Chambers

GLOBAL PRACTICE GUIDE

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

TMT

Romania
Cosmina Simion, Ana-Maria Coruga, Andrei Cosma and Teodora Popescu
Simion & Baciu

chambers.com

2020

ROMANIA

Law and Practice

Contributed by:
Cosmina Simion, Ana-Maria Coruga, Andrei Cosma and Teodora Popescu
Simion & Baciu see p.14

Contents

1. Cloud Computing

Laws and Regulations

Cloud is defined at national level by Law No 362/2018 on ensuring an increased common level of security for computer networks and systems, implementing at national level Directive (EU) No 2016/1148 concerning measures for a high common level of security of network and information systems across the European Union.

According to the legal definition provided at the European Union level and reiterated into the national normative act, cloud computing service is qualified as a digital service which permits the access to a configurable system of resources or computer services that can be grouped together.

Law No 362/2018 follows the Decision of Chamber of Deputies No 71/2016 on the adoption of the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions on the European Cloud Initiative – Building a competitive data and knowledge economy in Europe, used as an instrument for the legislative body to officially recognise the benefits and necessity of implementing cloud services in the course of private and public operators' activities in order to efficiently manage the current "big data" phenomenon (as described within works from European Commission) in a context of a constantly growing tendency towards organisational differentiation in both public and private sectors.

Law No 362/2018 applies to the digital services suppliers having their headquarters on the Romanian territory. In case of suppliers established outside the European Union, the provisions of Law No 362/2018 shall only apply to representatives in the European Union established in Romania.

Suppliers of cloud computing, as digital service providers, are obliged to observe a set of mandatory requirements imposed by the law, including the obligation to implement adequate and proportional technical and organisational measures in order to reach the minimal security conditions imposed by the law for the network and information systems and the obligation to immediately notify CERT-RO, the National Response Centre for Cybernetic Security Incidents in Romania, of any incident that has a significant impact on the provision of digital services.

In implementing the required measures, suppliers of cloud computing must consider the technical norms elaborated by CERT-RO, the competent national authority for the security of network and information systems.

The suppliers of digital services are subject to a national procedure of identification and registration. Methodological Norms of 2019, issued by the Ministry of Communication and Informational Society with respect to the identification of essential services operators and digital services providers, establishes the conditions under which the identification and registration of digital services suppliers shall take place. In brief, the procedure is initiated by the digital services provider through a self-evaluating process and is continued by designating a person responsible for the network and information systems security in order to ensure the communication with CERT-RO and transmit the data resulted from the self-evaluation procedure.

On the basis of the information provided, CERT-RO initiates the analysis procedure and decides whether or not to approve the registration of the digital services supplier with the register of digital services suppliers. Following a registration decision, the provider of digital services is subject to CERT-RO monitoring and control regarding the observance of the requirements of Law No 362/2018.

The sanctioning regime established by Law No 362/2018 provides for restrictive administrative sanctions. In case of repeated breach, the administrative fine can even reach 5% of the turnover of the economic operator.

From a data protection perspective, provision and use of cloud services within the Romanian territory and/or by Romanian subjects shall observe the legal requirements provided by Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (the General Data Protection Regulation, GDPR), as well by the subsequent national normative acts. Law no 362/2008 expressly states that CERT-RO will co-operate with the National Authority for Personal Data Processing (ANSPDCP) in any situation where incidents reported by essential services operators and digital services providers result in prejudices to personal data security.

Specific Industries with Greater Regulation

In terms of industries with greater regulation, the start point resides in the register of essential services operators which, according to Law No 362/2018, is created for specific sectors, as follows: energy, transport, banking, infrastructures of financial markets, health, provision and distribution of drinking water, and digital infrastructure. Law No 362/2018 expressly specify the subsectors of the sectors listed therein falling under the scope of the normative act.

In accordance with the law, the register of essential services operators shall have the legal regime of a classified document.

Law No 362/2018 and the Methodological Norms do not essentially link the register of digital services suppliers with specific sectors and subsectors of industry.

In addition to the requirements of Law No 362/2008 for digital services providers, the general legal regime established under GDPR and the subsequent national legislation shall be entirely applicable, along with the specific interdictions or restrictions provided in relation to certain industries, as the case may be.

There are certain industry sectors where the European and/or national competent bodies or institutions have issued guidelines, a report of recommendations or other supporting documents in order to provide sufficient guidance to operators both in the public and private sectors in outsourcing to cloud service providers (for example, Final Report – Recommendations on outsourcing to cloud service providers – EBA/REC/2017/03).

No express interdictions or restrictions are regulated in relation to personal data processing through cloud computing, as long as the requirements provided by the legislation in relation to mandatory technical and organisational measures to be undertaken are observed.

Processing of Personal Data

Since the European and national legislative framework have not been amended in order to ensure a sufficient legal background in relation to the use and provision of cloud service under the GDPR requirements, the specific issues that were raised in both the public and private sectors under Directive 95/46/EC remain on the table and continue to generate a certain degree of uncertainty among the providers and users of cloud services, on the one side, and the individuals whose personal data is processed through cloud computing, on the other side.

