COUNTRY COMPARATIVE GUIDES 2021

The Legal 500 Country Comparative Guides

Italy
TECHNOLOGY

Contributing firm

Morri Rossetti e Associati

Carlo Impalà

Partner and Head of TMT & Data Protection Department | carlo.impala@morrirossetti.it

Giorgia Valsecchi

Associate, TMT & Data Protection Department | giorgia.valsecchi@morrirossetti.it

This country-specific Q&A provides an overview of technology laws and regulations applicable in Italy.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

ITALY
TECHNOLOGY

1. What is the regulatory regime for technology?

There is no specific regulatory regime for technology per se in Italy. The invention, realisation, use, trade of technology and other related aspects are regulated under various different laws and regulations depending on the area involved. Consequently, technology companies must comply with various different sets of legislation on a case-by-case basis. Moreover, some areas falling within the scope of technology are specifically regulated, as also better indicated in the following sections (e.g. electronic communications, e-commerce, software and databases) while others, apart from a few instances of tailor-made legislation (e.g. Artificial Intelligence, Internet of Things, etc.), are regulated by applying general rules and principles applied in our legal system.

The regulatory framework for technology includes, among others:

- Electronic communications: regulated, at the European level, inter alia, by the so-called "**Telecoms Package**" (i.e. Directive 2002/19/EC, Directive 2002/20/EC; Directive 2002/21/EC and Directive 2002/22/EC) and by Directive (EU) 2018/1972, establishing the European Electronic Communications Code (which has yet to be transposed in Italy) and, at the national level, by Legislative Decree No. 259/2003 ("**ECC**") which implemented the EU regulatory framework established through the Telecoms Package.
- With regard to the European Electronic Communications Code, the Ministry of Economic Development ("**MISE**") has launched a public consultation procedure, which was concluded on June 18, 2021, concerning the draft legislative decree transposing Directive (EU) 2018/1972;
- Information society services, and in particular electronic commerce: regulated by Directive 2000/31/EC of the European Parliament and the Council ("**E-commerce Directive**"), implemented at the national level by Legislative Decree 70/2003 which sets forth rules governing liability on the part of internet service providers (i.e. access, caching and hosting providers);
- Data protection: regulated by the General Data Protection Regulation (EU) 2016/679 of 27 April 2016 ("**GDPR**"), followed by the adoption, at the national level, of Legislative Decree No. 101/2018 which amended Legislative Decree No. 196/2003 ("**Privacy Code**");
- Cybersecurity profiles: regulated by Directive (EU) 2016/1148 on the security of networks and information systems ("**NIS Directive**"), transposed into Italian legislation through Legislative Decree No. 65 of 18 May 2018 (also known as the "**NIS Legislative Decree**"), in force since 24 June 2018;
- Software and databases: regulated by Italian Law No. 633 dated 22 April 1941 (known as the "**Copyright Law**");
- Cybercrimes and technology–related offences: regulated and punished by the Italian Criminal Code and, in relation to the administrative liability of legal persons, by Legislative Decree No. 231/2001.

2. Are communications networks or services regulated?

Yes. The European legislative framework for communications networks and services has been laid down by the Telecoms Package, implemented at the national level by the ECC, which reorganised the sector, recognising and harmonising the regulations in force on electronic communications networks and services, for both public and private use.

Article 3 of Directive 2002/20/EC of 7 March 2002 on the authorisation of electronic communications networks and services provides that Member States shall ensure the freedom to provide electronic communications networks

and services.

The ECC honours the general principle that the provision of networks and services is free, thus achieving the complete opening of markets to competition by removing the remaining obstacles existing under the previous system (*e.g.* the extension of the general authorisation regime to all types of networks and services and the consequent abolition of the individual licence regime).

Pursuant to Article 1(1)(dd) of the ECC, electronic communications networks include transmission systems and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, networks used for broadcasting sound and television programmes, electricity transmission systems, to the extent that they are used for the purpose of transmitting signals, and cable TV networks, irrespective of the type of information conveyed.

Pursuant to Article 1(1)(gg) of the ECC, electronic communications services are services normally provided in exchange for remuneration, which consist entirely or mainly of the conveyance of signals on electronic communications networks, including telecommunications services and transmission services through networks used for broadcasting, but excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; the definition of electronic communications services also excludes information society services, as defined by Article 2(1)(a) of Legislative Decree No. 70/2003, which do not consist entirely or mainly of the conveyance of signals on electronic communications networks.

3. If so, what activities are covered and what licences or authorisations are required?

The ECC establishes comprehensive regulation of the sector, regulating, *inter alia*, (i) the means by which both network provision and electronic communications services may be permitted, (ii) the rights of use of radio frequencies and numbers, and (iii) electronic communications networks and infrastructures and the multiplicity of services related thereto (so-called "access and interconnection").

The ability to operate as a communication provider is generally subject to a general authorisation issued pursuant to Article 25 of the ECC by MISE following the submission of a specific Certified Notification of Initiation of Activities ("***SCIA***") including the applicant's declaration of its intention to start supplying specific services, as well as general and technical information about the company.

Once the declaration has been filed, the applicant may immediately start providing the service indicated in the SCIA. Within 60 days, if MISE finds out that the necessary requirements are not satisfied, it issues a reasoned resolution prohibiting the company from continuing its activity and revokes the authorisation.

The applicant is also required to be registered in the Register of Communications Operators ("**ROC**") kept by AGCom.

Please see answers to questions no. 2 and no. 3 with regard to limitations on the above-mentioned general authorisation regime.

4. Is there any specific regulator for the provisions of communications-related services?

Yes. The Authority for Communications Guarantees ("**AGCom**") is an independent authority that ensures fair competition among market operators and protection of users' fundamental rights and freedoms. AGCom is entrusted with regulatory, supervisory and sanctioning powers, the latter in the event of violations of the sector-specific legal framework.

The Competition and Market Authority ("**AGCM**") which is an independent authority that (i) protects competition and consumers; and (ii) determines whether there is a conflict between market operators. AGCM is entrusted with consultative and reporting powers as well as investigative, inhibitory and sanctioning powers.

AGCom and AGCM cooperate with each other, and at times their areas of competence overlap. This is due to the fact that pluralism of information (guaranteed by AGCom) cannot exist without pluralism of the market (guaranteed by AGCM).

Finally, MISE is also in charge of a number of important issues, dealing with the organisation and management of State functions in the field of industry, energy and commerce. The main sectors of interest refer to the secondary sector and can be grouped into three thematic areas: development of the production system, foreign trade and internationalisation of the economic system, communication and information technologies. MISE has various different powers including (i) national

and international regulatory powers; (ii) authorisation powers, with particular regard to the issuance of general authorisations to communication providers; (iii) supervisory and sanctioning powers; and (iv) administrative powers (*e.g.* approval of the frequency allocation plan).

5. Are they independent of the government control?

AGCom and AGCM are independent authorities even though they cooperate with the government by providing opinions in their respective areas of competence.

MISE is not independent since it is part of the government structure.

6. Are platform providers (social media, content sharing, information search engines) regulated?

Yes. Platform providers are regulated by the E-commerce Directive, implemented at the national level by Legislative Decree No. 70/2003, which sets forth a legal framework for governing the liability of operators providing information society services.

Information society services, as also indicated in Recitals 18 to the E-commerce Directive, include a wide range of economic activities which take place online (*e.g.* services which entail (i) selling goods online; (ii) offering online information or commercial communications; (iii) providing tools allowing for search, access and retrieval of data; (iv) the transmission of information via a communication network, (v) providing access to a communication network or (vi) hosting information provided by a recipient of the service).

