Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2023

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



Italy: Law & Practice

Carlo Impalà, Giorgia Valsecchi,
Giulia Castelli and Jun Jie Yang
Morri Rossetti e Associati

practiceguides.chambers.com

ITALY

Law and Practice

Contributed by:
Carlo Impalà, Giorgia Valsecchi, Giulia Castelli and Jun Jie Yang
Morri Rossetti e Associati see p.22



Contents

1. Metaverse p.3
1.1 Laws and Regulations p.3

2. Digital Economy p.4
2.1 Key Challenges p.4

3. Cloud and Edge Computing p.6
3.1 Highly Regulated Industries and Data Protection p.6

4. Artificial Intelligence and Big Data p.9
4.1 Liability, Data Protection, IP and Fundamental Rights p.9

5. Internet of Things p.11
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.11

6. Audio-Visual Media Services p.13
6.1 Requirements and Authorisation Procedures p.13

7. Telecommunications p.15
7.1 Scope of Regulation and Pre-marketing Requirements p.15

8. Challenges with Technology Agreements p.17
8.1 Legal Framework Challenges p.17

9. Trust Services and Digital Entities p.19
9.1 Trust Services and Electronic Signatures/ Digital Identity Schemes p.19

1. Metaverse

1.1 Laws and Regulations

Laws and Regulations

The metaverse can be described as an immersive and constant virtual 3D world where people interact through an avatar in order to do different activities, such as enjoy entertainment, make purchases and carry out transactions with crypto-assets.

The metaverse is not subject to specific legislation within the European and Italian legal framework.

However, in recent years the European Union (EU) has launched a regulatory revolution aimed at encouraging technological development while respecting fundamental human rights.

Key regulatory reforms that are relevant for this matter include:

- Regulation (EU) 2022/2065 (Digital Services Act – DSA);
- Regulation (EU) 2022/1925 (Digital Markets Act – DMA);
- "Proposal for a Regulation […] laying down harmonised rules on artificial intelligence (AI) and amending certain union legislative acts", COM (2021) 206 final (AI ACT); and
- Regulation (EU) 2016/679 (GDPR).

The expansion of the metaverse challenges the legislator with new and complex legal issues, as described below.

Data Protection

The gathering and processing of large sets of personal data in the metaverse is one of the main reasons users/avatars can have an increasingly realistic digital experience. However, it also creates considerable risks for the freedoms and rights of data subjects from a data protection point of view. In fact, the technologies driving the metaverse (eg, virtual and augmented realities, blockchains, 5G, AI, IoT, Cloud) enable the granular, real-time collection of personal data, including highly sensitive data, such as users' physical attributes (eg, movements, including eye movements, heartbeat or brain waves) and psychological attributes (eg, behavioural reactions and emotional states of individuals triggered by different experiences therein).

From the processing of such information and of the information that the user (or their avatar) disseminates in the metaverse (such as activities performed, interests, consumption habits, and political, religious and sexual opinions eventually expressed), a hyper-individual profile of a user is drawn based on their own individual characteristics and habits. This scenario could lead to various risks, including the following.

- Deeper profiling – the collection, storage and processing of an amount of personal data bigger than ever before to allow metaverse providers to classify people in precise profiles.
- Constant monitoring – the technologies used in the metaverse (eg, wearable devices, motion sensors, microphones, heart and respiratory monitors) may lead to constant observation of every aspect of the physical lives of users, implying a constant privacy invasion and creating risks of mass surveillance, discrimination, loss of autonomy, fraud or identity theft.
- Interference of special categories of data – the functioning of metaverse platforms is based on the monitoring of special categories of personal data such as biometric data, facial expressions, eye movements and vocal

inflections. Considering the direct interaction of the users with the platforms (such as visiting a specific place or participating in a particular event), other special categories of data can also be easily gathered, such as political beliefs and sexual orientation, increasing risks for the fundamental rights and freedoms of data subjects.

Cybersecurity

Given the amount of personal data circulating in the metaverse, companies and users may face several risks related to cybersecurity. Examples of risks that could affect both companies and users include information theft (users could unknowingly share their data with hackers, thus losing control of it) and identity theft (hackers could steal and illegally use the avatar to carry out illegal activities).

On the contrary, risks related only to companies include the fear of missing out (companies might feel obliged to provide services in the metaverse in order to be considered competitive in the technological market) and the compromise of integrity, as a company might expose its data in the metaverse without considering that such data could be processed in the same way as any other public data, and thus be exposed to the risk of possible data theft.

In any case, one of the main challenges from a cybersecurity perspective is certainly the proper protection of users' biometric data processed in the metaverse. Therefore, companies should prevent any possible cyber-attack by making their security systems safe, secure and free of vulnerabilities in order to prevent damages to the companies' economy and reputation, and also to users.

Intellectual Property

The metaverse creates several issues in connection to IP rights.

One of the first issues concerns the rights to software and information technology connected to the metaverse that can be protected by copyright or by an industrial patent.

Another aspect is related to the opportunity to file an application in order to obtain IP rights in relation to classes of goods related to software, such as in the field of trade marks, with the registration under Class 9 of the Nice Classification (software).

A further issue is the infringement of IP rights in the metaverse, particularly trade marks and other distinctive signs, which include domain names and designs. Since the metaverse does not have territorial boundaries, jurisdiction can also be considered an issue here.

2. Digital Economy

2.1 Key Challenges

Laws and Regulations

The e-Commerce Directive 2000/31/EC was implemented at the national level by Italian Legislative Decree No 70/2003 and constitutes the main legal framework for the provision of digital services in the EU.

