Chambers

GLOBAL PRACTICE GUIDES

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

TMT

France

Bertrand Liard, Clara Hainsdorf,
Saam Golshani and Guillaume Vitrich
White & Case LLP

practiceguides.chambers.com

2021

FRANCE

Law and Practice

Contributed by:
Bertrand Liard, Clara Hainsdorf, Saam Golshani and Guillaume Vitrich
White & Case LLP see p.15

Contents

1. Cloud Computing

1.1 Laws and Regulations

Cloud Computing

While there is no official definition of cloud computing, the notion usually covers the use of a remote information system, under the control of the client on a shared platform. Cloud services refer to a variety of services, such as infrastructure as a service (IaaS), software as a service (SaaS) or platform as a service (PaaS). They allow a client to switch part or all of its IT infrastructure and resources to the cloud, rather than managing it locally or internally.

Under French law, there is no particular contractual law category related to cloud computing contracts. As such, they are subject to common French contract law. Particular attention should be given to the content of the contract, notably regarding data integrity and security, service level agreements (SLAs), the clear division of the responsibilities of each party, and compliance with data protection laws and regulations. In addition, the termination of the contract should also be anticipated with the use of precise clauses such as notice periods, chain termination of contracts, reciprocal restitution, reversibility, etc.

Cybersecurity Implications

Cloud service providers are qualified as "digital service providers" under the EU Directive Network and Information Security (NIS Directive), which was transposed into French law, notably in Law No 2018-133 of 26 February 2018. As a result, they are subject to specific cybersecurity obligations such as carrying out risk assessments on their system, taking technical and organisational measures regarding the security of their systems, implementing processes for managing security incidents, and, if required, notifying the French National Cybersecurity Agency (ANSSI) of any such incidents.

Data Protection Implications

Cloud computing services usually involve storing and sharing data that may fall within the scope of regulations on the protection of personal data. Therefore, it is essential that any cloud project be compliant with data protection laws and regulations. As such, the General Data Protection Regulation (GDPR) and the French Data Protection Act of 1978, as amended in June 2019, will be applicable to the processing of personal data within a cloud project.

Importantly, it will be necessary to assess whether the cloud service provider will act as data controller or data processor regarding the personal data processed by the cloud service. In most cases, the cloud provider will be qualified as data processor and the client as data controller, but this may vary depending on the nature of the processing and the general cloud project. In addition, transfer of data outside of the EU must be carried out only with appropriate safeguards. To ensure this, a contractual framework must be put in place between the provider and the client, which must also address the requirements provided for in Article 28 of the GDPR regarding data processing.

Regulation in Specific Industries

The banking industry is subject to specific provisions regarding cloud computing. Indeed, on 25 February 2019, the European Banking Authority (EBA) adopted new guidelines on outsourcing. These guidelines include specific provisions – for instance, regarding the protection of confidentiality and personal or sensitive information; and the need to comply with all legal requirements relating to the protection of personal data, banking secrecy or confidentiality obligations concerning customer data. The French supervisory authority for banks and insurance (ACPR) has published a notice to ensure that these guidelines are followed in France.

Finally, the insurance industry is also subject to similar requirements. On 6 February 2020, the European Insurance and Occupational Pensions Authority (EIOPA) published its Guidelines on Outsourcing to Cloud Service Providers, which provides guidance to insurance and reinsurance providers on how outsourcing should be carried out to cloud service providers in order to comply with their industry-specific regulations. The ACPR has also published notices relating to the modalities for the implementation in France of the EIOPA guidelines.

2. Blockchain

2.1 Legal Considerations

Risk and Liability

Blockchain technology enables the creation of a decentralised and unmediated database or register that allows a transaction or entry (also called "token") to be automated, authenticated and time-stamped, while guaranteeing its immutability and inviolability. When public, the main characteristic of a blockchain is that it operates without a central control body and without intermediaries.

Blockchains' governance and the legal force of operations carried out using this technology are problematic, since there is currently no actual legal framework specifically for blockchain technology, leading to the application of numerous and sometimes unadapted and uncoordinated laws.

Up to now, few provisions relating specifically to blockchain technology have been incorporated into French law:

- Article 223-12 of the French Monetary and Financial Code allows the registration of minibonds in the blockchain, created by the ordinance No 2016-520 of 28 April 2016, Article 2;
- Order 2017-1674 of 8 December 2017 introduces into the French Monetary and Financial Code the registration and custody of securities and financial instruments in a "shared electronic registration system" (*"dispositif d'enregistrement électronique partagé"*, or DEEP), the name describing a blockchain;
- Decree No 2018-1226, relating to the use of a shared electronic recording device for the representation and transmission of financial securities and for the issue and sale of minibonds, was issued on December 24, 2018. Article R 211-9-7 of the French Monetary and Financial Code stipulates that the DEEP "*is designed and implemented in such a way as to guarantee the registration and integrity of the entries and to make it possible, directly or indirectly, to identify the owners of securities and the nature and number of securities held*";
- the PACTE law of 22 May 2019 gives issuers established in France the possibility of issuing utility tokens approved by the Financial Markets Authority (AMF), and provides for an optional regime for service providers on digital assets.

These provisions concern blockchain technology in its function of transferring or holding assets, but do not apply to other types of blockchain use cases – eg, smart contracts, bitcoin, etc.

"Regulatory sandboxes" may be one of the options allowing companies wishing to offer services related to blockchain technology to be protected against any risk of contravening current or future legislation. By giving legal certainty, these "regulatory sandboxes" give innovation a chance, while at the same time making use of existing resources and positive law.

Blockchain and Proof

Blockchain technology is of interest to many industries (entertainment, luxury goods, finance, insurance, food, etc), as it allows for reliable and secure information recording and tracing (dissemination of intellectual property rights on works, provenance of art objects, origin of products giving back confidence to the consumer).

