The Legal 500 & The In-House Lawyer
Comparative Legal Guide
Romania: Technology

This country-specific Q&A provides an overview to technology laws and regulations that may occur in the Romania.

It will cover communications networks and their operators, databases and software, data protection, AI, cybersecurity as well as the author's view on planned future reforms of the merger control regime.

This Q&A is part of the global guide to Technology. For a full list of jurisdictional Q&As visit http://www.inhouselawyer.co.uk/index.php/practice-areas/technology

Country Author: Maravela & Asociaţii

The Legal 500

Alina Popescu, Managing Partner

alina.popescu@maravela.ro

The Legal 500

Irina Radu, Senior Associate

irina.radu@maravela.ro

Sonia Fedorovici, Senior Associate

1. **Are communications networks or services regulated? If so what activities are covered and what licences or authorisations are required?**

Yes. The main legal instrument governing communication networks and services is the Government Emergency Ordinance no. 111/2011 on electronic communications ("GEO 111/2011"), which transposes the main EU provisions in

the field of electronic communications. This legal instrument covers all activities in the field of communications networks and services. The GEO 111/2011 establishes the general framework for regulation of electronic communications networks and services, the authorization of such activities and promotes competition on the market. In addition, there is special legislation encompassing laws and emergency ordinances on certain topics as well as secondary legislation (mainly government decisions and enactments of the telecom body).

The provision of electronic communications networks and services is subject to (i) general authorization and (ii) licenses for the use of limited resources for the provisions of electronic communications networks and services, such as radio frequencies, numbering resources and other associated technical resources. These licenses are subject to certain technical parameters and are granted for a limited period of time. The general authorizations as well as the licensees are issued by the National Authority for Management and Regulation in Communications ("ANCOM") in accordance with its decision no. 987/2012 on the general authorization regime for the provision of electronic communications networks and services.

2. Is there any specific regulator for the provisions of communications-related services? Are they independent of the government control?

Yes. The regulatory authority in the sector of electronic communications is the National Authority for Management and Regulation in Communications ("ANCOM") (in Romanian Autoritatea Națională pentru Administrare și Reglementare în Comunicații). ANCOM was established pursuant to the Governemnet Emergency Ordinance no. 22/2009 as an autonomous public authority under the control of the Romanian Parliament and financed entirely from its own revenues.

3. Does an operator need to be domiciled in the country? Are there any restrictions on foreign ownership of telecoms operators?

The Romanian legislation in the sector of electronic communications does not require an operator to be established on the territory of Romania.

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

4. Are there any regulations covering interconnection between operators? If so are these different for operators with market power?

Yes. ANCOM takes all necessary measures to ensure and encourage adequate access and interconnection as well as the interoperability of services in a way that promotes efficiency, sustainable competition, investment and innovation for

the benefit of end-users. To accomplish this, ANCOM may impose certain obligations on undertakings, as follows:

- in order to ensure end-to end connectivity, the authority may impose obligations on undertakings that control access to end-users to interconnect their networks;
- in justified cases and if it is necessary, the authority may also impose obligations on undertakings that control access to end-users to make their services interoperable;
- to the extent that this is necessary to ensure accessibility for end-users to digital radio and television broadcasting services to provide access to application programming interfaces or electronic program guides on fair, reasonable and non-discriminatory terms.

The obligations and conditions imposed as per the above must be transparent, objective, proportionate and non-discriminatory and must follow a certain procedure provided in the law. Also, such measures that may be imposed by the regulatory authority are without prejudice to the measures that may be taken regarding undertakings with significant market power.

One of the tasks of ANCOM is to promote competition on the market. To achieve this, the authority identifies the relevant market and the undertakings with significant market power. In the sector of electronic communications an undertaking is considered to have significant market power if, either individually or jointly with others, it enjoys a position equivalent to dominance, that is to say a position of economic strength affording it the power to behave to an appreciable extent independently of competitors, customers and ultimately consumers.