However, technologies and digital services have changed, necessitating an update of the applicable legal framework. To this end, in a document entitled "A European strategy for data", the European Commission (EC) expressed its intention to develop a legal framework aimed at regulating the data economy, in order to ensure respect for free market principles and competi-

tion in digital sectors, and to fight unfair business practices and limit the dominant position of Big Tech.

The data economy legal framework is as follows:

- the DSA, entered into force on 16 November 2022 and applicable from 17 February 2024;
- the DMA, entered into force on 1 November 2022 and applicable from 2 May 2023;
- Regulation (EU) 2022/868 (Data Governance Act – DGA), entered into force on 23 June 2022 and applicable from September 2023; and
- "Proposal for a Regulation [...] on harmonised rules on fair access to and use of data" (Data Act).

Considering that the Regulations are directly applicable to all member states, such rules will constitute the legal framework applicable at the national level as soon as they come into effect.

The DSA

The DSA applies to various online intermediaries and platforms, and complements sectoral regulations such as the Audiovisual Media Services Directive and the Copyright Directive.

It contains due diligence obligations that will apply (depending on the role, size and impact of the intermediaries and platforms on the online ecosystem) to all digital services that connect consumers to goods, services or content, and provides new procedures for the faster removal of illegal content and a comprehensive protection for users' fundamental rights online. Concretely, the DSA provides for (inter alia):

- measures to counter illegal goods, services or content online, such as a mechanism for users to flag such content and for platforms to co-operate with "trusted flaggers";
- new obligations concerning the traceability of business users in online marketplaces, to help identify sellers of illegal goods;
- effective safeguards for users, including the possibility to challenge platforms' content moderation decisions;
- a ban on certain types of targeted adverts on online platforms (when they target children or when they use special categories of personal data);
- transparency measures for online platforms; and
- obligations for very large platforms and very large online search engines to prevent the misuse of their systems by taking risk-based action and by undertaking independent audits of their risk management systems.

It is worth noting that the DSA does not define "illegal content" online, but it is based upon the concept of "what is illegal offline should also be illegal online". In order to classify illegal content, reference should be made to other European or national legislation, such as that which considers illegal terrorist content, child pornography or illegal forms of online hate speech. However, in the absence of a common understanding of "illegal content", the term's vagueness and broadness may trigger over-removals of content and affect the right to users' freedom of expression, and may also involve a cautious approach by platforms that could compromise the scope of the DSA.

The DMA

Considering that some large online platforms act as "gatekeepers" in the digital market, the DMA aims to ensure that such platforms behave online in a fair way, and to provide benefits to innovators and technology start-ups so that they

can compete in the online platform environment without having to comply with unfair terms and conditions imposed by the gatekeeper itself.

Moreover, consumers shall have more and better services to choose from, more opportunities to switch their provider, direct access to services, and fairer prices.

The DMA qualifies the "gatekeepers" by defining objective criteria that the online platform shall meet, such as the fact that a platform must have a strong economic position in the internal market and be active in multiple EU countries. Furthermore, the DMA provides "dos" and "don'ts" with which the gatekeeper must comply, as follows.

- Do:
  - (a) allow third parties to inter-operate with the gatekeeper's own services in certain specific situations; or
  - (b) allow their business users to access the data that they generate in their use of the gatekeeper's platform.
- Don't:
  - (a) treat services and products offered by the gatekeeper itself more favourably in ranking than similar services or products offered by third parties on the gatekeeper's platform; or
  - (b) track end users outside of the gatekeepers' core platform service for the purpose of targeted advertising, without effective consent having been granted.

In the event of non-compliance with the DMA rules, the EC may issue fines or periodic penalty payments. Additional remedies may be imposed for systematic infringements of the DMA obligations by gatekeepers.

On a final note, the DGA provides procedures and structures to facilitate data sharing between companies, individuals and the public sector, while the Data Act clarifies who can create value from data and under what conditions. The DGA and the Data Act seem to represent an attempt to identify the first rules regarding the monetisation of data, which, however, should always be consistent with the principles of the GDPR, such as free and specific consent, purpose limitation and data minimisation.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Laws and Regulations

Cloud and edge computing services are not subject to specific legislation within the Italian legal framework, but rather are regulated by various different laws and regulations, based upon, inter alia, the sector involved and the legal issues considered.

Cloud-based services

In this context, cloud-based services must be provided in compliance with various European and national laws, including the following.

- GDPR and Italian Legislative Decree No 101/2018, which amended Italian Legislative Decree No 196/2003 (Privacy Code), applicable when the services entail personal data processing.
- Directive (EU) 2016/1148 on the security of networks and information systems (NIS Directive), transposed at the national level by Italian Legislative Decree No 65/2018, pursuant to which cloud services have been expressly included within the relevant scope of application and classified as "Digital Service Provid-

ers", thereby becoming subject to the obligations set out therein. The NIS Directive was replaced by the NIS 2 Directive, which came into force on 16 January 2023.
- Italian Legislative Decree No 82/2005, which sets forth, inter alia, specific provisions and technical rules regarding the creation, reproduction, storage and transmission of digital documents that apply to public administrations, public service providers, public control companies and private individuals.

The DSA and the DMA, which are key regulations recently adopted by the EU, also provide relevant provisions concerning cloud-based services.

In addition, suppliers of cloud-based services can voluntarily adopt control measures and therefore comply with ISO certification standards (eg, ISO/IEC 17788:2014, ISO/IEC 27017:2015, ISO/IEC 27001/2017 and ISO/IEC 27001/2022).

