the computer online services are provided.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

As noted in the definition of “telecommunications” (see **5.1 Machine-to Machine Communications, Communications Secrecy and Data Protection**), 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 messaging. 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.

The IMDA was formally established on 1 October 2016 as a converged regulator for both the info-communications and media sectors but, in general, the telecommunications and media sectors continue to be governed by separate regulatory frameworks. For instance, the TA does not currently apply to the licensing of broadcasting services or any broadcasting apparatus, which instead falls under the BA. 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 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: facilities-based operations (FBOs) or services-based operations (SBOs). 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 networks, 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 under-

take 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 its 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 licensee), 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.

At 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 that 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 to 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 Guide-

lines 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 and maintain data confidentiality and integrity. As a result, organisations entering into IT service agreements with FIs may need 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 outside of Singapore, or if the solution involves cloud computing), the organisation should also consider compliance with cross-border data transfer requirements under the PDPA and PDPR; see **3.1 Highly Regulated Industries and Data Protection** (Specific Issues Regarding Personal Data Protection) 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 a business 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 provided 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 the sensitivity of the personal data into account 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; and

- 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 that 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:

- whether the transformation was created using the private key that corresponds to the signer's public key; and
- whether the initial electronic record has been altered since the transformation was made.

A digital signature can be treated as a secure electronic signature if it 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, which is 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.

On 2 August 2023, the Oaths, Declarations and Notarisations (Remote Methods) Bill and the Constitution of the Republic of Singapore (Amendment No 2) Bill were passed in Parliament. The Bills seek to introduce the option of making statutory declarations, oaths and affirmations and to notarise documents through remote means, in line with the government's ongoing efforts to facilitate electronic transactions, so as to implement greater convenience and efficiency for individuals and businesses in Singapore.

Trends and Developments

Contributed by:

Rajesh Sreenivasan, Steve Tan, Benjamin Cheong and Lionel Tan
Rajah & Tann Singapore LLP

Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore and South-East Asia. Highly attuned to the latest legal and market developments and cultural nuances, the firm has been at the leading edge of law in Asia, having worked on many of the biggest and highest profile matters in the region. The firm is also a member firm of Rajah & Tann Asia (RTA). Launched in 2014, RTA is one of the

largest regional networks, which brings together leading law firms and more than 970 fee earners across ten jurisdictions, augmenting each firm's cross-border expertise as the teams work closely on complex multi-jurisdictional matters. The firm's reach also includes Singapore-based regional desks dedicated to Brunei, Japan and South Asia.

Authors



Rajesh Sreenivasan is the head of Rajah & Tann Singapore LLP's TMT practice and co-ordinating partner for its multidisciplinary and cross-practice data and digital economy regional sector

group. He is also the director and co-founder of Rajah & Tann Technologies and Rajah & Tann Cybersecurity – the legal-tech arms of Rajah & Tann Asia. With more than 20 years of practice, Rajesh has been universally recognised as the region's leading TMT lawyer who is at the forefront of matters relating to technology procurement, AI, cybersecurity, data protection, analytics and governance, telecommunications, e-commerce, cloud computing, distributed ledger technologies, digital forensics and digital media.



Steve Tan is deputy head of Rajah & Tann Singapore LLP's TMT practice. His practice is in the areas of data protection, IT, IP, cybersecurity, communications, and digital

media/entertainment law. Steve is also the director and co-founder of Rajah & Tann Technologies and Rajah & Tann Cybersecurity and an adjunct professor at the Faculty of Law of the National University of Singapore. Besides being among the first to be conferred Senior Accredited Specialist (DDE) status by the Singapore Academy of Law, Steve was also named Data Privacy & Protection Lawyer of the Year at ALB SE Asia Law Awards 2023.



Benjamin Cheong is deputy head of Rajah & Tann Singapore LLP's TMT practice. He has practised in Singapore, Hong Kong and Shanghai and has been involved in numerous

complex cross-border, multi-jurisdictional deals across Asia. With clients spanning the industries of IT, telecommunications, life sciences and financial services, Benjamin has more than a decade of experience in advising on contentious and non-contentious matters, particularly on technology-related joint ventures, M&A, technology and IP licensing, technology outsourcing, and data protection compliance. He also has keen interest in cybersecurity, blockchain, fintech, insurtech, medtech, digital payments and AI, and sits within the Law Society of Singapore's IT committee.



Lionel Tan of Rajah & Tann Singapore LLP has a keen interest in the field of IT law, with special emphasis on the developing area of litigation practice in this arena.

Leveraging experience from acting in a wide spectrum of high-profile commercial and criminal litigation cases, Lionel regularly handles matters relating to internet defamation, internet fraud, online security breaches, trade secrets and misappropriation of confidential information, telecommunications regulatory issues, and software implementation and website development disputes. Lionel also advises on contentious and non-contentious IP matters, as well as compliance measures surrounding the Personal Data Protection Act (PDPA), and is a member of the National Council of Social Services' work group for the PDPA.

Rajah & Tann Singapore LLP

9 Straits View
#06-07
Marina One West Tower
Singapore 018937

Tel: +65 6535 3600
Email: info@rajahtannasia.com
Web: sg.rajahtannasia.com

RAJAH & TANN ASIA

Introduction

A key feature in the field of Technology, Media and Telecommunications (TMT) is its propensity for change and 2023 has demonstrated that such change can strike fast and furious. Whether it be due to advancements in technology or shifting trends, those in the field have found themselves having to adapt to a rapidly changing landscape.

At a national level, governments are seeking to keep pace with technological developments and manage their impact on business and society. In the Singapore context, much of this effort has been directed at formulating law and policy to facilitate controlled development and innovation, while also addressing the associated risks of new technology. The past year has thus seen a flurry of legal developments in the TMT sphere, with more initiatives set to come.

This article looks back at some of the key legal and regulatory developments in the area of TMT that have shaped 2023. In particular, it recounts the following developments:

- AI – Singapore has rolled out a number of key initiatives, including the AI Verify Foundation, the Generative AI Evaluation Sandbox, the Veritas Toolkit version 2.0 and an AI framework mapping exercise between Singapore and the USA;
- intangible assets – Singapore has taken steps to develop and launch an intangibles-specific disclosure framework;
- crypto-assets – the Singapore courts have issued landmark judgments relating to cryptocurrencies and crypto-assets; and
- trade digitalisation – Singapore has made significant inroads in advancing the framework for greater trade digitalisation.

The authors also look forward to the changes and developments that may be expected to take root in the year ahead, taking a cue from the dominant legal trends and impending legislative implementations. Specifically, the article considers the following plans in the area of AI.

- Generative AI – Singapore regulators are seeking to develop a Model AI Governance Framework for Generative AI.
- AI strategy – the Singapore government has introduced the National AI Strategy 2.0.
- Regulations and guidelines – Singapore regulators are also looking to develop a risk framework for the responsible use of Generative AI for the financial sector, as well as guidelines on personal data in the context of AI systems.
- Cybersecurity – the Cybersecurity Act is set to be amended to keep up to date with new cyberthreats.

Looking Back at 2023

AI

Sparked by the advent of ChatGPT in late 2022, interest in the development and adoption of AI technologies and solutions – particularly in generative AI – has truly been set ablaze. Acknowledging the importance of responsible development and deployment of AI, Singapore can be seen to have put in the yeoman's work to create an infrastructure that facilitates AI research and development, while also establishing a regulatory framework to handle novel risks and ensure security and standards.

What follows is a summary of some of Singapore's notable initiatives in the area of AI in 2023.

AI Verify Foundation

On 7 June 2023, the Infocomm Media Development Authority of Singapore (IMDA) announced

the launch of the AI Verify Foundation, which aims to harness the collective contributions of the global open-source community to develop the AI Verify testing tool for the responsible use of AI. The AI Verify Foundation's goals are as follows:

- foster a community to contribute to the use and development of AI testing frameworks, code base, standards, and best practices;
- create a neutral platform for open collaboration and idea-sharing on testing and governing AI; and
- nurture a network of advocates for AI and drive broad adoption of AI testing through education and outreach.

By way of background, AI Verify was developed by IMDA as a software toolkit that helps organisations validate the performance of their AI systems based on three principles: fairness, explainability, and robustness. It also allows users to record process checks and generate test reports for transparency and accountability.

Generative AI Evaluation Sandbox

On 31 October 2023, IMDA and the AI Verify Foundation announced the first of its kind Generative AI Evaluation Sandbox ("the Sandbox"). The Sandbox will bring together key global players to build capabilities in the testing and evaluation of generative AI and is part of larger efforts to have a common standard approach to assess generative AI.

The Sandbox offers a common language for the evaluation of generative AI through the Evaluation Catalogue, which details common baseline methods and recommendations for Large Language Models (LLMs). It will create a body of knowledge covering how generative AI products should be tested to help build evaluation

capabilities and will go towards developing new benchmarks and tests for evaluating model performance in specific areas that are important for use cases and for countries such as Singapore that have cultural and language specificities.

Veritas Toolkit version 2.0

On 26 June 2023, the Monetary Authority of Singapore (MAS) announced the release of the Veritas Toolkit version 2.0, an open-source toolkit to enable the responsible use of AI in the financial industry. It seeks to help financial institutions (FIs) carry out the assessment methodologies for the Fairness, Ethics, Accountability and Transparency (FEAT) principles.

The Veritas Toolkit version 2.0 builds on the earlier Veritas Toolkit version 1.0, which had been released in February 2022 and focused on the assessment methodology for Fairness. The Veritas Toolkit version 2.0 features an improved Fairness assessment methodology and new assessment methodologies for Ethics, Accountability and Transparency. The Veritas Toolkit is the first responsible AI toolkit developed specifically for the financial industry.

Singapore: US AI framework mapping

To facilitate the cross-border deployment of AI, Singapore and the USA have taken an important step towards technical standards equivalency. The inaugural US-Singapore Dialogue on Critical and Emerging Technologies was launched on 12 October 2023 and aims to upgrade the bilateral partnership between the countries, including information sharing and consultation on AI standards and collaboration on responsible AI research and development.

Notably, a mapping exercise was completed between the US National Institute of Standards and Technology's AI Risk Management Frame-

work and Singapore IMDA's AI Verify. By harmonising AI technical standards, the aligned approach provides businesses with greater certainty in meeting the requirements in both jurisdictions, which leads to lower compliance costs for AI deployment and innovation.

Intangible assets disclosure framework

With increased digitalisation and innovation, value creation in the global economy has shifted drastically towards intangible assets. In response, Singapore has taken the initiative to develop and launch an intangibles-specific disclosure framework. On 4 September 2023, the Accounting and Corporate Regulatory Authority and the Intellectual Property Office of Singapore jointly launched the Intangibles Disclosure Framework ("the Framework"), which aims to help enterprises commercialise their intangibles.