After conducting the market analysis and to the extent that it is necessary to promote competition on that market, ANCOM may impose, maintain, amend or withdraw, as the case may be, certain obligations on undertakings with significant market power. According to GEO 111/2011 and in line with the EU provisions (Access Directive) the authority may, in addition to the above impose, maintain, amend or withdraw the following in order to facilitate access to and interconnection of electronic communications networks and associated facilities:

- obligations of transparency in relation to interconnection and/or access, requiring operators to make public specified information, such as accounting information, technical specifications, network characteristics, terms and conditions for supply and use;
- obligations of non-discrimination in relation to interconnection and/or access that ensure in particular, that the operator applies equivalent conditions in equivalent circumstances to other undertakings providing equivalent services, and provides services and information to others under the same conditions and of the same quality as it provides for its own services, or those of it subsidiaries or partners;
- obligations of accounting separation in relation to specified activities related to interconnection and/or access;
- obligations of access to, and use of specific network facilities in situations where ANCOM considers that denial of access or unreasonable terms and conditions having a similar effect would hinder the emergence of a sustainable competitive market at the retail level, or would not be in the end-user's interest;
- obligations of price control and cost accounting obligations; and

- obligations of functional separations; this obligation may be imposed when the authority considers that the above listed obligations have failed to achieve effective competition and that there are important and persisting competition problems and/or market failures identified in relation to the wholesale provision of certain access product markets; this obligation requires vertically integrated undertakings to place activities related to the wholesale provision of relevant access products in an independently operating business entity.

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

GEO 111/2011 lays down the consumer protection regulations applicable for the sector of electronic communications.

Contracts concluded by consumers for the provision of access and interconnection to public electronic communications networks and services may be made on an initial period of up to 24 months. The offers and contracts designed for consumers must be transparent and offer the consumer sufficient information. For this reason, contracts concluded with consumers must contain the following minimum information:

- the identification data of the provider;
- the services provided, including in particular, if access to emergency services and caller location is provided, information with regard to the procedures for measuring traffic, the service quality levels offered, as well as the term for the initial connection;
- the prices and tariffs for each product or service covered by the contract, the way in which they are applied, as well as the means by which updated information on the tariffs for the provision of the electronic communications services and of the maintenance and repair services may be obtained;
- the duration of the contract, the conditions for renewal and termination of the contract, as well as the conditions under which service suspension operates;
- the applicable compensations and procedures in case the contracted service quality levels or other contractual clauses are not fulfilled;
- the means of initiating procedures for the settlement of disputes;
- the type of action that may be taken in reaction to security or integrity incidents or threats and vulnerabilities.

In addition, GEO 111/2011 contains certain provisions with regard to the conclusion of distance contracts. These provisions offer the consumers a favourable position in the sector of electronic communications.

Decision no. 158/2015 of the President of ANCOM regarding information obligations to end-users (“Decision 158/2015”)

is aimed at ensuring transparency concerning the relationships between telecom operators and end-users.

The said decision establishes the information that electronic communications services providers have to make known to users (e.g. information to be included in invoices, information regarding commercial terms, network coverages, etc.) and the various means whereby such information must be transmitted/published (website, client care, sales department). It also encompasses the terms and formalities for unilateral changes to contract conditions, information to be provided to the ANCOM, online archive of past commercial terms, etc.

Decision 158/2015 concerns Internet services providers and re-broadcasting providers in addition to telephony providers, who have such obligations since 2009. It thus applies to both providers of public communications networks and to providers of electronic communications services intended for the public.

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

Legislation on intellectual property is in line with international practice, Romania having adhered to most of the international conventions on intellectual property, as well as to EU legislation in the field. According to EU legislation, computer programs are considered literary works. In Romania, computer programs are protected under Law no. 8/1996 on copyright and related rights (the "Copyright Law"). Article 72 of the Copyright Law provides that the protection of computer programs includes any expression of a program, application programs and operating systems expressed in any kind of language, whether in source code or object code, the preparatory design material and the manuals.