Edge computing

There is no official definition of edge computing, but it is generally considered a subsection of cloud computing, as it is the deployment of cloud computing capabilities at the edge of the network. Edge computing is a distributed, decentralised IT architecture where computation and data storage are closer to the data source, reducing the need to process data in a remote data centre. In this case, therefore, data is processed and computed in connected objects closer to the data source and to the users, allowing for much faster operations and giving users more control over their data. Such data can be sent to a central data centre or cloud storage repository.

A hybrid infrastructure that includes edge computing could be a solution in several fields, such as big data analytics and IoT.

Cloud and Edge Computing in Specific Industries

A number of industries are also regulated by specific laws – eg, banking and insurance.

Indeed, cloud and edge computing constitute two important technology infrastructures applied and used within many sectors, and are frequently provided through outsourcing agreements.

On this point, the applicable legal framework sets forth general provisions concerning the regulation of the outsourcing of functions and outsourcing agreements, including:

- Directive (EU) 2014/65 on markets in financial instruments;
- Directive (EU) 2009/138, known as the Solvency II Directive; and
- Delegated Regulation (EU) 2015/35, known as the Solvency II Delegated Regulation.

Specific provisions are also set forth in guidelines and circulars issued by the competent authorities.

In the banking industry, reference shall be made to the "Guidelines on outsourcing arrangements" (EBA's Guidelines) issued by the European Banking Authority (EBA) in February 2019. The EBA's Guidelines establish measures for financial institutions' governance frameworks and require such institutions to:

- ensure that personal data is adequately protected and kept confidential;
- execute business continuity and contingency arrangements;

- guarantee greater certainty about the conditions under which subcontracting can take place; and
- provide specific documentation concerning outsourcing arrangements (eg, an updated register of information that shall include the cloud service, the deployment models, the type of data to be processed and the locations where such data will be stored).

EBA's Guidelines were implemented by the Bank of Italy through Circular No 285/2013, which was updated in November 2022. This Circular imposes specific requirements that banks must satisfy when using a cloud service, such as the implementation of a risk-based approach with reference to the location where data is stored and processed and the security of the information.

For the insurance industry, reference shall be made to:

- "Guidelines on outsourcing to cloud service providers" issued by the European Insurance and Occupational Pensions Authority, which provide guidance to market players on the measures to be implemented whenever insurance activities are outsourced to cloud service providers and on the requirements regarding documentation and notification to the supervisory authorities; and
- the final report supplementing the provisions of the "Guidelines on outsourcing to cloud service providers", published by the European Securities and Markets Authority (ESMA), applicable to a wide range of entities supervised by ESMA, which contain indications concerning the governance principles, documentation and mechanisms of the supervision and monitoring of cloud providers; the assessment and due diligence procedures to be followed by cloud providers; and the minimum content of outsourcing and sub-outsourcing agreements.

Data Protection

When cloud and edge services entail the processing of personal data, the GDPR and the Privacy Code shall apply, as well as guidelines and measures adopted by the relevant authorities.

Regarding cloud computing, one of the main challenges concerns the transfer, storage and processing of data in multiple locations, and the compliance with specific security obligations. Similar arguments could be extended to edge computing where data protections issues still arise, despite the data being transferred in a safer way.

With specific regard to data transfer, the GDPR prohibits any transfer of personal data outside the EU unless appropriate safeguards are put in place, as provided in Chapter V of the GDPR, which are applicable according to a layered approach. In this context, the location of servers is important in order to comply with the rules provided by the GDPR, and controllers are required to ascertain said location.

Moreover, cloud providers may voluntarily comply with Codes of Conduct enacted by the SWIPO (Switching Cloud Providers and Porting Data). Such Codes of Conduct are considered by certain associations (eg, Gaia-X) to be the standards to follow for data portability.

4. Artificial Intelligence and Big Data

4.1 Liability, Data Protection, IP and Fundamental Rights

Laws and Regulations

To date, there is no specific national legal framework applicable to AI and Big Data (BD) projects. However, with specific reference to AI, the EU is working on a package of measures (to date, still not applicable) to support the roll-out of AI by fostering trust, composed of:

- the AI ACT, aimed at establishing harmonised rules for the development, marketing and use of AI systems, with a risk-based approach;
- the "Proposal for a directive […] on liability for defective products" (Product Liability Directive); and
- the "Proposal for a Directive […] on adapting non-contractual civil liability rules to artificial intelligence" (AI Liability Directive).

The Directives complement each other and the AI ACT. More particularly, the Product Liability Directive modernises the existing EU-level strict product liability regime and will apply to claims against the manufacturer for damage caused by defective products, material losses due to loss of life, damage to health or property and data loss. It is limited to claims made by private individuals. The AI Liability Directive makes a reform of national fault-based liability regimes and will apply to claims against any person for fault that influenced the AI system which caused the damage (any type of damage covered under national law, including resulting from discrimination or breach of fundamental rights like privacy). Claims can be made by any natural or legal person.

Although the aim of the EU is to create a clear legal framework, AI and BD entail various different potential risks for individuals and, therefore, various different legal challenges are to be evaluated.

Data Protection

The successful performance of AI software depends mainly on the amount and type of BD (personal and non-personal data) collected and processed. When personal data is processed, the GDPR shall apply; when the processing involves "non-personal data", Regulation (EU) 2018/1807 shall apply.

Although the main goal of the GDPR is to grant data subjects full control over their personal data, some activities behind AI systems (ie, BD analytics) may be in conflict with such goal. However, the increasing availability of personal data raises the possibility of carrying out different types of processing activities, some of which are not even foreseeable. This approach violates the principle of data minimisation set forth in Article 5 of the GDPR, which requires controllers to process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

The use of AI software introduces additional risks. The processing of inaccurate data may lead to a wrong decision, which could lead to social discrimination or intrusion into people's personal lives.

