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

TMT

Italy

Law and Practice
Francesca Lodigiani, Luca Egitto,
Chiara Agostini and Gianluca Morretta
RP Legal & Tax

Trends and Developments
Luca Egitto
RP Legal & Tax

practiceguides.chambers.com
Contents

1. Cloud Computing p.3
   1.1 Laws and Regulations p.3

2. Blockchain p.4
   2.1 Legal Considerations p.4

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence p.5
   3.1 Challenges and Solutions p.5

4. Legal Considerations for Internet of Things Projects p.6
   4.1 Restrictions on a Project's Scope p.6

5. Challenges with IT Service Agreements p.7
   5.1 Legal Framework Features p.7

6. Key Data Protection Principles p.8
   6.1 Core Rules for Individual/Company Data p.8

7. Monitoring and Limiting of Employee Use of Computer Resources p.9
   7.1 Key Restrictions p.9

8. Scope of Telecommunications Regime p.10
   8.1 Scope of Telecommunications Rules and Approval Requirements p.10

9. Audio-Visual Services and Video Channels p.11
   9.1 Audio-Visual Service Requirements and Applicability p.11

10. Encryption Requirements p.12
    10.1 Legal Requirements and Exemptions p.12

11. COVID-19 p.13
    11.1 Pandemic Responses Relevant to the TMT Sector p.13
1. Cloud Computing

1.1 Laws and Regulations

Cloud Computing

Cloud services must be compliant, first of all, with privacy law provisions contained in the European General Data Protection Regulation No 679/2016 (GDPR) and the Legislative Decree No 196/2003 (Privacy Code), which set forth the security measures and the other obligations that a data controller must abide by when outsourcing cloud functionalities. In particular, the Privacy Code also provides criminal sanctions, differently from the GDPR, for the most severe cases of violation.

The Code of Digital Administration (Legislative Decree No 85/2005, CAD), regulates the creation, reproduction, storage and digital transmission of digital documents.

In the cybercrime sector the most relevant provisions are:

- the Criminal Code, that sets forth the specific criminal offences relating to IT and computer crime;
- Legislative Decree No 231/2001 on company criminal liability, which provides for sanctions against cybercrimes committed by such entities;
- Legislative Decree No 65/2018, which implemented the EU Directive on Networks/Information Systems’ security; and
- Prime Minister's Decree 131/2020, implementing Law Decree 105/2019 which aimed to establish a national cyber security perimeter.

In addition, Law No 633/1941 (Copyright Law) includes specific criminal sanctions against those making available to the public protected works, or parts thereof, by introducing them into IT networks.

Administration and Banking

More specific regulations have been provided with reference to certain industries, such as public administration and banking, for example. In respect of the first, Article 68 of the CAD imposes obligations on public administrations to acquire computer programs after conducting a particular market evaluation on cloud providers and other software solutions. Furthermore, circulars No 2 and 3 of 9 April 2018 issued by the Agency for Digital Italy (AgID) (as integrated by circular No 2 of 28 October 2020) specifically impose further obligations for cloud service providers regarding protection, recovery, interoperability and portability of data.

Starting from 1 April 2019, public administrations are required to acquire services only from cloud providers certified by AgID. In addition, AgID issued specific guidelines for emergency recovery of public administrations. Moreover, according to AgID’s 2019-2021 Three-Year Plan for IT in Public Administration, when defining a new project/service, public administrations will need to adopt a cloud paradigm as a priority, before any other technology (the “cloud first” principle).

In the banking industry, the Bank of Italy’s (Italian Central Bank) Circular No 263/2006 has introduced strict conditions for outsourcing banks’ functions (eg, cloud functionalities), including:

- the compliance with a specific internal policy when adopting decisions on outsourcing;
- the prohibition to delegate the bank's responsibilities;
- a clear definition of rights/obligations of banks and providers and the demanded service level (including in emergency cases) within the agreements with external cloud providers;
- the monitoring of the outsourced functions and the designation of an internal supervisor for each function;
- the notification to the Bank of Italy of their intention to outsource important functions 60 days prior to the assignment; and
- the delivery of a report, by 30 April of each year, to the Bank of Italy on the supervision carried out on important operational outsourced functions.

Moreover, under Circular No 285/2013 of the Bank of Italy, agreements with cloud providers must include several warranties for the banks, including:

- the indication of the location of the data centres processing the bank's data;
- the implementation of monitoring systems of the operations performed by the provider; and
- implementation of audit methods appropriate to the outsourced data and to the type of cloud service.

These agreements are subject to further obligations in compliance with the guidelines issued by the European Banking Authority, regulating outsourcing agreements.

Personal Data

The processing of personal data by means of cloud services may involve some challenges related to the security (loss of data due to the use of internet and remote applications and to the sharing of data, insider threats, organised crime, etc) and also to the compliance with regulations and standards the organisation is subject to. Moreover, a particular issue arising from use of cloud services is that data can be stored in foreign locations, and may
be transferred from one location to another repeatedly or may be located in multiple sites at a time, so that there may be a diminution or a loss of control over data and processing carried out on behalf of the data controller.

The Italian privacy legislation relating to cloud computing derives from GDPR and there are no other specific national laws on this matter. As legislation implementing GDPR is still quite recent, the Italian Data Protection Authority (IDPA) has only started issuing resolutions/opinions involving this specific practice area, addressing, for example, the following issues:

- (IDPA document 9260158) during an informal hearing for a draft law on wiretapping, the IDPA’s President declared that the use of cloud for storing data intercepted should be prohibited;
- (IDPA document 9487928) with the Opinion on AgID’s draft “Guidelines for the provision of public Wi-Fi free service”, also in light of the ECI’s recent ruling of the Schrems II case, the IDPA specified that with reference to the possible migration of the physical controller (ie, equipment administering the Wi-Fi network’s access points) to a cloud infrastructure, the choice of a supplier external to the administration must meet all GDPR safeguards for extra-EU processing.

2. Blockchain

2.1 Legal Considerations

Using distributed ledger technologies (DLT) is one of the biggest challenges when it comes to legal and regulatory matters in Italy. The regulatory and legal framework is extremely uncertain, although the Italian legislator has tried to (partially) provide for statutory definitions of DLTs, smart contracts and virtual currencies. However, such definitions do not form part of a complete regulatory system, being mere standalone clauses.

Under the Italian law, DLTs include “technologies and IT protocols using a shared, distributed, replicable, simultaneously accessible, architecturally decentralised registry grounded on cryptographic basis, such that data can be recorded, validated, updated and stored both in clear and further protected by encryption verifiable by each user, non-alterable and non-modifiable”. Many Italian blockchain experts highlighted the weaknesses of such provision, given that real “non-alterable” DLTs currently do not exist and that data cannot simultaneously be “non-modifiable” and “updated”.

A smart contract is “a computer program that operates on DLTs and whose execution automatically binds two or more parties on the basis of predetermined effects. Smart contracts meet the requirement of written form after computer identification of the parties involved, through a process that meets the requirements set by the Italian Digital Agency”. Moreover, “the storage of a digital document through the use of DLTs produces the legal effects of electronic time stamping as referred to in Article 41 of Regulation (EU) 910/2014”, as long as such DLTs meet the technical standards set forth by the Italian Digital Agency. Although such guidelines were meant to be adopted before summer 2019, they have not been enacted yet.