The Framework enables enterprises to disclose and communicate the value of intangibles such as brand value, patents, registered designs, human capital or internally generated intangibles by outlining the key principles that an enterprise should follow when disclosing their intangibles in a report. It details the four pillars for disclosure (strategy, identification, measurement and management), along with the requirements of each pillar, and provides guidance on how enterprises can disclose their intangibles.

In addition, the Framework also enables enterprises to better manage and generate value from their intangibles, attract investments or collaborations. It also aids enterprises in accessing financing.

First scheme of arrangement between crypto company and users

Section 210 of the Companies Act 1967 provides a tool for companies seeking to restructure

their debts in Singapore by way of a scheme of arrangement. Although the scheme of arrangement is now a fairly common restructuring tool, the case of Defi Payments Pte Ltd (HC/OA 378/2023) is the first of its kind between a cryptocurrency company and its users.

The applicant company provided online services relating to cryptocurrencies, including lending, staking and trading. It had approximately 150,000 account holders and managed cryptocurrency assets valued in the region of USD300 million. However, the company encountered financial and liquidity pressures.

The company obtained leave of the Singapore court to convene a meeting of creditors for the purposes of presenting a scheme of arrangement for voting by its creditors. The vote for the scheme received strong creditor approval, far exceeding the statutory threshold. Following the vote, the court granted sanction to the scheme, which has since taken effect.

The scheme of arrangement had unique features, including dual recovery tracks for creditors to select, a choice of cryptocurrency to receive distributions in, nomination of a creditor onto the company's board, and the opportunity to bid for an early exit via a Reverse Dutch Auction mechanism. The case demonstrates the flexibility and adaptability of the scheme of arrangement as a tool for restructuring, especially for unconventional industries such as the crypto space.

Restructuring of cryptocurrency business

In *Re Babel Holding Ltd and other matters* (2023) SGHC 98, the Singapore High Court had to apply Singapore's restructuring and insolvency framework in the context of a cryptocurrency-related business. The applicants were a group of cryptocurrency companies seeking to extend

a moratoria under Section 64 of the Insolvency, Restructuring and Dissolution Act 2018 to facilitate the formulation of a restructuring plan and to seal certain documents relating to the group's creditors.

The court allowed the extension of the moratoria, finding that the applicants had met the applicable statutory and common law requirements. The court also allowed the sealing of the documents, highlighting the need to safeguard the commercially sensitive information at this point in the restructuring process.

The decision demonstrates the application of Singapore's restructuring and insolvency framework to foreign companies and the court's approach to the grant of moratoria and sealing orders in the circumstances of cryptocurrency and other digital businesses.

Court affirms enforceable property rights of crypto-assets

In *ByBit Fintech Ltd v Ho Kai Xin and others* (2023) SGHC 199, the Singapore High Court sought to determine whether crypto-assets are property capable of being held on trust and, if so, what type of property they are.

The crypto-assets in this case were United States Dollar Tether (USDT). The court granted a declaration of a constructive trust over the USDT, holding that the USDT was property capable of being held on trust. In considering the type of property represented by the USDT, the court held that it was a chose in action recognisable by common law as being enforceable in court.

The court's decision is significant because earlier cases on crypto-assets had not determined whether such assets are things in action or a novel type of intangible property. The decision

also provides insight on the remedies available to claimants seeking the return or repayment of crypto-assets. Here, the court granted orders for the return of the traceable sums and tracing orders over the sums which had been converted.

First live Electronic Transferable Record cross-border trade

IMDA announced that it had successfully executed a fully paperless, live cross-border trade from Singapore to Thailand during the first quarter of 2023. This shipment was conducted using an Electronic Transferable Record via Singapore's TradeTrust framework, thereby allowing end users to digitally endorse, exchange and verify documents and effect title transfer.

The trade involved shipping liquid chemicals from Singapore to Thailand, using Bunkerchain as the digital platform provider. The electronic bill of lading was issued, surrendered and verified using different systems, and supported solely by statutory law without any contract law or rulebook.

IMDA has stated that this is the world's first Electronic Transferable Record cross-border trade. With countries increasingly looking to digitalisation of trade to utilise the advantages in efficiency, security and cost savings, Singapore has taken a position as a regional leader in trade digitalisation. Singapore is expected to continue to develop its capabilities in the use of Electronic Transferable Records to facilitate cross-border trade.

Looking Ahead to 2024

Generative AI has drawn intense focus as one of the most significant developments in the TMT industry. However, it is not without its own challenges. Although generative AI brings significant transformative potential, over and above

the opportunities presented by traditional AI, it has also enhanced the inherent risks of AI and raised new threats. To address this, Singapore has launched a number of key initiatives that are under development or consultation and are expected to see further progress in the coming year.

Model AI Governance Framework for Generative AI

On 16 January 2024, the AI Verify Foundation and IMDA announced the Draft Model AI Governance Framework for Generative AI (the “Draft Framework”). This expands on the existing model governance framework that covers traditional AI and was last updated in 2020.

The Draft Framework establishes a systematic and balanced approach to address generative AI concerns while continuing to facilitate innovation. It provides a summary of the principles and recommendations for each of nine identified dimensions, which offer practical guidance for model developers and policymakers. The nine dimensions are as follows:

- accountability;
- data;
- trusted development and deployment;
- incident reporting;
- testing and assurance;
- security;
- content provenance;
- safety and alignment research and development; and
- AI for public good.

The Draft Framework is open for public consultation until 15 March 2024 and welcomes views from the international community. This will support the finalisation of the Model AI Governance Framework in mid-2024.

National AI Strategy 2.0

Governments across the world have been racing to fully explore and adopt AI solutions, with efforts being driven towards issues such as responsible development, regulatory frameworks, and the building of infrastructure. In this regard, Singapore has been at the forefront of the AI movement, issuing its first National AI Strategy in 2019, which outlined plans to deepen the use of AI to transform the economy.

Singapore has now launched its National AI Strategy 2.0 (the “NAIS 2.0”) on 4 December 2023. The NAIS 2.0 introduces key shifts to propel Singapore as a leader in the field of AI and sets out 15 actions that Singapore will undertake across the identified systems and enablers to support Singapore’s AI ambitions during the next three to five years. This includes:

- efforts to intensify AI adoption across industries;
- ensuring a trusted regulatory environment that is pro-innovation and has appropriate guardrails;
- establishing both human and physical infrastructure (such as AI training programmes and data centres);
- updating AI governance frameworks, designing risk-based interventions, and contributing to international discourse on AI; and
- addressing risks in future legislation, such as negligence, breach of contract, product liability, data protection, human rights, and anti-discrimination.

Development of South-East Asia’s first LLM ecosystem

On 4 December 2023, IMDA announced that it would be partnering with AI Singapore and the Agency for Science, Technology and Research to launch the National Multimodal Large Language

Model Programme (NMLP). The NMLP seeks to be South-East Asia's first LLM ecosystem.

This new SGD70 million initiative will develop Singapore's research and engineering capabilities in multimodal LLMs and support the NAIS 2.0. In particular, the NMLP aims to:

- build skilled AI talent in Singapore;
- foster a thriving AI industry to develop LLM-enabled solutions; and
- enable Singapore to build a trusted environment in using AI and develop a base model with regional context.

IMDA has highlighted the importance of developing sovereign capabilities in LLMs. The NMLP thus hinges on the development of multimodal and localised LLMs for Singapore and the region to understand context and values related to the diverse cultures and languages of South-East Asia – for example, managing context-switching between languages in multilingual Singapore.

Generative AI risk framework for financial sector

Generative AI has proven to be both transformative and disruptive to the financial sector. Even though it helps FIs with efficiency and personalised customer experiences, it also introduces unique risks that go beyond those of traditional AI and potentially extend beyond the scope of the current FEAT principles.

To address this, MAS, financial industry participants and technology partners have collaborated on Project MindForge to develop a risk framework for the responsible use of generative AI for the financial sector. On 15 November 2023, MAS announced that Phase One of the project had successfully concluded with the development of a comprehensive generative AI risk framework

and a platform-agnostic generative AI reference architecture. The full White Paper detailing the generative AI risk framework is expected to be shared in 2024.

The White Paper will cover, among other things:

- key decisions about architecture and infrastructure that an FI needs to consider in the adoption of generative AI;
- a platform-agnostic generative AI reference architecture for FIs, as well as a list of the building blocks and components that organisations can use to create robust enterprise-level generative AI technology capabilities; and
- use cases to help the industry better understand generative AI's impact on cybersecurity, sustainability, business, society and other human factors.

The next phase of the project will involve developing strong industry use cases that can benefit from generative and other AI technologies, such as anti-money laundering, sustainability and cybersecurity. The project will also expand its scope to include FIs from the insurance and asset management industries and refine the generative AI risk framework for the entire financial industry.

Data protection in use of AI systems

We may also expect to see the release of Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems ("the Guidelines"). The Personal Data Protection Commission (PDPC) held a public consultation seeking views on the Guidelines from 18 July 2023 to 31 August 2023.

Some of the key issues in the use of AI systems that embed machine learning models relate to

the use of personal data in the training of such AI systems, including how it interacts with an organisation's data protection obligations under the Personal Data Protection Act 2012 (PDPA) and how to avoid the breach of such obligations. The Guidelines thus seek to clarify how the PDPA applies to the collection and use of personal data by organisations to develop and deploy AI systems, as well as to provide baseline guidance and best practices for organisations on how to be transparent about whether and how their AI systems use personal data to make recommendations, predictions or decisions.

The Guidelines are organised according to the stages of AI system implementation, as follows.

- Development, testing and monitoring – using personal data for training and testing the AI system, as well as monitoring the performance of AI systems post-deployment.
- Deployment – collecting and using personal data in deployed AI systems (business to consumer).
- Procurement – AI system or solution provider providing support to organisations implementing the AI system (B2B).

Updating the cybersecurity legislation

On the cybersecurity front, Singapore's legislative framework is expected to undergo certain amendments in order to keep up to date with emerging cyberthreats. The Cybersecurity Agency of Singapore (CSA) has introduced the draft Cybersecurity (Amendment) Bill (the "Draft Bill"), holding a public consultation seeking views on the Draft Bill from 15 December 2023 to 15 January 2024.