Furthermore, blockchain technology has interesting aspects in relation to time-stamping, electronic signature and electronic evidence in general.

Because of the traceability guaranteed by the time-stamping function and the immutability of the transactions, blockchain protocols could partly meet the specifications of the European regulation No 910/2014 of 23 July 2014 (known as the eIDAS regulation). In fact, on private blockchains, it is entirely possible to parameterise the technology so that it meets requirements to constitute legally binding evidence, and to have it contractually accepted by the participants. The legal effect is less certain in public blockchains, and it will be up to the judge to determine their probative value, in view of the circumstances of the case, as provided for by Article 1316-2 of the French Civil Code.

Blockchain and Contracts

Blockchain is used to create so-called "smart contracts". In reality, smart contracts are neither smart nor contracts, they are programs which execute pre-defined operations when certain conditions are met (eg, providing code to action lock when a financial institution confirms money has been received). They are execution modalities and necessarily part of a larger contract (in our example, a rental agreement).

Smart contracts need to be as simple as possible so that computers can execute them spontaneously. Therefore, negotiation and interpretation must be kept to a minimum. As a result, such contracts might not be used, in national law, when various procedural requirements must be fulfilled (formal notice, prior notification, handwritten mentions, etc).

Blockchain also poses difficulties regarding the conditions for the validity of the contract, the applicable law to transactions, and liabilities issues. The contract concluded on the blockchain, whether international or national, cannot exist without attachment to state laws. A recent decision of the Court of Cassation recalled the impossibility for the parties to have the contract governed by rules other than a state law (Court of Cassation, 1re civ, 17 May 2017, No 15-28.767).

Intellectual Property

One of the potential limiting factors of blockchains could come from intellectual property and the impossibility of protecting certain elements composing it. This is because the latter are not always protectable.

This is not the case for the source code, which can be protected under copyright. Software and graphic interfaces can also be protected by copyright (Intellectual Property Code, Article L 112-2). Tokens that are software could be protected as such. The software will often be a collaborative work within the meaning of Article L 113-3 of the Intellectual Property Code.

Under certain strict conditions specified by Article L 611-10 of the Intellectual Property Code, the software may also benefit from the protection provided by patent law.

Algorithms are, in principle, not protectable because the ideas are free to be used. However, they can be protected under the

protection of trade secrets (and confidentiality agreements), which only applies to private blockchains.

In public blockchains, the principle is to make the software and its source codes available to everyone, so that the entire community can use, copy, distribute, and even modify it to test security and improve performance.

The legislation relating to databases can apply to the data automatically stored in the chain.

We have seen the following applications of blockchain technology in the intellectual property field:

- to prove the anteriority of a work;
- to verify the authenticity of the works;
- to facilitate the payment of rights every time the work is sold or exploited.

Data Privacy

Blockchain technology raises interesting issues in relation to privacy. It could be used to foster privacy through the creation of a secure digital identity, but it could also be technically challenging for a blockchain system to comply with the privacy rules due to its very specific features (decentralisation, encryption, immutability, etc).

Controllers

In public blockchains there is no data controller, but there is one in private blockchains. The introduction by the GDPR of the notion of co-controllers and the reinforcement of the obligations of the processors, of the co-operation between the latter and the controller (assistance towards the data subjects, the deletion or return of all data, right to audit) and the joint and several liability of the data controller and the processor, will make it more complex to determine the liability of each of the parties involved in the blockchain, requiring a precise case-by-case analysis of the role of each of them.

The CNIL (French Data Protection Authority) provides some answers by proposing that a participant in a blockchain be qualified as a joint controller, who has a right to write in the chain and who participates in the same data processing. As for data-miners, they would only be users and in no way data controllers, insofar as they have not determined the purposes of the blockchain.

Data Transfer outside the EU

An open blockchain, which by definition is transnational, necessarily raises questions about data transfers outside the European Union. The CNIL advocates the development of private blockchains, which allow better control over the governance of personal data. Where appropriate, it is recommended to use binding corporate rules or standard contractual clauses applicable in private blockchains.

Right to Delete Data Entered in the Blockchain

Concerning the "right to be forgotten" and the securing of data once it has been put into the blockchain, the CNIL suggests a two-step system. First, the data storage must be as secure as possible, using the latest encryption techniques while excluding storing information in clear text. Second, the CNIL recommends acting via the encryption key: by destroying this key, no one will be able to understand the data. The user therefore remains in control of his data thanks to the encryption of the blockchain. An alternative to step two is the anonymisation of data.

Service Levels

Improved transaction times are quite often the main rationale of blockchain projects in the financial industry and this is why service levels matter. However, for public blockchains, by definition, no service level can be agreed upon with a central operator. The typical example of long transaction time is bitcoin, due to the decentralisation and heterogeneity of the network and the choice to require a proof of work (ie, mining).

On the other hand, operators of private blockchains are able to offer contractually guaranteed service levels, as for any other IT system. The type of service levels we have seen in such case are availability of the system and transaction times.

Jurisdictional Issues

To date, there is no case law in France concerning blockchain technology. In general, French courts are accepting of jurisdiction when damages are suffered on the French territory, and/or when the parties designate France as the jurisdiction in case of dispute.

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

3.1 Challenges and Solutions

As the issues and challenges of big data, artificial intelligence (AI) and machine learning are similar, the following points are common to all of them.

Big Data

Big data technologies have enabled the emergence of AI: this requires both high computing power and large volumes of data to train and test models. Companies are now looking to integrate AI into their business processes and information systems.

On issues such as image and voice recognition, AI innovations have reached an advanced level. Consequently, two major issues have arisen related to the big data: the protection of personal data and the reuse of public data with the phenomenon of "open data".