In light of such definitions, the primary aspect to deal with in addressing this matter is what blockchain is going to be used for. The answer to that can help to identify the appropriate legislative and contractual ground to rely on.

A primary distinction would be between projects aimed at giving rise or dealing with “crypto-assets” and projects using DLTs for other purposes.

DLTs can be used to generate “tokens” of different types. Certain tokens simply represent a pure virtual asset with no rights enforceable against a counterparty, and can be used as a currency (bitcoins are the most famous example). In that case, providers of DLT services should take into account anti-money laundering, currency exchange and tax regulations in the first place. In that context, the Italian Parliament implemented Directive (EU) 2018/843 which sets forth the definitions and the AML implications concerning “virtual currencies”, “custodian wallet providers” and “providers engaged in exchange services between virtual currencies and fiat currencies”.

A second type of token comprises virtual assets that incorporate rights enforceable against one or more parties. For example, such tokens can give rise to a right to immediate or deferred payment and therefore might fall under the definition of “security” and be subject to financial and security exchange regulations. Due to the strong legal uncertainties connected with the issue of security tokens (including ICOs), on 2 January 2020, the Italian Commission for Companies and the Stock Exchange (CONSOB) published a report on “initial offers and exchange of crypto-activities” which has been defined following a public debate involving market operators commenced in May 2019. The document is meant to contribute to the definition of a national regulatory regime on public crypto-activity offers and connected exchanges and is aimed at identifying potential solutions to regulate crypto-activities which are not comparable to financial instruments and therefore require specific and appropriate regulation for a new reference framework to operators and investors.

A third type of token gives the holder the right to an immediate or future service or asset. In such a case, offering coins might fall
under traditional civil code provisions on co-ownership, donation, public offering of goods or services, sale of future assets or unilateral undertaking to award goods or service upon certain conditions. Offering such items to the public at large can easily fall under consumer protection rules as well. Risks and liabilities, therefore, need to be assessed on the basis of the actual and specific nature of the intended DLT project.

Intellectual property can be either the bundle of rights arising from the development of a DLT project or the content of the transaction recorded on the blockchain. The architecture of a DLT project can certainly be a proprietary right, while the underlying software used to develop the applications necessary to operate on the blockchain is often open source or based on publicly available standard libraries of programming languages and protocols adopted to secure interoperability, but there are at the same time countless applications that are proprietary.

Blockchain, however, is an excellent tool to track and record property conveyance, IPRs generation, prior art, authorship and any information and transaction necessary to identify the time and parties material to an intellectual or industrial property right. The time stamp allocated to a bit of information on the blockchain is an effective method to give certainty to a specific right or assignment, and can make blockchain the new environment to protect and exploit IPRs. Applications are multiple in the IP realm and there are already many projects leading the way to this new environment for immaterial assets.

Data protection is one of the biggest challenges and issues when it comes to blockchain as its decentralised nature is often considered the main obstacle to identify a data controller and therefore the epicentre of the GDPR regulatory framework. However, there are certain types of blockchain which are “private” and subject to a central control which can easily fall under the scope of GDPR. At the same time, businesses that provide services connected to the blockchain environment (wallets, exchanges, trading platforms) are clearly subject to GDPR as they are distinct entities processing data for their own purposes.

In that context, on 7 May 2020 Italy's agency for digital services (AGid) published software development guidelines that also address the design of DLTS, stressing the importance of developing technologies that guarantee the availability, confidentiality and integrity of the information.

Another challenging aspect for service providers is defining accurate, realistic and feasible service levels for the activities they have to perform. Supplying DLT services is often an admixture of pure blockchain (decentralised and not subject to the control of the provider) and business services. A DLT service provider should carefully assess and identify those aspects that are realistically under his or her control and filter out from the KPIs those items that are entirely dependent on the blockchain, and therefore subject to events independent from the provider.

However, this is not the only critical issue on liability, as there is another one of relevant magnitude – this being jurisdiction. Identifying the applicable jurisdiction can be a headache in purely decentralised environments, while the issue becomes easier to handle when considering vertical services located in a specific place. Again, the primary aspect is to identify what DLT service is concerned and what type of blockchain (public, private) is going to be used.

3. Legal Considerations for Big Data, Machine Learning and Artificial Intelligence

3.1 Challenges and Solutions

Big data has been one of the most debated issues in recent years and has finally become “business” after years of discussions about its potential. The legal impact of big data needs to be assessed on the basis of the type of information to be processed and the service underlying the project. Needless to say, most big data projects concern personal data, and if that is the case then GDPR (as well as Italy's Privacy Code) is the main instrument to look at.

The ability of the provider to pursue its business scope in dealing with personal data depends on his or her degree of GDPR compliance and his or her skills in combining data protection with smart business solutions. When looking at a data set, if the intended purpose is making business out of such data, then we need to rely on a workable legal basis to process such data and, to the extent possible, to get rid of personal identifiable information at the earliest opportunity. Anonymised data sets are beyond the scope of GDPR and managing to create a large, anonymised consumer database can be a great business success, provided all necessary requirements are met.

Handling personal data in the wrong manner or, even worse, breaching GDPR when building a database can give rise to severe liabilities. Service providers and businesses in general are struggling to find adequate insurance coverage for data breaches and GDPR breaches, as there is still great uncertainty in connection with both sanctions applied by supervisory authorities and the amount of damages that can be claimed by affected data subjects.

Any business willing to run a big data project needs to be prepared to bear the regulatory burden the GDPR provides for data controllers, and invest in security to make sure that data subjects
are protected from data breaches and avoid computer crimes from being committed. Indeed, when big data concerns personal data, a large number of individuals can be exposed to serious offences that affect the fundamental right of individual privacy; GDPR is a key factor to preserve such rights and maintain effective safeguards against the danger surrounding big data.

The business of big data does not consist exclusively of making such information available against consideration, but also includes building databases that can be protected under copyright and a sui generis right provided for by Italy’s Copyright Law. A database can be considered “opera dell’ingegno”, a copyright work, when it entails original, creative methods to organise and present information. Such protection is identical to that granted to works of art or literature and can give rise to substantial economic value. The sui generis rights protect the creator of the database from unauthorised use or extraction and, although effective for a much shorter term (15 years), is also a valuable tool to generate value from data.

Data can be assets or commodities, and as such can be exchanged and traded, including cross-border. Such trading is not different from that of other intangible assets and gives rise to the legal issues usually concerned with international commerce. Harmonised EU laws on data protection, IP and commerce are an essential factor to promote cross-border business based on big data and constitute the main legal framework to look at when assessing the relevant aspects of an international big data project.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions on a Project’s Scope

The Concept of the Internet of Things (IoT)
The concept of the Internet of Things (IoT), as explained by the Working Party Article 29 (WP29) in its opinion 8/2014, refers to an infrastructure in which billions of sensors embedded in common, everyday devices are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.

Data Protection Impact Assessment in the IoT Context

Usually the IoT implies the processing of personal data – for example, in order to measure the user’s environment data or to observe and analyse his or her habits – which could result in a high risk to the rights and freedoms of natural persons.