The Cybersecurity Act governs the oversight and maintenance of national cybersecurity in Singapore. The Draft Bill seeks to update the Cybersecurity Act to ensure that Singapore's cybersecurity laws remain fit-for-purpose, including the following:

- updating existing laws on the protection of Critical Information Infrastructure (CII);
- extending the Commissioner of Cybersecurity's oversight over nationally important computer systems and entities of special cybersecurity interest; and
- enabling baseline cybersecurity standards for foundational digital infrastructure.

Specifically, the Draft Bill recognises the importance of entities in charge of key digital infrastructure other than CIIs, such as cloud service providers and data centre operators. The amendments seek to safeguard these entities by increasing oversight over their cybersecurity and requiring compliance with minimum standards.

SPAIN



Law and Practice

Contributed by:
Marina Villalonga
Asensi Abogados

Contents

1. Metaverse p.378

1.1 Laws and Regulation p.378

2. Digital Economy p.380

2.1 Key Challenges p.380

3. Cloud and Edge Computing p.384

3.1 Highly Regulated Industries and Data Protection p.384

4. Artificial Intelligence p.386

4.1 Liability, Data Protection, IP and Fundamental Rights p.386

5. Internet of Things p.389

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.389

6. Audio-Visual Media Services p.390

6.1 Requirements and Authorisation Procedures p.390

7. Telecommunications p.393

7.1 Scope of Regulation and Pre-marketing Requirements p.393

8. Challenges with Technology Agreements p.395

8.1 Legal Framework Challenges p.395

9. Trust Services and Digital Entities p.396

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.396

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 two 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 leads the M&A and corporate department as well as the TMT and data protection practice areas at the firm. She graduated in law in 2007 and she has worked in the corporate departments of top-tier firms,

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, No1, 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

1. Metaverse

1.1 Laws and Regulation

The Metaverse and its Regulation

The metaverse was considered the greatest technological revolution of recent years until the sudden and massive take-off of AI over the last 12 months unseated it as the more promising technology. The two are, however, strongly interconnected.

The metaverse refers to a three-dimensional virtual reality, in which individuals can interact through avatars much like they do in reality, through a fully immersive experience. It 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, despite the fact that it has evolved considerably over the last year. 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.

Even though AI is currently the focus of all regulatory efforts, it will make a significant contribution to the metaverse's development, allowing for much more realistic experiences. 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 and 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 addition, as digital identity is key to interaction in the metaverse, the adoption of EU Regulation eIDAS², which amends EU Regulation 910/2014, of 23 July 2014, on electronic identification and trust services for electronic transactions in the internal market (eIDAS), and whose approval by the EU Parliament took place on 29 February 2024, will be essential for the development of the economy in the metaverse.

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 supported with the standard Spanish contractual and consumer protection law.

The *Agencia Española de Protección de Datos* (AEPD), the Spanish data protection authority, has focused several times on the metaverse and the risks it poses to privacy. 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. These include the 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 a privacy point of view since the amount of data processed 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 might be used to personalise 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.

As the metaverse gradually becomes a common place for social interaction, one in which real-world transactions take place, trust mechanisms will become vital. Some of Spain's largest real estate companies are already selling properties in the metaverse, for instance.

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 face other challenges, beyond privacy or cybersecurity. For example, there are 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 addition, the sustainability and environmental impact issues arising from the high energy consumption required for interaction in the metaverse cannot be ignored, as well as the accessibility barriers, the mental health issues that can arise from addiction to technology, and the technological challenges of achieving interoperability between metaverses.

All these concerns have been highlighted by the European Parliament's Committee on Legal Affairs, which in December 2023 adopted a report outlining the challenges posed by virtual worlds.

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. These companies will set the pace for the future development of the metaverse, a technology that still has a long way to go.

2. Digital Economy

2.1 Key Challenges

Brief Introduction to the Concept of Digital Economy

The 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 have been adopted in recent months and the many others that are under legislative discussion, precisely because more and more aspects of our lives are developing in the digital environment and the inevitable and accelerating advance of technology.

Digital Regulation

Before discussing in detail the regulations that expressly regulate the digital economy, it is convenient to briefly review some of the most relevant provisions approved over the last year 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 regard, in September 2023, the first report on the state of the Digital Decade was published. It urged the member states to increase investment to accelerate digital transformation in Europe.

In this context, the declaration on European Digital Rights and Principles for the Digital Decade, adopted on 15 December 2022, must also be noted. 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 of Digital Services and Digital Markets

Having explained the foundational legislation that should govern any regulatory development in the digital field, we must highlight the 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 by 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 operators so that they can adapt to its provisions, which is why much of its articles have not been applicable, 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 to deter 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 search engines and very large

online platforms (VLOP), which reach more than 10% of Europe's 450 million consumers, to which a specific regime will apply. Once they have been designated by the Commission, they have four months to comply with their additional obligations.

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 kinds of service provider:

- digital services co-ordinators, to be appointed by each member state;
- trusted flaggers, to recognise and flag illegal content; and
- compliance officers, to be appointed by the VLOP.

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 other things, 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 does 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.

In April 2023, the Commission designated a first group of VLOPs including, Amazon, Facebook, TikTok and X (formerly Twitter). All this despite the fact that the Commission has recently initiated formal proceedings against X for breaches of the DSA.

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, three kinds of service provider are contemplated.

- 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 – this 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 most of its provisions have been applicable since 2 May 2023. In September 2023, the Commission designated, for the first time, a group of six gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft, who were given a six-month period to adapt to the specific provisions included in the DMA.

Brief Reference to Digital Finance

A discussion of 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 Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA) adopted on 16 May 2023, published on 9 June 2023 and entering into force on 30 June 2023. Its provisions will be applicable from July 2026, unless any member state decides to advance said application. Such is the case of Spain, where MiCA will be applicable by December 2025.

The MiCA Regulation is the first global standard regulating the issuance and trading of crypto-assets on platforms, excluding financial instruments, deposits, NFTs, the issuance of decentralised generated crypto-assets and decentralised finance. 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, which will be supervised by the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA).

Spain has designated the National Securities Market Commission (CNMV) and the Bank of Spain as competent authorities for the implementation of MiCA.

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 (the “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 been superseded by the aforementioned NIS 2 Directive (in fact, it repeals it with effect from 18 October 2024). The 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 there-

fore 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 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 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 role 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 ver-

sion. In any case, in the strategy set out in the Digital Compass 2030, the EU has highlighted the desirability of achieving European digital sovereignty, which is embodied in edge computing, bringing data processing closer to users and reducing dependence on clouds located outside the EU.

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.

When referring to non-personal data, it is mandatory to refer to the publication on 22 December 2023 of the Regulation (EU) 2023/2854 of 13 December 2023, on harmonised rules to fair access to and use of data (the “Data Act”). This Regulation urges providers of cloud and edge services to prevent unlawful access to the systems where non-personal data is stored and facilitate cloud interoperability. In addition, it encourages data sharing between competing providers at the user’s request, as the SWIPO Codes of Conduct to facilitate switching cloud providers and data porting have proved to have only limited effect.

The Data Act entered into force on 12 January 2024 and most of its provisions will be applicable from 12 September 2025.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights Regulations on Artificial Intelligence.

AI constitutes the ability of a machine to exhibit the same (or comparable) thinking capabilities

as humans, allowing learning or problem solving for specific purposes.

AI has seen an undeniably rapid rise in recent years in all areas. This has allowed the application of the technology 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 this technology offers, 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 regulation and about those in development.

Regulation is prolific both at EU level and in Spain, although currently only soft law instruments are in force. 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 would be known as the Artificial Intelligence Act (the “AI Act”). On 8 December 2023, the Council and the European Parliament agreed on such proposal, and it is expected to be fully applicable in 2026, although some aspects will enter into force on an earlier

stage. As pointed out, 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. Examples of such studies are 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 issued 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 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 and constitutes a pioneering standard in the regulation of this technology.

Although the final version of the text has not yet been published, the main features of this regulation are clear from the drafts that have already been distributed. The definition of AI is close to the OECD’s one and the regulation focuses especially on high-risk systems. Thus, worth highlighting are the establishment of the obligation to carry out a fundamental rights impact assessment for high-risk systems and the express prohibition of systems that pose unacceptable risks.

In order to ensure compliance with the provisions contained in the AI Act, the regulation is completed with a strong system of fines and penalties: up to 35 million euros or 7% of global turnover.

With all the above, the European Commission has initiated the so-called IA Pact to encourage key industry players to anticipate the implementation of the requirements of the AI Act by way of “declarations of engagement”, allowing to share their solutions among other participants.

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 (the “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 revision of the Directive of 25 July 1985 on liability for damage caused by defective products, including liability for AI systems.

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, as well as the implementation of the Artificial Intelligence Advisory Council. In addition, the Spanish Agency for the Supervision of AI was created in September 2023, with headquarters located in A Coruña, and became operational with the appointment of its governing board, in December 2023. With the creation of this Agency, Spain becomes the first EU country to set up such a body, anticipating the requirements of the AI Act.

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. It also calls for the promotion of ethical AI that respects fundamental rights.

Finally, on 7 November 2023, the government of Spain with the collaboration of the European Commission implemented the first EU regulatory sandbox on AI. The objective is a joint resolution by the competent authorities and companies

developing AI on the best practices that should serve as a basis for the application of the AI Act.

Legal Aspects of AI

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 must be resolved by resorting either to common national law in civil/commercial or criminal matters, or to sectoral legislation that regulates industrial and intellectual property, data protection or business secrets, among other things.

However, 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 AI seriously endangers 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 GDPR and the LOPDGDD must be complied with.

For example, AI may involve certain risks linked to discrimination for possible data processing based on predictions. Therefore, it is essential to constantly monitor the model for bias and adjust it to neutralise potential discrimination.

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 may arise around 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 must respect the principle of accountability and be developed with data privacy by default and by design built in.

In any case, the data must be processed lawfully, fairly and in a transparent manner, and the data subjects must be duly informed about the processing of their data.

Many privacy situations may arise regarding common forms of data treatments, such 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) has identified in a report on big data security, the different digital and cybersecurity threats for big data projects. This reinforces the transversal importance of cybersecurity in terms of AI, 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 The 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 detailing 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 technology. 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 of the 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, through 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 cybersecu-

rity 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, of the NIS 2 Directive regarding network and information security, which is applicable to IoT devices, and on the other hand, to the proposal for the Cyber Resilience Act (CRA), given that it will include a regulation on cybersecurity requirements for products with digital elements to ensure more secure hardware and software products. The European Parliament and the Commission agreed on 1 December 2023 on the final proposal of the CRA, which is expected to be adopted in early 2024.

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.