In Romania, copyright is protected provided that the work is original, takes a concrete expressive form and is able to be made known to the public. A copyright holder has the exclusive patrimonial right to decide whether, how and when its work will be used. In addition, he has the right to authorize or prohibit the following:

- the reproduction of the work;
- the distribution of the work;
- the import for trading on the domestic market, of copies of the work;
- the rental of the work;
- the communication to the public, directly or indirectly, of the work, by any means, including by making the work available to the public, in such a way that members of the public may access it from a place and at a time individually chosen by them;
- the broadcasting of the work;
- the cable retransmission of the work; and
- the making of derivative works.

Apart from the above general rights, copyright holders of computer software enjoy certain rights that are applicable especially to them. Thus, copyright holders of computer software have the exclusive right to do and authorise the

following:

- the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole, including where the reproduction is required for the installation, storage, running, execution, display or transmission in the network;
- the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program;
- any form of distribution to the public, including the rental, of the original computer program or of copies thereof.

As per Government Ordinance no. 25/2006 on strengthening of the administrative capacity of Romanian Office for Copyright ("ROC"; in Romanian "Oficiul Român pentru Drepturile de Autor"; "GO 25/2006") any producer of computer programs has the obligation to register with the national registry kept by ROC. However, said registration does not grant any copyright or ancillary rights.

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

Yes. According to Law no. 8/1996 on copyright and related rights (the "Copyright Law") a sui generis right for the protection of databases is provided for 15 years. The data base owner has the exclusive right to authorize or forbid the extraction or reuse of the whole or substantial part of the database. This sui generis right applies irrespective of the fact that the database or its content are protected under copyright or any other right.

8. What key protections exist for personal data?

On May 2018 the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR") became directly applicable in Romania.

As a consequence, the former Romanian national legal framework has been repealed and new attributions have been granted to the National Supervisory Authority for Personal Data Processing ("Data Protection Authority") by Law no. 129/2018 for modification and completion of Law no. 102/2005 regarding the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing and repealing Law no. 677/2001 with regard to the processing of personal data and on the free movement of such data ("Law 129/2018").

Law 129/2018 mainly refers to the powers of the President of the Data Protection Authority, the control and claims settlement attributions of the said authority and the judicial remedies available to data subjects.

In order to implement the provisions of article 9 paragraph (4) and articles 37-39, 42, 43, 83, 87-89 of GDPR, Romania has also adopted Law no. 190/2018 on GDPR implementing measures ("Law 190/2018").

The implementing measures provided by Law 190/2018 mainly refer to the following:

- the processing of genetic data, biometric data or data concerning health for an automated decision-making or profiling should be made based upon the explicit consent of the data subject or an express legal provision and with the establishment of appropriated measures;
- the processing of a national identification data (personal identification number, identity card's series and number, passport and driver license number, health social security number) and collection or disclosure of the documents that contain the same can be made only in accordance with article 6 paragraph (1) of GDPR; in case of a processing based upon letter f) of article 6 paragraph (1) of GDPR, the controller or the third party should establish certain warranties;
- data processing in the context of employment; in case an employer utilizes monitoring systems by electronic and / or video means, the processing of employees' personal data based on employer's legitimate interest is permitted only under certain specific conditions set out by Law 190/2018;
- for the processing of personal data and of special categories of personal data in the context of fulfilling a task carried out in the public interest, the controller or the third party should establish certain warranties set out by the law;
- the processing of personal data carried out for journalistic purposes or the purpose of academic artistic or literary expression can be made if the used data have been explicitly made public by the data subject or such data are closely linked to the capacity of the data subject as a public person or to the public character of the data subject facts;
- derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are granted pursuant to article 89 of GDPR;
- the processing of personal data and of special categories of personal data by political parties, nongovernmental organizations of citizens belonging to national minorities and nongovernmental organization is permitted without the consent of the data subject, subject to certain warranties;
- the designation and the tasks of the data protection officer are in line with the ones provided by articles 37-39 of GDPR;
- the accreditation of certification bodies provided by article 43 of GDPR shall be made by Romanian Accreditation Association (in Romanian language - Asociația de Acreditare din România – RENAR) according to the EN-ISO/IEC 17065 standard and supplementary