Moreover, a systematic analysis of BD, through sophisticated AI software, could also lead to a profiling of data subjects that is (in most cases) not grounded on the appropriate legal basis (ie, their consent) and to discrimination against such individuals based solely on automated (and often opaque) decision-making processes,

which are – in any case – forbidden by Article 22 of the GDPR.

Although the GDPR does not directly deal with BD and AI, it sets forth general provisions aimed at addressing the potential risks arising from the unlawful processing of personal data, profiling and automated decision-making, by referring to the controller's accountability with respect to all the necessary assessments in order to consider such processing operations "privacy compliant".

AI and Liability

Existing national liability provisions are not well suited for handling claims for damages caused by AI-enabled products and services. In fault-based liability claims, the damaged party is required to identify who to sue and explain the fault, the damage and the causal link between the two in detail. When AI is involved, this might not be easy due to the specific characteristics of AI, including complexity, autonomy and opacity, which may make it difficult or prohibitively expensive for victims to meet their burden of proof.

In order to enable victims to claim compensation for damages, the AI Liability Directive – which applies to damages caused by any type of AI system (both high-risk and non-high-risk) – introduces (inter alia) the presumption of causality measure (Article 4 of the AI Liability Directive).

Considering that it can be challenging for claimants to establish a causal link between non-compliance and the output produced by the AI system or the failure of the AI system to produce an output that gave rise to the relevant damage, Article 4 provides for a targeted rebuttable presumption of causality that can be considered "the least burdensome measure" to address the need for fair compensation of the victim.

However, notwithstanding the presumption of causality (which may find application when it can be considered likely that the given fault has influenced the relevant AI system output or lack thereof, to be assessed on the basis of the overall circumstances of the case), the claimant still has to prove that the AI system (ie, its output or failure to produce one) gave rise to the damage.

Articles 4 (2) and (3) of the AI Liability Directive distinguish between:

- claims brought against the provider of a high-risk AI system or against a person subject to the provider's obligations under the AI Act – in this case, the defendants' compliance with the obligations set forth therein have to also be assessed in light of the risk management system and its results under the AI Act; and
- claims brought against the user of such systems.

Article 4(4) of the AI Liability Directive establishes an exemption from the presumption of causality in the case of high-risk AI systems if the defendant proves that the damaged party has sufficient evidence, expertise or information to prove a causal link between the non-compliance and the harm suffered.

Conversely, in the case of non-high-risk AI systems, Article 4(5) of the AI Liability Directive establishes a condition for the applicability of the presumption of causality, whereby the latter is subject to the court determining that it is excessively difficult for the claimant to prove the causal link.

BD and IP

Under the Italian legal system, BD and the results obtained from the processing thereof are not specifically regulated and protected, even

under the legislation on copyrights (Italian Law 633/1941 – the Copyright Law) for the following reasons.

Database as an intellectual creation of the author

Articles 1, 2(9) and 64-quinquies of the Italian Copyright Law provide for legal protection of the expressive form of databases (and not their content), provided that such database meets the requirement of creativity, which can be inferred from the choice or the systematic and methodical arrangement of the material within the database.

Considering that the BD collection process is characterised by an indiscriminate and systematic collection of data originating from many different sources, such datasets can hardly be considered "creative" since the author, in such process, lacks the possibility of choosing which data to collect and determining its arrangement within the database.

"Non-creative" databases

Articles 102-bis and -ter of the Italian Copyright Law provide for the protection of "non-creative databases" through a sui generis right: the person who has made significant investments in the establishment of the database has the right to prohibit the extraction from the database and its re-utilisation.

Given that the activity of collecting BD is the product of an automatic collection from diversified sources such as sensors or machines, it may not be the object of a significant economic investment or the result of a "significant investment". Therefore, it seems difficult to consider BD datasets as non-creative databases.

5. Internet of Things

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

The concept of the Internet of Things (IoT), as clarified by Working Party 29 in its Opinion 8/2014, refers to an infrastructure in which billions of sensors embedded in common everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities.

There is no specific regulatory framework applicable to such technologies, at neither the European level nor the national level.

However, considering that the IoT is based on the collection of data and the interconnection of objects, which necessarily involves the transmission of signals between the objects themselves, the legislation applicable to the IoT includes:

- the GDPR and the Privacy Code, since the data processed may identify, directly or indirectly, the data subjects;
- Directive 2002/58/EC (e-Privacy Directive), implemented at the national level by Italian Legislative Decree No 259/2003 and recently amended by Italian Legislative Decree No 207/2021; and
- Directive (EU) 2018/1972 establishing the European Communications Code, implemented by Italian Legislative Decree No 207/2021, since the latter establishes an authorisation regime for the use of frequencies used by IoT technologies that, in compliance with the principle of proportionality, aims to ensure

"the development of innovative business projects".

Moreover, reference shall be made to the Data Act, which is a key pillar of the EU strategy for data and will ensure fairness by setting up rules regarding the use of data generated by IoT devices.

IoT and Data Protection Challenges

In the context of the development of IoT-based projects, attention shall be paid to the potential legal issues associated with the unlawful processing of data deriving from such use.

The interconnection of objects and systems involves the collection, recording and processing of personal data from users who are often unaware of it. In particular, such interaction between IoT objects generates data flows that can hardly be managed with the traditional tools used to ensure the adequate protection of data subjects' interests and rights. Therefore, in the absence of the possibility to effectively control how objects interact with one another, it may become extremely difficult for data subjects to control the generated data flow, to express valid consent for their processing and to control its subsequent use.

