COUNTRY COMPARATIVE GUIDES 2021

The Legal 500 Country Comparative Guides

France

TECHNOLOGY

Contributing firm

Marrache Avocat

Elisabeth Marrache

Partner | elisabeth.marrache@marrache-avocat.fr

Fréderique Allier

Associate | frederique.allier@marrache-avocat.fr

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

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

FRANCE
TECHNOLOGY

1. What is the regulatory regime for technology?

Strictly speaking, there is no legislation that applies only to technology. This sector rather covers a set of sectorial laws and regulations, largely derived from European law, and that govern various areas, including electronic communications, e-commerce, personal data, digital platforms, etc., but also more general provisions such as contract law, consumer law and criminal law.

Key sectoral regulations include:

- The French Post and Electronic Communications Code (the "CPCE"), recently modified to implement the European Electronic Communications Code (directive (UE) 2018/1972, the "EECC Directive");
- Law n° 78-17 of 6 January 1978 on information technology, files and freedoms (hereinafter the "French data Protection Act" or "FDPA"), as amended by the European General Data Protection Regulation 2016/679 (the "GDPR);
- Intellectual property law, mainly codified in the Intellectual Property Code (the "IPC"), including patent and copyright law ("*droit d'auteur*"), etc.

2. Are communications networks or services regulated?

For the most part, the rules relating to electronic communications networks and services are codified in the CPCE.

Other legislative texts may apply, such as the French Consumer Code, as so far as it regulates consumer information in relation to electronic communications service contracts.

The current French electronic communications law is largely derived from the European legal framework. Such framework if composed of several sets of European directives (Framework, Authorisation, Access, Universal Service and Privacy Directives) which date back from 2002 (as amended in 2009), referred to as the "*Telecoms Package*" as well as several EU regulations, such as EU roaming regulations.

The EU Telecoms Package creates a technology-neutral regime and was adopted to establish a harmonised framework for the regulation of electronic communications services (ECSs), electronic communications networks (ECNs), associated facilities and associated services. It requires Member States to adopt a consistent approach to electronic communications regulation that does not distinguish between fixed, voice and data services and it prohibits from implementing a system of prior authorization for the provision of telecommunications networks or services.

The Telecoms Package underwent a significant reform with the adoption of the Directive (UE) 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code, which was implemented in France on 26 May 2021 by the Order n° 2021-650.

The reform consolidates the existing rules contained so far in the Telecoms Package and also provides for significant improvements and in particular:

- answers to a long-lasting debate on the applicability of the ECS definition to "over the top" or "OTT" services providers, such as Whatsapp or Messenger. These operators are nevertheless subject to less stringent obligations;
- amends several legal obligations imposed on the ECS, including the suppression of the obligation of declaration to the ARCEP as a prerequisite for the exercise of such activities;
- aims to promote connectivity and encourages more investment in very high capacity networks
- strengthens the protection of consumers (*please refer to question 6 below*);
- marks an evolution of the ARCEP's powers in accordance with the above amendments.

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

The French legal framework on electronic communications covers the setting-up and operation of networks open to the public and the provision of electronic communications services to the public (Article 33-1 of the CPCE).

Article L32, 15° of the CPCE defines "*operator*" as "*any natural or legal person operating an electronic communications network open to the public or providing an electronic communications service to the public.*"

It should be pointed out that since the implementation of the EECC Directive in France, Article L32, 6° of the CPCE defines an electronic communications service as services provided through electronic communications networks and that includes at least one of the following types of services:

- an Internet access service;
- a service consisting entirely or mainly of the transmission of signals (such as transmission services used for the provision of machine-to-machine services and for broadcasting) and;
- an interpersonal communications service (e.g., WhatsApp, Gmail), defined as a "*service that enables the direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine the recipient(s).*" This notion includes both number-based and number independent services.

This change in terminology settles a long-standing debate in France about the status of service providers such as WhatsApp, Gmail or Skype, which are now legally considered as providing electronic communication services. As specified in question 1.1 above, the prior declaration as a mandatory prerequisite for the activity of electronic communications operator has been lifted.

Whatever their nature, operators are subject to common obligations, for instance the respects of:

- conditions of permanence, quality, availability, security and integrity of the network and service, including obligations to notify the competent authority of security incidents that have had a significant impact on their operation;
- conditions of confidentiality and neutrality with regard to messages transmitted and information related to communications;
- requirements required for the protection of health and the environment and for land use and urban planning objectives, including, where applicable, the conditions for occupying the public domain.