Legislative Decree No. 70/2003, in accordance with the provisions of the E-commerce Directive, has specifically regulated the liability of intermediary service providers regarding (i) mere conduit (Article 14) (ii) catching (Article 15) and (iii) hosting (Articles 16 and 17) services. The liability regime specifically applicable to these providers is separate and special compared to the ordinary regime and it differs depending upon the service provided. The exemptions from liability established in the E-commerce Directive cover only cases where the activity of the information society service provider is limited to the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored, for the sole purpose of making the transmission more efficient; this activity is of a mere technical, automatic and passive nature, meaning that the information society service provider has neither knowledge of nor control over the information which is transmitted or stored.

The case law decisions, at both the European and national level, have been fundamental for purposes of better delineating and regulating the liability regime applicable to intermediary service suppliers (*i.e.* CJEU 23 March 2010, in Joined Cases C-236/08 to C-238/08, *Google France SARL, Google Inc*; Court of Rome, Civil Section IX – 15 December 2009; *Consiglio di Stato*, decision No. 3851/2021).

Moreover, Regulation (EU) 2019/1150 "*on promoting fairness and transparency for business users of online intermediation services*", in force since 12 July 2020, addresses the imbalance in bargaining power between online platforms and small businesses conducting their business on such platforms. Starting from that date, the terms and conditions of online platforms must: i) be drafted in plain and intelligible language; ii) not be changed without at least 15 days advance notice; iii) exhaustively specify any reasons that could lead to the delisting of a business user; iv) list the main parameters that determine the ranking of search results (this also applies to search engines like Google); v) include information about any ways in which a platform that sells on its own marketplace might give preferential treatment to its own goods or services; vi) be clear about the data policy of the platform – what data they collect, whether and how they share data, and with whom. In addition, Regulation (EU) 2019/1150 makes it easier for business users to seek redress in case of problems.

With reference to e-commerce platform, Legislative Decree No. 21/2014, implementing European Directive 2011/83/EU on consumer rights, has amended Legislative Decree No. 206/2005 (known as the "**Consumer Code**"), with particular reference to the provisions relating to contracts executed on a remote basis, in a location other than the business premises, with the purpose of harmonising the consumer protection provisions regarding, *inter alia*, the compulsory information to be provided to consumers and the consumer's right of withdrawal.

Online content sharing platforms are also regulated by Directive (EU) 2019/790, which is aimed at regulating and standardising the legislation of Member States with regard to (i) exceptions to/limitations on copyright, digital environment and cross-border environment; (ii) the improvement of licensing procedures to ensure broader access to content; (iii) the inclusion of guarantees of proper functioning of the market for copyright. In particular, with regard to online content

sharing platforms (so-called "Video Sharing Platforms"), Article 17 of the Directive clarifies the applicable legal framework by laying down specific obligations concerning the use of copyright-protected content.

In any case, platform providers carrying on business in Italy are to comply with other relevant areas of law imposing specific obligations and standards, such as the rules governing personal data protection, consumer protection, misleading advertising, audio-visual services (where applicable), competition as well as specific tax provisions, where applicable.

Particular attention shall be focused on the two new legislative initiatives proposed by the European Commission to upgrade rules governing digital services in the EU: the Digital Services Act ("**DSA**") and the Digital Markets Act ("**DMA**"). The DSA and DMA have two main goals:

a. to create a safer digital space where the fundamental rights of all users of digital services are protected;
b. to establish a level playing field to foster innovation, growth and competitiveness, both in the European Single Market and globally.

The DSA refers to digital services which include a large category of online services, from websites to internet infrastructure services and online platforms. The rules specified in the DSA primarily concern online intermediaries and platforms (*e.g.* online marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms). On the other hand, the DMA includes rules governing gatekeeper online platforms. Gatekeeper platforms are digital platforms with a systemic role in the internal market that function as bottlenecks between businesses and consumers for important digital services. Some of these services are also covered in the DSA, but for different reasons and with different types of provisions.

7. If so, does the reach of the regulator extend outside your jurisdiction?

Yes, it can. For example, Article 5 of Legislative Decree No. 70/2003 (which incorporate the provisions of Article 3(4) of the E-commerce Directive in their entirety) provides that the free movement of a given service provided by an information society provider from another Member State can be limited, through a measure issued by the judicial authority or the regulatory oversight bodies or independent authorities in charge of the relevant sector (on the basis of their area of competence), for reasons of:

a. public policy, and in particular the prevention, investigation, detection and prosecution of criminal offences, including the protection of minors and the fight against any incitement to hatred on grounds of race, gender, religion or nationality as well as against violations of human dignity concerning individual persons;
b. the protection of public health;
c. public safety, including the safeguarding of national security and defence;
d. protection of consumers, including investors.

Moreover, as provided under Articles 4 of the Legislative Decree No. 70/2003 (which incorporate the provisions of Article 3(3) and Annex of the E-commerce Directive in their entirety), an **information society provider** established in other EU Member States will be subject to Italian law with respect to the following matters: (a) copyright, neighbouring rights, intellectual and industrial property, including the protection of databases and topographies of semiconductor products; (b) the issuance of electronic money; (c) advertising pursued by undertakings for collective investment in transferable securities; (d) insurance business, as regards compulsory insurance, scope and conditions of the authorisation of the insurance entity and firms facing financial difficulty or in an irregular situation; (e) matters regulated by legislation chosen freely by the parties; (f) contracts entered into with consumers, as regards the obligations arising under those contracts; (g) the validity of contracts concerning rights in real estate where such contracts are subject to mandatory formal requirements; and (h) the permissibility of unsolicited advertising sent by e-mail.

On a final note, it should be noted that, with regard to platform providers, the applicable Italian legal regime consists for the most part in a transposition of the relevant European regulations so that a certain level of harmonisation of these rules exists at the European level.

8. Does a telecoms operator need to be domiciled in the country?

No, the operator does not need to be domiciled in Italy. Indeed, the telecoms sector has been liberalised and the capability to supply telecoms services is only subject to a general authorisation issued by MISE.

9. Are there any restrictions on foreign ownership of telecoms operators?

No. Under the Italian legislation there are no foreign ownership restrictions with regard to telecom operators.

As a matter of principle, foreign entities that provide telecom services in Italy need to follow the same authorisation procedures provided for Italian entities. However, as provided under Article 3(3) of the ECC, limitations may exist, stemming from the requirements imposed under national law regarding security, defence, civil protection, public health and environmental protection and the confidentiality and protection of personal data.

10. Are there any regulations covering interconnection between operators?

Yes, interconnection between operators is regulated by Chapter 3 of the ECC. The general framework defined by the ECC provides that operators may negotiate with each other agreements on technical and commercial provisions relating to access and interconnection. AGCom, including through the adoption of specific resolutions, guarantees that there are no restrictions that prevent operators from entering into interconnection and access agreements. Therefore, access and interconnection agreements are concluded in accordance with the regulated negotiation model, *i.e.* under the supervision of AGCom.

Article 41 of the ECC defines the rights and obligations of operators with regard to access and interconnection providing for a general principle according to which network operators have the right/duty to negotiate interconnection if requested by other operators even if they do not hold a general authorisation of the same type. This is a fundamental principle in order to ensure the interoperability of networks and the right on the part of anyone connected to a network to reach all users of its own or another network.

Moreover, the second part of paragraph 1 of Article 41 requires operators to offer access and interconnection services at terms and conditions consistent with the obligations imposed by AGCom pursuant to Articles 42, 43, 44, and 45 of the ECC and in accordance with the principles set out in Article 13 of the ECC.

11. If so are these different for operators with market power?

Yes, the Italian regulatory framework imposes different rules for operators with market power.