For instance, in order to train AI's system or machines to best fit users' or companies' needs – advertising, internet of things (IoT), etc – AI requires a huge amount of data. Nevertheless, merging and exploiting several datasets during the processes of data mining sometimes delivers information that can allow the inference of very intimate personal information with a very high degree of accuracy. As a result, the governance arrangements for the collection and processing of digital data have very profound implications for human rights and accountability. On a more down-to-earth approach, companies may have to collect, process and store personal data on databases for business purposes and for a certain amount of time. Therefore, some warranties have to be given by the companies processing such data.

Data Protection

The protection of personal data is ensured by the EU General Data Protection Regulation (GDPR) implemented in France in the law of 6 January 1978 entitled *Informatique et Libertés*. The GDPR grants rights to users whose data is processed, including the rights of rectification, deletion and access in order to give the user control over his data. It also obliges data controllers to take effective and precise security measures to avoid endangering the personal data being processed. The obligations of the data controllers also include an obligation to minimise data, transparency and legitimacy in relation to the purpose of the processing. Individuals whose data are being collected, processed or stored must be informed of the purposes of such processing, which also has to rely on one of the legal bases given by the GDPR and embedded in the French law.

These rights, and especially the purpose restriction and prior information, must be considered when launching a big data project, since it is unlikely that the user would have been informed of a purpose and processing that had not even been envisaged when the data were collected.

One way to address this issue is to anonymise or pseudonymise the data so that it is impossible to identify individuals by gathering the data, but this is not always technically feasible.

Responsibility/Liability

As AI can take decisions with a degree of autonomy, a key legal issue is responsibility/liability. As of today, no legal regime is in place to deal with the liability of a robot or a machine that would act according to an autonomous AI process – autonomous cars, for example. Does the damage come from a failure of the algorithm or the decision-making of the robot itself? Who is responsible if there is no human driver?

The problem of the liability regime applied to AI lies in the unpredictability and stability of AI systems, because it is sometimes complicated to understand why a system has reacted in such and such a way. In France, it is then necessary to look for the legal basis in the tort liability of Articles 1240 and the Civil Code, which states that any damage caused must be remedied by the person who caused it. Regarding tort liability, French law sets out three conditions that need to be fulfilled for liability to be attributable to a party: fault, damage and a causal link between the two. The burden of proof lies with the claimant. However, this regime is not adequate in that it requires the presence of a legal personality to be applied, and AI systems do not have such personality.

Intellectual Property

Many elements of a big data and/or AI systems may be protected by intellectual property rights (or assimilated): content, algorithms under certain conditions, computer programs, models, robots, database, etc. It is necessary to take into account the protection of each element (patent, copyright if original and specific form for content, for example, or computer programs, designs for robots, etc).

Of particular interest is the protection of creations by AI, since AIs are already creating a lot, from works of art to algorithms and computer programs. It is obvious that the intellectual property protection system is based on human creativity, which will render the works of AI difficult to protect under the prevailing circumstances. We have not identified any case law in France, but, in the DABUS case, the European Patent Office has denied patent protection of an invention by AI on the grounds that no human was named as inventor. There are workaround solutions, such as naming a physical person as inventor or author, but this does not fully solve the issue, and a legislative intervention seems necessary on this topic.

4. Legal Considerations for Internet of Things Projects

4.1 Restrictions on a Project's Scope

Liability

The question arises as to who is responsible in the case of damage caused by a connected object. As French law stands, there is no specific legal framework applicable to the liability for connected objects or connected robots. General liability rules will then apply. A distinction must be made between contractual and extra-contractual liability. In addition, several liability regimes

may apply, in particular defective products or the custody of the object.

However, these regimes do not fully meet the challenges related to connected objects and artificial intelligence in general. It seems necessary either to adapt the existing regimes or to create a specifically adapted regime. At the present time, no specific regime is in gestation for connected objects; these are only envisaged in relation to personal data.

Data Protection

The French Data Protection Act of 6 January 1978, amended following the implementation of the GDPR, regulates the liability of the various actors involved in the data collection, processing and storage process. It imposes obligations of security and transparency vis-à-vis the data and the user for both the data controller and the data processor or subcontractor. It also allows individuals, whose data are being collected to access their data, modify them or erase them. The difficulty lies in the identification of these different actors in IoT projects. This can be complicated due to the interoperability of the connected objects and their communication system allowing them to exchange data at any time.

Beyond the obligations imposed by GDPR and French data protection law, the *Commission Nationale Informatique et Libertés* (the French authority enforcing data protections legislations) also recommends to proceed to Data Protection Impact Assessments when implementing IoT projects before processing personal data in order to highlight the purposes of the processing and the legitimate means of achieving them.

Consent

Consent is one of the legal bases for any data processing. In IoT devices, it is not always possible to request consent directly. Therefore, in order to implement the GDPR requirements for freely given, specific, informed and unambiguous consent, IoT manufacturers must find other ways to collect consent.

Consent may have been given for a specific processing only when the data is in fact communicated from one object to another, and collected or even used by the manufacturer of this object, and so on.

Cybersecurity

In January 2019, the French National Institute for Research in Digital Science and Technology (INRIA), published a white paper on cybersecurity. This study shows that vulnerable connected objects represent a risk because a breach in their components can have an impact on thousands of people. Breaches can thus be exploited to divert objects from their main uses, such as involving them in large co-ordinated cyber-attack (eg, an attack using Mirai software).

INRIA has developed SCUBA, a tool which automatically evaluates the risk of a connected object in its environment. SCUBA allows to audit the security of a connected device in its global environment.