requirements issued by the Data Protection Authority;the corrective measures and penalties for public authorities and bodies are derogatory and refer to a remedy plan and the level of maximum fine (Ron 200,000, proximately EUR 43,000).

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

The transfer of personal data abroad is subject to the provisions of GDPR, no national regulations being enacted in this respect.

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

The maximum applicable fine is the one provided by article 83 paragraph 5 of the GDPR (administrative fine up to EUR 20 000 000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher), except for the public authorities and bodies for which the maximum fine is of Ron 200,000 (approximately EUR 43,000).

11. Are there any restrictions applicable to cloud-based services?

Cloud-based services are of significant importance in light of data protection law, since the data stored in the cloud moves freely between different jurisdictions. The data protection legislation does not provide per se restrictions applicable to cloud-based services. However such restrictions are implied from data protection rules and principles.

One of the data protection principles provides that data must be safeguarded and not transferred to third countries unless adequate safeguards are in place. For this reason, data controllers are legally required to conclude agreements when contracting with cloud service providers with a view to store data in the cloud. When storing personal data in the cloud the data controller must ascertain that the location of the data is known. This is of utmost importance, since the data may be stored on servers located in another country that may or may not provide an adequate level of protection as required under Romanian law.

In other words, the data controller must ensure that the agreement concluded with the cloud service provider is in line with data protection rules. Throughout this agreement the data controller must make sure that he will not be in breach of any rules with regard to processing and transfer of personal data.

The provisions of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (“NIS Directive”) related to cloud computing services will be applicable in Romania after its transposition into national legislation. A draft law concerning cyber security in Romania is under legislative procedure.

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

Article 4 of Law no. 455/2001 on electronic signature (implementing the eIDAS Regulation), defines the electronic signature (e-signature) and the extended e-signature. The latter is the equivalent of the advanced e-signature in eIDAS Regulation and it must fulfill four conditions in order to be valid:

- it is uniquely linked to the signatory;
- it ensures the identification of the signatory;
- it is created using electronic signature creation data that the signatory can use under his sole control;
- it is linked to the data signed therewith in such a way that any subsequent change in the data is identifiable.

Under Article 5 of the said law, an extended e-signature ensures the validity of an electronic document if it is based on a qualified certificate and generated by a secure signature creation device. Simultaneously, Article 6 recognizes the validity of an electronic document if e-signatures were used. Moreover, in the instance where one of the parties does not recognize the e-signature, the court must have it verified by an expert.

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

When a company is outsourcing certain services that can be seen as a stand-alone function, and the outsourcing supplier also takes over the outsourced activity as such or certain assets/equipment pertaining thereto, there is a chance that we are dealing with a transfer of undertaking. In this case, the outsourcing supplier has the obligation to take over the employees attached to the relevant activity/assets/equipment.

The relevant provisions for the transfer of undertaking may be found in the Labour Code (Law no. 53/2003) and in Law no. 67/2006 on safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses, which transposes EU Directive 2001/23 on the approximation of the laws of the Member States relating to the safeguarding of employees' rights in the event of transfers of undertakings, businesses or parts of undertakings or businesses and the provisions of article 5 of EU Directive 2015/1794 of the European Parliament and of the Council of 6 October 2015 amending Directives 2008/94/EC, 2009/38/EC and 2002/14/EC of the European Parliament and of the Council, and Council Directives 98/59/EC and 2001/23/EC, as regards seafarers. Both enactments provide that all rights and obligations of the initial employer are automatically transferred in their entirety to the outsourcing supplier. A transfer of undertaking may not constitute ground for dismissal.