The responsibility allocation, for example, continues to represent the main issue for providers and users of cloud services. Even in the majority of situations, where the cloud client is the controller with respect to the processing of personal data, the responsibility allocation remains a potential source of uncertainty within the contractual relationship, thus resulting in a lack of clarity with respect to the roles played by the provider, on the one side, and the cloud client, on the other side, with the final consequence of potential inadvertent damages being produced in relation to personal data processed through cloud services.

The security, transparency and legal certainty that the cloud service provider should be able to ensure for the client also remains an issue, since the latter is bound to a high diligence and attention in securing sufficient guarantees in terms of technical and organisational measures to be implemented by the cloud service provider. As indicated through opinions of relevant working groups within European Union under Directive 95/46/EC, the first step to be undertaken by the cloud client in contracting a cloud service provider should consist in performing a comprehensive and thorough risk analysis in relation to the cloud services offered. This diligence obligation incumbent upon the cloud client, as operator in relation to personal data processing, is even more important under the provisions of GDRP.

Once valid solutions are offered to the main issues presented above, other specific aspects identified as being problematic in relation to the provision and use of cloud services could also be considered as solved. Against a background of security, transparency and certainty on the guarantees offered by the cloud provider with respect to personal data subject of processing, and where the responsibility allocation is clearly established and implemented according to the agreement between the parties and in observance of the applicable legal requirements, issues such as the lack of control over personal data will no longer be on the agenda of the cloud client.

2. Blockchain

Romania has so far not enacted a specific legislation regulating blockchain technology or the cryptocurrencies based on such technology. Therefore, the legal implications deriving from the use of blockchain or cryptocurrencies (including liability, data privacy, contract formation, etc) are to be determined by reference to the general legal principles and common-ground provisions of the Romanian legal system.

Nevertheless, at a governmental level, it is worth noting that in May 2018 Romania has joined three initiatives of the EU Commission, namely the European Blockchain Partnership, the Declaration of Cooperation on Artificial Intelligence and the Innovation Radar. Through these initiatives, the EU aims to invest more than EUR1 billion in the near future on supercomputers, artificial intelligence (AI) and blockchain in order to keep the pace with the technological developments existing in other areas around the globe (eg, China, USA).

Risk and Liability

In relation to the specific matter of cryptocurrencies, the National Bank of Romania has expressed the official position that these cannot be qualified as fiat money, being only speculative assets, and has warned consumers about the potential negative implications arising from trading/exchanging bitcoin or other blockchain-based currencies. As long as the cryptocurrencies are considered simply assets and not financial means/instruments, their trading will not be under the direct supervision of the Romanian financial regulators and, as a consequence,

exchanging cryptocurrencies is to be treated as any other transfer of immaterial assets. This lack of regulation may generate risks for the consumers which cannot properly benefit from all the instruments and rights granted by the consumer protection legislation.

In addition, it is worth noting that certain banks in Romania are no longer accepting any deposit of money derived from the exchange of cryptocurrencies. Furthermore, in practice, there are also cases where the bank has refused to commence a business relationship with providers of blockchain technology.

Intellectual Property
The blockchain technology does not seem to have been applied so far in the intellectual property (IP) domain existing in Romania. Nevertheless, this technology may theoretically offer several possibilities for IP protection and registration and also as probation means, either at the registry stage or in front of a court of law. Potential cases may include:

- evidence of creatorship and provenance authentication, registering and clearing IP rights;
- controlling and tracking the distribution of (un)registered IP;
- providing evidence of genuine and/or first use in trade and/or commerce;
- digital right management (eg, online music websites);
- establishing and enforcing IP agreements, licences or exclusive distribution networks through smart contracts;
- transmitting payment in real-time to the holders of IP rights.

Blockchain may technically be used also for authentication and provenance purposes in the detection and/or retrieval of counterfeit, stolen and parallel-imported goods.

Data Privacy
Blockchain may also entail privacy-related implications. The GDPR regime is inherently applicable also in Romania and hence an application based on blockchain technology which is offered in Romania must be compliant also with the data privacy regime. One of the rights conferred to the data subjects is the "right to be forgotten"; this seems to create a challenge in the context of blockchain, since one of the core characteristic of the technology refers to the immutability of the records entered into the blockchain/ledger.

Service Levels
Using blockchain in the context of service levels agreements (SLAs) does not seem to be a practical application of this technology in Romania at this date or, in any event, it is not widespread. Nevertheless, certain inherent advantages of this technology and the smart contracts underlying on it, such as automation and the high degree of security, may technically be put into practice also for SLAs existing in Romania, since it may ensure in a more efficient way that the services offered complies with the SLA and any deficiencies are rectified in a swift manner.

Jurisdictional Issues
Since the blockchain technology is currently unregulated in Romania, jurisdictional issues may technically arise in the scenario of a blockchain system/application involving both Romanian and foreign parties. Such issues may include the law governing a potential conflict or the rules determining the competent court/forum for resolving the dispute.

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

Big Data
Starting and managing a project involving big data may raise specific legal challenges, starting with the mandatory requirements applicable in terms of data processing and continuing with the general liability aspects and intellectual property rights-related challenges.

Data processing
In terms of data processing requirements, a preliminary distinction should be made between personal data, subject to GDPR and subsequent national regulations, and general data which may be covered, as the case may be, by a legal confidentiality requirement.

In order to distinguish between the two data categories and further apply the corresponding legal regime, it is essential that a big data project uses an adequate IT system so as to enable the controller and/or the data processor to qualify the large volume of data handled. A viable solution is considered to be the cloud computing service, subject to our discussion above.