To this end, to protect the rights and freedoms of data subjects with regard to the processing of their personal data, companies wishing to develop IoT systems must, in general terms, comply with the provisions of the GDPR and the Privacy Code and, in particular:

- fulfil the necessary obligations provided for by the GDPR and guarantee an "informational self-determination" to data subjects, ensuring that they:
  - (a) are aware of the risks that may arise from the direct or indirect use of smart objects, in order to assess their impact on their privacy;
  - (b) have the ability to control and monitor the collection and processing of their personal data; and
  - (c) are aware of possible uses/abuses of their personal data by third parties, outside their sphere of action;
- ensure that data subjects do not give consent based on a lack of information and not for all the purposes actually pursued, therefore being aware of all the purposes;
- ensure that data is only used for such purposes and not for other purposes that are unknown by data subjects;
- ensure compliance with the GDPR's obligations (eg, carrying out a data protection impact assessment, when necessary; ensuring that devices are secure by design and default; appointing a data protection officer);
- make an assessment of the privacy roles of the parties involved in the processing, considering that the IoT context relies on the coordinated intervention of a significant number of stakeholders (ie, device manufacturers; data aggregators; application developers; social platforms; device lenders or renters); and
- implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, considering that the greatest risks that may arise are related to the theft or unlawful use of data.

In this regard, extensive safeguards are requested in the IoT sector, from the physical security of the device and the interconnected device, to the granting of confidentiality, integrity and availability of the information acquired, stored, processed or transmitted by the devices.

To this end, during 2022, the International Organization for Standardization (ISO) together with the International Electrotechnical Commission (IEC) published ISO/IEC 27400:2022, which will be followed by other ISO standards applicable to the IoT sector during 2023.

The new ISO provides guidelines on risks, principles and controls for the security and privacy of IoT solutions.

Security System

Considering the security risks that IoT products and software may present, the EU Commission adopted the "Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020" (Cyber Resilience Act – CRA), which aims to safeguard consumers and businesses buying or using products or software with a digital component by introducing mandatory cybersecurity requirements for manufacturers and retailers of such products.

The CRA would complement existing legislation, specifically the NIS2 Framework, and apply to all products connected directly or indirectly to another device or network, except for specified exclusions such as open-source software or services that are already covered by existing rules, which is the case for medical devices, aviation and cars.

The CRA will guarantee:

- harmonised rules for products or software with a digital component that is intended to be placed on the market;
- a framework of cybersecurity requirements governing the planning, design, development and maintenance of such products, with obligations to be met at every stage of the value chain; and
- an obligation to meet a duty of care for the entire lifecycle of such products.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

Pursuant to the current applicable legal framework, audio-visual media services are intended to be all mass media – ie, media intended for reception by a substantial proportion of the public, placed under the editorial responsibility of a media service provider, the main purpose of which is the provision of programmes aimed at informing, entertaining or educating the general public, via electronic communications networks, encompassing activities that are primarily economic. The provision of such services is subject to the obtainment of an authorisation, granted following a defined procedure and provided that certain requirements are met, which vary depending upon the services provided.

The Italian legal framework was updated in December 2021 with Italian Legislative Decree No 208/2021, which transposed Directive (EU) 2018/1808 and amended Italian Legislative Decree No 177/2005 (the Consolidated Law on Radio and Audio-Visual Media Services – AVMS Code). Specific provisions are also provided for by various Resolutions of the Authority for Communications Guarantees (*Autorità per le Garanzie nelle Comunicazioni* – AGCOM), which establish the relevant framework for different types of services.

The AVMS Code includes the general principles for the provision of audio-visual and radio digital media services and video sharing plat-

form services, regulating different audio-visual services, such as the transmission of television programmes (linear and on-demand), radio programmes and data programmes, as well as regulating the provision of associated interactive services and conditional access services on any broadcasting platform, including audio-visual commercial communications and video-sharing platform services.

Article 2 of the AVMS Code defines the scope of application of the Italian framework for audio-visual and radio media services by providing a series of requirements (such as having the principal office in Italy, taking the main editorial decisions in Italy and having a significant presence of operators in the Italian territory) that entail being subject to the Italian provisions.

Authorisation Procedure

For the provision of linear services, the legal framework requires different authorisations, depending on the broadcasting method: the Ministry of Economic Development (MISE) is responsible for the provision of cable services and for digital broadcasting on terrestrial frequencies, while AGCOM is responsible for those services provided via satellite and other electronic means of communication (as indicated in Articles 18 and 19 of the AVMS Code). The competent authority may deny the authorisation through its own reasoned decisions, based on reasoned grounds.

In detail:

- linear audio-visual media services transmitted by cable require the operator to hold a general authorisation issued by MISE that follows the submitting of a specific form to AGCOM; and
- pursuant to AGCOM Resolution No 127/00/CONS, linear audio-visual media services transmitted by satellite require the operator to hold a general authorisation from AGCOM. Satellite authorisations issued within 60 days of application are valid for a period of six years, and are renewable. For the purposes of granting and/or renewing authorisations, Article 6 of the Resolution establishes the payment of a financial contribution by way of reimbursement of the costs of the preliminary review for the decision on the application for authorisation.

The broadcasting of audio-visual and radio media services through platforms consisting of the internet network, including broadband and mobile networks (ie, on other electronic means of communication) is permitted in both linear and on-demand services.

These services are subject to different legal disciplines: in one case it is necessary to obtain a specific authorisation title, while in the other a general authorisation is required. For both of them, annual revenues "deriving from advertising, teleshopping, sponsorships, contracts and agreements with public and private entities, public subsidies and pay television offers" are limited, and must exceed EUR100,000.