In addition, operators with a turnover above a certain threshold are subject to specific obligations, such as:

- the individualization of the accounting of their activity;
- the contribution to the financing of the universal service, in case of excessive burden for the provider operator, which is determined annually by the ARCEP along with the amounts of the contributions;
- obligations relating to interconnection.

The use of scarce resources regime, such a numbering resources, remains unchanged and still requires an individual authorisation from the ARCEP.

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

The main competent French authority when it comes to electronic communications is the "*Autorité de Régulation des Communications Électroniques et des Postes et de la distribution de la presse*" (ARCEP). The ARCEP fulfils regulatory, advisory and sanctioning missions.

For instance, the authority imposes obligations on the operators, allocates frequency or numbering resources, ensures the financing and provision of universal service, issues opinions or reports at the request of Parliament and the Government etc.

The following entities also play a role in specific aspects of electronic communications:

- The "*Agence nationale de la sécurité des systèmes d'information*" (ANSSI) is invested with missions in relation to information systems security, which include monitoring, detecting, alerting and reacting to computer attacks. The agency provides its expertise and technical assistance to government agencies and companies, with a reinforced mission for operators of vital importance (OIV).
- The "*Agence Nationale des Fréquences*"(ANFR), which activity covers:
- frequency band management and forecasting

(this includes conducting prospective studies on the use and valorization of the spectrum, updating the national table of allocation of frequencies and any other documents on the use of frequencies etc.);
- frequency assignment and site management;
- frequency management on behalf of the assigning authorities (this includes for instance preparing the frequency use authorizations (AUF) which are delivered by the ARCEP) and;
- control actions of space, terrestrial or shipboard radioelectric equipment in order to y the respect of their regulatory conditions of implementation.

5. Are they independent of the government control?

The ARCEP is an independent administrative authority ("AAI"). It regulates the electronic communications, postal and press sectors on behalf of the State, but in complete independence from political power and economic players.

To guarantee the independence of the members of the ARCEP, their mandate is neither revocable nor renewable. They are also subject to a regime of incompatibility of functions and to ethical obligations.

In this respect, Article L.32-1, 3° of the CPCE states that the function of regulating the electronic communications sector, which is carried out by the Minister for Electronic Communications and by ARCEP, is independent of the operation of networks and the provision of electronic communications services.

The ANSSI and the ANFR however are placed under the government authority.

The ANSSI is placed under the supervision of the Secretary General of Defense and National Security ("SGDSN") and is in charge of assisting the Prime Minister in the exercise of his responsibilities in matters of defense and national security.

The ANFR is granted a certain administrative and financial autonomy in order to fulfil its mission but is placed under the authority of the Minister of Electronic Communications.

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

Article L. 111-7 of the French Consumer Code defines the notion of "platform operator" as a professional offering an online public communication service based on:

- the classification or referencing, by means of computer algorithms, of content, goods or services offered or put online by third parties or;
- the bringing together of several parties with a view to the sale of a good, the provision of a service or the exchange or sharing of a content, good or service.

This definition targets digital platforms in the broadest meaning, including E-commerce platforms, search engines, social networks as well as ad websites.

In France, online platforms are subject to several sets of laws and regulations, which it is difficult to list exhaustively.

The following are worth being mentioned:

Consumer information

French Law for a Digital Republic of 7 October 2016 (codified under Articles L. 111-7, L. 111-7-1 and L. 111-7-2 of the Consumer Code) and its three implementing decrees of 29 September 2017, require operators to deliver clear, fair and transparent information to the users of their platforms. This obligation covers in particular the criteria for ranking and referencing products, services and content posted online and the general terms and conditions of use.

Contract and competition practices

At the European level, Regulation n° 2019/1150 "Platform to Business" of 20 June 2019, which entered into force on 12 July 2020 and is directly applicable in Member States, regulates the activity of BtoC platform operators, governing in particular the contractual relations between the operator and the referenced merchants. This text imposes a number of obligations on providers of online intermediary services and search engines.

French Law n° 2020-1508 of 3 December 2020 "containing various provisions adapting to European Union law in economic and financial matters" took into account the provisions of the Platform to Business Regulation, completing for instance the list of restrictive competition practices in the French Commercial Code (Articles L. 442-1 et seq.).

Illicit content

In the presence of illicit content, French Law n° 2004-575 of 21 June 2004 provides for a lightened liability regime for web hosting providers who, unlike web publishers, are not subject to a general monitoring obligation and are required to promptly remove illicit content only as they become aware of it.