For example, SCUBA made it possible to detect a security breach between a connected doorbell and its service in the cloud. The doorbell, with a camera, sends a picture of the person at your door to the cloud and then sends it to your phone. However, this communication between the doorbell and the cloud is not encrypted and the photo is sent in a clear message, allowing an attacker to intercept the message containing the photo and replace it with another one.

5. Challenges with IT Service Agreements

5.1 Legal Framework Features

Parties' Level of Expertise

Most issues arising from IT service agreements relate to late or wrong performance of the parties' respective contractual obligations. Because of the technical aspect of an IT service agreements, the allocation of responsibilities between the parties is key. In many instances, customers are not very familiar with the technology supplied by the service provider, which is therefore subject to an obligation of advice and information during the negotiation (Article 1112(1) of the Civil Code) and the performance of the agreement (Article 1104 of the Civil Code). This obligation implies (i) an obligation to provide information (the service provider must inform itself about the customer's needs and wishes); and (ii) an obligation to warn (eg, in the event the service provider considers that the customer's expectations are unlawful or risky, it has a duty to inform the customer and may even refuse to contract with the customer on this basis). As for the customer, it has a duty to collaborate with the service provider.

Furthermore, in 2016 French law extended the protection against unfair clauses to B2B agreements. As a result, most of those IT service agreements, which customers cannot actually negotiate because they are imposed on customers by service providers, may qualify as pre-formulated standard agreements (*contrat d'adhésion*), which terms may be unfair if they create a significant imbalance between the rights and obligations of the parties. Unfair clauses are deemed unwritten, and if essential clauses are thus unenforceable then the whole IT service agreement may be also unenforceable.

Liability of the Service Provider

One of the main challenges in IT services agreements is to assess the existence and the extent of the provider's liability, as providers usually tend to impose an exclusion or a limitation of liability clause. It is thus strongly recommended to clearly indicate whether providers are subject to a performance obligation (where the provider must reach a specific result) or an obligation of best efforts. In particular, providers will try to exclude or limit their liability by excluding indirect damages; such exclusion is authorised under French law, although providers will try to have a broad definition of "indirect damages" to include loss of data, loss of clients, breach of data privacy, etc. Unless these liability clauses deny the essential obligation of the provider – in which case they are prohibited – liability clauses (including the amount of the liability cap, if any) are often one of the key topics of the parties' service agreement negotiations.

However, because the parties do not have the same bargaining power, especially when customers are consumers or businesses with no IT expertise or when the product is complex or customised, those clauses may be more easily challenged and unenforceable. In order to better identify providers' contractual breach, customers would be advised to detail their needs as much as possible and to set out clear specifications in terms of performance (eg, through a service level agreement) or in terms of timeframe (eg, including provision for liquidated damages).

Service Level

In order to assess whether the service provider has complied with its obligations under IT service agreements, in particular its obligation to reach a specific result, the parties usually agree on service levels and a quality assurance plan. This implies the definition of key performance indicators and the payment of penalties in the event those indicators are not met.

Changes in the Economic Situation of the Parties

The COVID-19 pandemic has recently illustrated that, in some cases, the parties' economic situations may change and that IT service agreements may need to be adjusted accordingly. Article 1195 of the Civil Code allows a party to any agreement, if a change in circumstances unforeseeable at the time of the conclusion of the agreement makes performance excessively onerous for such party that had not agreed to assume the risk, to request a renegotiation of the agreement with the other party. Note, however, that parties may agree not to apply Article 1195.

In addition, parties may also agree on a price revision mechanism, usually by providing indexation clauses (although Article L 112-2 of the French Monetary and Financial Code prohibits indexation on the general price level, the prices of goods, or products and services unrelated to the subject matter of the agreement), benchmark clauses (that allow the financial adjustment of the agreement according to the prices charged by the service provider's competitors), or hardship clauses (that provide for a renegotiation of the IT service agreement in the event of a disruption in the economic conditions of the agreement or an exit from the agreement).

Specific IT Service Agreements

With respect to software license agreements, one of the main issues is whether the licensee is allowed to repair or correct any bug – in other words, whether the licensee may perform, or have performed by a third party, the maintenance of the software, or if such maintenance must/can only be carried out by the licensor. French law allows software editors to retain the right to correct bugs, which creates serious difficulties for licensees that have not entered into a maintenance agreement with the editor/licensor.

In the event a customer enters into a license agreement and a maintenance agreement (and/or any other IT service agreements) with the same service provider, those agreement may or may not be interdependent. It is therefore highly recommended to provide contractually whether the expiration or early termination of one IT service agreement automatically puts an end to the other IT service agreements. Once IT service agreements are terminated or expired, customers will often enter into new IT service agreements with third parties, in which case it is key to ensure that a reversibility clause will allow customers to benefit from a smooth transition from a service provider to another.

6. Key Data Protection Principles

6.1 Core Rules for Individual/Company Data

Core Rules Regarding Data Protection

The core rules regarding data protection in the French jurisdiction are embedded in the French Data Protection Act (Law No 78-17 of 6 January 1978 relating to data processing, the files and freedoms, *Loi Informatique et Libertés*), which implemented the GDPR. Both GDPR and the French Data Protection Act set up several transparency and security obligations for the data controller and data processor, as well as several rights and warranties for the individuals. According to Article 3, the French Data Protection Act is applicable with respect to national provisions referred to by GDPR, whenever the data subject resides in France (hence, including when the data controller is not established in France).

As opposed to the legislation of many countries, the French Data Protection Act also governs the personal data of deceased persons, per the request of the data subject himself or herself before his or her death, or by the data subject's heirs. It also provides for specific rules with respect to personal data on health.

The French Data Protection Authority (the *Commission Nationale Informatique et Libertés* or CNIL) is in charge of ensuring compliance with the French Data Protection Act and the GDPR (including by issuing sanctions). It also issues regular guidelines and clues for interpretation on several important issues such as the internet of things, data conservation, the legal basis for consent, etc.