In detail:

- pursuant to AGCOM Resolution No 606/10/CONS, linear or radio audio-visual media services transmitted by other electronic means of communication (ie, web-TV, IPTV and mobile TV) require the operator to hold a general authorisation from AGCOM. The activity covered by the authorisation request may be started following the 60-day period in which it is due to receive silent consent; and

- pursuant to AGCOM Resolution No 607/10/CONS, for on-demand audio-visual services, the operator is required to submit a Certified Notification of Initiation of Activities (SCIA) to AGCOM, as provided by AGCOM's application form. The activity covered by the authorisation request may be commenced from the date of submission of the certified report to commence activity.

With regard to these two latter points, authorisations are valid for a period of 12 years and are renewable. Article 6 of both the abovementioned Resolutions prescribes that the person applying for the issue/renewal of the authorisation is required to make a payment to AGCOM, by way of reimbursing the costs of reviewing the application for authorisation.

Video-sharing Platform Services

Video-sharing platform services are regulated by Chapter II of the Title IV of the AVMS Code and have the same obligations as audio-visual service providers in respect of advertising and other content restrictions, considering the limited control they can exercise over advertising on their platforms that is not marketed, sold or arranged by them. In this regard, AGCOM is entrusted with the power, through its regulations, of defining and adopting measures by which the free circulation of programmes, user-generated videos and audio-visual commercial communications conveyed by a video-sharing platform may be limited for the purpose of combating incitement to racial, sexual, religious or ethnic hatred, and the violation of human dignity.

Furthermore, providers of video-sharing platforms established in Italy pursuant to Article 41(1-5) of the AVMS Code shall be governed by Articles 3, 4, 5 and 14 to 17 of Italian Legislative Decree No 70/2003 on certain legal aspects of information society services in the internal market, in particular electronic commerce.

On a final note, online content sharing platforms are also regulated by Directive (EU) 2019/790 (Copyright Directive) which is transposed at the national level by Italian Legislative Decree No 181/2021 and aims to regulate and standardise the legislation of member states with regard to:

- exceptions to/limitations on copyright, the digital environment and the cross-border environment;
- the improvement of licensing procedures to ensure broader access to content; and
- the inclusion of guarantees of proper functioning of the market for copyright.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

The Italian legal framework regarding telecommunications rules was updated in December 2021 with Italian Legislative Decree No 207/2021 (EECC Decree), which transposed Directive (EU) 2018/1972 at the national level and established the European Electronic Communications Code, combining the previous rules on electronic communications into a single regulatory text.

The new features introduced by the EECC Decree include new definitions of electronic communication services, which take into account the technological and market developments and allow over-the-top (OTT) services to be brought within the scope of the EECC Decree.

Technologies and Services Falling Within the Scope of the EECC Decree

Article 1 of the EECC Decree entirely replaced Articles 1–98 of Italian Legislative Decree No 259/2003 and subsequent amendments (the Electronic Communications Code, or Italian ECC). Pursuant to Article 1 of the EECC Decree, which amended the former Article 2, the following technologies fall within the scope of the Italian telecommunications rules:

- electronic communications networks and services for public use, such as phone centres, internet points, internet service providers' products, telephone traffic resale, Voice over Internet Protocol, fax services, public telephone services, public network supplies, satellite services, networks used for the broadcasting of sound and television programmes, and cable television networks;
- closed user groups, defined as a plurality of subjects linked by a stable professional or common user interest so as to justify the internal requirements of confined communication, satisfied by means of exclusive, closed electronic communications networks and services;
- electronic communications activities for private use, such as radio amateurs and low-power equipment to support companies (eg, radio stations used for taxis, security services, civil protection associations);
- submarine electronic communications installations; and
- radio-electric services.

With particular regard to the technologies falling within the scope, the EECC Decree extends the definition of "electronic communication service" to include:

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

The EECC Decree defines an "interpersonal communications service" as a service, normally concerning payments, that enables the direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine their recipient(s), including services such as traditional voice calls between two persons, email messages, messaging services and group chats. In this way, most of the so-called OTT companies are covered by the definition, which does not include services enabling interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service.

Requirements

Pursuant to Article 11 of the EECC Decree, which replaced the former Article 25, the provision of electronic communication networks or services (other than number-independent interpersonal communications services number), without prejudice to the specific obligations referred to in Article 13 of the EECC Decree, shall be subject to a general authorisation issued by MISE following the submission of a specific SCIA that shall include:

- the applicant's declaration of its intention to start supplying specific services;
- general information about the operator's organisation (nationality, registered office, VAT number, contact information, details of the legal representative); and

- technical information such as a description of the network or service to be provided.

Once the declaration has been filed, the applicant may immediately start providing the service indicated in the SCIA.

Within 60 days, MISE will issue a reasoned resolution prohibiting the company from continuing its activity and revoke the authorisation if it finds out that the necessary requirements are not satisfied.

The applicant is also required to be registered in the Register of Communications Operators kept by AGCOM, and to pay the relevant administrative costs.

The general authorisation has a duration of 20 years and is renewable for no more than 15 years by submitting a new SCIA to MISE.

After consulting with AGCOM on matters falling under its competence, MISE may define – by publishing specific regulations in accordance with the requirements of the EECC Decree – detailed schemes for specific regimes for the general authorisation for particular categories of networks or services, with which the company intending to offer these networks or services must comply.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

"Technology agreement" is a broad term that can cover several kinds of services (eg, licensing, maintenance, outsourcing or even the development of software; selling and purchasing of hardware; providing cloud computing services; engineering). Moreover, with the advancement and rapid development of technology and services provided via the internet, such definition does not cover homogeneous categories of services and agreements, and has become increasingly dynamic. New developed technologies include machine learning, 5G, AI, IoT, cloud and cognitive systems designed to predict and detect errors in software.