From a data protection perspective, and without prejudice to the application of the GDPR, it is mandatory to refer to the Data Act, as it sets rules on the exchange of data generated through the use of connected products, such as those that form part of the IoT, allowing users to access the data they generate, as well as public sector bodies in cases of public interest.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Legislative Overview

The emergence of new forms of audio-visual content consumption led to a review of the regulation of audio-visual 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 (the “Audiovisual Media Services Directive”). This Directive lays down EU-wide media content rules for the provision of audio-visual media services, including traditional television broadcasts, on-demand services and platform video sharing.

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 audio-visual 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 Law 13/2022, of 7 July (the “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 recommended 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 audio-visual communication service providers;
 - (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 audio-visual work is promoted by reserving certain percentages for its broadcasting.
- The production of audio-visual works by women is encouraged, as well as the promotion of co-official languages in Spain.

Influencers

As noted above, the 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;
- aim is to inform, entertain or educate;
- are offered through electronic communication systems; and
- organise their content 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 for which they earn significant income;
- 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.

The requirements for significant income and followers need further development as they were not defined by the General Law on Audiovisual Communication. To this end, a proposal for a royal decree was published on 7 December 2023 which considers that:

- revenues equal to or greater than EUR500,000 are significant; and
- influencers that exceed 2 million followers and have uploaded at least 24 videos in the previous year have a significant number of followers.

This proposal was submitted to public consultation until 20 December 2023, so it now awaits

final approval. Until this happens, the legal provisions affecting influencers cannot be enforced.

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 audio-visual 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 radio 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, the operation of which is regulated by the Spanish Royal Decree 1138/2023 of 19 December, in force since 21 December 2023, 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 (the “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 the following should be highlighted:

- 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 this 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 give prior notice to 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 commencing installation.

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 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 authorisations, individual authorisations, administrative decisions or concessions. 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 correctly advise their clients in this growing sector.

Main Features of Technology Agreements

As indicated, there are no specific provisions in the Spanish legal system for this type of contract. However, they usually contain certain clauses. 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 GDPR, 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 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 annexe.
- 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 gen-

erate trust among users, way beyond the simple insertion of the scanned handwritten signature.

EU

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.

Each of the aforementioned types of signatures is distinguished below depending on whether it allows identification of the signatory with certainty, security regarding the possible manipulation of the content of the contract and 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.
- The advanced electronic signature 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.

Spain

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 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 EUR1.5 million, except if they belong to the public sector. Such insurance may be replaced by a bank guarantee.

- 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.

Spain is the EU country with the highest number of trust service providers.

The Future of 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 (so-called eIDAS2) aims to ensure universal access to secure and reliable electronic identification and authentication, all through a personal digital wallet stored on the mobile phone.

It should be noted that since 2006 Spain has issued more than 60 million electronic IDs that allow the electronic signature of documents and its citizens, therefore, are familiar with electronic identification. However, the adoption of the new European digital identity will be voluntary for citizens, although it will have the same legal effects as the traditional ID card.

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.

The user will have full control over their personal data, deciding when, how and with whom to share it. The e-wallet will allow users to identify themselves online and prove specific personal attributes, such as age, without having to disclose their full identity or other personal data. Users will therefore take control over their own identities.

“Trilogues” between the EU institutions ended on 8 November 2023 with an agreement on the proposal for eIDAS2, which was finally adopted on 29 February 2024 by the EU Parliament, with the e-wallet expected to be ready on 2026.

Trends and Developments

Contributed by:

Marina Villalonga

Asensi Abogados

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 two 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 leads the M&A and corporate department as well as the TMT and data protection practice areas at the firm. She graduated

in law in 2007 and she has worked in the corporate departments of top-tier firms,

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, No1, 1º
07012 Palma de Mallorca
Balearic Islands
Spain

Tel: +34 971 90 92 19
Email: contact@asensi.es
Web: www.asensi.es

ASENSI
ABOGADOS

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 also the case 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.

Also noteworthy in this regard is the inauguration of a supercomputer in Barcelona on 21 December 2023, the MareNostrum 5, considered one of the ten most powerful supercomputers in the world and the greenest supercomputer in Europe, since it runs entirely on sustainable energy and the heat it generates will be used to heat the building in which it is located.

MareNostrum 5 will be used for important tasks such as medical research and its capabilities will be exploited for the development of AI. In fact, it will be available for European AI start-ups to train their models.

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 off, 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 fig-

ures 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.

Finally, the process of institutional digitisation that the country is experiencing is remarkable. On the one hand, in November 2023, the notarial electronic protocol came into force in Spain, which will allow, for instance, the obtaining of electronic copies of notarial documents or the granting of certain mercantile acts without the need for the physical presence of the parties, as is the case with the incorporation of online companies.

In addition, Royal Decree-Law 6/2023, of 19 December 2023 was recently passed to regulate the digitalisation of justice, which involves, among other measures, the telematic relationship of citizens with the administration of justice, the keeping of electronic files and identification by electronic means for the formalisation of procedures that until now required the physical presence of the participants.

This article will consider two topical examples of national regulation of and involvement in specific matters that have great practical application, either at present or in the near future. Discussion will firstly cover the issues arising from the age verification systems on adult content websites and in connection with the digital identity to be regulated on eIDAS2. The second part covers the form in which crypto-asset advertising is regulated in the Spanish territory, awaiting the full application of the corresponding regulation on crypto-assets by the EU.

Age Verification Systems in the Context of Digital Identity

Introduction

In December 2023, the *Agencia Española de Protección de Datos* (AEPD), the Spanish data protection authority, introduced an age verification system for the protection of minors from inappropriate content on the internet. This system is based on ten principles and is accompanied by three proofs of concept that implement age verification in different operating systems.

This is a pioneering initiative in the European Union and is fully compatible with the regulation on digital identity foreseen in the future eIDAS2 Regulation.

The protection of minors on the internet finds its legal source in Spain in Article 84.1 of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights, by virtue of which the holders of parental authority must oversee the responsible use of digital devices by minors for the suitable protection of their dignity and fundamental rights. Likewise, Law 13/2022, of 7 July (the “General Law on Audiovisual Communication”) requires video sharing service providers to establish age verification systems with respect to content that may be harmful to minors.

At the European level, the need for this protection is referred to both in the European Commission’s Communication of 11 May 2022 on the new European strategy for a better internet for children, and in the Digital Services Regulation (DSA).

The AEPD points out that the systems for the protection of minors are intended to guard them from inappropriate content, which is the ultimate objective of the proposed systems. Age verifica-

tion is therefore merely an instrument for articulating such protection. Thus, any protection system must be designed with the best interests of the child and the protection of their intimacy and privacy in mind, carrying out the mandatory impact assessments for the protection of data of the interested parties.

Characteristics of the age verification systems proposed by the AEPD

The implementation of age verification systems for access to adult content should be subject to the general principles set out in data protection regulations. Thus, such systems must be suitable, necessary, and proportionate, and may not process special categories of data.

With regard to the latter, it should be borne in mind that Article 28 of the DSA expressly states that age verification and the protection of the interests of minors does not constitute a legal basis for the further processing of the child’s data.

Taking all of the above into consideration, the AEPD has established a set of ten principles that must govern any system for the protection of minors using the internet, which can be summarised as follows.

- Systems should not allow the identification of minors among internet users, therefore, any system based on the fact that the minor must disclose their underage status should be avoided. This is in order to prevent minors from being located. Therefore, it should not be possible to directly infer that the user is a minor merely because they have not been able to verify they are an adult. The risks are clearly minimised when verification by intermediary third parties is avoided, but the

identity information is processed from the user's own device.

- The age verification must prove the status of "person authorised to access" and in no case should it seek accreditation of the condition of "minor".
- The processing of access accreditation by internet service providers and third-party entities must be anonymous and independent of other processing. Authorisation should be done using attributes that prevent linking to the user.
- Age verification should only be carried out when the content is unsuitable for minors since, in general, browsing must be free and anonymous.
- Age verification should give a certain value, not an estimate, as the estimate is subject to errors, biases, and discrimination. However, content providers should under no circumstances address specific age.
- Websites will need to be tagged to determine whether they host adult-only content, but tagging may not involve user profiling. Running age verification locally from the user's device would eliminate the risk of profiling or monitoring.
- The system should not allow the linking of the activity of the same user between different services, as this could lead to the identification of the user.
- The exercise of parental authority by the parents must be guaranteed. Systems must set up their governing policies by taking families into account.
- Any verification system must guarantee respect for fundamental rights in internet access; therefore, access to content cannot be limited expansively and indiscriminately. A balance must be struck between the reliability of the age verification solution and usability

(requesting evidence that constantly hinders navigation should be avoided).

- All child protection systems should define a governance framework that ensures compliance with the above principles and that should be auditable by public authorities or independent companies.

Proofs of concept

Following the above criteria, the AEPD has developed three proofs of concept in different environments, creating three alternatives for the implementation of age verification systems that are fully compliant with data protection regulations.

The systems can be deployed on a computer, video game console or smartphone. All of them are based on the installation of certain local applications that allow the age attribute to be verified from identity e-wallets, upholding the anonymity of the user since the information is not shared with the content provider.

These proofs of concept have been developed as a starting point so that different operators have models with which they can develop solutions that meet the criteria and characteristics set out above. These are examples of how an age verification system should be articulated that respects the applicable principles of data protection and at the same time respects the fundamental rights and best interests of the child. The National Commission on Markets and Competition (CNMC) will assess the suitability of the systems that are proposed, following a report from the AEPD.

A public consultation has recently been launched for stakeholders to find out about the current state of age verification systems and to develop tailored solutions.

In any case, it should be borne in mind that technology is not without risks and that any system that is developed must undergo the necessary monitoring and updates to resolve vulnerabilities and minimise the risks of cyber-attacks. Such systems should therefore be subject to the supervisory processes laid down under the NIS2 Directive.

Conclusions

The age verification system proposed by the AEPD is a milestone and its application has already been proposed at European level since most of the systems currently used, such as self-declaration, sharing credentials with the content provider or the existence of intermediary entities, have proven to be ineffective (or not fully compliant with current legislation). It also represents a step forward in terms of the future implementation of the European digital wallet as it has been configured in strict compliance with the provisions included in the eIDAS2 regulation and in line with its principles: only the relevant attribute will be shared, in this case, the legal age.

All of this will facilitate regulatory compliance by adult content providers, protecting minors while ensuring the anonymity of users who, once their status as a “person authorised to access” is verified, will be able to access the content without having to reveal their identity.

It should be stressed that age verification systems must in any case be aimed at adults who intend to access content that is inappropriate for minors, so that it will always be them, and not minors, who are the recipients of such systems and who, where appropriate, install the relevant applications on their devices for the purpose of proving their legal age.