Further on, personal data shall be processed in full consideration of GDPR requirements, with the provision of the relevant guarantees and insurances as established by the law, while data covered by a legal confidentiality obligation is to be processed in accordance with the specific conditions provided by the relevant legislation.

Both controllers and IT technologies' suppliers – acting as processors – will face a major challenge in adjusting their solutions to the relevant legal requirements provided by GDPR, as the imperative data minimisation principle or the restrictive conditions imposed in relation to processing of sensitive data. By

way of example, at national level, Law No 190/2018 regarding the measures aimed at implementing GDPR provides that processing of genetic and biometric data as well as data concerning health for the purpose of performing an automated decision-making process or for creation of profiling is only permitted based on an explicit consent or in consideration of an express legal ground and only when corresponding protection measures have been implemented. Law No 190/2018 also permits the processing of certain sensitive data in performing a duty serving the public interest, provided that the restrictive conditions established by the national law are fully observed.

In addition to the necessity of an efficient structuring of the information in order to identify and apply the relevant legal regime to each data category involved, the controllers are bound to correctly qualify the processing means used and the purposes pursed in relation to personal data falling under GDPR in order to identify whether an assessment on the protection of personal data of the envisaged processing operations is to be performed through said mechanism.

When regulating the operations triggering the obligation to implement a DPIA, Decision No 174/2018 on the List of Operations for which the Data Protection Impact Assessment is required seems to focus on one essential element of the processing, namely the automatised means used or innovative technologies implemented.

Intellectual property

In terms of intellectual property rights, an efficient structuring and qualification of data is also relevant in order to identify whether said data is covered by protection deriving from third-party intellectual property right or whether the use of said data is conditioned by specific restrictions or limitations of any kind.

Entry into force of Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market represents a considerable step forward in relation to, inter alia, the digital market since the harmonisation of the copyright protection within member states shall relieve the assessment necessary to be made in a big data project because any technical mechanism shall now refer to the same general criteria for data originating from different member states. This will only apply from 7 June 2021, the date marking the end of the transposition deadline.

A big data project could involve aspects of database protection. According to Law No 8/1996 on copyright and neighbouring rights, as republished, the person that has created a database has the exclusive patrimonial right to authorise and prohibit the retrieval and/or the use of the whole or of a substantial part of the database.

Liability

When discussing legal liability, any potential prejudices caused to third parties within a big data project will trigger the liability of the person designated by the legislation regulating the infringement.

In terms of data protection infringement, for example, the liability shall stay with the operator, joint operators and/or the data processor, as the case, under the conditions provided in Article 82 of GDPR. No specific conditions are regulated in this respect at the national level, in addition to the provisions of GDPR.

Liability for copyright infringement is regulated under the applicable national legal framework. Law No 8/1996 on copyright and neighbouring rights, as amended provides a strict sanctioning regime for copyrights infringements, including criminal penalties. By way of example, actions aiming at neutralising technical protection measures applied on works in digital form are to be sanctioned, under Law No 8/1996, as a criminal offence.

Machine Learning

Data processing

Data processing in a context of machine learning raises the same issues as presented above. Efficient and correct structuring of data is essential in order to avoid breaches of legal confidentiality of general data or of the personal data under GDPR. It is even more clear here that, under GDPR and Decision No 174/2018, using a machine learning-based mechanism could lead to the obligation of the controller to carry out a data protection impact assessment (DPIA) in accordance with the legal requirements, since the automatised character of the processing means is evident.

Intellectual property

In terms of intellectual property rights (IPRs), the use of machine learning, as a subset of AI, raises essential issues in relation to all intellectual property rights categories, starting with their protection and continuing to their enforcement. The challenge is also due to the lack of adaptation of the national legislation to the current innovations in terms of technology.

Under the national legislation in the field of intellectual property rights, both natural and legal persons may have legal standing for protection and exploitation of intellectual property rights, under the conditions provided by the law. In the field of patents and copyright, however, the human factor appears at an essential element within the creation/development processes that may lead to works subject to protection. Law No 8/1996 defines the author as the natural person or persons that created the work and provides for the author as remaining sole owner of moral rights, even when an assignment is operated,

where patrimonial rights only are subject to appropriation by the legal persons.

While there are works that can be generated by machine learning-specific algorithms that are not covered by intellectual property rights (eg, compilation of raw data to the extent it does not fulfil the criteria of a copyrightable data base), machine learning has the potential to create, at least theoretically, works covered by such protection. In this sense, the legal challenges appear even in the incipient phases of protection application requests since the word and rationale of the law appear to not allow, at this point in time, to appropriate the work to a natural or legal person.

Thus, the applicant would have to be the designer, the manufacturer, the programmer or the person under whose control the algorithm was at the moment of creation and/or registration; such a list is not exhaustive.

Moving forward, the qualification of the subject of protection – the work itself – may appear as challenging under the national legislation. In this sense, the procedure in seeking patent protection for a machine learning mechanism as a computer-implemented invention may pose serious problems to the competent public institution called to analyse the application, under the provisions of European Patent Convention and national Law No 64/1991.

Liability

As a subset of AI, machine learning is characterised by limited predictability, an aspect which places the person operating a machine learning-based mechanism in an uncertain position in terms of liability.