However, a significant evolution has been brought in this area by the Order n° 2021-580 of 12 May 2021 which transposed the European Directive 2019/790 of 17 April 2019 on copyright and related rights in the digital single market (codified under articles L137-1 ad seq. of the French Intellectual Property Code). Although the order does not establish a general obligation to monitor, it introduces a specific liability regime, more restrictive than that of the 2004 law, against providers of online content sharing services, when such providers organize and promote the content for the purpose of making a profit (platforms such as YouTube are typically targeted).

This liability remains lighter than the French general copyright law, as the relevant service providers are liable for unauthorized acts of exploitation of protected works or objects of related rights, in the absence of authorization from the right holders, unless they demonstrate that they have adopted certain diligence and "appropriate measures", as defined in Articles L. 137-2, III and L. 219-2, III of the French IPC. These diligences may vary according to the age and size of the platform.

The 2021 order further imposed on these content sharing service providers new obligations to inform rights holders, now codified in the new Articles L. 137-3 and L. 219-3 of the IPC.

Green commitments

French Law n° 2020-105 of 10 February 2020 on the fight against waste and the circular economy also has an interesting impact on platform operators.

First, it imposes on sellers of electrical and electronic equipment including those who use an online platform to proceed with the sale of these products an obligation to provide an index of reparability and sustainability of products, starting 1 January 2021.

The platform operator will have to ensure that the sellers concerned provide such an index.

Furthermore, as of 1 January 2022, platform operators will have to pay an eco-contribution to cover the costs of prevention, collection, transport and management of waste from the producers of waste-generating products they list, unless they can demonstrate that these sellers have already paid the said contribution (new Article L. 541-10-9 of the Environmental Code).

Lastly, the 2020 law requires that providers of access to online public communication services inform their subscribers of the amount of data consumed in the course of such activity and indicate the equivalent of the corresponding greenhouse gas emissions, as of 1 January 2022.

Future changes in the legislation are to be expected, as the European Commission presented its two proposals for regulations to regulate the digital single market, the Digital Service Act (DSA) and the Digital Market Act (DMA), on 15 December 2020.

The DSA aims at introducing a harmonized framework of rules for online intermediary services, mainly in terms of moderation of illegal content and transparency of service. The new obligations applicable to the intermediary services providers will vary according to their role, their size and the impact they may have online.

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

As a general principle, regulators are only competent to regulate platform providers' activity within the French jurisdiction.

However, these regulators could be led to sanction entities established outside of France as certain texts have an extraterritorial application.

This is for instance the case of the GDPR and the Platform to Business Regulation, when companies established abroad target people on the national territory.

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

No, an operator does not need to be domiciled in France to provide electronic communications networks and services.

The principle of freedom of establishment, which is provided for under the European Union Treaties, is regularly confirmed by the European Court of Justice (C-475/12 *UPC DTH Sàrl v Nemzeti Média- és Hírközlési Hatóság Elnökhelyettese*, of 30 April 2014), and by the texts applicable to electronic communications.

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

The EECC and Article L.32, 1 of the CPCE set out a number of objectives, including the creation of a legal framework guaranteeing the freedom to provide electronic communications networks and services and ensuring the predictability of the applicable rules, in particular to encourage sustainable investment.

There are however some restrictions due to the sensitive nature of the electronic communications sector.

Under Article L151-3 of the French Monetary and Financial Code, prior authorization by the Minister in charge of the economy must be obtained for any foreign investments in an activity in France which, even on an occasional basis, participates in the exercise of public authority or falls within an activitiy "*likely to undermine public order, public security or the interests of national defense*".

Within the meaning of Article R151-3 of the same code, these activities include the integrity, security or continuity of operation of electronic communications networks and services.

Article R151-2 further specifies that the following operations concerning an entity governed by French law constitute such "*foreign investment*":

1. acquiring control;
2. acquiring all or part of a branch of activity;
3. crossing the threshold of 25% of the voting rights.

10. Are there any regulations covering interconnection between operators?

The rules governing interconnection are set out in Articles L34-8 et seq. of the CPCE.

Under this regime, operators have the obligation to negotiate with every operators who request access and interconnection, including those established in another Member State of the European Union or in another State party to the Agreement on the European Economic Area. The content of the interconnection agreement is nevertheless freely negotiated by the operators.

The operator may refuse to execute an agreement only on the following grounds: (i) he doesn't have the capacity to provide the requested access or (ii) he is able to demonstrate that the requested access does not correspond to the other operator's needs. The refusal must be motivated.