As highlighted by the WP29 this risk is identified especially in situations where, without IoT devices, personal data could not have been interconnected (or it might but only with great difficulty).

Therefore, pursuant to Article 35 of GDPR and following the list of processing operations which require a data protection impact assessment provided by the IDPA (Resolution No 467/2018), the data controller shall carry out a privacy impact assessment before any new applications are launched in the IoT.

This assessment should enable the data controller to implement the appropriate measures, particularly during the design stage, in order to mitigate the risks identified.

Privacy by Design and by Default

Moreover, every stakeholder in the IoT system should apply the principles of privacy by design and privacy by default pursuant to Article 25 of the GDPR.

This also means that the design of the data processing methods within the IoT infrastructure should minimise the presence of redundant or marginal data and avoid any potential hidden bias and any risk of negative impact on the fundamental rights and freedoms of the data subjects.

Therefore, personal data that is unnecessary for the services offered through the IoT system should not be collected and stored “just in case” or because “it might be useful later”.

In any case, when personal data is not necessary to provide a specific service run on the IoT, the data subject should at least be offered the possibility to use the service anonymously.

Moreover, personal data collected and processed in the context of IoT shall be kept for no longer than necessary for the purpose for which the data was collected or further processed. This necessity test must be carried out by each stakeholder in the provision of a specific service on the IoT, as the purposes of their respective processing can, in fact, be different. For instance, when a user does not use the service or application for a defined period of time, the user profile should be set as inactive. After another defined period of time, the data should be deleted. The user should also be notified before these steps are taken.

Security in the IoT Context

The data controllers and the data processors in the IoT context should also note that, under Article 32 of the GDPR, they shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In this regard, ENISA in its guidelines for securing the internet of things – issued in November 2020 – highlights that the security by design and by default approach is of paramount importance as IoT security needs to be considered at all stages of the supply
chain, from the early conceptual design to the end user delivery and maintenance. It is therefore important to analyse the relevant supply chain security threats and, accordingly, to set forward security measures and guidelines that help avoiding the risks that affect trustworthiness of the IoT supply chain.

Therefore, any stakeholder acting as a data controller or a data processor remains fully responsible for the security of the data processing. Consequently, it is necessary for these subjects to perform security assessments of systems as a whole, including at the level of components applying principles of composable security. In the same regard, use of certification for devices, as well as the alignment with internationally recognised security standards, can be implemented in order to improve and demonstrate the overall security of the ecosystem of the IoT.

Additionally, while devices that are designed to be accessed directly via the internet are not always configured by the user, security practices based on network restrictions, disabling by default non-critical functionalities, preventing use of untrusted software update sources (thus limiting malware attacks based on code alteration) should be implemented in order to contribute to limiting the impact and the extent of possible data breaches.

Furthermore, an adequate data breach policy can also help to limit the negative effects of software and design vulnerabilities, by spreading knowledge and providing guidance on those issues.

**Transparency in the IoT Context**

Finally, the data controllers shall provide the data subjects with an adequate privacy notice under Articles 13 and 14 of the GDPR, which provides clear information on data processing, categories of data collected, purposes of processing, all the subjects involved in the data flow, data retention period, modalities and means used for the processing, possible personal data transfer to an extra-EU country and appropriate safeguards used to lawfully allow this transfer, the description of data protection rights and how data subjects can exercise them. Depending on the applications, this privacy notice could be provided, for instance, on the connected item, using the wireless connectivity to broadcast the information, or through a QR code or a flashcode printed on the product.

5. Challenges with IT Service Agreements

5.1 Legal Framework Features

Local laws are always a challenging issue when it comes to service agreements to be performed in Italy. The magnitude of the impact of local legislation depends on what services are specifically awarded to the service provider. A system integration project involving hardware/wiring work to be performed on-site at the premises of the client can trigger burdensome obligations regarding health and safety and employment regulations protecting workers from environmental and workplace hazards and from failure of their employer to pay wages and social security allowances. Such obligations usually involve both the client and the contractor, which are jointly liable for certain mandatory obligations regarding employment protection.

Applying to become a supplier of a local organisation in Italy often requires a qualification process that includes filing certificates and declarations for compliance, anti-bribery, anti-money laundering and anti-corruption purposes. Responding to a call for tender issued by a public entity also requires specific formal requirements for the submission and entails disclosure of specific documents from the prospect contractor.

When services consist of software development or application design, a crucial aspect is copyright and other intellectual property rights (IPRs) that may arise in connection with the development of computer programs or digital content. Italy's copyright law requires written evidence of copyright assignment and it is always strongly recommended to draft the IP section of the service agreement accurately to identify the foreground IP that may be assigned and govern any relevant aspect of the background IP of the parties.

Additionally in this context, data protection and data security are the most debated issues when it comes to IT services agreement. Service providers contracted to provide storage, hosting, application management, maintenance or even bug-fixing might need to access or handle personal information. In such cases, their relationship with the client is almost certainly that of processor-controller under Article 28 of the GDPR and that triggers a number of contractual issues, ranging from security measures the processor is required to implement (and their impact on costs and revenues) to the liability such processor is going to incur when processing data on behalf of the controller.

The Italian legal environment is challenging when it comes to the processor's liability, as such liability under GDPR is often mistaken by controllers as an ordinary contractual liability; as a consequence, data processing agreements (DPAs) under Article 28 of the GDPR are often drafted by controllers with open-ended, unlimited, all-round liability and “hold-harmless” clauses that can turn out to be simply unworkable for many service providers acting as controllers. On the other hand, tech giants operating as processors impose their own DPAs with liabilities capped at very low amounts, which leave controllers with a substantial risk of finding themselves unable to recover satisfactory damages from processors that breach their obligations.
However, after the ECJ decision on the “Schrems II” case in July 2020, things became even more complicated as such decision heavily impacted on Privacy Shield and the Standard Contractual Clauses (the two main grounds used by controllers to export data to non-EU processors before such decision) by wiping out the first and leaving the latter on a very fragile ground. Currently, exporters willing to transfer data to processors or controllers in the US in order use their services and willing to rely on SCCs need to follow the EDPB Guidelines and seek supplementary security measures, and avoid transferring data in the event such security measures are not available or are not sufficient to preserve the effectiveness of the SCCs within the legislative context of the jurisdiction of the importer. Exporters are now required to undertake a “transfer impact assessment” before transferring data to service providers outside the EU, following the EDPB Guidelines.

6. Key Data Protection Principles

6.1 Core Rules for Individual/Company Data Protection Laws

The main data protection law is the GDPR, which came into direct legal effect in all EU member states on 25 May 2018, and the Italian Privacy Code, as amended by the Legislative Decree No 101/2018, enacted to harmonise the local law with the GDPR (the “Data Protection Laws”).

Data Protection Laws lay down rules relating to the protection of personal data, their processing and their free movement, as well as to the protection of fundamental rights and freedom of data subjects. They apply only to personal data, not to data regarding legal entities.

According to their material scope, Data Protection Laws apply to the processing of personal data wholly or partly by automated means and to the processing which is part of a filing system or is intended to be part of it. As to the territorial scope, they apply to the processing of personal data in the context of the activities of an establishment of a controller or a processor in Italy, regardless of whether the processing takes place in this country or not, and to the processing of personal data of data subjects who are in Italy by a data controller or a data processor not established there, if the processing activities are related to the offering of goods or services to these data subjects or to the monitoring of their behaviour.