The *Fábrica Nacional de Moneda y Timbre* (National Mint and Stamp Office), the Spanish public entity dedicated to the production of banknotes, identity documents and electronic certification, is already working on the development of an application for identity verification based on the AEPD’s criteria and proofs of concept.

The Advertising of Crypto-Assets

The growing presence of crypto-assets in the financial market is an incontestable reality and, although it presents opportunities, the hitherto scarcity in terms of regulation has posed a risk for investors who decided to opt for these assets because they were 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.

The phenomenon of social networks and influencers affecting promoting cryptocurrencies cannot be ignored in this context. Users can be 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 has finalised, within the framework of its Digital Finance Package, the Regulation on markets in crypto-assets (known as the MiCA Regulation), which resulted from its aim to develop and promote new technologies in the financial sector, particularly blockchain and distributed ledger technology (DLT). Thus, the MiCA Regu-

lation 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 MiCA Regulation to become applicable, 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. It is worth noting that said Circular letter was issued even before the MiCA Regulation was adopted, displaying the clear intention of the Spanish authorities to maintain a leading position in the regulation of new technological trends.

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 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.

In addition, for the Circular to apply, 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 websites 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 that are 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.

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 cryptocurrencies 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.

Since the publication of the Circular, there has been widespread compliance with its provisions. However, on 31 October 2023, the first sanctioning procedure against a company for violating the regulation was initiated. This shows that the CNMV has not ceased its work of constant vigilance.

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 new Spanish Securities Markets and Investment Services Act, adopted on 17 March 2023 and implemented by the Royal Decree 815/2023, of 8 November.

It should be noted that this new regulation 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 MiCA Regulation. In this sense, the CNMV is designated as the competent authority for the supervision of compliance with the MiCA Regulation

SWEDEN

Trends and Developments

Contributed by:

John Neway Herrman, Erik Ålander, Linus Larsén and Agne Lindberg
Delphi



Delphi is a progressive law firm with respected specialists in most areas within business law. It has a total workforce of 200 employees, of which more than 150 are lawyers. With offices in Stockholm, Gothenburg, Malmö and Linköping, its tech practice is one of the strongest in Sweden. For more than 20 years, the Delphi TMT group has been at the forefront of TMT practice in Sweden. The team comprises 11 partners and 35 associates, and offers in-depth knowl-

edge and as a significant part of the overall Delphi business. At the core, its sourcing, IT contract and privacy practices are apparent – but in recent years, fintech, e-commerce, information security and cloud services in a wider sense have become important areas for its combined offering. The firm also regularly advises its clients when utilising new technologies; blockchain, AI, IoT, proptech, e-health and other cutting-edge areas.

Authors



John Neway Herrman is a senior associate with a special focus within the areas of commercial contract law, tech and outsourcing and co-heads Delphi's fintech practice. In his areas of expertise, he advises clients in regard to outsourcing deals and other tech- and IT-related contracts. John regularly represents banks, insurance companies, payment service providers and other regulated entities in regard to various regulatory frameworks such as DORA, PSD2 and guidelines from EBA and EIOPA.



Erik Ålander is a senior associate in Delphi's corporate commercial team and has a special focus on commercial contracts in general and IT in particular. In his area of expertise, Erik advises clients on sales and purchases of goods and services, IT contracts, legal questions related to cryptocurrencies, issues related to compliance with regulatory frameworks such as the GDPR and the PSD2, as well as strategic partnerships and competition law. Erik also provides strategic advice to help clients commercialise their intellectual property. Furthermore, he facilitates seminars on topics related to his areas of expertise, including blockchain technology and cryptocurrencies.

SWEDEN TRENDS AND DEVELOPMENTS

Contributed by: John Neway Herrman, Erik Ålander, Linus Larsén and Agne Lindberg, **Delphi**



Linus Larsén is a senior associate in Delphi's tech and IP group, and works primarily with giving advice to clients on topics related to data protection, IT agreements, intellectual property

rights and issues related to new, cutting edge-technology such as AI and blockchain/crypto-assets. He is a frequent lecturer and writer on topics related to his practice area, especially legal issues concerning cutting-edge technology. Linus is co-responsible for Delphi's technology blog, Delphi Tech Blog, which addresses many issues around law and technology.



Agne Lindberg is a partner and the head of Delphi's tech and IP practice in Stockholm. Agne has extensive experience of IT law and regulatory matters in relation to tech industry,

including banking and finance as well as healthcare. He advises clients within cybersecurity, IT contracting, data privacy and disputes. Agne is a frequent lecturer on topics related to tech law. He is ranked as a leading lawyer within the tech area. He is a member of the Swedish Bar Association, IBA, Itech Law and a board member of TechLaw.

Delphi

Mäster Samuelsgatan 17
111 44 Stockholm
Sweden

Tel: +46 8 677 5400
Email: agne.lindberg@delphi.se
Web: www.delphi.se

Delphi

Tech Law in Sweden: An Introduction

Sweden's technological landscape is undergoing rapid transformation, marked by growth, a significant increase of regulatory requirements, and the increasing importance of digital innovation – not least by different AI applications. The following article delves into various commercial and legal aspects of this development, including matters related to the gaming industry, advancements in AI, considerations in cybersecurity and protective security, and the field of fintech.

Considerations for Gaming Companies Operating in Sweden

The last few years have seen Swedish game developers experience growth in terms of number of companies, revenue, employees, and gender diversity, despite challenges, primarily the persistent skills shortage. According to the report *Swedish Games Industry 2023* from the trade organisation *The Swedish Games Industry (Dataspelsbranschen)*, the industry's revenue reached EUR3.1 billion (a 13% increase for Swedish-registered companies) in 2022. Including subsidiaries, the total industry revenue was EUR8.1 billion; a 40% rise. The sector employed over 8,000 people in Sweden and roughly 16,000 abroad, with a global increase fuelled by several acquisition-driven leading Swedish gaming companies.

Gaming companies operating in Sweden must navigate various legal considerations. These include adherence to consumer protection laws, ensuring clear information, warranties, and product quality for digital content. Compliance with the GDPR, imposing strict rules on collecting and processing personal data, is crucial. Furthermore, companies must respect copyright and intellectual property laws.

Additionally, gaming companies looking to raise capital in the EU must adhere to the new EU Foreign Subsidies Regulation (FSR). The FSR, which entered into force on 12 January 2023, and has applied since 12 July 2023, aims to ensure fair competition between European and non-European companies by monitoring significant transactions and public procurement procedures to address distortions in competition arising from subsidies granted by non-EU countries to companies in the EU single market.

The regulation introduces procedures in which the Commission can investigate concentrations where the acquired company, one of the merging parties or the joint venture generates an EU turnover of at least EUR500 million and the parties were granted foreign financial contributions of more than EUR50 million in the last three years. A similar procedure can be used to investigate public procurement bids where the estimated contract value is at least EUR250 million and the bid involves a foreign financial contribution of at least EUR4 million per third country in the last three years. Additionally, the Commission can initiate an ex officio procedure to investigate all other market situations. If the Commission finds that such financial contributions constitute distortive subsidies, it can impose measures to redress their distortive effects.

Gaming companies should also be mindful of competition laws to avoid anti-competitive practices and ensure compliance. The Digital Single Market (DSM) initiative seeks to harmonise digital regulations across EU member states, impacting digital content distribution, copyrights, and cross-border access to online services.

Health Data Usage in Sweden

The sharing of health data offers great potential within precision medicine. While the EU is nego-

tiating to regulate health data through the European Health Data Space proposal, Sweden is already one step ahead. A recent public inquiry addresses current problems in the Swedish health data infrastructure. It suggests amending Swedish legislation, particularly the Patient Data Act, to cover the secondary use of health data for health care and research purposes. While the Swedish report focuses on national legislation, it also anticipates adjustments in response to the forthcoming EU regulations. Furthermore, the report also touches upon the implications for the private sector, noting the competitive disadvantage that the current proposals might create for private healthcare and pharmaceutical companies. Currently, the proposals only apply to the public healthcare sector.

Artificial Intelligence in Sweden

On 9 December 2023, the Commission, Council of Ministers and Parliament reached an agreement on the EU AI Act. The new proposal includes transparency requirements for basic models, limitations on biometric identification systems, clarification of specific requirements for high-risk models, and enhanced rights for the individual. Once the regulation has been formally adopted, it is time for member states to take the necessary and appropriate implementation measures to ensure coherence in national legislation and compliance with the AI Act. The AI Regulation is characterised by a risk-based approach, dividing the usage of AI into levels of risk. Unacceptable uses of AI are prohibited, and high-risk uses of AI are subjected to certain obligations.

The AI industry in Sweden is experiencing significant growth and development. The Swedish government has recently established an AI Commission, focusing on leveraging AI to bolster Swedish welfare and competitiveness. The

initiative indicates a firm commitment from the Swedish government to integrate AI into various sectors.

AI Sweden, the Swedish National Centre for Applied AI, also plays an integral part in this development. The centre is supported by the Swedish government and collaborates with partners within the public as well as private sector across the country. Its mission is to increase and accelerate the use of AI to benefit Swedish competitiveness. Recently, AI Sweden and its partners have launched ground-breaking AI initiatives crucial for Sweden's competitive edge and ability to deliver high-quality societal services.

One of the significant initiatives of AI Sweden is the release of GPT-SW3, the first large Nordic language model, as an open model for businesses and organisations to use in their products and services, providing significant opportunities for technological advancement in the region.

The Data Factory at AI Sweden is another initiative aimed at driving innovation and implementing AI. It serves as an infrastructure and a knowledge environment, enabling partners from various sectors to utilise state-of-the-art infrastructure and benefit from collaborations and interactions with AI Sweden's technical, strategic, and legal experts.

One of the key aspects of the Data Factory is its ability to help organisations accelerate innovation, which is achieved through strategy development, projects, talent development, and research. The Data Factory offers open access to all partners, allowing them to use conference rooms, participate in events, test hardware, and engage in various expert groups.

Moreover, the Data Factory at AI Sweden simplifies turning ideas into fully running experiments through a streamlined process involving initial discussions, knowledge sharing, and recommendations on equipment and datasets. The Data Factory team helps partners formulate and advance their AI concepts quickly while also addressing legal considerations for innovation, particularly in relation to GDPR compliance, and offering “pre-approved” datasets to simplify the process.

These developments are part of a broader trend where AI is increasingly becoming an integral part of various industries and sectors in Sweden, reflecting the commitment to innovation and technology-driven growth.