The interconnection agreement must be negotiated in good faith and must define at least the technical and economic conditions of the relationship.

The ARCEP may require the operators to review their interconnection contract and to amend it.

It should be noted that operators controlling access to end-users (with the exception of providers of number-independent interpersonal communications services) may have obligations imposed on them to ensure the proper functioning and interconnection of their networks as well as access to services provided on other networks.

As an exception to that rule, and following the implementation of the EECC directive, providers of number-independent interpersonal communications services with significant coverage and usage may also have interconnection obligations imposed on them under specific conditions.

Any disputes concerning interconnection must be submitted to the ARCEP which decisions can be appealed before the Paris Court of Appeal.

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

Yes, the CPCE (Article L.37-2) and the EECC directive (Article 63) provide for specific obligations for undertakings having significant market power in certain circumstances and with the objective to achieve a fair competition in the electronic communications market.

Under these texts, an undertaking shall be deemed to have significant market power if, either individually or jointly with others, it enjoys a position equivalent to dominance, namely a position of economic strength affording it the power to behave to an appreciable extent independently of competitors, customers and ultimately consumers.

Where an undertaking has significant market power on a specific market, it may also be designated as having significant market power on a closely related market, where the links between the two markets allow the market power held on the specific market to be leveraged into the closely related market, thereby strengthening the market power of the undertaking.

In this context, operators deemed to have significant market power may be imposed several obligations in relation to interconnection and access and in particular:

- publish a reference offer;
- provide non-discriminatory conditions of

interconnection and access;
- comply with tariffs obligations;
- accept reasonable requests of access to, and use of, i) specific network elements and associated facilities, ii) civil engineering (including, but not limited to, buildings or entries to buildings, building cables…) in situations where, having considered the market analysis, the ARCEP concludes that denial of access or access given under unreasonable terms and conditions having a similar effect would hinder the emergence of a sustainable competitive market and would not be in the end-user's interest.

The ARCEP only imposes obligations to these operators in the absence of sustainable and effective competition of a relevant market and lifts such regulation as soon as competition exists.

If the ARCEP withdraws such regulation, it must define an appropriate notice period to ensure a sustainable transition and take into account the existing agreements between access providers and access seekers that have been entered into on the basis of the imposed obligations.

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

There are a number of key principles, such as universal service, net neutrality and the principle of data anonymization set out in Article L34-1 of the CPCE (*see question 12 of this Guide*), which were laid down in the European directives and more recently reaffirmed in the EECC directive.

Moreover, French law provides for various other consumer protection provisions applicable to the telecommunications sector, which would be difficult to list exhaustively.

Among the specific regulations and recent developments, the following are worth mentioning:

Electronic communications contracts

The Consumer Code provides for a section dedicated to the provisions relating to the rights of consumers with respect to contracts for electronic communications services (Articles L. 224-26 to L. 224-42-4), which was amended by the transposition of the EECC Directive.

The new provisions strengthen consumer protection, in particular with the obligation to communicate at the pre-contractual stage a summary that centralizes, in a single document, the substantial elements of the offer (price, quality of the service provided, term, personal data processed during the contract term…).

In addition, a new mechanism of consumer compensation for clearly identified breaches has been created (for instance in the event of i) delay in accessing to number portability requests, ii) loss of the user phone number when portability was requested; or iii) failure to attend a service and installation appointment related to a change of provider, under Article L. 224-42-1 of the Consumer Code).

Consumer is also granted the possibility to terminate the contract more easily.

Regulation of marketing communications

Operators are prohibited from sending direct marketing communications by means of an automated electronic communications without the user consent. (*see question 12 of this Guide*).

Regulation of prices of electronic communications services

Although the CPCE provides for the freedom to negotiate interconnection and access contracts, the ARCEP is competent to regulate prices applicable by certain operators who have significant market power.

In general, operators must set the amount of their prices in an objective and transparent manner.

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

Under Article L. 112-2 of the ICP, computer software, including preparatory design material, is considered to be an intellectual work eligible for protection under French copyright law ("*droit d'auteur*").

Such protection may be granted to an intellectual work (i) which has been materialized, as mere ideas may not be protected, and (ii) which is found to be "original", that is, it reflects the author's personality.

The originality of the software has to be determined on a case-by-case basis. However it is established case law in France that for a software to be considered as original, it must reveal "*a personalized effort characterizing the choices made by its creator*", which "*must go beyond the simple implementation of an automatic and constraining logic, the materialization of this effort*

residing in an individualized structure" (for a recent example of ruling: Court of Appeal of Douai, 5 April 2018).