From a general civil liability perspective, the provisions of the Romanian Civil Code regulating the liability for prejudices caused by goods shall apply. An essential aspect to be considered is that, under the Romanian Civil law, the person having a good under their authority shall be liable for the prejudices caused by said good, irrespective of the existence of any fault, where the authority shall be understood as independent supervision and control over the good serving that person's own interests. The distinction between supervised and unsupervised machine learning will not result in an exoneration of liability for the latter, since the notions do not overlap in terms of legal regime.

The general liability-related provisions shall, of course, be superseded by specific legislation in regulated fields, or specific legislation on areas such as data protection, anti-money laundering, etc.

Artificial Intelligence (AI)

Where acting as an umbrella for machine learning, AI engages the same problems and legal challenges presented above.

In terms of AI, however, an interesting discussion can be made in relation to potential infringements caused by AI itself – namely, who is liable for the prejudices caused by AI?

From a procedural perspective, the first challenge is the procedural capacity of the AI to stand as defendant in front of the court of law. Would the defendant be the designer, the manufacturer, the programmer, the person under whose supervision the AI was at the moment when the musical work was created and/or brought to public knowledge? Most probably the court of law would have to analyse the potential causal link between the illicit action of AI and the defective element that lead to said action (in order to identify the human fault in the creation of AI).

It would be challenging for a court of law to find an appropriate solution to all of the questions raised above based on the substantial legal provisions in force regarding the subject of liability. The Romanian Civil Procedural Code clearly states that the procedural capacity results from the identity between parties and subjects of the dispute, as brought in front of the court of law.

Going forward, the court of law would also have the responsibility of analysing the form of liability of AI/the person being held liable in respect of committing the infringement. This is challenging, since the diligence and the predictability capacity the AI is expected to have will not be evaluated under the same considerations as an average human being.

4. Legal Considerations for Internet of Things Projects

While the Romanian legislation currently in force does not impose particular restrictions for internet of things (IoT) projects, offering a device or service pertaining to this disruptive technology may generate legal challenges stemming from the general legislation, particularly from a privacy or security perspective. Similar to other jurisdictions, concerns may arise in relation to the consent that must be given by the user of IoT, in an informed manner, to the processing of the personal data stemming from the use of a connected device – especially the multiple and complex purposes on the basis of which data is processed, not only by the manufacturer of the device, but also by other third parties involved in development of related applications. Furthermore, in line with the privacy regulation and also the general legislation in the field of consumer protection,

connected devices should ensure robust security safeguards against issues such as unauthorised use or hacking.

In addition, depending on the particular configuration of an IoT-related service, the provider of such service may be potentially qualified as a digital service provider in the sense of Law No 362/2018 which implements the EU NIS Directive, and hence certain security-related obligations may become applicable (for further details, please refer to **1. Cloud Computing**).

5. Challenges with IT Service Agreements

The main challenge encountered in relation to IT services agreements with operators in Romania is in relation to rights ownership. In this sense, it should be borne in mind that, under the national legislation, copyright in any work created by an IT service provider for the benefit of a contracting company stays with the former, except for the situation where a contrary clause is included in the agreement between the parties, in observance of the legal requirements regarding the mandatory content of said clause.

In case of computer programs created under a labour relationship, as an exception to the rule under Law No 8/1996, the rights in works belong to the company – the employer – to the extent works are created under the express instructions of the employer or in according with the employee's job description.

The relevant legal provisions of Law No 8/1996 regulating the mandatory content (patrimonial rights transmitted, modalities of use, duration and territory, remuneration of copyright holder) of the rights assignment clause should be taken into consideration in any situation when contracting IT services as beneficiary. In addition to assignment of rights, aspects as price revision restrictions could also become problematic in the context of competition law or public procurement procedures.

Also, one should consider legal restrictions on data storage locations that are in place in regulated industries (eg, gambling, financial services).

From a data protection perspective, it is essential that the agreement between parties clearly and unequivocally establishes the responsibility allocation on data processing, depending on the attribution assignment agreed by the parties.

6. Key Data Protection Principles

Core Rules Regarding Data Protection

National legislation in the field of data protection maintains the core rules provided under GDPR and other subsequent normative acts at European Union level. Law No 190/2018 provides for specific measure for ensuring the applicability of GDPR in Romania in matters in relation to which GDPR permits the member states to intervene with own regulations, as follows:

- processing of specific categories of personal data (sensitive data and national identification number);
- processing of personal data in context of employment relation;
- processing of personal data, including sensitive data, in the context of fulfilling a duty serving the public interest;
- derogations in relation to processing of personal data in journalistic purposes or the purpose of artistic or literary expression; and
- processing of personal data for purposes of historical or scientific research, statistical or archiving purposes in serving a public interest.

Law No 190/2018 also provides for certain requirements in relation to the data protection officer, regarding the designation and the attributions of the latter, as well as with respect to the accreditation of certification bodies and includes provisions related to the sanctioning mechanisms in place in implementing GDPR within the national territory.

Distinction Between Companies/Individuals

National legislation in the field of data protection maintains the scope ratione personae of GDPR which states in paragraph (4) of the Preamble that the processing of personal data should be designed to serve mankind.

It is worth underlining that the national authority's practice assimilates to natural persons the authorised natural persons ("*persoana fizica autorizata*"). Respectively, where the commercial activities are performed by a natural person directly, any fiscal or other identifiers obtained by such persons for tax purposes will be treated as personal data as they lead to the identification of the natural person.