Cybersecurity and Protective Security in Sweden

Cybersecurity has emerged as a pressing concern in Sweden, driven by a series of notable cyber-attacks and IT incidents. An illustrative case occurred in late 2022 when a suspected cyber-attack forced the Swedish federation of unemployment insurance funds (*Sveriges A-kassor*) to shut down a crucial IT system, causing delays in unemployment benefits payments. While disruptions to critical systems are severe cybersecurity risks, they represent just one aspect. Other significant threats include data loss, exposure of confidential information, hefty administrative fines, and potential damage to public goodwill.

In Sweden, cybersecurity regulation is still evolving, with a primary influence coming from EU directives like the NIS1 and NIS2 directives, the Cybersecurity Act, and the GDPR. Notably, these regulations not only have a direct impact but also exert an indirect effect through contractual agreements. Supply chain control will

be introduced as a core element of regulatory requirements on cybersecurity. Regulatory initiatives often necessitate negotiations between organisations and their suppliers to ensure compliance. Below, we summarise some of the most important areas of cybersecurity requirements.

Protection of national security interests

A closely related issue to cybersecurity is protective security. In Sweden, protective security pertains to preventive measures safeguarding security-sensitive activities of public agencies and companies against espionage, sabotage, and various crimes that may jeopardise their operations. Security-sensitive activities are activities that are of importance to Sweden's security or are covered by an international protective security commitment that is binding for Sweden. Additionally, protective security also refers to the protection of security-sensitive information.

However, the scope of the Swedish Protective Security Act (2018:585) (*Säkerhetsskyddslagen*) is somewhat vague. The assessment of whether an organisation falls under its scope is based on whether an activity is of importance to Sweden's external or internal security. As such, this likely includes sectors such as defence, energy, water, banking, healthcare, digital infrastructure, AI, and automotive industries. The obligation falls on each organisation to determine if it conducts security-sensitive activities, requiring a case-by-case assessment.

The Protective Security Act mandates that all public authorities or companies engaged in security-sensitive activities ensure sufficient protection. The Act outlines essential provisions, including the obligation to enter into protective security agreements, security screening of personnel, and screening of contracts. Additionally,

it imposes restrictions on which suppliers and subcontractors may be used.

Nasdaq's requirements for governance and information security in the stock exchange

Another notable development related to cybersecurity is Nasdaq Stockholm's (a major Swedish stock exchange) establishment of stringent governance and information security requirements for listed companies. These requirements include identifying material risks in IT systems, implementing internal governance control, including developing IT policies and information security guidelines, including cybersecurity measures, as well as monitoring thereof.

Confidentiality obligations for IT outsourcing suppliers

The Act on Secrecy in Public Sector Outsourcing of Technical Processing or Storage of Data (2020:914) (*Lag om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter*), effective from January 2021, facilitates IT outsourcing for public authorities, imposing a duty of confidentiality on personnel involved in technical processing or storage of data. The obligation of professional secrecy extends to employees of private IT suppliers and subcontractors, mirroring the standards applicable to public employees.

Swedish implementation of the NIS2 directive

The NIS2 directive, effective in early 2023, introduces enhanced security requirements for essential and important services. This directive brings significant changes, with a broader scope and more detailed security requirements than its predecessor, the NIS1 directive. Many operators in critical sectors may need substantial resources to comply, particularly when renegotiating agreements to align with new regulatory requirements. NIS supervision in the digital infrastruc-

ture sector falls under the Swedish Post and Telecom Authority (*Post och telestyrelsen*).

The field of cybersecurity in Sweden faces challenges due to the vulnerability of digital solutions. While cybersecurity is commonly perceived as an IT matter to be handled individually by each organisation, there have been recent legislative initiatives, primarily driven by the EU, aiming to protect operators in key sectors. The landscape is dynamic, with ongoing negotiations and legal uncertainties impacting the implementation of cybersecurity measures. Future EU initiatives, such as the Cyber Resilience Act, are expected to play a crucial role in shaping the cybersecurity landscape further.

In Sweden, organisations generally show a strong commitment to cybersecurity laws, striving to meet high standards. However, there is a need for more attention to how regulatory demands impact contracts, particularly in terms of passing on requirements to suppliers. This aspect often involves substantial negotiation on the allocation of risks. Due to the level of complexity involved, as well as the ever-increasing obligations coming from the EU, it is more important than ever that cybersecurity is taken seriously and put on the agenda across all levels of company management and governance teams. It is a topic that can no longer be seen as an IT department issue.

Fintech: Staying Ahead of Regulations

Sweden has a robust fintech ecosystem, with a considerable number of startups and innovative ventures. According to fintech Baltic, the country was home to 332 fintech companies as of 2022, accounting for 27.5% of all fintech startups across the Nordics and Baltics. However, the fintech sector faces challenges due to an increasingly complex regulatory environ-

ment. Higher interest rates make it difficult for start-ups to access venture capital funding, and the funding is linked to profitability rather than just growth. Despite regulatory challenges and economic recession, most companies in the industry believe their business will see increased growth in 2024, and many plan to expand their workforce. Below, we summarise some of the most important areas related to fintech.

DORA

The Digital Operational Resilience Act (DORA) is set to bring significant changes to the financial sector. The Act, which entered into force on 16 January 2023, and will apply from 17 January 2025, aims to strengthen the IT security of financial entities such as banks, insurance companies, and investment firms. It focuses on ensuring that the financial sector in Europe can remain resilient in the event of severe operational disruptions.

In Sweden, major changes in the powers of the Swedish as well as European supervisory authorities are expected. DORA mandates closer monitoring and regulation of financial entities by supervisory authorities. This includes regular checks to ensure compliance with DORA's requirements, such as ICT risk management, third-party risk management, incident reporting, and digital operational resilience testing. Companies will need to maintain transparent and open communication with these authorities, regularly updating them on their compliance status and any significant ICT-related developments.

Blockchain

Sweden's commitment to technical innovation is evident in its stable investments in research and development, with blockchain technology emerging as a key area of interest. Both private and public sectors are exploring blockchain's

potential, recognising its ability to add trust and security to information through traceability. Despite global market fluctuations, Sweden continues to invest in blockchain, with new startups and projects illustrating the technology's diverse applications, from finance to healthcare. At the same time, regulatory challenges like GDPR compliance remain vital considerations.

The Swedish mapping, cadastral and land registration authority (*Lantmäteriet*) experiment with blockchain for land registry transfer is a notable example of public-private collaboration in the blockchain sector, as is the Swedish Companies Registrations Office's (*Bolagsverket*) Proof of Business blockchain project which aims to offer real-time, accurate company information.

Regulatory oversight, particularly by the Swedish Financial Supervisory Authority (SFSA), is focused on AML compliance in the crypto space. Together with the EU's Markets in Crypto-Assets (the "MiCA") Regulation, which entered into force in June 2023, it indicates a growing need for clear regulations in the blockchain industry. When the provisions of the MiCA Regulation begin applying in the summer of 2024, more Swedish companies will fall under the supervision of the SFSA. However, the regulation is welcomed by many companies, as the blockchain industry benefits from more robust consumer protection and serious companies.

Another exciting development is the e-krona project, a significant initiative by the Swedish Central Bank (*Riksbanken*) which explores a blockchain-based digital currency. Its pilot phases have tested the feasibility and integration of e-krona in banking systems and the potential for offline transactions. Legal considerations, particularly concerning financial secrecy and data protection laws, are critical in this venture. Swe-

den's participation in the European Blockchain Partnership (EBP) and projects like Icebreaker, focusing on Central Bank Digital Currencies (CBDCs) for cross-currency payments, further emphasise Sweden's commitment to exploring blockchain's potential in various domains.

Open finance – PSD3, FIDA and PSR

The PSD2, enacted in 2015, aims to level the playing field in EU payments, fostering competition and innovation by opening the market to new providers accessing financial data. It mandates banks to provide payment account data access via APIs to third-party providers. While PSD2 has advanced open banking in payments, it does not extend to the broader financial sector. In response, the Commission has proposed the third Payment Services Directive (PSD3), the Payment Services Regulation (PSR), and Financial Data Access (FIDA), transitioning from open banking to open finance, addressing the limitations identified in the PSD2.

On 28 June 2023, the SFSA released a report on open financial services in Sweden. The SFSA, on behalf of the Swedish government, surveyed Swedish fintech companies to analyse risks and opportunities associated with these services. The SFSA's report concludes that Swedish fintech companies have been early adopters of open financial services compared to the rest of Europe, especially regarding payments. This is credited to the highly digitised nature of Sweden's financial industry, the innovation within its fintech companies, and the widespread use of mobile e-IDs at an early stage. However, payment initiation services face stiff competition, indicating the need for the FIDA regulation to expand fintech services beyond payments.

The suggested framework for financial data access marks a positive step for innovation

in the financial sector, opening avenues for already-established financial entities and emerging fintech firms. While FIDA is navigating the EU legislative process, potentially lengthened by the impending EU election, financial institutions must capitalise on this stretch and make proactive preparations to facilitate a seamless implementation when FIDA is eventually enacted.

Concluding Remarks

Sweden stands at the forefront of digital innovation, as evidenced by its tech and financial sectors. The spirit of technological optimism is not just confined to the private sector; politicians are enthusiastically on board as well, cultivating a dynamic collaboration between the public and private sectors, jointly guiding the country towards excelling in innovation.

While the strive for continuous innovation and growth keeps pushing private as well as public actors within the digital space, comprehensive regulatory changes are around the corner. As discussed in this article, the regulatory changes aim to secure a competitive and stable digital market within the EU while at the same time ensuring the protection of fundamental rights, ensuring implementation of well-structured and clear security processes and protecting matters of national security.

In order to ensure compliance with the ever-changing regulatory framework, significant efforts and investments will be required by organisations operating within digital markets. Delphi's view is that, while burdensome, especially for smaller companies, the focus on these matters will continue to strengthen the individual actors, as well as Sweden's position as a hub for digital innovation.

SWITZERLAND



Law and Practice

Contributed by:

Lukas Morscher and Nadja Guberan-Flühler
Lenz & Staehelin

Contents

1. Metaverse p.417

1.1 Laws and Regulation p.417

2. Digital Economy p.419

2.1 Key Challenges p.419

3. Cloud and Edge Computing p.419

3.1 Highly Regulated Industries and Data Protection p.419

4. Artificial Intelligence p.423

4.1 Liability, Data Protection, IP and Fundamental Rights p.423

5. Internet of Things p.424

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.424

6. Audio-Visual Media Services p.425

6.1 Requirements and Authorisation Procedures p.425

7. Telecommunications p.427

7.1 Scope of Regulation and Pre-marketing Requirements p.427

8. Challenges with Technology Agreements p.428

8.1 Legal Framework Challenges p.428

9. Trust Services and Digital Entities p.431

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.431

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



1. Metaverse

1.1 Laws and Regulation

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 blockchain, stable coins and, most recently, also on staking services.