Unlike trademarks and patents, software cannot be registered. For that matter, it is a common practice for right holders and authors to deposit the software source codes with organizations such as the Agency for the Protection of Programs (APP).

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

French law provides for two types of protection of databases: the general law of copyright and a "*sui generis*" right of the database producer.

Protection under French copyright law

The notion of database was introduced into the IPC upon the implementation of the European Directive 96/9/EC of 11 March 1996 on the legal protection of database by French Law n° 98-536 of 1 July 1998.

The structure/architecture of the database can be protected by French copyright law as long as it meets the unique criterion of protection: originality.

As far as databases are concerned, the originality can arise from the choice or the arrangement of the materials, or in the rules of organization of the database (Article L 112-3, para. 1 of the IPC). The database must be more than a simple compilation of data.

"*Sui generis*" right of the database producer

This protection, which may be acquired by the producer of the database, aims at protecting the "*content*" of a database. This protection is independent and is exercised without prejudice to those resulting from the copyright or another right on the database or one of its constituent elements (Article L. 341-1 of the IPC).

Such protection will be granted provided that the constitution, verification or presentation of the content of the database attests to a substantial financial, material or human investment.

As a database producer, the latter has the right to protect such investment by opposing (Article L.342-1 of the IPC):

- the extraction or the re-use of a substantial part of the contents of this database and;
- the repeated and systematic extraction or reuse of non-substantial parts, when the borrowings clearly exceed the conditions of normal use of the database.

As a recent example of the application of this rule, the Paris Court of Appeal ruled that the classified website Leboncoin.fr constitutes a database and that Leboncoin is a database producer, but also recognized that the reproduction of essential contents of the website by a third party without its authorization may constitute a prohibited extraction, even if the third party's reproductions were accompanied by a hypertext link to the original site (*CA Paris, 2 February, 2021*).

15. What key protections exist for personal data?

In France, the protection of personal data is governed by the French Data Protection Act (the "FDPA"), amended by Law n°2018-493 du 20 June 2018 and supplemented by decrees n°2018-687 of 1 August 2018 and n°2019-536 du 29 May 2019, which together adapted the national law in light of the GDPR.

The GDPR is driven by a general principle of "*accountability*". Concretely, this means that personal data controllers and processors shall be able to demonstrate at any time their compliance to the Regulation with internal documentation, as they are responsible for the choice of the appropriate technical and organisational measures to apply.

The GDPR provides for the following key protections:

- **Lawfulness**: personal data processing operations must each be based on one of the 6 valid lawful basis provided under the GDPR.
- **Fairness**: personal data should not be processed in a way that is unjustifiably detrimental, unlawfully discriminatory, unexpected or misleading to the data.
- **Transparency**: the controller must be clear and open with the data subject about how they will collect, use and share personal data.
- **Purpose limitation**: each processing operation of personal data must answer a specific purpose. When the data is processed for several separate purposes, each of those purposes must rely on a legal basis.
- **Data minimization/proportionality**: the controller or processor must process the data only to the extent strictly necessary for the completion of the purpose.
- **Storage limitation**: personal data may not be stored for an indefinite period of time. Such duration must be limited to the time

necessary to fulfill the purpose(s) for which the data was collected. The data may be retained for a longer period to take into account:
    - legal or regulatory obligations;
    - limitation periods under applicable law;
    - potential litigation and ;
    - guidelines established by the relevant data protection authorities, including the CNIL.
- **Security of the data**: the controller and processor are required to implement appropriate technical and organizational measures to ensure an appropriate level of security, in consideration of the risk.
- **Data subjects rights**: data subjects are entitled to certain number of rights in relation to their personal data, which the controller must facilitate. This includes the right to:
    - be informed as to the identity of the controller and characteristics of the data processing operations;
    - rectification of the data;
    - deletion of the data;
    - restriction of the use of the data;
    - portability of the data – In certain circumstances, data subjects have the right to receive data in electronic form and/or to request the controller or processor to transfer this information to a third party where technically possible.

Relevant provisions can also be found in Article 82 of the FDPA which transposes into French law Article 5.3 of Directive 2002/58/EC on privacy and electronic communications (or "ePrivacy"). In particular, it provides for the obligation, except in a number of limited cases, to obtain the consent of Internet users before any operation to use cookies and other tracers, which may constitute personal data.

It should be noted that a draft of an updated "ePrivacy" regulation is currently being examined at the European Union level. This text is expected to cover various aspects of electronic communications, such as electronic and telephone marketing, and security of the electronic communications services, but also cookies and other tracers.