Data regarding legal persons are not covered by the national requirements in the field of data protection. It should be borne in mind, however, that data of legal persons that could lead to a direct or indirect identification of a natural person may fall under the scope of applicability of GDPR and subsequent national normative acts.

General Processing of Data
Processing of data not falling under the scope of GDPR may be subject to confidentiality-related restrictions or prohibitions, as established by law or by mutual agreement binding between contracting parties. Legal grounds for confidentiality obligations may be found in specific normative acts (eg, legislation on protection of trade secrets or intellectual property rights, legislation on patient's rights). By way of example, Law No 46/2003 on patient's rights expressly states that all information on the patient's condition, results of investigation, diagnostic, prognostic, treatment and personal data are confidential even after the patient's death. Similar restrictions may exist in various other regulated industries, such as financial services, gambling, etc.

Processing of Personal Data
General processing of personal data of natural persons in Romania should fully observe the requirements provided within GDPR, which are entirely applicable.

As indicated, Law No 190/2018 provides for special requirements, stricter than the GDPR rules, with respect to specific categories of personal data. In this regard, one of the categories covered by Law No 190/2018 consists of genetic and biometric data and data concerning health in the sense that the national normative acts expressly states that processing of genetic and biometric data as well, as data concerning health for the purpose of performing an automated decision-making process or for creation of profiling, is only permitted based on an explicit consent or in consideration of an express legal ground and only when corresponding protection measures have been implemented.

7. Monitoring and Limiting of Employee Use of Computer Resources

The monitoring of employees through means of electronic communications (including through their use of company computers) entails a set of implications and restrictions from the perspective of the processing of personal data, aspects which benefit from a set of specific regulations at the level of Romanian law. Moreover, since electronic communications made inside company headquarters may be included in the notion of "private life" and "correspondence" within the meaning of Article 8 paragraph 1 of the European Convention on Human Rights, monitoring and limiting employee use of computer resources is further limited from the perspective of this fundamental right to respect for the employee's private life and communications.

Firstly, in addition to the general principles set out by the GDPR, Law No 190/2018 (Article 5) provides that processing the data of employees by using monitoring systems through electronic means of communications and/or video surveillance at work, in view of fulfilling the legitimate interests of the employer is allowed only under certain strict conditions. These conditions are expressly set by law and are the following:

- if the legitimate interests of the employer are duly justified and prevail over the interests or rights and freedoms of the data subjects;
- the employer must inform the employees in advance, in a complete and explicit manner regarding this kind of processing;
- the employer consulted the syndicate or, as appropriate, the employees' representatives before introducing such monitoring systems;
- other less intrusive means for meeting the purpose pursued by the employer have not previously proven their effectiveness; and
- the duration of the storage of personal data is proportional with the purpose of the processing, but is not more than 30 days, except for the situations that are expressly regulated by law or duly justified cases.

According to the Guidelines – Q&A Regarding the application of the Regulation (EU) 2016/679 – published on the website of the National Supervisory Authority for Personal Data Processing (RO Data Protection Authority), the Romanian authority states that the above aspects, and thus the fulfilment of these conditions, must be documented in thoroughly substantiated records held by the employer, from which the prevalence of the employer's legitimate interest over the interests and rights of the employees must result in order for such monitoring to be considered allowed.

Both for the notion of legitimate interest and for guidelines regarding data processing at work, the RO Data Protection Authority may scrutinise, when assessing the adequacy of certain instances of this type of processing of employee data, such documents as Opinion 06/2014 on the notion of legitimate interests of the data controller or, in the context of new technologies, Opinion 2/2017 on data processing at work of Article 29 Working Party.

In addition to the above restrictions, Decision No 174/2018 provides that for large-scale data processing of employees through automated means of monitoring and/or the systematic recording of behaviour, a data protection impact assessment must be carried out before such processing takes place.

While the Romanian Labor Code (Law No 53/2003 on the Labor Code) contains general provisions regarding the employer's right to exercise managerial control over the employee's activities and thus also monitor the latter's work activity, the employer

is bound also to respect the employee's rights (including the fundamental right to private life and correspondence). In this sense, the monitoring of employee use of computer resources should be performed for legitimate and lawful reasons, in a transparent, proportional and necessary manner.

To illustrate, in recent case law that originated in Romania, the European Court of Human Rights ruled against the Romanian state, in the case Barbulescu v Romania, where the Court deemed that Article 8 of the European Convention had been violated as Romanian courts failed to afford adequate protection of the employee's right to respect for his private life and correspondence, failing to strike a balance between the interests of the employer and of the employee.

In this particular case, Romanian courts had upheld the employer's decision to dismiss the employee for having used the company computer for private conversations with family members and failed to verify, according to the European Court of Human Rights, that the monitoring carried out by an employer of his employee's private conversations had been done without prior notification to the employee of such monitoring, of the nature or the extent of the monitoring, or of the degree of intrusion into his private life and correspondence.

8. Scope of Telecommunications Regime

The main laws governing the telecommunications industry in Romania is Emergency Government Ordinance No 111/2011 (EGO 111/2011) relating to electronic communications and implementing Directive No 2002/21/EC (Framework Directive), Law No 154/2012 regarding the infrastructure regime for electronic communications networks and Law No 159/2016 regarding the physical infrastructure regime for electronic communications networks, as well as for establishing measures to reduce the cost of installing electronic communications networks.