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 inter-

national 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, papertrail) 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 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 regulations. The Swiss legislature strives to keep laws technology-neutral, thus general rules (including as regards data protection) apply to the digital economy (see also **1.1 Laws and Regulation** regarding the metaverse; **4. Artificial Intelligence** 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 Post and Telecommunications of 18 March 2016, as amended (SPTA), 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).

On 1 January 2024, the Federal Act on Information Security (ISA) and its implementing ordinances entered into force. While the ISA primarily focuses on government cyber security, a revision adopted on 29 September 2023 requires critical infrastructure operators, including private parties, to report cyber-attacks to the National Cyber Security Centre within 24 hours. This obligation applies, inter alia, to Swiss-based providers of cloud computing services, search engines, digital security and trust services, data centres, as well as manufacturers of certain hardware or software used in critical infrastructures. It is expected that such obligation will take effect as of 1 January 2025.

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. On 1 September 2023, the revised Federal Data Protection Act of 25 September 2020 (DPA) and the revised Ordinance to the Federal Data Protection Act of 31 August 2022 (DPO) entered into force, which govern the processing of what in Switzerland is referred to as “personal data” by

private parties or federal bodies. The revision responds to technological advancements and aligns Swiss data protection law with today’s international data protection standards (see below). 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 Federal Code of Obligations sets forth restrictions on the processing of employee data, and Ordinance 3 to the Federal Employment Act (Employment Act) limits the use of surveillance and control systems by the employer.

The Federal Act on Telecommunications of 30 April 1997, as amended (TCA), regulates the use of cookies.

The 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 Federal Act on Combating Money Laundering and Terrorist Financing in the Financial Sector stipulate specific duties to disclose information.

The Federal Act regarding Research on Humans, the Federal Act on Human Genetic Testing and the 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 (natural) person. 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” is to be considered as a special category of personal data that is 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 affiliation to a race or ethnicity;
- genetic data;
- biometric data that uniquely identifies a natural person;
- administrative and criminal proceedings or sanctions; or
- social security measures.

Furthermore, the DPA provides for stricter processing rules for certain processing activities, including “high-risk profiling” and “automated individual decision-making”. High-risk profiling refers to any form of automated processing of personal data to use such data to evaluate certain personal aspects relating to a natural person that involves a high risk to the personality or fundamental rights of that natural person, by pairing data that enables an assessment of essential aspects of the personality of such natural person. Automated individual decision-making is any decision based exclusively on automated

processing of personal data that has a legal consequence for, or a considerable adverse effect on, the data subject.

As a general principle, personal data 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 data 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 data 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 Federal Council has published a list of jurisdictions that provide adequate data protection in appendix 1 to the DPO. The countries of the EEA and Andorra, Argentina, Canada, the Faroe Islands, Gibraltar, Guernsey, the Isle of Man, Israel, Jersey, Monaco, New Zealand, United Kingdom and Uruguay are generally considered to provide an adequate level of data protection as regards personal data, 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 EU-US Data Privacy Framework, which has been recently negotiated between the EU and the USA and for which the European Commission adopted its adequacy decision on 10 July 2023. Switzerland and the USA are currently in negotiations regarding a Swiss-US 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 data 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 manage-

ment, 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 recognises the new set of standard contractual clauses, issued by the European Commission on 4 June 2021 pursuant to the Implementing Decision 2021/914/EU (EU SCC), 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 these EU SCC (the old EU standard contractual clauses, the Swiss Transborder Data Flow Agreement and the Council of Europe model contract to ensure equivalent protection in the context of cross-border data flows may no longer be used for such transfers).

EU SCC (provided that the necessary adaptations and amendments are made for use under Swiss data protection law) are considered pre-approved by the FDPIC. For other data transfer agreements (eg, data protection clauses in agreements between the controller and processor not based on EU SCC or binding corporate rules), the FDPIC has to be notified of the use of such agreements accordingly.

Data Protection Officers

The appointment of a data protection officer is not mandatory for private controllers. However, by designating a data protection officer, this data protection officer may be consulted instead of the FDPIC in case of a high-risk processing

activity. Aforementioned release to consult with the FDPIC only applies if the data protection officer exercises its functions towards the controller in a professionally independent manner and is not bound by any instructions, does not carry out any activities that are incompatible with its tasks and has the required expertise, and the controller publishes the data protection officer's contact details and notifies the FDPIC thereof.

A reporting portal for contact details of data protection officers is publicly accessible on the FDPIC's website. In contrast to private parties, federal bodies are required to designate a data protection officer.

The data protection officer serves as contact point for data subjects and for the authorities responsible for data protection in Switzerland. Further tasks include, in particular, training and advising the controller in matters of data protection and providing support on applying the data protection regulations.

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 Protection 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.

On 1 September 2023, the revised DPA entered into force. The revision aligned 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).

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

Artificial intelligence (AI) offers 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 AI. As regards the processing of personal data, the right to privacy and the protection of personal data must be safeguarded (see 3. **Cloud and Edge Computing** regarding data protection principles). While government authorities periodically review developments as regards AI, it is currently 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 AI 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. On 1 December 2023, the Competence Network for Artificial Intelligence (CNAI) published a fact sheet focusing specifically on the use of generative AI tools in the Federal Administration.

However, in light of recent technological developments, opportunities and challenges associated with AI, the Federal Council has instructed the Federal Department of the Environment, Transport, Energy and Communications (DETEC) to prepare an overview of possible regulatory approaches to AI by the end of 2024. The overview will focus on compliance with fundamental rights, regulatory approaches compatible with the EU's AI Act and the Council of Europe's AI Convention and shall consider technical standards as well as financial and institutional implications. The overview shall provide a basis for a concrete mandate for an AI regulatory proposal in 2025.

In relation to data protection concerns regarding AI, the FDPIC issued non-binding guidance for AI applications on 4 April 2023, emphasising that providers of AI applications must inform users in a transparent and comprehensible manner of the purpose and means of the processing of personal data. Further, on 24 August 2023, the FDPIC published a joint statement with nine other national data protection authorities urging social media platforms and website operators to take measures to protect personal data against data scraping, including for AI model training. Finally, on 9 November 2023, the FDPIC published a statement pointing out that the DPA is directly applicable to AI-supported processing of personal data (see 3. **Cloud and Edge Computing**).

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 legislature – 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 impor-

tance 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 3. **Cloud and Edge Computing** 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, NCSC 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;
- keeping devices up to date and installing updates;
- using protocols allowing only encrypted connection;
- securing access via the internet by means of a VPN connection or restricting access by using an IP address or GeoIP filter; 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 be incurred 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.

Quota and Investment Obligation in Swiss Film Production

On 15 May 2022, the introduction of a quota and an investment obligation in Swiss film production for streaming services was approved by the Swiss people. The amendment of the Film Act of 14 December 2001, as amended (FiA), entails adjustments to the existing Film Ordinance of

3 July 2002, as amended (FiO), and requires a new ordinance with implementing provisions for the implementation of the European quota and the obligation to invest in Swiss filmmaking (*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.

These amendments entered into force on 1 January 2024. In October 2023, the Federal Office of Culture issued practical guidance on the quota and investment obligation on its website.

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 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 a head 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; and
 - (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 outsourcing 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 Financial Institutions 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 carefully 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 (E ID Act) 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 conducted a consultation in 2022 on a new draft of the E ID Act. On 22 November 2023, the Federal Council

adopted the draft bill and dispatch for attention of the Parliament. The E ID 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. The Federal Council plans to offer the eID as of 2026. In order to keep to this schedule, the preparatory work for building the required infrastructure has already begun.

USA



Law and Practice

Contributed by:

Mike Ryan, Aaron Burstein, Patricia Werner and Mike Dover
Kelley Drye & Warren LLP

Contents

1. Metaverse p.436

1.1 Laws and Regulation p.436

2. Digital Economy p.438

2.1 Key Challenges p.438

3. Cloud and Edge Computing p.439

3.1 Highly Regulated Industries and Data Protection p.439

4. Artificial Intelligence p.444

4.1 Liability, Data Protection, IP and Fundamental Rights p.444

5. Internet of Things p.446

5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.446

6. Audio-Visual Media Services p.447

6.1 Requirements and Authorisation Procedures p.447

7. Telecommunications p.449

7.1 Scope of Regulation and Pre-marketing Requirements p.449

8. Challenges with Technology Agreements p.450

8.1 Legal Framework Challenges p.450

9. Trust Services and Digital Entities p.451

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.451

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.

Contributed by: Mike Ryan, Aaron Burstein, Patricia Werner and Mike Dover, **Kelley Drye & Warren LLP**



Patricia Werner is a partner 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.



Mike Dover is a special counsel at Kelley Drye & Warren LLP and focuses on advising communications and technology providers, including with respect to cable and franchise

regulations, cable transaction regulatory management, broadband deployment, and broadband communications infrastructure. Michael has taken a lead role in managing regulatory approvals for a multi-billion cable and broadband provider acquisition and multiple stock and asset entity acquisitions involving regulated entities, as well as providing advice on broadband deployment programmes. Michael has represented an international provider in carrier access and interconnection negotiations involving non-US originated traffic, and continues to expand his expertise to new and evolving technologies, including with respect to regulatory concerns involving cloud computing, cryptocurrency, and artificial intelligence.

Kelley Drye & Warren LLP

3 World Trade Center
New York
NY 10007
USA

Tel: + 1 212 808 7800
Fax: + 1 212 808 7897
Email: crubsamen@kelleydrye.com
Web: www.kelleydrye.com



1. Metaverse

1.1 Laws and Regulation

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. User-generated digital content and digital assets, such as non-fungible tokens (NFTs), raise novel intellectual property issues including those summarised below.

Copyright

Copyright is a type of intellectual property that protects original works of creators. Copyright owners have the exclusive right to reproduce the work, display it, distribute copies of it, and to authorise others to exercise those rights. In the metaverse, copyright protects user-generated digital content including avatars, virtual buildings, and digital artwork.

Business and individual users should carefully consider platform-specific terms regarding the use and ownership of copyrighted content. Moreover, content created in the metaverse that is similar to copyrighted content in the physical world may give rise to claims for copyright infringement. For example, an avatar or NFT in the metaverse that is similar to copyrighted work 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 to sell their products in the

real world. Using another party's trade marks in these ways can trigger a trade mark infringement claim.

Torts

As with other platforms, tort law governs conduct between users in the metaverse. For example, a business or individual user may be liable under tort law for fraudulent or defamatory statements made on a metaverse platform. Other user-generated content and conduct may also give rise to tort claims.