Interconnection between operators with market power is regulated by specific provisions of the ECC, and in particular by Articles 45 to 50bis.

It should be noted, first and foremost, that operators with market powers are identified as a result of the market analysis carried out by AGCom pursuant to Article 19 of the ECC; the market analysis is a detailed procedure governed specifically by the ECC due to the particular complexities/subtleties involved in the definition of the relevant market and the proper assessment with regard to the necessity of an *ex ante* intervention by AGCom.

AGCom, based on the market competitiveness assessment:

a. where the authority finds that a given market is not effectively competitive, shall identify the undertaking(s) with significant market power and, at the same time, impose the typical regulatory obligations deemed appropriate by introducing new remedies or upholding/enforcing those already imposed;
b. where the authority concludes that the market is competitive, it shall refrain from imposing regulatory obligations and where it has previously introduced such obligations, it shall withdraw them promptly.

Pursuant to Article 45 of the ECC, once AGCom has assessed that the relevant market is not competitive and has identified the operators with significant market power, the authority shall impose the typical regulatory obligations provided under Articles from 46 to 50*bis*. Therefore, Article 45 of the ECC serves as a link between the rules on market analysis and those on typical obligations by providing for two possible scenarios.

In the first scenario, provided under paragraph 1 of Article 45 of the ECC, once AGCom has found that there is a lack of effective competition in a relevant market due to the presence of an undertaking with significant market power, it is obliged to impose on the latter, depending on the circumstances, at least one of the typical obligations provided under Articles from 46 to 50*bis*, *i.e.* obligations of transparency, non-discrimination, accounting separation, access to and use of certain network resources, price control and cost accounting, and functional separation (the latter only as an exceptional measure).

In the second scenario, set out in paragraph 3 of Article 45 of the ECC, AGCom may, in exceptional circumstances, impose further obligations for interconnection and access in addition to those set out in Articles from 46 to 50. For the imposition of these “atypical” obligations, AGCom is required to submit a request to the European Commission, which may or may not authorise the adoption of the measures.

12. What are the principal consumer protection regulations that apply specifically to telecoms services?

The Italian regulatory framework includes special consumer protection rules specific to telecoms services. Such rules supplement the general legal framework on consumer protection set forth in the Consumer Code.

Moreover, in the field of consumer protection, AGCom carries out different regulatory activities: the rules that AGCom lays down and updates on the basis of the changing market structure mainly concern the quality of the services provided and the transparency and completeness of the information, which are elements necessary to enable users to make informed choices and to defend their rights more effectively. Special attention is also paid to the regulation of services falling within the scope of the "Universal Service", as better described below, and to the rules protecting disadvantaged groups or those in emergency situations.

Quality, transparency and completeness of the information

In a fully competitive market context, quality is one of the basic requirements of the services provided to end-users. AGCom's interventions in this area are aimed, in particular, at:

a. defining quality levels that operators must guarantee in the provision of services; pursuant to Article 72 of the ECC, AGCom issued a package of measures aimed at requiring companies that provide electronic communications services to publish comparable, adequate and up-to-date information on the quality of the services offered, thus providing end-users with an adequate tool for comparing different offers;
b. checking compliance with quality levels and the effectiveness of services; AGCom has adopted a system for measuring operators' performance based on so-called "quality indicators", meaning those aspects of services deemed most important for users' satisfaction (*g.* activation time, billing accuracy, malfunctioning rate, line drop rate on mobile networks, etc.)
c. disseminating more in-depth information and knowledge of the rules governing the service relationship between users and operators: to this end, AGCom carries out constant monitoring activities aimed at verifying the adoption and publication by each electronic communication service provider of a specific Service Charter.

The wide range of offerings in a constantly evolving technological market, such as the electronic communications market, requires a strengthening of the principles of transparency, correct information and communication, in order to guide users towards reasoned choices and make them aware of the available means of protection.

Through the "*Guidelines on communications to the public on the supply of telecommunication services*" (resolution no. 417/01/CONS) and the "*General Directive on quality and service charters*" (resolution no. 179/03/CSP), AGCom affirmed the right of users to receive complete information on legal, economic and technical modalities regarding the provision of services and laid down precise criteria (completeness, transparency, clarity and timeliness) for disclosure of information to end-users.

Universal service

Universal service is a set of services made available to all end-users at an established level of quality and accessible price, regardless of geographical location ("**Universal Service**"). The legal framework governing Universal Service is set forth in Articles 53 to 64 of the ECC, which implemented Directive 2002/22/EC on Universal Service end-users' rights relating to electronic communications networks and services.

The services subject to the Universal Service obligations are established every two years by MISE, after consulting with AGCom. Currently Universal Service includes:

a. service of providing access to the public communications network from a fixed location (Article 54 of the ECC), for voice, fax and data (at a speed of 56 kbps);
b. public telephony service (Article 56 of the ECC), which also allows for free emergency calls;
c. services for which there are economic facilities reserved for disadvantaged categories, such as low-income families (50% discount on voice fees) and deaf people (total exemption on voice fees).

Net neutrality

Regulation (EU) 2015/2120 (the "**Regulation**") introduced a new set of rules regarding net neutrality into European law, providing national regulators with new regulatory, supervisory and enforcement functions and powers to ensure users' right to an open internet

(Articles 3, 4 and 5 of the Regulation). According to the principle of net neutrality, access to the Internet must be treated in a non-discriminatory manner, irrespective of content, application, service, terminal, sender and recipient.

National regulatory authorities are required to promote the availability of Internet access at quality levels that reflect the technological progress and in a non-discriminatory manner. To this end, they may impose technical quality of service requirements and other appropriate and necessary measures on electronic communications operators and Internet access service providers.

Member States shall lay down rules on penalties applicable to infringements of Articles 3, 4 and 5 of the Regulation and shall take all measures necessary to ensure that they are implemented. In this regard, Law No. 167 of 2017, setting forth "*Provisions for the fulfilment of obligations arising from Italy's membership of the European Union- European Law 2017*", bolstered the deterrent power of AGCom's supervisory action, thanks to the introduction of a specific sanctioning regime that provides for the possibility of imposing administrative fines ranging from 120,000.00 EUR to 2,500,000.00 EUR in cases of ascertained infringement of net neutrality regulations.

Furthermore, the Regulation provides that the national regulatory authorities shall publish annual reports on supervisory activities carried out as well as the main results achieved, transmitting them to the European Commission and the European Regulators Group ("**BEREC**").

The BEREC Guidelines – published on 30 August 2016 – provide guidance for the implementation of European net neutrality rules by national authorities, with particular reference to: freedom of use of terminal equipment; technical and commercial practices, including so-called zero rating offers; traffic management measures; and transparency measures in supply contracts.

Other provisions

Consumer protection provisions include:

a. the right of withdrawal or cooling-off period, provided under Article 52 *et seq*. of the Consumer Code: in particular, the consumer has the right to withdraw from contracts executed at on a remote basis or at a location other than business premises (*g.* through e-commerce platforms, etc.). This right may be exercised, without any penalty and without the need to provide any reason, within a 14-day period starting from the execution of the contract (in case of service contracts) or within a different term applicable to the other types of contracts listed in Article 52.2 of the Consumer Code (*e.g.* sales contracts, etc.). The right of withdrawal is excluded in the cases set forth under Article 59 of the Consumer Code;
b. right to terminate: under Article 1(3) of Law No. 40/2007, which converted, with amendments, Law Decree No. 7/2007, subscription contracts concluded with operators of telephony, television and electronic communications networks, irrespective of the technology used, must provide end-users with the right to withdraw from the contract or to transfer the utility subscription to another operator without incurring time constraints, unjustified delays and/or unjustified costs; contractual obligations introduced by operators which oblige end-user to give more than 30 days' notice for exercising their termination right are null and void.