Key Data Protection Principles

Key data protection principles can be summarised as follows:

- lawful processing – personal data must be processed lawfully, on the basis of a legal base provided by the GDPR, that, for businesses, are predominantly the consent of the data subject, the fulfilment of a contractual obligation or a pre-contractual action required by the data subject, compliance with legal obligations or a legitimate interest;
- transparency – personal data must be processed fairly and in a transparent manner, after having served an adequate privacy notice to data subjects;
- purpose limitation – personal data may be collected only for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes;
- data minimisation – personal data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- accuracy – data must be accurate and, where necessary, kept up to date;
- retention – data, at least in a form that permits the identification of data subjects, must be stored for no longer than is necessary for the purposes for which this data is processed;
- security – data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing or against accidental loss, destruction or damage, using appropriate technical or organisational measures;
- accountability – the data controller shall be responsible for, and be able to demonstrate compliance with, the above key principles in relation to its data processing.

Data Controller’s Responsibilities

In practice, each data controller shall start a data processing only after having clearly identified the perimeter of the processing activities that it wants to pursue and their compliance with the above key data protection principles.

Moreover, each data controller shall check whether said processing will be protected by adequate organisational and technical security measures.

The data processing, in particular, must be clearly described to data subjects with an adequate privacy notice, that, in a concise, transparent, intelligible and easily accessible form, shall provide information on the data controller and its data protection officer, where applicable, the type of data collected, the purposes of processing, the recipients or categories of recipients of personal data, if any, information on the possible data transfer to an extra-EU country and the appropriate safeguards used to lawfully allow this transfer, the data retention period, the description of the data protection rights and the modalities under which data subjects can enforce them with the data controller.
Organisational Measures

Concerning organisational measures, data controllers shall check the internal and external personal data flow in order to give appropriate instructions to all its staff and its providers that process this data, implementing an audit system to assess compliance with the instructions. Where applicable, the data controller shall appoint a data protection officer and shall put in place policies to appropriately manage data processing, such as the following procedures:

- a data breach policy, setting forth the process to be followed in case of data breach in order to comply with the GDPR;
- a privacy by default and privacy by design policy suitable to ensure that, for any projected data processing, collection, storage and handling of data and the relevant data retention period will comply with the data protection key principles and will be limited to what is necessary for the intended purpose and safeguarded by appropriate technical and organisational measures;
- a data subject request policy;
- an IT policy regulating the use of IT and company devices, the use of business email and the internet at work;
- a data protection impact assessment procedure, in order to carry out a DPIA where the type of the processing that data controller wants to put in place is likely to result in a high risk to the rights and freedoms of a natural person;
- a deletion policy, in order to ensure the deletion of personal data at pre-defined periods.

Furthermore, the data controller and data processor shall implement the record of processing activities, in which they have to register and keep up to date all the relevant information on the categories of data processing.

Technical Security Measures

Finally, in relation to technical security measures, data controllers and data processors, 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 for the rights and freedoms of natural persons, shall implement appropriate technical measures to ensure an appropriate level of security, such as pseudonymisation and encryption of personal data, the ability to ensure confidentiality, integrity, availability and resilience of processing, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident and a process to regularly test and evaluate the effectiveness of these measures in ensuring the security of the processing.

7. Monitoring and Limiting of Employee Use of Computer Resources

7.1 Key Restrictions

The Context

The workplace is a community where it is necessary to ensure that data subjects’ rights, fundamental freedoms and dignity are protected. To that end, employees are entitled to a reasonable protection of their privacy in personal and professional relationships.

Transparency on Inspections

The employer is required to provide clear-cut, detailed information on the appropriate use of the equipment that is made available to the employees as well as on whether, to what extent and how inspections are carried out.

Data subjects have the right to be informed in advance and unambiguously about any processing operations that may concern them in connection with possible inspections.

The purposes of such controls shall be specified by the data controller in its privacy notice pursuant to Article 13 of the GDPR and may relate to specific organisational, production and/or occupational safety requirements. They may also relate to the submission of, or a defence from, a legal claim.

How Inspections Can Be Carried out Lawfully

In performing inspections on the use of electronic devices, the guidelines applying to the use of emails and the internet in the employment context issued by the IDPA specify that unwarranted interferences with the fundamental rights and freedoms of employees must be prevented.

Inspections are only lawful if the relevance and non-excessiveness principles set forth by the law are complied with. Therefore, preference should be given, where feasible, to preliminary inspections on aggregate data related to the whole business and/or specific units.

Additionally, anonymous inspections could result in the issuance of warnings on the non-standard use of the electronic tools made available by the company, whereby all the entities concerned might be called upon to comply strictly with the relevant instructions. Such warnings might be only addressed to the employees working in the department/unit where inappropriate use of company devices was detected. In the event no subsequent unacceptable device use is detected, further inspections focused on individual employees are not admitted in principle.

However, prolonged, continued and/or blanket inspections are, in any case, inadmissible.
Web Traffic Monitoring
With reference to web traffic monitoring aimed at preventing inappropriate use of the internet (such as browsing for reasons that are not connected to work), the employer is required to take suitable measures in order to prevent ex post inspections on the employees.

In particular, the employer may take appropriate measures such as specifying the categories of website that are regarded as related/unrelated to work and configuring systems to prevent certain operations from being performed (eg, uploading files, or accessing blacklisted sites and/or downloading certain files or software).

Private Use of Company Email
On the private use of company email, the guidelines suggest adopting a specific policy in order to avoid that the employee and/or third parties expect certain types of communication to be kept confidential.

Measures Regarding Relevance and Non-excessiveness Principles
In any case, it is appropriate to take measures to prevent processing operations likely to be in breach of the relevance and non-excessiveness principles applied in the Italian jurisdiction in connection with employee inspections and monitoring.

Such measures include the availability of specific user-friendly functions to allow automatic out-of-office reply messages in case an employee is not at work and the implementation of policies aimed at allowing trusted colleagues to access the content of emails considered of relevance for the employer in the event an employee is unexpectedly not at work or is going to be on leave for a long period.

8. Scope of Telecommunications Regime

8.1 Scope of Telecommunications Rules and Approval Requirements
Technologies Falling Within the Scope of Telecommunications
The technologies currently falling within the scope of telecommunications rules (pursuant to Article 2 of the Legislative Decree No 259/2003 – the Electronic Communications Code – which constitutes the main regulation of the telecommunications field) are:

- electronic communications networks and services for public use, such as phone centres, internet points, internet service providers’ products, telephone traffic resale, voice-over-IP, fax services, public telephone services, public network supplies, satellite services, networks used for the broadcasting of sound and television programmes and cable television networks;
- electronic communications activities for private use, such as radio amateurs and low-power equipment to support companies (eg, radio stations used for taxis, security services, civil protection associations);
- protection of submarine electronic communications installations;
- radio-electric services.

Instant messaging is still not included. Providing this service does not require a general authorisation (requested for the other services above), however platforms supplying such service must be registered with the Communications Operators’ Registry (Registry) kept by the Telecommunication Authority (AGCOM, Autorità per le garanzie nelle comunicazioni).