The telecommunication regime applies to any provision of electronic communications that meet the cumulative criteria listed in EGO 111/2011.

According to Article 4 (1) 6 of EGO 111/2011, an electronic communication network (ECN) is defined as a transmission system and, where applicable, switching or routing equipment and any other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed and mobile terrestrial networks, including internet, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed.

According to Article 4 (1) 9 of EGO 111/2011, an electronic communication service (ECS) must meet the following criteria: the service is normally provided for remuneration, it consist wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services.

As such, the current telecommunication regime is mostly limited to traditional electronic communication services and/or networks – ie, mobile terrestrial networks, fixed internet, radio, cable, satellite, wire.

Pursuant to Article 5 of EGO 111/2011, the provision of electronic communications networks (ECN) and electronic communication services (ECS) is free and is carried out in accordance with the general authorisation regime for the provision of public electronic communications networks and services, except for the provision of services that require use of scarce resources (ie, radio frequencies or numbers from the National Numbering Plan where the legal provisions stipulate that a licence has to be granted by the National Authority for Management and Regulation in Communications (ANCOM).

The authorisation procedure in view of gaining the right to provide public electronic communications networks or publicly available electronic communications services is free. The interested party is required to notify ANCOM and communicate information grouped into the following categories: data necessary to identify the provider and to communicate effectively with them, a description of the types of networks and/or services that the person or entity intends to provide and the estimated start date of the activity.

The person who submitted the notification according to the legal provisions is considered a provider for the types of electronic communications specified in the notification, gaining the rights and obligations under the general authorisation, from the date indicated in the notification as the estimated date for starting the provision of the respective types of network or service, but not earlier than the date when the notification was submitted.

All the authorised providers are required to pay an annual monitoring tariff to ANCOM if their turnover or revenues obtained exclusively from such activities exceed EUR100,000. The annual monitoring tariff is a percentage of the turnover or

of the revenues obtained from the provision of electronic communications networks and services, registered in the previous year, based on each provider's choice. The percentage applied, based on the provider's choice, cannot exceed 0.4%, as a ratio of (i) ANCOM administrative expenditures minus revenues from other sources, also taking into consideration the amounts of the annual surplus resulted from the execution of the previous years' budgets, and (ii) the cumulated turnover, corresponding to the previous year, of all the providers of electronic communications that owe the annual monitoring tariff.

The use of radio spectrum requires a frequency licence issued by ANCOM based on an application submitted by the service provider with the information related to the technical documentation that supports the proposed solution for the electronic communications network based on the minimum technical requirements established by ANCOM. The licences for the use of radio electric frequencies are granted directly, upon request or, if it is the case, following a selective, competitive and comparative procedure where a fee based on the licence's value will be established and paid. The annual tariff for the use of radio spectrum id determined according to the territory and frequency it is granted for and may vary up to EUR2.3 million per 5 MHz pair block allocated at the national level.

A licence is also granted for use of the numbering resources through an application submitted to ANCOM and is based on the following criteria:

- the designation of the service for which the right to use the numbering resources was granted, including any requirements related to the provision of that service, such as the tariff principles or maximum tariffs that may be applied for calls to certain numbers or blocks of numbers;
- the effective, rational and efficient use of numbering resources;
- requirements regarding number portability;
- the duration for which the right of use is granted, subject to the modification of the National Numbering Plan; and
- any obligations assumed by the supplier in question during a competitive or comparative selection procedure.

The annual tariff for the use of numbering resources is owed during the entire period in which the supplier holds the right to use the numbering resources and can vary between EUR75 and EUR7,350.

OTT, VoIP and Instant Messaging

An OTT service is defined as any service available on the internet without the involvement of a traditional communications operator such as voice-over internet protocols (VoIP) and instant messaging apps.

In Romania, the general consensus is that all over-the-top services (OTT) are not considered to fall under the scope of electronic communication rules for not fulfilling the cumulative criteria listed for the ECS – ie, a service which is normally provided for remuneration and consists wholly or mainly in the conveyance of signals on electronic communications networks.

By conveyance of signals, CJUE considers that the operator is responsible vis-à-vis the end-users for transmission of the signal which ensures that they are supplied with the service to which they have subscribed (30 April 2014, UPC DTH, C-475/12, paragraph 43).

On 5 June 2019 the Court of Justice of the European Union (CJEU) ruled in case C-142/18 Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT) that all OTT communications with a fee-based PTSN (public switched telephone network) breakout feature will be deemed to fall under the scope of the electronic communication regime.

The Court concluded that the SkypeOut service consists "mainly" in the conveyance of signals, considerations that cannot be applied for the "bundle of services, which are not at issue in the main proceedings, including, on the one hand, a service allowing users to make free audio and/or video calls between terminal equipment connected to the internet and, on the other hand, a number of services such as screen-sharing services, instant text messaging, file sharing and simultaneous translation, which cannot be classified as 'electronic communications services' as they do not consist wholly or mainly in the conveyance of signals" (paragraph 42 C-142/18).

In light of the CJEU's judgement, it can be expected for ANCOM to take enforcement action against services with features comparable to SkypeOut.