Lastly, the Italian Criminal Code also protects the secrecy of correspondence pursuant to Article 616, which provides for imprisonment in case of violation, abduction and suppression of correspondence, including in relation to computer and telematic correspondence.

13. What legal protections are offered in relation to the creators of computer software?

In Italy, software is protected primarily by Law No. 633/1941, ("*Legge sul diritto d'autore*") ("**Copyright Law**").

In particular, pursuant to Article 2(8) of the Copyright Law, computer programs, regardless of their form, are protected as long as they are "original". The protection also covers "preparatory material". On the other hand, the ideas and principles underlying any element of the program are excluded from protection.

The requirement for software protection is therefore its "originality". As is the case for most of the works protected by copyright, for software as well, the case law considers sufficient the presence of so-called "simple" creativity and states that the originality of software exists even if the work is comprised of simple ideas and notions, falling within the common heritage of experts in the field, provided that they are formulated and

organised in an autonomous way with respect to previous ones (Court of Bologna, Specialised Business Section, 8 August 2014).

As is the case for all works protected by copyright, software protection starts with the creation of the work itself. A Public Register for Software is kept at the SIAE ("*Società Italiana degli Autori ed Editori*") where all computer programmes can be registered, but the filing is for evidentiary purposes only.

The economic rights conferred on the author of software are provided under Articles 64-*bis et seq.* of the Copyright Law and consist, in particular, in reproduction, translation, adaptation, transformation, modification and distribution rights.

Implementing Directive 91/250/EEC, Article 12-*ter* of the Copyright Law provides that, in the case of software created by an employee as part of his work duties, the rights of economic use of the software are vested in the employer.

Like other works protected by copyright law, the economic rights to the software last for the life of its author and up to seventy years after his death.

Pursuant to Article 45 of the Industrial Property Code (Legislative Decree No. 30/2005), software is not patentable. However, since the provision excludes software "as such" from patentability, Italian case law admits the patentability of the computer program in which the program produces a technical effect internal to the computer and of the program that manages, via the computer, an apparatus or industrial process external to the computer. The term of the patent is 20 years from the date of the application.

14. Do you recognise specific intellectual property rights in respect of data/databases?

Yes. In Italy databases are protected by copyright.

Article 2(9) of the Copyright Law defines databases as collections of works, data or other independent elements systematically and methodically arranged and individually accessible by electronic means or otherwise.

Implementing Directive 96/9/EC, the Copyright Law offers a twofold level of protection to databases.

Firstly, databases satisfying the creativity requirement are protected by law, *i.e.* those which due to the choice or arrangement of the material constitute an intellectual creation of the author (Article 1 of the Copyright Law).

The "creativity" requirement must therefore be found alternatively (or cumulatively) in the "choice" or in the "arrangement" of the material. What must be creative is therefore the criterion of choice used by the author who, by selecting from among many data and materials, uses only some of them.

As is the case for most works protected by copyright, case law requires a "low" level of creativity, which is found whenever the author has made a choice from a sufficiently broad range of variants.

The rule makes it clear that the protection of databases is not extended to their contents and it is without prejudice to existing rights on those contents.

The economic rights conferred to the author of a creative database by Articles 64-*quinquies* and 64-*sexies* of the Copyright Law are similar in content to those provided under Articles 12 *et seq.* for other protected works, and consist mainly in the rights of reproduction, translation, distribution and communication to the public.

The second level of protection is offered by Articles 102-*bis* and 102-*ter* of the Copyright Law, which grant a one-of-a-kind right to the so-called "maker of a database", *i.e.* the person who makes significant investments toward the establishment of a database or its verification or presentation, dedicating, to this end, his/her own financial means, time and labour.

In this case, this right does not pertain to the form but rather the information contained in the database.

The constitutive element of this right consists of the investment made for purposes of obtaining, verifying and presenting the content of the database. The investment may consist in the use of financial and/or human and technical resources and it must be quantitatively or qualitatively significant.

The maker of a database shall have the right to prohibit the extraction or re-utilisation of the database, in whole or in substantial part, which right expires 15 years after 1 January of the year following the date of completion of the database (Article 102-*bis*).

The two forms of protection may coexist in the same database.

15. What key protections exist for personal data?

Key and main data protection legislation in the EU is established under the GDPR, which repealed Directive

1995/46/EC and led to a heightened harmonisation of data protection law across the EU Member States.

The GDPR has introduced a substantial change in personal data management systems based on the "accountability" principle. In particular, taking into account the nature, scope, context and purposes of processing, as well as the risks of varying probabilities and severities of possible adverse effects on the rights and freedoms of data subjects, controllers (as defined by the GDPR) shall implement appropriate technical and organisational measures to ensure and to demonstrate that processing is carried out in compliance with the GDPR. Therefore, controllers shall be responsible for ensuring and must be able to demonstrate that processing of personal data are carried out in compliance with the following rules: (i) lawfulness, fairness and transparency; (ii) limitation in purpose; (iii) data minimisation; (iv) accuracy; (v) storage limitation and (vi) integrity and confidentiality.

Moreover, Article 25 of the GDPR has introduced the principles of "Data protection by design and by default", according to which the controller shall:

a. "*both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects*" ("**Privacy by design**"); and
b. "*implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed*" ("**Privacy by default**").

In Italy, key protections for personal data are also set forth in the Privacy Code (Legislative Decree No. 196/2003 as amended by Legislative Decree No. 101/2018 in order to adapt the provisions of the Privacy Code to the changes introduced by the GDPR) which is the main Italian legislation on data protection matters.

Moreover, further Italian legislation establishes specific rules that impact data protection, including, most notably, (i) the Consumer Code; (ii) Law No. 300/1970 known as the "**Workers' Statute**"; (iii) Law No. 5/2018 known as the "**Telemarketing Law**".

In addition, rules and guidelines on the protection of personal data are also established, at the European level, by the European Data Protection Board ("**EDPB**"), which is an independent European body that contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation among the EU's data protection authorities and, at the national level, by the Italian Data Protection Authority (i.e. "*Garante per la protezione dei dati personali")* ("**Italian DPA**").

The EDPB supplemented the regulatory framework on personal data protection with rules and guidelines regulating different areas, including, by way of example and without any limitation, the following which are the most important provisions dedicated to the technology field: (i) Guidelines 8/2020 on the targeting of social media users adopted on 13 April 2021; (ii) Guidelines 02/2021 on Virtual Voice Assistants adopted on 9 March 2021; (iii) Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility-related applications adopted on 9 March 2021; (iv) Guidelines 2/2019 on the processing of personal data set forth in Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, adopted on 8 October 2019; (v) Guidelines on Automated individual decision-making and profiling for the purposes of the GDPR adopted on 3 October 2017, as last revised and adopted on 6 February 2018; (vi) Opinion 2/2010 on online behavioural advertising issued by the Article 29 Working Group (replaced by the EDBP).

The Italian DPA also regularly issues decisions on specific sectors and data protection issues, as well as recommendations and guidelines, including most notably (i) Guidelines on the processing of personal data for online profiling, adopted in 2015, (ii) Guidelines on cookies and other tracking tools still open for public use/available to the public (the current version in force is that published in 2014, but a new version is currently undergoing the public consultation procedure); and (iii) Prescriptions to providers of publicly accessible electronic communication services carrying out profiling activities, adopted in 2009. It should be noted that the decisions adopted by the Italian DPA before the entry into force of the GDPR, pursuant to Article 22(4) of the Privacy Code will continue to apply as long as they comply with the provisions of the GDPR and the Privacy Code.