Radio frequencies needed for RFID devices are subject to the regime of “free use” under Article 105, paragraph 1, letter (o) of the Electronic Communications Code. This was established by the Ministerial Decree of 12 July 2007 of the Ministry of Communications, which stated that these radio frequencies may be freely used (such RFID devices having the technical characteristics set out in EU Decision 2006/804/EC) on a non-interference basis and without the right to protection.

General Authorisation
The provision of electronic communications networks and services is subject to a general authorisation from the Ministry of Economic Development (the Ministry), pursuant to Article 25 of the Electronic Communications Code. To this purpose, operators must submit certain information (concerning, for example, their legal representatives, their offices, the description of the type of network involved, the offered services, apparatus used and their location) by means of the so-called “certified notification of starting activity”, and can exercise the activity from the date of filing said notification.

Procedure
Within 60 days from the application the Ministry verifies the existence of the prerequisites and, if necessary, can prohibit the further continuation of the activity.

Specific conditions to obtain the general authorisation may be required in relation to certain telecom technologies. For example, a company interested in obtaining/renewing an authorisation for offering telephone services to the public (including resale of telephone traffic, VoIP, etc) must submit a certificate of the criminal records of the legal representative or a self-certifi-
cation and a self-certification of registration with the Chamber of Commerce with anti-mafia clearance.

Each year, by 31 January, administrative fees must be paid for the general authorisations above (pursuant to Annex No 10 of the Electronic Communications Code).

Costs
Specifically, for providing public communication networks, an operator is required to pay:

- for the entire national territory – EUR127,000;
- for a territory with more than one million and up to ten million persons – EUR64,000;
- for an area with more than 200,000 and up to one million persons – EUR32,000;
- for a territory with up to 200,000 inhabitants – EUR17,000;
- for companies providing their service primarily to end-users equal to or less than 50,000 – EUR500 per thousand users.

The number of users is calculated on the amount of lines activated for each end user.

For providing public telephone services, an operator must pay:

- for the entire national territory – EUR75,500;
- for a territory with more than one million and up to ten million people – EUR32,000;
- for an area with more than 200,000 and up to one million people – EUR12,500;
- for a territory with up to 200,000 inhabitants – EUR6,400;
- for companies providing their service primarily to end users equal to or less than 50,000 – EUR300 per thousand users.

The number of users is calculated on the amount of numbers activated for each end user.

For providing mobile and personal communication services, an operator must pay:

- for companies that provide their service to end users equal to or less than 50,000 – EUR1,500 per thousand users;
- for companies that provide their service to more than 50,000 end users – EUR75,000.

For providing, even jointly, electronic network or communication services by means of satellite, an operator must pay EUR2,220 for up to ten stations, EUR5,550 for up to 100 stations, and EUR11,100 for more than 100 stations.

Companies holding a general authorisation for providing other electronic communications services, not included in the ones above, must pay EUR600 for each location in which the switching devices are installed.

Authorised operators have also to pay an annual contribution to AGCOM for being registered in the Registry. This contribution is annually determined as a percentage of the net turnover of each operator. In 2020, this was 1.3% (AGCOM Resolution No 434/19/CONS).

9. Audio-Visual Services and Video Channels

9.1 Audio-Visual Service Requirements and Applicability
Requirements for Audio-Visual Services
The provision of audio-visual services is subject to the obtainment of an authorisation, granted following a procedure and in presence of certain requirements which vary upon the service, pursuant to Legislative Decree No 177/2005 (Radio TV Law).

Authorisation for Digital Terrestrial Television and Radio Services
A national Digital Terrestrial Television (DTT) authorisation can be requested by joint-stock companies or co-operatives having their registered office in Italy or in the European Economic Area (EEA), or by companies having their registered office in third countries which apply a reciprocal treatment to Italian organisations (pursuant to AGCOM Resolution No 353/11/CONS).

The applicant companies must also have as their business purpose, radio/television or publishing activity or in any case activity related to information or entertainment and their directors or legal representative must not have received certain criminal convictions or precautionary and/or security measures.

The authorisation is granted by the Ministry, upon the payment of a fee of EUR7,000 (which is lower for European authorisations operating at national or local level, for local or provincial authorisations), within 30 days from the submission of the application, unless the term is postponed for further 30 days for additional verifications. It is valid for 12 years, can be renewed for equal periods and can be assigned to third parties in presence of certain conditions.

For providing, even jointly, electronic network or communication services by means of satellite, an operator must pay EUR2,220 for up to ten stations, EUR5,550 for up to 100 stations, and EUR11,100 for more than 100 stations.

Companies holding a general authorisation for providing other electronic communications services, not included in the ones above, must pay EUR600 for each location in which the switching devices are installed.
Authorisation for Associated Interactive Services or Conditional Access Services on Television Terrestrial Frequencies

The provision of associated interactive services or conditional access services on television terrestrial frequencies, including pay per view, is subject to the obtainment of a general authorisation, by submitting to the Ministry, pursuant to Article 25 of the Electronic Communications Code, a declaration (the so-called “certified notification of starting activity”) after which the applicant can start its activity immediately, while the Ministry verifies the possession of the prerequisites within the subsequent 60 days, issuing, where necessary, the order not to continue its activity.

The general authorisations have a validity not exceeding 20 years (their expiry date is on 31 December of the last year of validity) and can be renewed.

Authorisation for Satellite and Coaxial Cable

A satellite authorisation, granted by AGCOM pursuant to AGCOM Resolution No 127/00/CONS, is subject to the payment of a fee of EUR6,026.96, while the coaxial cable authorisation is granted by the Ministry pursuant to AGCOM Resolution No 289/01/CONS, upon the payment of a fee of EUR7,000.

Both authorisations can be granted only to joint-stock companies, having their registered office in Italy or in the EEA (or in countries applying a reciprocal treatment as above), whose directors and legal representatives have not been sentenced as for the DTT authorisation, after a procedure that lasts up to 60 days, or 90 in the case of postponement for additional verifications. They are valid for six years and can be renewed.

Authorisation for “Linear” and “Non-linear” Services Transmitted through “Other Means of Electronic Communication”

A different regulation applies to services transmitted through “other means of electronic communication” – that is, the electronic communications networks other than those via satellite, DTT and coaxial cable (which include mobile networks excluding the transmissions through DVBH, internet, IPTV, web TV and therefore also video channels online such as YouTube), depending on whether they are in “linear” mode (streaming or simulcast services) or in “non-linear” mode (downloading or on-demand services).

In the first case, the authorisation for transmitting audio-visual or radio services through “other means of electronic communication” is granted by AGCOM to joint-stock companies or partnerships, co-operatives, foundations, incorporated and unincorporated associations and natural persons having their registered office or residence in Italy or within the EEA, or in a third country on condition that it applies a reciprocal treatment towards Italian citizens. Also in this case, the applicants must have as their business purpose the radio television or publishing activity, or in any case related to information or entertainment, and their directors or legal representative must not have received certain criminal convictions or precautionary and/or security measures (AGCOM Resolution No 606/10/CONS).

Such authorisation, granted upon the payment of a fee of EUR500 (or EUR250 in the case of radio services) has a validity of 12 years, can be renewed for equal periods and can be assigned to third parties in possession of the prerequisites.