RFID Tags

RFID tags fall under the scope of Government Ordinance No 740/2016 (GO 740/2016) regarding the market availability of radio equipment and implementing the Radio Equipment Directive (RED) No 2014/53/EU.

According to Article 2 (1) 5 of GO 740/2016 a radio equipment represents an electrical or electronic product, which intentionally emits and/or receives radio waves for the purpose of radio communication and/or radiodetermination, or an electrical or electronic product which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination.

As such, RFID tags must meet essential technical requirements with regard to the protection of health and safety of persons and of domestic animals and the protection of property and an adequate level of electromagnetic compatibility in order to be used.

Pursuant to Article 4 (1) 9 of EGO 111/2011, RFID tags are generally considered to fail at the "editorial control" criterion, as electronic communication services which provide, or exercise editorial control over the content transmitted using electronic communications networks and services, are excluded from the electronic communication scope.

9. Audio-Visual Services and Video Channels

Main Requirements

Providing audio-visual services on the Romanian territory is mainly regulated via Audiovisual Law No 504/2002 which transposes the Audiovisual Media Services Directive (Directive 2010/13/EU) and the secondary legislation issued by the National Audiovisual Council (the Romanian regulator in the audio-visual field). In addition, depending on the type of audio-visual service intended to be offered on the market (ie, analogue/digital), the respective activity may also fall under the competence and regulatory powers of the telecom regulator, namely the National Authority for Management and Regulation in Communications (ANCOM).

Provision of audio-visual services in Romania may entail the legal requirement to obtain certain specific licences and authorisations, depending on the legal status of the broadcaster and the type of service sought to be transmitted.

The broadcaster is defined by the Audiovisual Law as "the provider of audiovisual media services in the domain of television programme services and/or radiobroadcasting".

The legislation regulates the following types of licences/authorizations.

Audio-visual licence

This permit is issued by the National Audiovisual Council to broadcasters which fall under the Romanian jurisdiction and grants the right to broadcast, in a certain area, a certain programme service. The audiovisual licence may be analogue or digital, depending on the technical means of transmission.

Broadcasting licence

This permit is issued by ANCOM, being required pursuant to the issuance of an analogue audio-visual licence. The broadcasting licence grants the right to use, for a certain period, one or more radio-electric frequencies, as the case may be, according to the analogue audio-visual licence. Additionally, the broadcaster (after the construction of the broadcasting station(s) under Romanian jurisdiction) is bound to obtain the technical authorisation to be issued by ANCOM.

Retransmission authorisation

This permit is issued by the National Audiovisual Council and grants the right to retransmit a programme service on the Romanian territory. In light of the principle of free retransmission stipulated by the Audiovisual Media Services Directive, the retransmission authorisation is not necessary for broadcasters under Romanian or EU jurisdiction or to broadcasters under the jurisdiction of states with which Romania has an international agreement for free retransmission.

The audio-visual licence is granted via a selection procedure, in case broadcasting is performed via terrestrial radio-electric transmission or via a decision of the National Audiovisual Council, in case the broadcasting is performed digitally, through an electronic communication network.

Obtaining an audio-visual licence requires the submission of a documentation with the National Audiovisual Council which shall include documents such as:

- the editorial strategy for the validity period of the licence (the audio-visual licence is valid for nine years);
- the editorial project describing the general format of the programme services, including the classification of the programmes based on their type (news, educational, entertainment, cultural, etc);
- the technical project of the broadcaster;
- the grid of programmes for a period of one week;
- the financial forecast, including the financing sources, the initial value of the investment as well as the advertising resources.

Besides the audio-visual licence, which is applicable for linear audio-visual services, the Romanian legislation regulates also the regime for audio-visual services upon request (ie, video on demand). This type of services are defined in the regulation as non-linear audio-visual media services, provided by a media service provider for viewing programmes at the moment chosen by the user and upon his individual request on the basis of a catalogue of programmes selected and transmitted by the media service provider.

A broadcaster falling under the Romanian jurisdiction (in accordance with the criteria provided by the Audiovisual Law) which intends to offer on-demand audio-visual services in

Romania is required to notify the National Audiovisual Council with at least seven days in advance of the commencement of the activity. The notification must include several information about the broadcaster and the type of service (eg, name of the service and related internet domain name, financing sources, type of access, categories/types of programmes, etc). The right to broadcast on-demand audio-visual services shall be granted solely based on the Council's approval which can be awarded following the submission of the notification.

Online Video Channels
The decision of the National Audiovisual Council which regulates the legal regime for on-demand audio-visual services sets forth that this regime shall not apply to "websites which provide audio-visual content generated by private users, for the purpose of sharing or exchanging within a community, such as YouTube, Google or Vimeo". Therefore, the legislation stipulates expressly that online platforms such as YouTube do not fall under the legal framework applicable for on-demand audio-visual services.

10. Encryption Requirements

Legal Requirements
The national and EU legislation provides legal requirements regarding the use of encryption for specific cases.

As per Law No 182/2002 regarding the protection of classified information, the authorities, institutions and any other third party working with state classified information are required to use encryption elements reviewed and vetted by the competent authorities in order to guarantee a high level of safety in the gathering and transmission of classified data and information.