However, the immersive nature of the metaverse poses novel questions under tort law. For example, US courts have not explored whether and when conduct in the metaverse can constitute tortious assault, conversion, or emotional distress. Most platforms engage in some degree of real-time content moderation, but anecdotal evidence suggests it is insufficient to protect all users.

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 or 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 went 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.

Digital commodities such as non-fungible tokens (NFTs) pose unique intellectual property challenges. Recent cases in the Southern District of New York have found liable defendants that minted NFTs which appropriated the likeness and trade marks of physical goods (Nike, Inc v StockX LLC and Hermès v Mason Rothschild).

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 jurisdiction over consumer protection and competition enforcement across broad areas of the US economy, is 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 rule-making 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**, 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 educational 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 insti-

tutions, healthcare 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 are some of the more-frequently implicated laws and standards 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. Significant revisions to the Safeguards Rule went fully into effect on 9 June 2023, and a breach notification requirement takes effect on 13 May 2024.

In addition, on 8 February 2023, the US Department of Treasury issued a report on financial institutions’ adoption of cloud services. Generally, the report states that “applicable federal regulatory requirements place responsibility for effective and appropriate management of technology operations and related risks... on financial institutions, regardless of whether any particular activities or operations are outsourced to third parties”. In addition, the report notes that the GLBA requires federal and state regulators to provide guidance, and notes that the US Federal Deposit Insurance Corporation (FDIC), the US Federal Reserve Board (FRB), and the US Office of the Comptroller of the Currency (OCC) issued Interagency Guidelines Establishing Information Security Standards pursuant to their authority under GLBA.

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. Generally, Covered Entities' use of cloud and edge computing services must comply with HIPAA.

Entities participating in federal programmes

Requirements applicable to activities by federal agencies and their contractors include the Federal Information Security Modernization Act (FISMA). FISMA establishes federal agency roles and responsibilities for information technology security. In addition, the Federal Risk and Authorization Management Program (FedRAMP), which was previously a policy for over a decade, was adopted as a federal law in early 2023, codifying several key aspects of the security assessment and authorisation for cloud service providers.

Auditing standards

The Statement on 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 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 statements 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 Council has created the Payment Card Industry Data Security Standard (PCI DSS) to address data security for any company that stores, processes or transmits "Cardholder Data" or "Sensitive Authentication Data" as defined by the PCI DSS, though the requirements are not statutorily

mandated. Nevertheless, it is standard industry practice for a service provider receiving Cardholder Data or Sensitive Authentication Data to be required to meet the extensive requirements of 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, such as pursuant to the EU's General Data Protection Regulation (GDPR), have become major issues and especially following the Court of Justice for the European Union's July 2020 Schrems II decision. Subsequently, the US and the EU have implemented frameworks relating to the exchange of personal information, including the US's October 2022 "Executive Order on Enhancing Safeguards For United States Signals Intelligence Activities" and the EU's December 2022

“Declaration on Government Access to Personal Data Held by Private Sector Entities” as well as the EU’s 2023 Data Act relating to access and use of information. In addition to requisite processes to evaluate and respond to government demands, cloud providers increasingly also 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 and several have enacted comprehensive structures, including in California, with the California Consumer Privacy Act (CCPA), Virginia, with the Virginia Consumer Data Protection Act (VCDPA), and

others, including Colorado, Connecticut, Texas, and Utah. In general, these privacy structures require contracts with service providers/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 the 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.

In addition, in 2023, California expanded this list to include citizenship and immigration status, starting 1 January 2024.

Under the CCPA and CPRA, consumers have the right to limit or opt out of certain uses of sensitive personal information. And, beginning in 2026, consumers are permitted to request deletion of their information across all data brokers using a single deletion request.

- 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 with certain material variances such as an exemption to the right to delete personal data where the information was obtained from a third party. However, Virginia does afford 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. In addition, entities will be required to accept opt-out requests through a universal mechanism starting 1 July 2024. In general, the CPA is generally more closely aligned with the VCDPA than the CCPA. Violations of CPA are 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

At least nine other states have enacted 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' varying coverage.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

Artificial intelligence (AI) in general terms refers to the use of computers to solve problems or perform activities traditionally requiring the application of human intelligence. The term has been in use for many decades, but an enormous amount of publicity has resulted from the recent release of "generative AI" tools, such as ChatGPT. Generative AI tools use sophisticated algorithms to analyse very large data sets and identify patterns and then, in response to a user's prompt, create new output closely resembling human-created content. For example, generative AI may be used to create text, images or software code.

There is no comprehensive current federal statutory structure in the US dedicated to the regulation of AI. As a result, businesses involved in AI-related activities will need to consider a variety of laws at the federal, state and local level that may impact those activities.

Federal AI Approach

The Biden Administration released Executive Order (E.O.) 14110 on Safe, Secure, and Trust-

worthy Development and Use of Artificial Intelligence on 30 October 2023. The Order covers more than just generative AI and uses the following definition of artificial intelligence to establish its scope: "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments". This order seeks to establish responsible AI development and deployment by providing direction to numerous federal agencies related to a variety of AI-related areas, including safety and security, innovation and competition, work support, AI bias and civil rights, consumer protection, privacy, the federal use of AI, and international leadership. While the Order is directed towards specific federal agencies, it is likely to also influence additional legislation as well as best practices.

Entities that hold personal information about consumers and businesses should consider privacy, disclosure, equal opportunity/non-discriminatory uses, and transparency concerns. For example, 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. In November 2023, the FTC adopted a resolution streamlining its ability to issue civil investigative demands for AI products that potentially violate Section 5 of the FTC Act. In September 2023, the CFPB issued guidance on the use of AI in credit denials, explaining that creditors are required to explain the specific reasons for taking adverse actions even if companies use complex algorithms and black-box credit models to make such decisions.

Employment-Related AI Regulation

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.

A number of states and municipalities have adopted laws specifically regulating the use of automated tools in the employment area. For example, New York City adopted a law effective 1 January 2023, with broad application to the use of AI by employers, including prohibiting the use of AI tools to screen candidates unless a bias audit has been conducted, and establishing liability for employers and third-party vendors alike.

AI Privacy Considerations

AI implicates privacy, disclosure, equal opportunity/non-discriminatory uses, and transparency considerations, and generative AI raises additional considerations. Generative AI often 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 AI algorithmic processes.

In addition, various states have generally-applicable statutory restrictions on the collection, retention and use of personal information, generally, or with respect to specific types of personal information.

AI Intellectual Property Issues

In the case of generative AI, a number of intellectual property-related issues arise regarding ownership of intellectual property associated with both the AI itself and the output from the use of AI. Many of these issues are the subject of current litigation. An entity engaged in creating generative AI or using generative AI for the creation of output (whether text, software, images or music) will need to consider the intellectual property issues associated with such use.

Recent decisions have established that AI cannot be either the inventor of a patent or the author for purposes of copyright protection (see *In Thaler v Vidal*, 43 F.4th 1207 (Fed. Cir. 2022) and *Thaler v Perlmutter*, Case No 1:22-cv-01564, (D.D.C. 2022)). However, a number of intellectual property-related issues remain outstanding, such as whether an AI-generated work is owned by the AI's software programmer and the ability to protect intellectual property created jointly by a human and an AI tool.

In addition, a number of cases have been filed alleging that the process used to "train" generative AI tools violated the intellectual property or other rights of the plaintiffs, including with respect to the use of open source software, books and recordings for training generative AI tools and the failure to obtain consent of consumers (see, for example, *J. Doe et al. v GitHub et al.* (November 2022), *Sarah Silverman v OpenAI* (July 2023) and *P.M. et al. v OpenAI* (June 2023)).

Liability and Risk Allocation

In addition to the legal issues described above, generative AI tools will regularly produce wrong or offensive answers to prompts, known as “hallucinations”.

An entity utilising AI in its products or services, whether generative AI or otherwise, will need to consider the potential product liability issues. Courts in the United States are in the process of examining the manner in which the use of AI in products and services implicates traditional concepts of product liability for negligence (eg, failure to act as a reasonable person under the circumstances) and strict liability (eg, liability associated with putting a defective product or service into the stream of commerce without regard to the standard of care used, or contractual relationships).

In light of the potential risks, entities considering the use of generative AI should ensure proper risk allocation and precautions are considered. For example, an acquirer of an AI tool from a third party will need to carefully consider (i) the terms and conditions under which the tool is provided, including indemnification protection from third-party claims and disclaimers, and limitations of liability; (ii) the business risk associated with the use of output from an AI tool and the practical ability to mitigate the risk of use of the output; and (iii) the legal and business risks associated with allowing an AI tool to utilise data provided by the end user to conduct additional “training” of the AI tool.

AI Policies and Governance

The use of generative AI offers a variety of potential business benefits and efficiencies and is rapidly becoming more reliable. Many entities in the United States are establishing policies and committees of internal stakeholders in order to

analyse and manage the use of these AI tools and the risks described above.

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 (IoT) 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, 2. **Digital Economy**, 3. **Cloud and Edge Computing**, 4. **Artificial Intelligence**, and 8. **Challenges with Technology Agreements**. 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 intercepting 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, in August 2023, the US Federal Communications Commission (FCC) instituted a proceeding proposing a voluntary cybersecurity labelling programme based on cybersecurity standards for IoT devices and products. The FCC may implement that programme in 2024.

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 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. At this time, the FCC states that it is not accepting new AM broadcast station applications.

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, show the following.

- Include the proposed new channel, class, and the community to be served.
- The proposed new allotment site meets the spacing requirements of (the FCC's rules) to other stations, prior-filed applications, and vacant allotments.
- 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. At this time, the FCC states that it is not accepting new FM commercial broadcast station applications.

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. 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 a limited amount of 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 federal 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 videos available online. For example, a distribution of online videos may implicate the 21st Century Communications and Video Accessibility Act (CVAA), 47 USC §613, Copyright Act protections, and FCC rules where the video was previously published or shown on television. Further, the applicability of some statutes, such as Title III of the federal Americans with Disabilities Act (ADA), 42 USC §12182, are open to interpretation and may be subject to change through judicial interpretation as to whether specific requirements apply to videos online. For example, the federal Video Privacy Protection Act (VPPA), 18 USC §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 make 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. However, in October 2023, the FCC proposed to re-classify broadband as

a Title II service, with certain forbearances, in its proposed “Net Neutrality Rule”. That proposal may be adopted in 2024. Currently, 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 transmission 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, videoconferencing, instant messaging, 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 as 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 each state uniquely handling the question of VoIP jurisdiction.

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-enabled 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 a 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 biom-

etric 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 independent 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).

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