In the second case, non-linear audio-visual media services can be provided upon the submission at AGCOM of the “certified notification of starting activity”, while the other prerequisites and conditions are the same as for linear services, including the duration and the fees (AGCOM Resolution No 607/10/CONS).

In both cases, the authorisation for providing the linear or non-linear audio-visual media services through “other means of electronic communication” must be obtained only when the following conditions are cumulatively met:

- providers have the editorial liability over the content transmitted in any form exercised;
- such services are provided with a view to profit and in competition with the television; and
- they have minimum revenues deriving from advertising, TV sales, sponsorship, contracts and agreements with private and public entities, public funds and/or pay TV services, equal to EUR100,000 per year.

Providers of audio-visual media or radio services on DTT, satellite or coaxial cable can carry out the simultaneous and full re-transmission over the “other means of electronic communication”, at no cost, upon prior notification to AGCOM and to the Ministry. Such notification is due also by the providers of linear or non-linear audio-visual media services through “other means of electronic communication” which broadcast via satellite or coaxial cable.

10. Encryption Requirements

10.1 Legal Requirements and Exemptions

Encryption has been known for decades by the Italian legislator. One of the first regulations which referred to encryption was adopted in 1967 (Decree of the President of the Republic No 18/1967) and is still in force. Such regulation governs the functioning of the Ministry for Foreign Affairs and states that offices involved in these matters are equipped with encryption.
technology which shall be used in order to ensure the secrecy of the communications between the Ministry and the branches located abroad.

Since then, several laws and regulations have been approved but a complete and certain legal framework is still needed. Although one may observe a number of legal provisions recalling encryption, most of them are intended to lead public administrations and other public-related entities to the adoption of IT structures which ensure high levels of safety in data protection and data security. A brief overview of the matters where encryption is used may clarify how it appears in the Italian legal system.

The most important tool, especially for lawyers and professionals, is the so-called “digital signature” which captures the signatory’s intent to be bound by the terms of the signed document, like its handwritten counterpart in the offline world. Since this tool allows the pairing of a document to the relevant signatory, the technological requirements are set forth specifically by the law. In particular, digital signatures shall be based on a system of public and private cryptographic keys in order to ensure certainty and safety to the digital document. The digital signature is currently used to create and sign documents which have to be filed before both Italian courts and other public bodies, so that professionals, judges and public employees are required to own a personal digital signature and deal with encryption on a daily basis, although they do not need any technical expertise.

Moreover, encryption is used by the public administration in the context of the transmission of data which requires secrecy and safety. For instance, the data gathered on slot machines or the questions submitted during the written examination of the bar exam shall be transmitted using encryption methods and cryptographic keys. Also, the operators on the financial market have to use bilateral authentication and encryption keys in the context of communications with the Bank of Italy. Finally, encryption is used to ensure the anonymity of public employees who are resolved to notify to the Italian Anti-Bribery and Corruption Authority a breach of law noted at work (ie, whistleblowing).

All the above implementations of encryption technologies impose public administrations to adopt specific procedures and are aimed at guaranteeing a high level of safety in gathering and transmitting data and information. However, as to the core of the issue, none of those requires companies to specifically use encryption technology, except for the digital signature (which is a tool based on encryption technology, but is not a direct use of encryption by companies or professionals).

Encryption is indirectly used by companies for communications with public administrations or other private entities. Nevertheless, it seems that the current legal framework lacks provisions which allow the exemption from certain rules where the relevant company enacts the use of encryption technologies.

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

Emergency Legislation, Relief Programmes and Other Initiatives

A significant set of legislative/regulatory measures has been adopted to address the COVID-19 pandemic in the TMT sector, mainly introduced to implement Law Decree 18/2020 (Decree), the emergency law adopted to face the health risks related to the spread of the virus.

Telecommunications

With respect to telecommunications, given the increase in consumption of traffic on electronic communications networks, the Decree provided that network/service providers must upgrade infrastructure, ensure the functioning of networks and the operability/continuity of services, communicating the measures taken to AGCOM.

It has also been provided that companies providing electronic communications networks and services may carry out excavation, installation and maintenance work on fibre-optic communication networks, through simplified procedures.

AGCOM has adopted guidelines and several measures implementing the Decree (through, inter alia: Circular of 20/3/2020; Resolutions No 131/20/CONS, 154/20/CONS, 384/20/CONS), to, for example:

- avoid situations of ultrabroadband congestion and social exclusion of non-connected customers;
- ensure higher quality of services and facilitate smart working;
- reduce the costs of one-off contributions for massive migration to ultrabroadband services;
- change the notice from 30 to ten days for the announcement of new ROEs (building optical distributors) open for sale, which enable fibre to the home line (FTTH) coverage for buildings;
- reduce the one-off fee for FTTH activation;
- approve the initiative of operator TIM to supply ADSL at no cost for users already paying for certain TIM’s services, in order to extend participation opportunities in social/economic life through distance learning and smart working.
In addition, AGCOM launched a public consultation (through Resolution 604/20/CONS) on measures to ensure that disabled consumers have equivalent access to electronic communication services from fixed and mobile locations.

**Media**

In the media sector the Decree has provided for:

- 10% allocation of the 2019-20 “private copying” fees, applied on blank phonographic/audio-visual media for allowing recordings of copyright-protected works and paid to the collecting society, SIAE, to support workers in the entertainment industry; and
- the creation of two emergency funds to support the entertainment field (whose resources have been employed, for example, in the form of tax incentives, contributions, support for cinemas, closed for almost all the pandemic period).

Moreover, considering the increased tv audience and the programming’s changes due to the health emergency, AGCOM reminded audio-visual/radio service providers, through Resolution 129/20/CONS, to ensure truthful information coverage on CoVID-19.

In this regard the Ministry of Health highlighted how fake news can be detrimental to citizens’ adherence to anti-COVID-19 measures, drawing up a list of the most common fake news and launching a partnership with search engines so that after typing, for example, “virus” they would return links to health institutions first.

**Technology**

In the field of technology, one of the main initiatives was the creation of Immuni, a free app aiming to help to reduce the spread of the virus through contact tracing (and subject to several limitations to ensure privacy compliance). However, only a very small part of the population downloaded it and many argue that it has been ineffective.

Furthermore, to ensure social distancing the government has adopted measures encouraging/imposing smart working and distance learning. This led to the adoption of regulations aimed at supporting the population through financing measures for digitalisation (eg, vouchers for digital products’ purchase), and to a stronger need for protection against cyberthreats. An innovative step was taken in this regard through Prime Minister’s Decree 131/2020, implementing Law Decree 105/2019, which aims to ensure a general high level of IT security, through the establishment of a national cybersecurity perimeter (ie, a defence shield against cyber-attacks).

**Amendments of Existing Regulations Due to the Pandemic**

Due to the circumstances caused by the pandemic, certain amendments of existing regulations were necessary – for example, through Resolution 111/20/CONS AGCOM delayed from 1 April to 15 June the deadline for the payment of the 2020 contribution due to AGCOM by electronic communications/media operators with a turnover of EUR50 million or less.