Considering the above, one of the main challenges is often the impossibility/difficulty to include these agreements within the categories and institutions of the Italian civil law system.

Indeed, since the technology agreements, lato sensu intended, do not have a precise definition, it cannot be possible to refer to a specific regulation under Italian civil law: they are not typical/standard contracts – in the technical legal sense provided under the Italian civil law system – and, therefore, are not subject to a specific legal framework.

For this reason, when negotiating and drafting a technology agreement, it is important to appropriately qualify the characteristics of the services or technologies to be provided in order to identify the applicable legal framework, which may include the joint application of different types of contracts and their specific provisions; with a complete and well-drafted technology agreement, some legal issues can be prevented.

As a general rule, the provisions of the Italian Civil Code regarding purchase agreements (*vendita*), service contracts (*appalto di servizi*) and supply contracts (*somministrazione*) shall apply, even though a specific assessment on a case-by-case basis shall always be made.

Moreover, it is necessary to consider further issues that are relevant to the regulation of technology agreements, such as:

- intellectual and industrial property matters;
- personal data protection;
- representations and warranties of the parties;
- tax matters (eg, connected to the e-commerce sector);
- consumer protection matters (eg, the Italian Consumer Code, recently reformed by Italian Legislative Decree No 173/2021, which implemented Directive (EU) 2019/770, which regulates certain aspects about the supply of digital content and digital services between consumers and sellers); and
- the application of mandatory provisions related to health and safety in the workplace (to be deemed applicable when the services to be rendered may entail on-site activities) and to employment, accident prevention, wage and social insurance regulations.

IP

In Italy, software and computer programs are protected primarily by the Italian Copyright Law, since they are considered works of intellect, pursuant to Article 2575 of the Italian Civil Code. Considering this, it shall be necessary to guarantee the protection of the software and the relevant IP rights, whether pre-existing or specifically created as a result of commissioning the development.

Data Protection

When the technology solutions entail the processing of personal data, the parties shall comply with the data protection legislation that is applicable in Italy, in particular the GDPR and the Privacy Code, such as by:

- appointing the contractor as processor pursuant to Article 28 of the GDPR;
- specifying the security obligations of the parties;
- defining the liability regime of the parties; and
- limiting the transfer of personal data outside the EU, unless adequate safeguards are put in place.

Therefore, in order to provide requested technology solutions, the service provider may be required to satisfy specific requirements under Italian law (eg, declarations and certificates aimed at affirming and demonstrating compliance with anti-bribery, anti-money laundering and anti-corruption provisions). Further requirements may be imposed when the client is an Italian public entity.

Technology Agreements Related to Specific Industries

The technological evolution has an impact in various industries that are also regulated by dedicated provisions, such as banking, insurance and public administration.

In the banking sector, new technologies (such as AI, machine learning, cloud, robotics, Application Programming Interfaces and cybersecurity) are going to be frequently used, with a wide variety of agreements (eg, outsourcing and complex services agreements, development and licensing agreements, collaboration agreements, cloud services agreements, reseller agreements and marketing agreements). Therefore, in various specific industries, such as the banking sector, the national and European regulators prescribe strict standards, requirements and indications that companies must meet (eg, cybersecurity, regulatory compliance and service continuity). Greater restrictions could be identified on the

basis of the sector involved and the legal issues considered.

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

The Italian legal framework in relation to the delivery of trust services, the use of electronic signatures and digital identity schemes is set forth at the European and national level with particular reference to Regulation (EU) 910/2014 (eIDAS Regulation) and Italian Legislative Decree No 82/2005 (as subsequently amended – CAD).

The eIDAS Regulation aims to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the EU.

In Italy, the regulation is set forth by the CAD, the provisions and related technical rules of which apply to public administrations, public service operators and public control companies. Moreover, pursuant to Article 2(3) of the CAD, its provisions concerning, inter alia, electronic documents, electronic signatures, the reproduction and storage of electronic documents, digital domicile and electronic communications also apply to private individuals.

The Agency for Digital Italy (*Agenzia per l'Italia Digitale* – AgID) plays a key role in the implementation and enforcement of the CAD rules.

Trust Services

In the eIDAS Regulation, a trust service is defined as an electronic service (normally provided for remuneration) consisting of:

- the creation, verification and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services;
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.

A qualified trust service is a trust service that meets the requirements laid down in the eIDAS Regulation and provides the relevant guarantees in terms of security and quality; therefore, the qualified services provided are characterised through the use of the EU trust mark for qualified trust services. In Italy, such providers are permitted to provide qualified trust services pursuant to Article 29 of the CAD and are supervised by the AgID, which publishes the list of trust service providers established in Italy, together with information on the relevant services.

Electronic Signatures

The legal framework regulates different types of electronic signatures (simple, advanced, qualified and, in Italy, the digital signature defined by Article 1(1)(s) of the CAD), which have linked different legal effects and add consequent different value to the electronic documents to which they are affixed.

In this regard, the "simple" electronic signature provides a lower level of legal certainty, since, in any legal proceedings, the suitability of the document to which it is affixed to satisfy the requirement of written form and its evidentiary

value are freely assessable in court, in relation to the characteristics of security, integrity and unchangeability. However, pursuant to Article 25(1) of the eIDAS Regulation, an electronic signature shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic signatures.

Different and greater legal effects of advanced and qualified electronic signatures, on the other hand, can be attributed to the following, in particular.