16. Are there restrictions on the transfer of personal data overseas?

Yes. Under the GDPR, personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in Chapter V of the GDPR.

The GDPR provides for the following conditions, applicable in accordance with a layered approach:

a. the transfer of personal data from the EU to non-EU Countries is prohibited, unless the non-EU Country guarantees an adequate level of protection based on an adequacy decision issued by the European Commission;
b. in the absence of a decision by the EU Commission, the following adequate safeguards are required:
    i. legally binding and enforceable instrument between public authorities and public bodies;
    ii. binding company rules;
    iii. standard data protection clauses adopted by the EU Commission in accordance with established procedures;
    iv. approved Code of Conduct and certification mechanism approved in accordance with the procedure;
c. in the absence of a decision by the EU Commission and appropriate safeguards, derogations are provided in the following cases:
    i. the data subject has explicitly consented to the transfer after having been informed of the possible risks;
    ii. the transfer is necessary for the performance of an agreement concluded between the data subject and the data controller;
    iii. the transfer is necessary for the conclusion or performance of an agreement concluded in the interest of the data subject, between the data controller and another natural or legal person;
    iv. reasons of public interest apply;
    v. it is necessary to establish, exercise or defend a right in court;
    vi. it is necessary to safeguard vital interests of the data subject.

With regard to transfers to the USA, on 16 July 2020, through the so-called "Schrems II" decision, the Court of Justice of the European Union ("**CJEU**") invalidated the Decision (EU) 2016/1250 adopted by the European Commission pursuant to Article 45 of the GDPR on the adequacy of the protection provided by the EU-US Privacy Shield. The invalidity was due to the United States federal that allows public authorities to access – for national security purposes – personal data transferred from the European Union. In particular, the CJEU considered that such legislation (i) by limiting the protection of personal data, did not meet the requirements of the EU law; and (ii) did not grant data subjects enforceable legal rights against the United States authorities.

Following such decision, the EDPB:

i. on 23 July 2020, adopted the FAQ "*on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems*", stating, *inter alia,* that no grace period applied for continuing to transfer data to the USA on the basis of the Privacy Shield and therefore any transfer of personal data based on it was, to date, illegal and that nevertheless, organisations could still transfer personal data to the USA and, in general, to other non-EU countries by adopting the other mechanisms provided under the GDPR;
ii. created a task force to look into the 101 complaints lodged – in the aftermath of the CJEU Schrems II judgement – with EEA Data Protection Authorities against several controllers regarding their use of Google and Facebook services (e.g., Google Ads and Facebook Connect) which involve the transfer of personal data; and
iii. on November 2020, adopted Recommendations 01/2020 "*on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" and Recommendations 02/2020 "*on the European Essential Guarantees for surveillance measures*".

Moreover, on 19 February 2021, the European Commission launched the procedure for the adoption of the adequacy decision for transfers of personal data to the United Kingdom, under the GDPR. The publication of the draft decision constitutes the beginning of a process toward its adoption. This involves obtaining an opinion from the EDPB and a green light from a committee comprised of representatives of the EU Member States. Once this procedure is completed, the European Commission will adopt the adequacy decision.

It is worth noting that on 4 June 2021, the European Commission issued updated standard contractual clauses ("**SCCs**") under the GDPR for data transfers from controllers or processors in the EU/EEA (or otherwise subject to the GDPR) to controllers or processors established outside the EU/EEA (and not subject to the GDPR), providing for 4 different models: (i) controller to

controller transfer; (ii) controller to processor transfer; (iii) processor to processor transfer; and (iv) processor to controller transfer.

These modernised SCCs will replace the three sets of SCCs that had been adopted under the previous Data Protection Directive 95/46 EC.

With regard to the compliance profiles connected to the transfer of personal data in accordance with the new SCCs, on 21 June 2021, the EDBP adopted the final version of the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of personal data protection. The Recommendations 01/2020 are helpful to check "*Local laws and practices affecting compliance with the Clauses"* (pursuant to Clause 14 of the new SCCs) and the possible need to implement supplementary measures.

17. What is the maximum fine that can be applied for breach of data protection laws?

The maximum applicable fine is the one provided under Article 83(5) of the GDPR (administrative fine up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of total worldwide annual turnover of the preceding financial year, whichever is higher).

However, Article 83(1) of the GDPR states that supervisory authorities must impose administrative fines that must be effective, proportionate and dissuasive.

When deciding whether to impose an administrative fine and the amount of the administrative fine in each individual case, due regard shall be given to the specific criteria delineated under Article 83(2), including (a) the nature, gravity and duration of the infringement, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of harm suffered by them; (b) the intentional or negligent nature of the infringement; (c) any action taken by the controller or processor to mitigate the harm suffered by data subjects; (d) the degree of responsibility of the controller or processor, taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32 of the GDPR; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority; (g) the categories of personal data affected by the infringement.

In order to comply with the principle set forth in Article 83(1) and the criteria indicated in Article 83(2), the Article 29 Working Party (replaced by the EDPB), on October 2017, issued the Guidelines on the application and setting of administrative fines for the purposes of the GDPR.

18. What additional protections have been implemented, over and above the GDPR requirements?

Additional protections are provided under the Italian legislation for the protection of personal data, the Privacy Code, as well as in the form of measures adopted by the Italian DPA for the protection of personal data.

The Privacy Code introduces important provisions concerning issues such as (*inter alia*) information and consent regulated by the GDPR with particular regard to the provisions on minors, students, and the processing of genetic, biometric and health data, sanctions, the rights of the data subject, the usability of data acquired in breach of applicable provisions, the grant to the Italian DPA of stronger powers and additional tasks, information services and minors, the processing of special categories of data for purposes of scientific research, statistical research, historical research and important public interests, etc..

In particular, the Privacy Code includes among the additional protections granted:

a. Consent of minors in relation to information society services (Article2-*quinquies* of the Privacy Code)

The minimum age required for a minor to give consent has been lowered to 14. Below this threshold, consent must be given by the person exercising parental authority in order to be considered lawful;

b. Processing of health, genetic and biometric data (Article 2-*septies*, 100, 104 and 110 of the Privacy Code)

Consent is no longer required for the processing of health, genetic and biometric data if such data are processed for purposes of diagnosis, treatment, scientific, biomedical or epidemiological research. Given the sensitive nature of the data, it is up to the Italian DPA to provide indications on the security measures to be adopted and implemented in the processing of such data;

c. Right to inheritance of data in case of death (Article 2-*terdecie*s of the Privacy Code)

The rights relating to deceased persons may be exercised by those who have an interest of their own or are acting on behalf of the data subject, as his/her

representative or for family reasons deserving protection;

d. Alternative form of protection for the data subject (Article 140-*bis* of the Privacy Code)

If the data subject is of the view that his rights under data protection laws have been violated, he must choose which form of "protection" to activate. He may choose to lodge a complaint with the Italian DPA or, alternatively, to appeal to the competent judicial authority. One form of protection excludes the other;

e. Unwanted communications (Article 130 of the Privacy Code)

The use of automated calling or communication systems without the intervention of an operator for sending advertising or direct sales material or for carrying out market research or commercial communications is permitted with the consent of the contracting party or user.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

Cloud-based services are not subject to specific and dedicated legislation within the Italian legal framework and the same present different legal aspects to be considered (please see answers below).

Security of networks and information systems

Directive (EU) 2016/1148 on the security of networks and information systems ("**NIS Directive**"), has been transposed into our legislation through Legislative Decree No. 65/2018 (also known as the "**NIS Legislative Decree**"), in force since 24 June 2018.

The sectors falling within the scope of the NIS Legislative Decree are in fact only those expressly provided under the NIS Directive. Cloud computing services are expressly included within the scope of the new provisions as "Digital Service Providers".