Pursuant to Article 16 of Regulation No 1093/2010 establishing a European Supervisory Authority, the European Banking Authority released Final Guidelines on the Security of Internet Payments (EBA/GL/2014/12 Rev1) stating that minimum security requirements must be put in place by financial institutions, competent authorities and third-party e-merchants who store, process, or transmit sensitive payments. Such security requirements relate to the implementation of strong and widely recognised end-to-end encryption techniques, meaning that the information is encrypted within or at the source end system, with the corresponding decryption occurring only within or at the destination end system.

According to Article 32 of GDPR, the controller and the processor of personal data shall implement appropriate technical and organisational measures in order to ensure a level of security of personal data appropriate to the severity of the risks. The regulation lists the encryption as one of the criteria to be considered when choosing methods to secure personal data. As it can be seen, it does not mention explicit encryption methods in order to accommodate for the fast-paced technological progress. Although, strictly speaking encryption is not mandatory under the GDPR, it is highly recommended where processing could result in a high risk to the data subjects. In addition, in case of a data breach, the authorities must positively consider the use of encryption in their decision on whether and to what amount a fine is imposed, as per Article 83 of the GDPR.

Moreover, encryption techniques are also found in electronic signatures, which are tools based on encryption being used to capture the signatory's intent to be bound by the terms of the signed document in order to create and sign documents which afterwards can be filed before authorities. As per Law No 455/2001, an electronic signature is defined as cumulatively fulfilling the following conditions: it is created and is uniquely linked to the signatory, ensuring its identification and it is attached to a document in such a way that any subsequent modification is identifiable.

Exemptions
Pursuant to articles 33 and 34 of GDPR, data controllers that used strong and widely recognised encryption techniques, may be exempted from notifying a personal data breach to the affected data subjects, unless the data protection authority commends it to be necessary.

Simion & Baciu is a partnership formed by Cosmina Simion and Ana-Maria Baciu as a spin-off of several lawyers and consultants from the largest and oldest law firm in Romania. Comprising three partners and four associates, the firm strives to provide excellence in various areas of law and regulated industries, particularly media, technology, intellectual property and life sciences, with a particular focus on gambling and entertainment, consumer protection and advertising. Highlights of the firm's activity include ongoing assistance to prominent clients active in the technology, retail and FMCG sectors on the Romanian market, but also to land-based and remote gambling operators and their B2B suppliers, on issues ranging from licensing regime, technical and regulatory requirements, advertising, IT, technology and consumer protection matters.

Authors

Cosmina Simion is managing partner of the firm, and is an intellectual property, regulatory and technology lawyer, with more than 20 years of professional experience, and expertise in various industries, with an emphasis on the media and entertainment, online and gaming industries. Prior to setting up Simion & Baciu, she co-ordinated teams of individuals at the largest Romanian law firm, set up and headed the IPT practice of a global law firm, as well as acted as in-house CEE regional counsel for a US media group. She regularly advises software development companies, as well as private equity funds, in relation to the protection of their intellectual property, drafting and negotiation of software and trade mark licence agreements, joint venture agreements, assignment agreements, SaaS agreements, etc, as well as telecom operators in relation to intellectual property risks arising in the context of retransmission agreements and white label agreements. Cosmina is a member of: the Bucharest Bar; the Romanian National Chamber of Industrial Property Attorneys; the International Masters of Gaming Law (IMGL), General Member; the International Trademark Association (INTA); and the American Chamber of Commerce (AmCham).

Andrei Cosma is a senior associate with more than five years of expertise as a fully qualified business lawyer specialised in regulated industries. In addition to having regulatory gambling experience, Andrei is well-versed in dealing with new technologies, including blockchain, cryptocurrencies, artificial intelligence and fintech. He has been involved in a wide variety of complex legal projects for prominent clients in the gaming field, foreign investors, media giants and high-profile retail operators. Andrei is a frequent contributor to specialised international publications and a regular presence at international conferences in the industries he is focusing on. He is a member of the Bucharest Bar and the American Chamber of Commerce in Romania (AmCham).

Ana-Maria Coruga is a senior associate lawyer whose expertise spans several practice areas such as intellectual property, data protection, technology, media and advertising for clients in various industry sectors worldwide. While involved in various life science, intellectual property and data protection projects, Ana-Maria tailors her assistance to the client's needs within a rapidly growing digital market, confronting and overcoming operational and legal challenges enacted by the new technologies, including in sectors of high interest and impact. She also advises clients from the retail and FMCG sector on a regular basis on issues such as labelling and product recalls, promotions and sweepstakes as well as distance rules. Ana-Maria is a member of the Bucharest Bar and the American Chamber of Commerce in Romania (AmCham).

Teodora Popescu is an associate at the firm, handling a wide area of legal matters, ranging from civil, commercial, and employment law issues, to new technologies, IT and gaming matters, where she assists clients on detailed regulatory and licensing issues. In addition, she has also advised clients active in the retail and FMCG sectors on different regulatory matters, including consumer protection and advertising. Prior to getting a degree in Law, Teodora achieved a BA and an MA in Languages and Literatures, practicing as a certified translator of English and Spanish. She is a member of the Bucharest Bar and the American Chamber of Commerce in Romania (AmCham).

Simion & Baciu

11 Maior Alexandru Campeanu St
1st floor, Unit 3
Bucharest 011235
Romania

Tel: +40 31 419 04 88
Fax: +40 31 419 04 88
Web: www.simionbaciu.ro