Moreover, while the GDPR only deals minimally with the criminal field, it is Directive No 2016/680 of 27 April 2016, known as the "Police-Justice" Directive, that governs the special regime applicable to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences and the enforcement of criminal sanctions.

While many obligations contained in the GDPR and this directive are identical, the directive contains additional specific obligations. For instance, the data controller has to establish, where appropriate and to the extent possible, a clear distinction between the personal data of different categories of data subjects, such as persons convicted of a criminal offence, victims of a criminal offence, third parties to a criminal offence, etc. It also has to identify whether personal data are factual data or data based on personal assessments and verify the quality of the data. Such processing must be lawful – that is to say, necessary for the performance of a task carried out by a competent authority for the purposes laid down by this Directive and based on EU law or the law of a member state. Processing of sensitive data may only be authorised in cases of absolute necessity (Article 10).

Distinction between Companies/Individuals

As the GDPR, the French Data Protection Act only applies to individuals to the exclusion of companies. Data relating to companies (ie, non-personal data) may, however, be protected by non-disclosure agreements, trade secrets or professional secrecy.

General Processing of Data

General data processing concerns all data, both personal and non-personal. Non-personal data are regulated by Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the Re-use of Public Sector Information and the Regulation of the European Parliament and of the Council on European Data Governance (2020/0340 (COD)) published on 25 November 2020. When a data controller processes personal data and related non-personal data, it must verify that its processing complies with the GDPR.

GDPR defines data processing in a very extensive way: "Any operation or set of operations carried out or not using automated processes and applied to personal data or sets of data, such as collection, recording, organization, structuring, conservation, adaptation or modification, extraction, consultation, use, communication by transmission, dissemination or any other form of making available, approximation or interconnection, limitation, erasure or destruction". This definition also applies to processing of non-personal data.

The general processing of data covers a large scope of operations carried out on data, whether automated or manual. The processing of data is not necessarily automated: paper files are also concerned and must be protected under the same conditions.

Processing of Personal Data

Regarding the processing and the retention of personal data, individuals whose data are being processed or held must be informed of the rights they can summon before the data controller such as a right to rectification, modification, access, deletion, opposition and limitation. Furthermore, when data are being processed, data controllers or processors must comply with a principle of data minimisation. Personal data is "*any information relating to an identified or identifiable natural person*" (eg, an ID number or a credit card number) as defined in Article 4 of the GDPR. Therefore, if personal data is processed by companies responsible for processing, the personal data concerned must have rights over the personal information they transmit. The French Data Protection Act supplemented the GDPR in relation to a few issues:

- age of consent (15 years old);
- personal data that can be transferred internationally on the basis that the transfer is necessary to protect the public interest;
- personal data of deceased persons;
- health, biometric and genetic data;
- processing of personal information relating to criminal offences or convictions, which can be carried out by any person for the purposes of legal proceedings and enforcement, for a period strictly proportionate to these purposes.

The CNIL has issued a list of 14 processing activities for which an Impact Assessment is mandatory, and another list of 13 processing activities for which an Impact Assessment is not necessary.

7. Monitoring and Limiting of Employee Use of Computer Resources

7.1 Key Restrictions

The Use of Professional IT Equipment

The employer has the right to access and to consult the files on an employee's professional computer, except for documents identified as personal by the employee with a specific mention along the lines of "personal" or "private". The employer does

not have to justify any particular steps to have the activity of its employees, at the time and place of work, monitored by a superior or an internal company department (Court of Cassation, Social Chamber, 5 November 2014 No 13-18427; Court of Cassation, Social Chamber, 26 April 2006, No 04-43582).

Words such as "my documents", "confidential", "employee's first name" do not constitute identification of personal files (Court of Cassation, Social Chamber, 8 December 2009, No 08-44.840; 21 October 2009, No 07-43.877). Additionally, an employee should not use the entire hard disk of his professional computer, which is supposed to store professional data, for private use (ECHR, 22 February 2018, No 588/13). Case law considers, however, that downloading large personal files on a professional laptop does not constitute serious misconduct or a real and serious cause of dismissal (Court of Cassation, Social Chamber, 25 October 2017, No 16-11.173).

In any case, the employer must exercise caution in using the possibilities offered by technology to control its employees. In particular, the company's social and economic committee, like the works council, must be informed and consulted on the means or techniques used to monitor employee activity (Article L 2312-38 of the French Labour Code; Article L 2328-1 of the French Labour Code).

Use of Remote-Control Software

With the health crisis of COVID-19, teleworking has become generalised in many companies. Employers may more easily control employees' activities remotely. However, the use of remote-control tools does not comply with the principle of proportionality and finality provided for by French law. Such use must therefore be strictly controlled. The user must be informed prior to collection, and agree to give permission to the IT administrator before any intervention on his or her workstation.

Traceability of maintenance operations must also be provided for. IT service agreements concluded by the employer should also specify obligations borne by the maintenance provider to only access computer data that are strictly necessary for their missions and ensure their confidentiality.

Internet Connection Control

An employer cannot prohibit in a general and absolute manner the use of professional computer equipment for personal purposes, as case law prohibits the employer from infringing on individual freedoms in a disproportionate manner. Only clear abuse or illicit use of the computer tool for personal purposes can be prohibited (CA Dijon, Court of Cassation, Social Chamber, 27 May 2004, No 03/00584). For example, case law considers connections for non-business purposes for 41 hours per month to be abusive (Court of Cassation, Social Chamber, 26/02/13, No 11-27.372; Court of Cassation, Social Chamber, 18 December 2013, No 12-17.832). An employer who dismisses an employee for excessive use of the internet for personal purposes must, however, ensure that he or she is indeed the author of these connections (Court of Cassation, Social Chamber, 3 October 2018, No 16-23.968). An employer also cannot dismiss an employee for time spent sending tweets that are unrelated to work during working hours when the time actually spent is rather limited, here four minutes per day (CA Chambéry, 25 February 2016, No 15.01264).