Pursuant to the NIS Legislative Decree, Digital Service Providers are required, *inter alia*:

1. to identify and to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering their services;
2. to take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services that are offered within the EU, with a view to ensuring the continuity of those services;
3. to notify the competent authority or the Competent authorities or the computer security incident response teams ("**CSIRT**") without undue delay of any incident having a substantial impact on the provision of a service that they offer within the EU. Notifications shall include information to enable the competent authority or the CSIRT to determine the significance of any cross-border impact. Notification shall not make the notifying party subject to increased liability.

Personal data protection

Cloud-based services, when the entail the processing of personal data, are also subject to data protection legislation, and in particular the GDPR and the Privacy Code.

With regard to data protection issues related to cloud-based services, it is worth pointing out that, even though the data protection legislation does not provide for specific restrictions applicable to cloud-based services, the general restrictions provided under such legislation may apply. In particular, the GDPR provides for specific security obligations and also introduces limitations on the transfer of personal data outside the European Union, by prohibiting such transfer to non-EU countries unless adequate safeguards are provided. Therefore, within the context of cloud services, the geographic location of servers is important in order to comply with the provisions of the GDPR, and controllers are required to ascertain the same.

Furthermore, it should be noted that the Italian DPA has issued a guideline called "*Cloud computing: guidance for the conscious us of services".* With a view to promoting the correct use of the new methods of providing services, especially those provided through public clouds, which entail the outsourcing of data and documents (public clouds) the Italian DPA provided specific information aimed at protecting the important information-based asset/wealth consisting of personal data.

Legal qualification of the cloud computing contract

Contracts regulating cloud-based services are not specifically regulated by Italian law and they are not typical contracts – in the technical-legal sense provided under the Italian civil law system – and are not subject to

a specific and univocal legal framework.

It follows that the framework of the contractual relationship between cloud providers and users of the service can become complex, especially in the presence of elements foreign to a given legal system.

The noteworthy legal issues that may arise include, in addition to the issues related to the identification of the applicable law, under Italian law, the methods of signing cloud computing contracts which, in most cases, are executed online through subscription forms prepared unilaterally by the cloud provider. Indeed, in the Italian legal system, this method of executing a contract falls within the category of subscription contracts executed on a remote basis, outside business premises, through the use of computerised tools – and through the so-called "point and click" system.

In order to be valid, contracts executed in this manner must necessarily comply with the rules protecting the "weaker" contracting party set forth under Articles 1341 and 1342 of the Italian Civil Code, if the user is a professional user. Moreover, if the cloud user is a consumer, the provisions of the Consumer Code, contained in Articles 33 to 38, concerning the unfairness of clauses, shall apply.

Guidelines of the European Banking Authority ("EBA")

The recommendations on outsourcing to cloud service providers, dated 20 December 2017 ("**Recommendations**"), aim to clarify the EU-wide supervisory expectations if institutions intend to adopt cloud computing, so as to allow them to leverage the benefits of using cloud services, while ensuring that any related risks are adequately identified and managed. To address the specificities of cloud outsourcing, the Recommendations include, *inter alia*, (i) guidance on the security of the data and systems used and (ii) specific requirements for institutions to mitigate the risks associated with "chain" outsourcing, where the cloud service provider subcontracts elements of the service to other providers.

20. Are there specific requirements for the validity of an electronic signature?

Yes.

At the European level, the validity requirements for electronic signatures are established by Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market ("**eIDAS Regulation**").

The eIDAS Regulation regulates different types of electronic signatures, providing for the specific requirements for the validity of the same.

Pursuant to Article 26 of the eIDAS Regulation, an advanced electronic signature shall meet the following requirements: (a) it must be uniquely linked to the signatory; (b) it must be capable of identifying the signatory; (c) it must be created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and (d) it must be linked to the related data signed using such signature in such a way that any subsequent change in the data is detectable.

The qualified electronic signature is a type of advanced electronic signature, defined by the eIDAS Regulation (Article 3(1) no. 12) as a signature "*created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures*", whose requirements are regulated by Annex II and Annex I to the eIDAS Regulation, respectively.

At the national level, the legal framework is set forth in Legislative Decree No. 82/2005, as subsequently amended, the so-called "**Digital Administration Code**" ("**CAD**"), the provisions and related technical rules of which apply to Public Administrations, public service providers and public control companies. Moreover, pursuant to Article 2(3) of the CAD, its provisions concerning, *inter alia*, electronic documents, electronic signatures, reproduction and storage of electronic documents, as well as digital domicile and electronic communications also apply to private individuals.

With regard to the validity of an advance electronic signature, the requirements established under Articles 55 to 61 of the Decree of the President of the Council of Ministers dated 22 February 2013.

Moreover, the Italian framework specifically regulates another type of electronic signature called the "digital signature". The digital signature, defined by Article 1(1)(s) of the CAD as a particular type of qualified signature based on a system of cryptographic keys, one of which is public and the other private, correlated with each other, enabling the holder of the electronic signature by means of the private key and a third party, by means of the public key, respectively, to establish and to verify the provenance and integrity of an IT document or a set of IT documents.

As has also been clarified by the "Comparative analysis of the various typologies present in national and EU legislation", published in December 2019 by the **Digital Italian Agency** ("*Agenzia per l'Italia digitale*"), the various types of signatures are linked to different legal

effects and to the consequent differing value of the IT documents bearing them. This is without prejudice to the provision of Article 25(1) of the eIDAS Regulation, according to which "*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*".

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

It should be noted, first and foremost, that the term outsourcing does not identify a specific and autonomous type of contract but rather indicates a particular way of organising a company based on entrusting certain production activities (such as IT services) to subjects outside the company.

Therefore, outsourcing contracts are not typical contracts – in the technical-legal sense provided under the Italian civil law system – and are not subject to a specific and univocal legal framework.

Outsourcing contracts may consist in a transfer of individual services or in an outsourcing of a set of services, to be considered in its entirety.

Depending on the specific case and the elements characterising the case, the legal framework governing outsourcing contracts may be found in the Italian civil law provisions applicable to service contracts or in the civil law provisions applicable to the transfer of business units, given that, in this latter case, it is necessary to assess on a case-by-case basis what is meant by outsourcing and, in particular, what can actually be outsourced, with specific reference to the implementation limits linked to the lawful or unlawful nature of the specific object of a transfer of a business unit.

With regard to service contracts, the same are regulated by Article 1655 *et seq*. of the Italian Civil Code, pursuant to which a procurement contract is a contract whereby one party undertakes, through the organisation of the necessary means and management at its own risk, the performance of work or services in exchange for consideration.

Outsourcing entails the outsourcing of not only structural resources but also human resources. It follows that it is a contract characterised by a strong nexus established between the parties, which may include exclusivity clauses and a careful customisation of the service, but it does not entail an automatic transfer of any resources, since the same are already owned and organised by the provider. Moreover, Article 1406 of the Italian Civil Code provides that each party may have itself replaced by a third party in relations arising out of a contract for consideration, if the latter has not yet been performed, provided that the other party grants its consent in such regard.

Therefore, detailed contractual provisions negotiated between the parties may include a transfer of a third-party contract, when envisaged under the agreement with the latter.

On the other hand, Italian civil law establishes different rules in the event of transfer of a business or a business unit. Pursuant to Article 2555 of the Italian Civil Code, the business ("*azienda*") is the set of assets organised by the entrepreneur for the operation of the enterprise. The business may be the subject of acts of disposal of various kinds, including with reference to one or more business assets, taking into consideration, however, that the rules governing the transfer of a business – and not those governing the transfer of individual assets of the business – apply when certain requirements are met.