Moreover, some operators have proposed to AGCOM temporary changes to the telecommunications regulations in view of the emergency. For example, with respect to the request of renewal of the rights to use frequencies in the 900 and 2100 MHz bands to align all operators in view of the transition to 5G, AGCOM intervened and accepted it, after launching a related public consultation.

**Other Initiatives Relevant to the TMT Sector**

Other initiatives have been taken by AGCOM through the establishment of four roundtables on: electronic communications, postal services, traditional media and online platforms.

For instance, one of these roundtables announced a project proposed by Facebook addressing misinformation about COVID-19, based on a fact-checking service provided by an independent party and performed through WhatsApp.
RP Legal & Tax provides assistance in the television, cinema, internet, technology and music sectors, with a team of eight partners and 12 associates. It has major national and international operators and top sector talents among its clients, with offices in Milan, Turin, Rome, Aosta, Bergamo, Bologna and Busto Arsizio. Assistance ranges from specialist contractual issues and disputes to financing contributions and instruments such as tax credits and product placements, from regulatory aspects to relations with the relevant authorities, ministries, the SIAE, and other collecting entities, including M&A operations regarding top companies operating in the sector. In the musical field, the firm can boast particular experience in drawing up contracts with record companies, copyright agreements, negotiating tours, and in the sale and licensing of recording and publishing catalogues. Assistance in the cinema and television sector covers the entire production chain, from relations with cinematographers right up to co-production with national and international partners, executive production, distribution, etc.

Authors

Francesca Lodigiani is a former partner, now of counsel, and co-head of the firm’s TMT department. Since the mid-1980s she has provided assistance to international and national clients in the TMT sector, experiencing the technological and legislative evolution during that time, and the convergence in the media, telecom and IT industries. Francesca advises clients – today mainly in the media, entertainment, data protection and IT sectors – with reference to regulatory matters; contractual and operational matters in relation to TV channels’ distribution (satellite, cable, DTT, etc), theatrical and audio-visual production and distribution; home video distribution; TV advertising; film acquisition; and tax credit and local incentives.

Luca Egitto practises IT and IP law. He started at RP Legal & Tax as a trainee in the commercial IP department and has progressed as an IP-IT lawyer, becoming a partner in 2015 and the head of IP in 2018. He is a data protection officer, certified under UNI 11697:2017. His main focus is technology, intellectual and industrial property, and data protection. The predominant industries are software development, application management, e-commerce, web marketing, fashion and digital entertainment. He is a member of ITechLaw, INTA and Adlaw International; his publication credits include "Privacy – La Nuova Disciplina Europea" in Il Sole 24 Ore and “The AGCOM Resolution on the Proposed Online Copyright Enforcement Regulation” in Computer Law Review International, 2013 and the chapter on intellectual property in the book "Blockchain e Smart Contract – Funzionamento, profili giuridici e internazionali, applicazioni pratiche".

Chiara Agostini practises in data protection, IP law and TMT and is a data protection officer certified under UNI 11697:2017. She is a partner of RP Legal & Tax and is a member of Adlaw International, ITechLaw, INPLP and Privacy Rules. Chiara provides extra-judicial and judicial assistance to national and international clients, operating in the business communication, internet, e-commerce, advertising, marketing, media, fashion, life science and hospital sectors. She offers assistance in drafting all the legal deeds, policies and contracts aimed at making data processing compliant with the GDPR, in big data management, IoT projects, extra-EU transfer of databases and OBAs.

Gianluca Morretta has provided assistance to international and national clients in the TMT sector as an expert in contentious matters since the mid-1990s. Gianluca has progressed to be a leading IP expert in the technology industry, with a strong focus on software, patents and technology transfer. He joined R&P Legal as a partner in 2009 after serving as partner and founding member of another IP firm in Milano. Gianluca is currently head of the firm’s technology litigation and is a senior patent litigater. He is a member of INTA, AIPPI and Adlaw International.
Technology in the Pandemic
The COVID-19 pandemic significantly affected many facets of life in 2020. Public and private institutions struggled to find means to cope with this unprecedented crisis, often looking at technologies to help and support people in their battle against the disease and to deal with the dire consequences of the outbreak.

Governments in most countries of the world faced huge pressure from scientists and health experts to curb any social activity likely to facilitate the spread of the virus, while simultaneously facing desperate calls from entrepreneurs and businesses not to suffocate the economy with lockdowns and restrictions.

The almost unbearable tension arising from such conflicting viewpoints gave rise to multiple ideas for innovation and technology to support the fight against the virus while keeping the economy rolling.

Digital Contact Tracing
In the early days of the outbreak, most of the attention focused on contact tracing technologies. This was perceived by many as a powerful tool to allow prompt identification of people exposed to an individual who had tested positive, subsequently testing and isolating them with the hope of leaving the remaining population relatively free to live their lives, and thereby preventing the economy from collapsing.

Examples such as South Korea, Taiwan and Singapore appeared promising, but the contact tracing technologies proved to be not as effective as expected without a test and treat system as powerful as that of South Korea. Indeed, the second wave of the pandemic overwhelmed most countries, leaving their healthcare workforce with no options other than disregarding contact tracing in order to provide basic support to patients and emergency medical care.

However, the push for technologies meant to support the fight against COVID-19 while preserving social interaction is still strong. Further to contact and proximity tracing, more and more prototypes have been presented to help communities in getting back to an almost-normal life while still keeping safety measures in place: wearable technologies to guarantee minimum distancing at social events, virtual “immunity” badges, digital vaccination passports, and healthcare wallets carrying medical information. These are all designed to be interoperable and operate cross-border, holding out the hope of being able to go back to international travel and social events at some point in the near future.

All such technologies prompt serious legal concerns, in particular regarding privacy and data protection and the potential harm to civil rights and liberties that ill-conceived technologies might trigger.

Experiences and Perspectives
Keeping an eye on legislative, administrative and institutional developments taking place during this pandemic is a key to understanding how digital and mobile technologies can give birth to innovation, effectively helping societies to leave behind the worst results of COVID-19 and return to social life. In that context, looking at how contact/proximity tracking was dealt with by the legislator and the supervisory authority in Italy (consistently with the EDPB) can help us understand how data protection issues are addressed when it comes to COVID-19-related technologies. The position maintained by the Italian government and the Data Protection Authority in the discussions on contact tracing is likely to affect future developments in this area and deserves to be summarised.

Contact tracing aims at urgently alerting people who have come into contact with an infected person so as to optimise the measures of containment (quarantine) and prevention (awareness, hygiene, social distancing). Manual tracing, which is still the backbone of containment strategies, has some inherent problems that make it unsuitable for effectively controlling the pandemic. It requires a considerable use of manpower and suffers from several shortcomings in detection (imperfect execution of the interview, difficulty of the interviewee in reconstructions, inability to identify close contacts that do not belong to the circle of the infected person, and inability to predict places and events most at risk).

Digital contact tracing brings the possibility of identifying contacts unknown to the infected subject (eg, a contact made on public transport) and was introduced in some countries (Taiwan, South Korea) after the Ebola, SARS and MERS epidemics, proving to be effective in keeping infection rates relatively low.

EU researchers and lawyers pushed for a slightly different approach, this being proximity tracing: in such case, technologies tracking proximity contacts do not necessarily require use
of location data and are more consistent with minimisation principles set forth by the GDPR. They allow exposure notification to be made in a decentralised manner, preventing central authorities from conducting mass surveillance or simply becoming a huge attack-surface for malicious adversaries.