Before an employer can implement any connection-monitoring system (ie, website filtering devices, monitoring tools, virus detection, etc), the employees' representative bodies must be informed and consulted and each employee must be individually informed of the purposes, the recipients of the data, the right of access and rectification and the right to object for a legitimate purpose they may have.

In addition, an employer may review employee internet connections, since they are presumed to be of a professional nature (Court of Cassation, Social Chamber, 9 July 2008, No 06-45.800; Court of Cassation, Social Chamber, 9 February 2010, No 08-45.253).

Phone Tapping

Considering the risks of invasion of privacy, the employer is not allowed to listen to employees' telephone conversations, except on an ad hoc basis and for training or assessment purposes (eg, for staff training to improve telephone reception) and in accordance with strictly supervised procedures.

In such cases, before the listening or recording system is set up, the employee must inform employees by any means and consult with employee representatives.

However, the employer can set up a system to control phone communications within the company, to ensure the non-abusive use of the business telephone line from the switchboard and from call records.

Control of Internet Usage and Employee's Messaging System

Employers can implement tools to measure the frequency of sending and/or the size of messages, "anti-spam" filters, etc. However, such control should by justified by a legitimate interest (ie, security problems, preservation of trade secrets, the need to avoid abusive or prejudicial uses to the company, etc).

As a principle, emails exchanged by an employee are professional by nature. The employer can therefore have access to and read them, including in the absence of the employee. However,

if the email is clearly identified as personal – for example, if the subject line clearly states that it is a private or personal message – the employer should not read it, and must respect the secrecy of correspondence. In order for an employee to have access and read personal emails or documents, the employer must first call the employee, and if the latter does not answer, it can access the emails but only in case of a specific event or risk.

Emails sent by an employee from his or her personal messaging inbox, including when such personal messaging inbox is used from a professional IT equipment, may not be accessed by the employer.

8. Scope of Telecommunications Regime

8.1 Scope of Telecommunications Rules and Approval Requirements

Relevant Technologies

Local telecommunications rules traditionally apply to electronic communication networks (ECNs) and electronic communication services (ECSs) (Article L 32, No 2 and No 6 of the French Postal and Electronic Communications Code).

At an EU level, however, the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (the EECC Directive) modified and updated the applicable framework. The EECC Directive should have been transposed in EU national laws before 21 December 2020. In France, the EECC Directive must be transposed by an ordinance, which has not been published yet.

Importantly, the EECC Directive expands the definition of ECSs by including so called "interpersonal communications services", defined as services normally provided for remuneration that enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s).

Accordingly, and subject to the transposition ordinance of the EECC Directive, voice-over internet protocol (VoIP) and instant messaging falls under the new scope of the telecommunications rules. This was confirmed by Recital 15 of the EECC Directive, and is in line with ECJ's previous ruling, which considered that SkypeOut offering a VoIP service constitutes an ECS (ECJ, 5 June 2019, C-142/18).

The qualification of radio-frequency identification (RFID) as ECS remains unclear, as it is not specifically covered by the new scope of the telecommunications rules. However, the French telecommunication authority (*Autorité de Régulation des Communications Électroniques et des Postes* or ARCEP) considers RFID technology as radio-electric installations, which can be used on certain frequencies only and with defined technical settings.

Applicable Requirements

Currently, the provision of ECSs, as well as the establishment and operation of ECNs, are free and must only comply with the declaratory regime in place (Article L 33-1 of the French Postal and Electronic Communications Code). It must be noted, however, that such a declaratory regime would no longer be applicable with the EECC Directive.

The declaration (which can be found online) must:

- be sent to the ARCEP by registered letter with acknowledgement of receipt;
- be written in French; and
- include the identity of the applicant, including its name, full address, legal status, registration documentation, as well as a brief description of the nature and characteristics of the ECS or ECN, geographical coverage area, and a schedule for deployment.

The ARCEP then has a period of three weeks to issue a declaration of receipt, or to inform the applicant that the declaration does not comply with the requirements and ask the applicant to complete or correct the declaration. The ARCEP also has the power to register ex officio, on its own initiative, an ECS or ECN the activity of which falls within the scope of telecommunication law but which has not registered itself with the ARCEP.

As an exception to the declaratory regime, ECSs and ECNs can be subject to a prior authorisation of the ARCEP, when resources are rare (frequencies such as 5G or numbers).

In France, every operator must pay an administrative tax under the conditions provided by the finance law. It must also pay an additional fee in case of use of a specific frequency or the provision of a specific numbering.

In addition, in accordance with the EECC Directive, providers of ECNs and/or ECSs are required to take measures to safeguard the security of their networks and/or services, and to prevent or minimise the impact of security incidents.

Notably, providers of instant messaging are subject to stricter data protection law requirements with regard to messages under the Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communi-

cations sector (the ePrivacy Directive). This Directive notably obliges member states to ensure the confidentiality of communications and the related traffic data by means of an ECN or ECS through national legislation.

9. Audio-Visual Services and Video Channels

9.1 Audio-Visual Service Requirements and Applicability

Requirements and Procedure for Providing Audio-Visual Services

Audio-visual services traditionally cover TV, radio and on-demand audio-visual media services (AVMS). AVMS include services commonly referred to as on-demand video services (VOD), catch-up television and audio podcasts.

Audio-visual services are subject to the Law 86-1067 of 30 September 1986 on the freedom of communication and regulated by an independent administrative authority, the *Conseil Supérieur de l'Audiovisuel* (CSA).