The rules governing the transfer of a business also apply in the case of the transfer of a particular branch of the business provided that it has organisational capacity. To this end, it is necessary and sufficient that a set of assets to be transferred be potentially suitable for use in conducting a particular business activity.

Without prejudice to the foregoing and, in any case, provided that the relevant conditions are met, when there is a transfer of a business, specific provisions apply, aimed at fostering the maintenance of the economic unity of the business.

In particular, pursuant to Article 2558 of the Italian Civil Code, unless otherwise agreed between the parties, the purchaser of the business shall take over the contracts concluded for the operation of the business which are not personal in nature, subject to the right of withdrawal of the third-party contracting party within three months of notification of the transfer and only for just cause, without prejudice to the liability of the transferor.

With regard to employees' rights in the event of transfer of a business, as a matter of principle, Article 2112 of the Italian Civil Code provides for the automatic transfer of employees guaranteeing that the employees retain all rights arising from the transferred employment relationship.

On a final note, also from a GDPR perspective, it is

worthwhile analysing which categories of personal data must be shared between the company which is outsourcing services and the outsourcer, in order to comply with the data minimisation principle.

Moreover, the applicable legal basis for the data transfer should be assessed and properly identified. In order to comply with transparency requirements, employees must be informed as regards the data transfer, as per articles 13 and/or 14 of the GDPR, as the case may be.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

The liability for malfunctions of a software program which purports to be an early form of A.I. is still a topic of debate within the European and Italian legal framework. In particular, it is currently being discussed whether the current categories of liability are adequate to govern the actions of A.I. systems.

The current general framework for governing such liability is the Product Liability Directive (85/374/EEC as amended by Directive 99/34/EC) implemented at the national level by the Consumer Code. Under this regime, if the machine is considered to be a product, the manufacturer's liability regime set out therein would apply. The injured party would therefore have to prove the damage, the defect and the causal relationship but not the fault of the manufacturer. The manufacturer, which is subject to liability, may be exonerated if it proves either the absence of a causal link or the conformity of the product.

However, this liability regime may turn out to be not entirely suitable from a standpoint of both the burden of proof imposed on the injured party and the level of autonomy of the A.I. system and predictability of actions (in the context of the legal debate, it has been argued that if the system's actions are foreseeable, the programmer or user is undoubtedly liable, but if the actions are totally random and the result of autonomous learning, then there would be no causal link to justify a strict liability regime).

The need to provide an answer to these questions was also perceived by the European institutions (the noteworthy adopted documents include (i) the "*White Paper on Artificial Intelligence*" published by the European Commission of 19 February 2020; (ii) the Draft Report with recommendations to the Commission on a Civil liability regime for artificial intelligence, which includes a motion for a European Parliament Resolution and detailed recommendations for drawing up a European Parliament and Council Regulation on liability for the operation of artificial intelligence-systems, issued by the European Parliament on 27 April 2020, and updated on 5 October 2020 (the "**Draft Report**"); and (iii) the Study – commissioned by the Policy Department C at the request of the Committee on Legal Affairs – on Artificial Intelligence and Civil Liability (published on 14 July 2020). In the above-mentioned acts, the European Institutions pointed out the need to regulate the allocation of liability for damages arising from the use of AI systems and caused by defects and malfunctions of the same, while also specifying that a complete overhaul of the general European legal framework on civil liability is not required, but rather the legislation in force should be adapted and new provisions introduced.

The Draft Report provides for a new form of liability for the party deploying the AI-system – defined as "*the person who decides on the use of AI-systems, exercises control over the associated risks and benefits from its operation*" – based on a risk-based approach differentiating between high-risk AI systems and AI-systems not defined as a high-risk AI-systems.

According to the definition provided by Article 3 (c) "high risk" means "*a significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected; the significance of the potential depends on the interplay between the severity of possible harm or damage, the degree of autonomy of decision-making, the likelihood that the risk materializes and the manner and the context in which the AI-system is being used;*".

Chapter II of the Draft Regulation governs the regime applicable to high-risk AI-systems and, in particular, provides for a strict liability regime for these AI-systems. In line with other legislation regarding civil liability in critical and high-risks sectors, the Draft Regulation provides for a compulsory insurance cover and establishes the maximum amount of compensation damages.

Chapter III, on the other hand, governs the regime applicable to other AI-systems according to which the deployer of such AI-system shall be subject to a fault-based liability for any harm or damage caused by a physical or virtual activity, device or process driven by the AI-system.

Moreover, the Draft Regulation introduces other provisions regarding damages (amount of compensation and extent of compensation), limitation period, multiple tortfeasors, aimed at reaching a balance between the protection of user rights collectively and the creation of new and innovative technologies.

Furthermore, in certain circumstances, it should be noted that the malfunction of an A.I. system may entail a criminal offence; in such case, the issue of fault will be analysed on a case-by-case basis.

Nonetheless, since it happens on a worldwide level, the question of accountability for A.I. systems and their results may raise rather difficult issues that need still to be addressed by the decision-makers both at European and national levels.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

a) obligations concerning the maintenance of cybersecurity;

The main obligations as to maintenance of cybersecurity are established under the following main legislations:

a. NIS Directive (implemented at the national level by NIS Legislative Decree) that defines the measures necessary to achieve a high level of security of networks and information systems and applies to **Operators of Essential Services** ("**OES**") (*e.* energy, oil, natural gases, air transport, railway transport, water transport, road transport, banking, financial market infrastructure, health, water supply, digital infrastructure), and **Digital Service Providers** ("**DSP**") (*i.e.* online marketplaces; online search engines; cloud computing services), as better identified therein. Both OESs and DSPs are required (i) to identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering their services; (ii) to take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services that are offered within the EU, with a view to ensuring the continuity of those services; (iii) to notify the relevant supervisory authority of any security incident having a significant impact on service continuity without undue delay;
b. Regulation (EU) 2019/881 of April 2019 which expands the role of the **European Union Agency for Cybersecurity** ("**ENISA**"), introduces a common cybersecurity certification framework covering a broad range of digital products and services and European certification schemes on information and communications technology. With regard to the measures adopted, it is worth mentioning that on 19 November 2020, ENISA published the "*Good practices in innovation on Cybersecurity under the NCSS*" (National Cyber Security Strategies);
c. GDPR, with regard to the protection of personal data, which imposes various obligations on data controllers and data processors. In terms of data security, personal data must be processed in a way which ensures security and safeguard against unauthorised or unlawful processing, accidental loss, destruction of and damage to data. In particular, Article 32 of the GDPR, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying probabilities and severities of adverse effects on the rights and freedoms of natural persons, requires data controllers and data processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including pseudonymisation and encryption of personal data;
d. Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market, implemented at the national level by Legislative Decree No. 218 of 15 December 2017, which came into force on 13 January 2018;
e. Law Decree No. 82/2021 on urgent provisions on cybersecurity, the definition of the national cybersecurity architecture and the establishment of the National Cybersecurity Agency ("**NCA**") – that redefines the national organisational structure dedicated to the governance of the cybersecurity sector and establishes the NCA granting specific regulatory powers to the same;
f. ECC that provides, *inter alia*, that the regulation of electronic communication networks and services is aimed at safeguarding, in compliance with the principle of free movement of persons and goods, the constitutionally guaranteed rights of secrecy of communications by adopting appropriate technical and organisational measures to ensure the security of publicly available electronic communications networks and services and to ensure the integrity of networks. These measures shall also be aimed

at preventing and limiting the consequences of security incidents for users and interconnected networks.

b) the criminal nature of hacking/DDOS attacks?

Hacking and DDOS attacks amounting to criminal offences are punished in Italy by the Italian Criminal Code.