Moreover, the applicable legal framework provides that before any transfer of undertaking/outsource occurs, the employer and the outsourcing supplier must inform the employees on the following:

- the date of the transfer or a proposed date;
- the reasons why such transfer occurs;
- the legal, economic and social consequences of such transfer for the employees;
- any measures that may be taken with regard to the employees;
- the working conditions.

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

Currently the Romanian national legal framework does not contain any explicit provisions with regard to any form of A.I. Therefore, the general rules on civil contractual liability and tort law, as well as administrative and criminal liability would apply on a case-by-case basis, depending on the specific circumstances of the case.

15. What key laws exist in terms of obligations as to the maintenance of cyber security?

Government Decision no. 271/2013 regulates Cyber security strategy of Romania.

The provisions of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union ("NIS Directive") related to cloud computing services will be applicable in Romania after its transposition into national legislation. A draft law for cyber security in Romania is under legislative procedure.

16. What key laws exist in terms of the criminality of hacking/DDOS attacks?

The following cyber crime related laws are particularly relevant:

- Law no. 161/2003 on certain measures for transparency in the exercise of public functions and the business environment and for the prevention and sanctioning of corruption - Title III - Prevention of cyber crime;

- Law no. 64/2004 ratifying the Council of Europe Convention on Cybercrime (E.T.S. no. 185, November 23, 2001); since said ratification, Romanian national laws have been amended so as to comply with the requirements of the convention regarding the collection, search, seizure, making available and interception of data; and
- the Criminal Code (Law no. 286/2009).

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

It is hard to name only one technology development that would have the biggest legal impact, since any such important development has the ability to produce equally important legal change.

In Romania, as well as worldwide, one of the closest technology developments that have an appreciably effect on society is the development of the Internet of Things (IoT). We now live in a world in which all of our devices are connected to the Internet and the cloud. IoT has developed beyond just laptops, smartphones and tablets and now, includes everything from fitness trackers to even "smart" toys ("smart" fashion toys, like "My friend Cayla" - that has been recently designated as a spy tool by authorities across Europe).

One of the biggest problems that the IoT has is security. When all of your devices constantly collect data and communicate between themselves and even interact with the environment around them, one must be sure that they are not easily "corrupted" and that one`s data is not "stolen". Moreover, there is a need to develop devices and networks with an intense focus on security and create a compatible platform for the IoT. Currently, there are apps and devices that are unable to communicate between themselves due to lack of standardization. Hence, security and standardization are two major aspects to be dealt with by coming legislation.

In addition, the use of IoT also means that all of our data is collected and further processed for commercial purposes, as companies rely more and more on Big Data Analytics (i.e. the process of collecting, organizing and analyzing large sets of data to discover patterns and other useful information) to understand and predict human behavior, laws will need to cover not only more efficient data privacy mechanisms.

Although efforts are being made in enhancing security and protecting privacy, one still cannot keep up with the fast pace of technology.

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

By and large, EU and Romanian legal framework are very favorable to commerce and development. Therefore, while there is always room for improvement in our view, there is at present no regulatory major impediment to economic development and commerce.

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

Our legal system is aligned with the EU legislation in the field of digital services. At the EU level, as well as in Romania the digital environment is regulated by laws that are currently outdated (see as an example the legislation for the electronic commerce sector, which was enacted in 2000), as well as encompassing many grey areas, since many aspects of the digital environment are largely unregulated. As a consequence, the current frameworks as well as case law fail to provide legal certainty for the development of digital services.

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

The Romanian legal system is neither less nor more prepared than other legal systems to deal with the risks and legal issues associated with artificial intelligence. Currently, there is no national or European legal framework in the sense of AI tailor-made legislation. Whilst for the moment existing legislation may seem as largely sufficient, once the AI will spread and become more sophisticated there will be a stringent need for dedicated legal framework.