While the requirements and associated procedure for providing an audio-visual service will depend on the nature of the service, there are general obligations to which all providers are subject to. Indeed, the CSA will make sure that providers do not undermine the dignity of the human person or the rights relating to privacy and comply with specific provisions concerning the protection of minors. In addition, programmes must promote the use of the French language, not undermine the protection of public order, and must be free from any incitement to hatred or violence.

For TV and Radio Providers

The CSA must grant authorisation to TV and radio providers using the network on assigned frequencies before they can provide their services. Private providers have to participate in a call for applications and be selected by the CSA in order to be provided with an assigned frequency. The applications must be presented by the provider of the services, and must notably contain the general and technical characteristics of the service, the forecasts of expenditure and income and the composition of the applicant's shares, governing bodies and assets.

The provider must also sign an agreement with the CSA, which sets the specific rules applicable to the service, taking into account its coverage and its share of the advertising market, as well as the compliance with competition rules. The authorisation provided by the CSA may not exceed ten years for TV services and five years for radio services, but can be renewed up to two times without going through a new call for application.

For other services provided without using the assigned frequencies, the applicable procedure will depend on the service. As a principle, such services may be broadcast only after entering into an agreement with the CSA, defining their specific obligations and the contractual penalties available to the regulator in case of non-compliance. However, services with a budget under EUR75,000 for radio and EUR150,000 for TV are only required to make a prior declaration rather than entering into an agreement.

Finally, distributors of audio-visual services not using assigned frequencies (for instance, providers offering a television "package" service) are subject to a prior declaration before distributing such services. Such declaration must notably include the corporate form, the name or business name and the address of the head office of the service distributor, the list of services and the structure of the offer of services made available to the public, as well as a letter of intent to conclude a distribution agreement from a paid television service.

For AVMS Providers

AVMS must be declared to the CSA prior the provision of such services. The purpose of such declaration is to facilitate the identification of AVMS, better ensure their regulation and be able to verify their obligations. This declaration must notably include the description of the service and the designation of a responsible person, and can be completed online.

Requirements for Companies with Online Video Channels with User-Generated Content

Video-sharing services were traditionally excluded from the scope of AVMS when the user content was provided without the editorial control of the service provider.

A major reform was conducted at the EU level via the revised Audiovisual Media Services Directive (Directive (EU) 2018/1808 of 14 November 2018). This Audiovisual Media Services Directive extends certain audio-visual rules to video-sharing services, such as YouTube. It has been transposed in France by an ordinance dated 21 December 2020 and published on 23 December 2020.

In order to be considered as a video-sharing service, the service must meet the following conditions:

- it is provided by means of an electronic communications network;
- it provides user-created programmes or videos to inform, entertain or educate as its main purpose;
- it has no editorial responsibility for the content;
- it is related to an economic activity.

Such video-sharing services are subject to specific obligations. In addition to ensuring that the services comply with the general obligations regarding content, the CSA will also have additional powers – for instance, being in charge of dispute resolution between users and providers of these services or making sure that these providers comply with transparency obligations.

Note that these powers are limited to video-sharing platforms which are established in France, as the principle of country of origin applies. However, video-sharing services established in other member states may be subject to the French system of contributions to the production of cinematographic and audiovisual content, even though they will remain regulated by their country of origin.

Specifically, regarding the possibility for online video channels with user-generated content operated by companies to be considered as an AVMS, this assessment needs to be made on a case-by-case basis.

In this respect, the ECJ qualified as an AVMS the catalogue of videos proposed by an online press website with a content independent from that of the written press articles, since these videos, produced by a local television publisher, were comparable to those of other services of the same nature (ECJ, 21 October 2015, C-347/14). On the contrary, the ECJ found that a commercial video on a YouTube channel could not be considered as AVMS as it did not inform, entertain or educate viewers (ECJ, 21 February 2018, C-132/17).

In France, the CSA qualified as AVMS pages of radio stations' websites offering a catalogue of video programmes, which constituted an autonomous offer of other contents (CSA, decision of 29 May 2013). Similarly, the CSA considered that an online video channel – here, a YouTube channel, *Les recettes pompettes by Poulpe?* operated by a company – qualified as an AVMS and was thus subject to the obligations applicable to this category of services, notably relating to the protection of young audiences (CSA, decision of 9 November 2016). More recently, the CSA held that the YouTube channel of a television channel operated by a company also fell under the definition of AVMS (CSA, decision of 3 July 2019).

It follows from such decisions that programmes offered on video-sharing services (eg, "channels") may be considered as AVMSs should the on-demand channel include content organised by the editor of that service, allowing the user to choose from a catalogue of content.

10. Encryption Requirements

10.1 Legal Requirements and Exemptions

The law for confidence in the digital economy (No 2004-575 of 21 June 2004, LCEN) distinguishes between providers of cryptology means and providers of cryptology services.

Providers of cryptology means are online platforms that provide cryptology services – ie, hardware or software "designed or modified to transform data" with the aim of "guaranteeing the security of data storage or transmission, by making it possible to ensure confidentiality, authentication or integrity control" (Article 29 of the LCEN).

Cryptology services are defined as any operation aiming at implementing means of cryptology on behalf of a third party (Article 29 of the LCEN).

The LCEN provides for a specific and distinct regime for these different providers.

Rules for Providers of Encryption Means

Under French law, use of encryption means is free (no need for prior notification or authorisation). Likewise, the supply and transfer from an EU member state or import of cryptographic means is free to the extent it is exclusively for authentication or data integrity control functions.