In particular, the types of crime conceivable are:

- cyber fraud (pursuant to Article 640-*ter* of the Criminal Code).

Cyber fraud is committed by a person who provides himself or others with an unfair profit causing harm to other people, by altering the functioning of a computer or telematic system or by operating without permission data, information or programs contained in a computer or telematic system. A typical example of cyber fraud is phishing, which is a cyber-attack where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware;

- abusive access to a computer or telematic system (pursuant to Article 615-*ter* of the Criminal Code).

Italian law also punishes with imprisonment any person who illegally enters a computer or telematic system protected by security measures or remains there without the owner's consent. In the first case, the offender is not authorised to access the system, in the second case, there is permission to access but the offender remains in the system performing actions other than those permitted;

- unlawful possession and dissemination of access codes to computer and telematic systems (pursuant to Article 615-*quater* of the Criminal Code).

The unlawful detention and dissemination of access codes to computer or telematic systems concerns any person who illegally procures, reproduces, disseminates, communicates or delivers codes, keywords or other means to access a computer or telematic system, protected by security measures, or in any case provides indications or instructions suitable for this purpose, in order to procure a profit for himself or others or to cause damage to others;

- dissemination of equipment, devices or computer programs aimed at damaging or interrupting a computer or telematic system (pursuant to Article 615-*quinquies* of the Criminal Code).

The Italian Criminal Code punishes any person who procures, produces, reproduces, or simply makes available to others, computer programs that are designed to illicitly damage a computer or telematic system, the information, data or programs contained in it or to allow for the total or partial interruption or alteration of its operation. This category includes various types of malware such as trojans, spyware and dialers;

- damage to information, data and computer programs (pursuant to Article 635-*bis* of the Criminal Code).

The Italian Criminal Code punishes persons who cause damages computer and telematic systems. The rule provides for the imprisonment for any person who destroys, deteriorates, deletes, alters or suppresses information, data or computer programs.

These crimes are also included in the list of offences for which legal persons could be liable under Legislative Decree No. 231/2001. Articles 24 and 24-*bis* of Legislative Decree No. 231/2001 provide for the application of monetary sanctions to companies in the event that the above-mentioned criminal offences are committed by a company's managers or employees in the interest or to the advantage of the company.

24. What technology development will create the most legal change in your jurisdiction?

In light of the underlying legal issues, in terms of identifying the applicable legal framework and the consequent regulation of civil liability and compensation for damages, as well as considering the rapid and massive technological development that has characterised the sector in recent years, we believe that the most significant legal change in our jurisdiction will stem from AI systems – with particular reference to the development of robots and systems capable of developing autonomous learning.

Moreover, AI systems give rise to legal issues concerning intellectual property law and, in particular, the grant of ownership of rights arising from the creative activity of intelligent systems (such as artistic, musical or literary works) as well as data protection law in consideration of the impacts that new technologies applied to AI may have on the processing of personal data of the subjects interacting with it.

In addition, other technologies may have a significant impact on the legal framework. Particular attention shall also be paid to the strong interconnection between AI and IoT systems and 5G, meaning the new technology and fifth generation data connection standard, which will replace the current one bringing several advantages. In light of the new scenarios, even the most sophisticated generation networks will be so complex and fast that they can be controlled mainly by artificial intelligence. What is at the root of the complex legal issues expected to stem from these novel technologies is, therefore, essentially the relationship between IoT, networks and artificial intelligence.

With reference to these issues, the use and transmission of a huge amount of data that will be collected by these systems, connected to the new generation networks, certainly constitute crucial aspects which could lead to significant changes in the legal system, for which a precautionary regulation, which also addresses the fundamental area of ethics, appears to be of utmost importance.

25. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

The Italian tax regime may be considered the greatest impediment to economic development and commerce in the digital sector. By way of example, the Italian Digital Services Tax – introduced on 1 January 2020 and aimed at taxing revenues generated by the provision of certain digital services and ensuring tax fairness and fair competition – presents some criticalities that could hinder economic development and trade, for two specific reasons. First of all, since it is essentially a tax applied to revenue, it will most likely be passed on to individual users, thus penalising, at the same time, Italian companies themselves, which would consequently have lower margins. Secondly, both the revenue thresholds and the selection of the services covered by the tax make it discriminatory on the basis of nationality, in that the tax constitutes a full-fledged import duty on digital services provided by large foreign companies.

Furthermore, it is worthwhile to point out that, in consideration of the rapid development of new technologies that may have a plethora of impacts on many areas – from a legal standpoint as well (*i.e.* issues related to liability, products safety, use and ownership of data and protection of personal data) – the lack of appropriate regulation of those technologies may have adverse effects on economic development and commerce.

Indeed, the lack of specific regulation may create an obstacle to economic development, or at the very least slow such development, which is increasingly digitalised and based on such systems, also leading to the need for balancing among the various needs involved – on the one hand, the protection of rights, freedoms and interests of users (including the rights to personal data protection) as well as the predictability of the regulatory framework and, on the other hand, the need for economic operators to develop increasingly sophisticated services and products by exploiting the benefits of using, for example, big data, AI and IoT systems.

26. Do you believe your legal system specifically encourages or hinders digital services?

As a member of the European Union, Italy and the Italian legal system benefit from the attention and focus dedicated by the European policies to digital services and, generally speaking, to digitisation, which have certainly contributed, and continue to contribute toward this encouragement, most recently through the DMA and DSA proposals and the e-privacy regulation proposal. However, it should be noted that the European legislation process, in some cases, has been a reason for delays in the development and regulation of digital services. Reference is to be made to the very long discussion process that characterises the adoption of the e-privacy Regulation (the Proposal of e-Privacy Regulation has been adopted for the first time in 2017 by the European Commission and has been agreed by Council of the European Union on February 2021, after more than four years of negotiations and 14 text proposals) aimed at regulating, *inter alia*, (i) the use of cookies; (ii) direct marketing by e-mail and telephone; (iii) the use of electronic communications content and metadata; and (iv) directory enquiries, calling line identification and nuisance calls. It is worth noting that the regulation on the use of cookies is also important in the context of online and digital advertising (for example, with regard to online behavioural advertising).

Nevertheless, it can be said that the Italian legal system features advanced legislation governing the digital and technology sectors. Furthermore, Italy was among the first countries in the world to regulate the digital signature, one of the first European countries to notify the national system for digital identity and to recognise the full validity of the blockchain and smart contracts by introducing the definition (Article 8-*ter* of Law No. 12/2019) of distributed ledger-based technologies and smart contracts.

However, it cannot be denied that the country's state of digitisation is less advanced than that of other European countries, as shown by the 2020 DESI ("*Digital Economy and Society Index*"), although there is certainly hope that this trend will improve over the next few years, also in view of the recent policies adopted by the government (such as the "National Recovery and Resilience Plan" of 2021) of which digitisation constitutes a fundamental pillar.

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

As widely discussed also in legal debate, the Italian legal system offers tools and legal mechanisms that allow for the delineation and regulation of legal issues related to AI and the Italian institutions have shown strong interest in regulating these matters, it being understood that there still remains a need to put in place a specific legal framework on this matter, which would preferably be adopted at European level for harmonisation purposes.

On July 2020, MISE published the final document with the proposals for the "Italian Strategy for Artificial Intelligence". The aim of the document is to reap the benefits that AI can bring to the country, by following an approach that integrates technology and sustainable development and always puts the individual and his or her context at the centre.

Contributors

Carlo Impalà
Partner and Head of TMT & Data Protection Department carlo.impala@morrirossetti.it

Giorgia Valsecchi
Associate, TMT & Data Protection Department giorgia.valsecchi@morrirossetti.it