In both cases, the use of mobile devices is considered crucial given the very high adoption of such technology (close to the entire relevant population). Epidemiologists and virologists have stated unequivocally that public health authorities cannot do without digital technologies to support manual contact tracing.

However, these technologies give rise to privacy challenges and risks, in connection with individuals testing COVID-19-positive (and their contacts), and create opportunities for adversaries to create fear or panic, perpetrate frauds, spread misinformation, or worse, mass surveillance and/or profiling.

**A View from the Supervisory Authority**

Such issues were addressed by the Italian Supervisory Authority (Garante per la Protezione dei Dati Personali, SA) in charge of reviewing the draft legislation meant to introduce digital contact tracing in Italy. The SA issued its opinion on 30 April 2020, recommending the following:

- any contact tracing app should be voluntary (download, activation, use of the app and notification of the disease are all independent actions, each to be carried out voluntarily) so that any failure to use the app does not entail disadvantages or adversely affect the exercise of any rights;
- the legal basis for processing data should be the need to perform a task of public interest, in particular for public health policies;
- the technology should be fully transparent and compliant with the obligations set out in the GDPR;
- a DPIA should be carried out on the app and the surrounding infrastructure and then be made available for public consultation;
- the app should be open-source and free;
- the purpose of processing should be strictly limited to curbing the disease, excluding any other purpose;
- the data collected must be able to trace close contacts only and not the movements or location of the data subject;
- data should be collected only where strictly necessary for the purposes of identifying possible contagions, with reliable anonymisation and pseudonymisation techniques;
- the retention period of the data should be limited to the time strictly necessary on the basis of the decisions of the health authority;
- the algorithmic process should be non-exclusive and the exercise of DSRs under Articles 15 to 22 of GDPR should be guaranteed at all times;
- the app should be interoperable with other contact tracing systems used in Europe;
- reciprocal anonymity between app users should be guaranteed throughout the process.

The Italian government issued an urgent decree (No 28, on 30 April 2020, later ratified by the Parliament) consistent with these recommendations, providing for a digital contact tracing system:

- to be developed and hosted in Italy and to operate as support to traditional contact tracing;
- with the Ministry of Health operating as data controller, conducting one or more DPIAs as necessary and providing the utmost security in data processing;
- giving data subjects full prior information and complying with privacy by design and by default principles;
- designed to allow proximity tracing, using anonymous or pseudonymous IDs and avoiding any type of location data processing;
- with minimum data retention and easy, user-friendly DSR tools;
- that is harmless and non-discriminating for those deciding not to use it.

The system proposed to operate as the proximity tracing app in Italy and authorised by the Italian government is Immuni. This met the above requirements after some changes to its technology necessary to comply to the specifications set forth by the SA.

Immuni is an app for iOS and Android, implementing the so-called decentralised protocol (based on user-to-user interaction with no central processing backbone operated by the controller, which is prevented from accessing diagnosis data and the identities of users that tested positive or were exposed to a positive individual) using BLE and adapting to the exposure notification framework of Google and Apple.

The backend of the system performs functions of data collection, dissemination of pseudonymous IDs, interaction with other information systems (such as that of healthcare providers), and data analysis. While there are some centralised functions performed, these do not affect the decentralised nature of the technology, namely storing data locally on the mobile phones of the user.
The purpose of the app is not exactly contact tracing but rather “exposure notification”, in accordance with the D3PT approach, as suggested by the EDPB and the SA (and consistent with the Google-Apple framework).

The user independently decides whether to use the app, to upload a positive test and allow notifications about COVID-19-positive contacts in co-operation with public health authorities.

Users who test positive may decide to notify this to “proximity contacts”, these being the individuals that were in close contact for a time sufficient to determine an epidemiological risk. The risk is based on proximity and timing calculated by the Bluetooth device and is notified to users that fall under such “risk parameter” and are therefore advised to isolate and test, without ever knowing the personal details of the person who tested positive and gave rise to the exposure notification.

The path that led to the authorisation of the contact tracing technology and the introduction of Immuni in Italy is an excellent lesson to follow when conceiving health-related technologies in the time of pandemics.

**Health-Tech on the Rise**

Mobile technologies are powerful, widespread tools which can be used to fight diseases and help people preserve their health, but are also a potentially harmful vehicle for surveillance, fraud, discrimination and consent-manufacture.

Health-tech is definitely a growing sector, and anything that may be useful to fight COVID-19 has a tremendous chance of success, provided it can guarantee protection from mass surveillance and control, profiling, unfair commercial practices, scams and malicious attacks. Such technologies can empower people and give them the means to act responsibly, by protecting privacy and complying with data protection principles set forth under the GDPR and the ePrivacy Directive.

The EDPB made repeated statements in the health-tech context in 2020, which are worth recalling since they outline high-level, wide-ranging principles to follow in product design. According to the EDPB, apps should:

- exchange the minimum possible personal information;
- process pseudonymous data;
- be interoperable;
- avoid location data;
- be transparent and subject to scrutiny by independent watchdogs and supervisory authorities;
- enforce maximum security;
- offer effective and easy data subject rights requests tools.

These key principles are a fundamental guide as they represent one of the first, major practical implementations of the GDPR at institutional level in the health-tech industry.
RP Legal & Tax provides assistance in the television, cinema, internet, technology and music sectors, with a team of eight partners and 12 associates. It has major national and international operators and top sector talents among its clients, with offices in Milan, Turin, Rome, Aosta, Bergamo, Bologna and Busto Arsizio. Assistance ranges from specialist contractual issues and disputes to financing contributions and instruments such as tax credits and product placements, from regulatory aspects to relations with the relevant authorities, ministries, the SIAE, and other collecting entities, including M&A operations regarding top companies operating in the sector. In the musical field, the firm can boast particular experience in drawing up contracts with record companies, copyright agreements, negotiating tours, and in the sale and licensing of recording and publishing catalogues. Assistance in the cinema and television sector covers the entire production chain, from relations with cinematographers right up to co-production with national and international partners, executive production, distribution, etc.

Author

Luca Egitto practises IT and IP law. He started at RP Legal & Tax as a trainee in the commercial IP department and has progressed as an IP-IT lawyer, becoming a partner in 2015 and the head of IP in 2018. He is a data protection officer, certified under UNI 11697:2017. His main focus is technology, intellectual and industrial property, and data protection. The predominant industries are software development, application management, e-commerce, web marketing, fashion and digital entertainment. He is a member of ITechLaw, INTA and Adlaw International; his publication credits include “Privacy – La Nuova Disciplina Europea” in Il Sole 24 Ore and “The AGCOM Resolution on the Proposed Online Copyright Enforcement Regulation” in Computer Law Review International, 2013 and the chapter on intellectual property in the book “Blockchain e Smart Contract – Funzionamento, profili giuridici e internazionali, applicazioni pratiche”.

RP Legal & Tax
Piazzale Cadorna 4
20123 Milan
Italy

Tel: +39 02 87 31 31
Fax: +39 02 87 31 33 22
Email: milano@rplt.it
Web: www.rplt.it