However, intra-EU transfers (ie, import or export from or to France) of means of encryption must be declared, notified or authorised except for specific means of encryption. More specifically, providers of such means of encryption are required to notify the French Prime Minister in advance of any import into France (whether from another EU member state or a third country) of a cryptographic means, not limited to authenticating or checking the integrity of a message. Note that a "transfer" means any import or export of the cryptology means by any person holding that means (seller or seller's customer), whether the transfer takes place from the EU or from a country outside the EU.

However, Decree 2007-663 of 2 May 2007 provides for exceptions to this rule, and lays down exemptions for certain categories of products and certain operations. More specifically, this Decree provides, for instance, that "banking equipment" products (ie, "equipment specially designed and limited for use in banking or financial transactions for the general public and whose cryptographic capacity is not accessible to the user") are exempt from any prior declaration to the French Prime Minister.

Rules for Suppliers of Encryption Services

The provision of these services also requires prior notification to the French Prime Minister (Article 31 of the LCEN). According to Article 33 of the LCEN, providers of cryptology services for confidentiality purposes and those providing certification services are presumed to be liable, under the performance of their services, for the loss suffered by their clients, unless they can prove lack of any wilful misconduct (*faute intentionnelle*) or negligence.

The provision of cryptology services to perform confidentiality functions in breach of the obligation of prior notification is punishable by two years' imprisonment and a fine of EUR30,000 (Article 35 of the LCEN). However, supplying services that are not intended to provide confidentiality functions in breach of the obligation of prior notification is punishable by the penalties provided for fines of the fifth class (EUR1,500).

Finally, it should be added that providers of cryptology services, which are responsible for informing their clients, are subject to professional secrecy (Article 226-13 of the Criminal French Code), and thus subject to a penalty of one year's imprisonment and a fine of EUR15,000 in case of breach of such secrecy.

11. COVID-19

11.1 Pandemic Responses Relevant to the TMT Sector

In the context of COVID-19 and following the implementation of lockdown measures and subsequent increases in digital use, Ordinance No 2020-320 of 25 March 2020 adapted the timeframes and procedures applicable to the installation or modification of electronic communications equipment to ensure the availability of electronic communications services and networks.

Four administrative procedures were adapted by the Ordinance:

- suspension of the obligation to transmit an information file to the mayor for the operation or modification of a radio installation;
- discretion given to the operators of radio stations to establish equipment without prior agreement from the National Frequencies Agency;
- reduction of the time required to process applications for electronic communications installations installed temporarily and as part of urgent interventions; and
- exemption from permission for construction, installation and development necessary for the continuity of electronic communications networks and services of a temporary nature.

Despite the extension of the state's public health emergency, these temporary provisions are no longer in force as of May 2020.

Contributed by: *Bertrand Liard, Clara Hainsdorf, Saam Golshani and Guillaume Vitrich,* ***White & Case LLP***

White & Case LLP has 44 offices across 30 countries, making it a truly global law firm, uniquely positioned to help clients achieve their ambitions in today's G20 world. Not only is White & Case a pioneering international law firm, it is also one of the oldest US/UK law firms in France (opened in 1926), with a history of excellence. The Paris office has 180 lawyers, including 47 partners, who work with some of the world's most respected banks and businesses, as well as start-up visionaries, governments and state-owned entities. Its TMT practice is made up of a large group of dedicated lawyers across numerous practices. The practice has deep experience with a wide range of technologies in areas that include both hardware and software across a variety of applications, uses and deployment, such as data centres, analytics, communication infrastructure, on-premises and SaaS, embedded technologies, internet of things, security, privacy and data protection, semiconductors and more.

Authors

Bertrand Liard heads the intellectual property and information technology practice of White & Case in Paris, offering services in both contentious and non-contentious domains. Bertrand advises clients on use and development of their IP (licences in and out, R&D agreements), IP enforcement (infringement and fight against piracy), IT and the internet, particularly in sourcing and outsourcing transactions and internet litigation, as well as on complex contractual arrangements, such as strategic alliances and partnerships. Bertrand is a frequent speaker, author and commentator on privacy, technology and fintech issues. He is a member of the Strategic Orientation Committee of CashWay and of the European Outsourcing Association.

Clara Hainsdorf is a partner in the intellectual property and information technology department of White & Case in Paris. Clara has a thorough knowledge of legal issues related to information and communication technologies (ICT) – technology licences, e-commerce and social media – as well as in relation to complex industrial and commercial contracts. Clara has extensive experience in the field of privacy and data protection, especially in litigation and international contexts. She advises clients notably in relation to international data transfers, discovery and investigation procedures, as well as compliance with the GDPR. Clara is a frequent speaker and author on privacy and cybersecurity.

Saam Golshani is a partner in the EMEA private equity team of White & Case's global mergers and acquisitions practice. He has more than 20 years' experience representing clients in all manner of M&A, private equity and restructuring transactions, in all industries, notably in the tech sector. Ranked as a leading lawyer in his field by top legal directories, Saam's reputation is based on a record of accomplishment and he is distinguished as a key expert in the technology sector. Saam is a frequent speaker, author and commentator on private equity and restructuring issues. He is a member of the Iranian/French lawyers association.

Guillaume Vitrich is a partner in the EMEA private equity team of White & Case's global mergers and acquisitions practice. Well known as a leading corporate practitioner on the French market, Guillaume's practice covers a wide range of both domestic and international private equity, corporate and M&A transactions, notably across Europe and Africa in the digital and tech sectors. An innovative lawyer with an ability to lead pioneering work on behalf of his clients, Guillaume has developed a reputation for – and a strong expertise in – venture capital-related matters, advising venture capital funds, large tech companies, and start-ups.

White & Case LLP

19, place Vendôme
75001 Paris
France

Tel: +33 1 55 04 15 15
Fax: +33 1 55 04 15 16
Email: bliard@whitecase.com
Web: www.whitecase.com