- As provided for by Article 20(1-bis) of the CAD, their ability to enable the electronic document to satisfy the requirement of written form as well as the particular effectiveness of such document envisaged by Article 2702 of the Italian Civil Code. Their legal effectiveness is guaranteed, since these signatures are considered reliable as to the identity of the signatory, and the private contract is full evidence (until an action of fraud) of the declaration's provenance from the person who signed it, if the person against whom the private contract is produced recognises the signature, or if it is legally considered as recognised.
- Their probative value and the regime of burden of proof, to be understood as the identification of the person who, in the event of a dispute, must provide evidence to prove the validity or invalidity of the disputed signature.

In this regard, there is a difference between advanced electronic signatures and qualified (and digital) electronic signatures:

- when an advanced electronic signature is used, the party to whom the signature relates may disown it, and it is the party wishing to avail itself of the legal effects of that signature which has to prove compliance with the legal requirements; and
- when a qualified electronic signature is used, pursuant to Article 20(1-ter) of the CAD, the signature is presumed to be attributable to the holder of the electronic signature, unless said holder proves otherwise, and thus the burden of proof is reversed.

Furthermore, in light of the greater security they can guarantee with regard to the integrity and provenance of the document, qualified and digital signatures produce broader legal effects:

- Article 25(2) of the eIDAS Regulation states that "A qualified electronic signature shall have the equivalent legal effect of a handwritten signature";
- they can be further used for the signing of the categories of acts referred to in Article 1350 of the Italian Civil Code (so-called contracts with written form ad substantiam), which must be stipulated in the form of a public deed or private deed, under penalty of nullity; and
- pursuant to Article 25(3) of the eIDAS Regulation, there is a principle of mutual recognition of qualified electronic signatures in that, if "based on a qualified certificate issued in one Member State, it shall be recognised as a qualified electronic signature in all other Member States".

Digital Identity

The Public Digital Identity System (SPID) has been implemented in Italy since 2019, allowing citizens to access the online services of public administrations and private entities with a single digital identity, in a unique, safe and secure manner. The service is provided by a list of authorised

identity providers, which are entities accredited by AgID that, in compliance with the rules issued by AgID, provide digital identities and manage user authentication.

With Determination No 157/2020, AgID published the "Guidelines for the electronic signing of documents" pursuant to Article 20 of the CAD, recognising the possibility for citizens (ie, natural persons) to sign deeds and contracts with SPID and, therefore, regulating a fifth type of electronic signature: the electronic signature with SPID, which is recognised as having the same legal value as a handwritten signature. The SPID Guidelines allow SPID to be used in accordance with Article 20(1-bis) of the CAD, pursuant to which an electronic document satisfies the requirement of written form and produces the effects referred to in Article 2702 of the Italian Civil Code.

Furthermore, with Determination No 318/2019, AgID has published the "Guidelines for the issuance of digital identity for professional use", which identify the procedures to be followed by identity providers when issuing identities for professional use, allowing the data of the organisation for which one is acting on a service made available by a service provider to be conveyed through SPID in addition to the data of the individual. SPID credentials for legal persons must mandatorily be requested by the company's legal representative who, once in possession of such credentials, may request the issue of additional credentials for professional use for persons authorised to operate on behalf of the company.

Morri Rossetti e Associati provides integrated consultancy to Italian and international clients in a variety of legal and tax matters. The TMT and data protection department operates through a multidisciplinary team of professionals specialising in multiple areas of law (corporate and commercial, IT, media, data protection, cybersecurity, tax advisory and tax compliance), providing assistance in the telecommunications, media and technology, digital innovation, e-commerce and online advertising sectors, with a particular focus on national, EU and international regulatory developments. The team is able to offer highly innovative and tailor-made solutions, together with a strong sensitivity and ability to understand the opportunities and the business models of such sectors, as well as the legal and tax-critical features of the technological evolution. Recent clients include leaders in the data centre market, clients operating in the programmatic advertising market, and a number of start-ups operating in different sectors.

Authors



Carlo Impalà is a partner at Morri Rossetti and head of the TMT and data protection department. He is a member of the Italian Bar and a certified Data Protection Officer. His practice focuses on corporate and commercial law, extraordinary corporate transactions, and the preparation and implementation of corporate governance and compliance models (in particular with reference to data protection law). He has particular expertise in drafting and negotiating national and international commercial agreements, with a specialisation in antitrust and regulatory profiles, mainly in the automotive, ICT, insurance, fashion, organised large-scale distribution and advertising sectors. Carlo is a member of national and international professional associations and working groups, and has written several publications on corporate law and corporate compliance.



Giorgia Valsecchi is an associate at Morri Rossetti and works within the TMT and data protection department on law and regulation applicable to privacy and data protection, internet, online publishing and advertising, e-commerce and information technology. She also focuses on the negotiation and drafting of commercial contracts in different sectors. Giorgia qualified as a lawyer in 2020, and is a member of the Italian Bar Association in Milan.



Giulia Castelli is an associate at Morri Rossetti and works within the TMT and data protection department, with a focus on the regulation applicable to privacy and data protection, the telecommunications sector and information technology. Before joining the firm, she did an internship in the business department of a multinational television broadcasting company, dealing with contractual compliance. Giulia qualified as a lawyer in October 2022, and is a member of the Italian Bar Association in Milan.



Jun Jie Yang is a junior associate at Morri Rossetti and works within the TMT and data protection department, providing legal assistance to Italian and foreign companies in corporate and commercial law, the regulation applicable to internet, telecommunications, ICT, media and online advertising and data protection law. Before joining the firm, Jun Jie started her professional experience in a Beijing-based business advisory firm.

Morri Rossetti

Piazza Eleonora Duse, 2
20122
Milan
Italy

Tel: +39 02 7607 971
Fax: +39 02 7607 97206
Email: Carlo.Impala@morrirossetti.it
Web: www.morrirossetti.it

MORRI ROSSETTI

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