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

Any data controller or processor who wishes to transfer personal data overseas must ensure that such operation is based on one of the legal mechanisms provided for in Chapter V of the GDPR. The CNIL has aligned itself with the interpretation of this text adopted by the European Data Protection Board (EDPB), which adopted several recommendations and guidelines on the issue.

Compliance with Chapter V first involves checking whether the country in question is the subject of an adequacy decision under Article 45 of the GDPR, by which the European Commission has recognized that the recipient country offers a satisfactory level of data protection.

Processing may also be carried out if it falls within one of the derogations provided for under Article 49 of the GDPR, such as obtaining the consent of the data subjects or the need to carry out such transfers to perform a contract between the controller and the data subject. However, reliance on this ground should remain exceptional and occasional.

Otherwise, it will be necessary to rely on one of the legal tools of Article 46 of the GDPR, in order to implement appropriate safeguards (binding corporate rules ("BCR"), standard contractual clauses ("SCC"), code of conduct…), and to ensure that data subjects are provided with effective means to exercise their rights.

Such legal tools may be insufficient to guaranty the requited level of protection, in which case supplementary measures should be applied. The Recommendations 01/2020 adopted by the EDPB on 18 June 2021 provides for practical guidelines to assist data exporters on assessing the effectiveness of the transfer tools and in determining which supplementary measures they should apply.

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

Following controls or complaints, in the event of non-compliance with the provisions of the GDPR or the law by data controllers and processors, the European data protection authorities (in France, the CNIL) may impose the following sanctions:

- Under Article 83 (4) of the GDPR: up to 10 million euros or, in the case of a company, 2% of annual worldwide turnover for breaches of, among others, the principle of Privacy By Design, the principle of Privacy By Default, rules applicable to Privacy Impact Assessments, etc.;
- Under Article 83 (5) of the GDPR: up to 20 million euros or, in the case of a company, 4%

of annual worldwide turnover for breaches of, among other, the basic principles of a processing operation, including the conditions applicable to consent, the rights of data subjects (rights of access, rectification, opposition, deletion, etc.) and rules relating to transfers of personal data to a recipient located in a third country or to an international organization.

In 2020, the CNIL conducted 247 inspections, issued 49 formal notices to comply, and imposed 14 sanctions, including 11 fines.

These sanctions concern a wide range of actors and sectors of activity, and are mainly related to insufficient data security or the lack of information and consent from individuals, in particular concerning the use of cookies.

On 7 December 2020, the CNIL issued the most important sanction ever pronounced in the field of personal data in France to date, imposing on GOOGLE LLC a 60 million euro fine and GOOGLE IRELAND LIMITED a 40 million fine, in particular for having placed advertising cookies on the computers of users of the search engine google.fr without prior consent or satisfactory information.

Based on this assessment of the situation in 2020, the CNIL has decided to focus its controls on three target themes in 2021: cookies, data sovereignty and security.

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

Although the GDPR is of direct application, Member States were granted flexibility with respect to the implementation of a certain number of its provisions, either to specify certain aspects, to mitigate derogations or, on the contrary, to grant more guarantees than those provided for under European law.

French law provides for the following additional protections:

Electronic communications

The CPCE contains a number of provisions relating to the protection of personal data, including:

- Provisions relating to the prohibition of unsolicited marketing communications (Article L34-5 of the CPCE).

In addition, under Article L. 223-1 of the Consumer Code, consumers who do not wish to be commercially solicited by telephone have the possibility register free of charge on a list of opposition to cold calling (the “Bloctel” list).

- Any subscriber may object to the identification his subscriber number (Article L34-6 of the CPCE).
- Electronic communications operators, and in particular persons whose activity is to offer access to online public communication services, are required to delete or anonymize any data relating to traffic (Article 34-1 of the CPCE).

This rule is subject to several exceptions. For instance, operations of deletion and anonymization of certain categories of data may be deferred, under certain conditions, for the purposes, among other grounds of billing and payment of electronic communications services, criminal proceedings, to investigate on serious crimes, or in order to ensure national security.

Further, Article 6 of Law n° 2004-575 of 21 June 2004 requires web hosts and Internet service providers to store certain identification data of anyone who has contributed to the creation of the content of the services they provide, to provide the means identification, and to communicate this data upon request of a judicial authority.

Such a legal framework has been the subject of controversy in France, a part of the doctrine and the society considering that it represents a disproportionate infringement to the right to privacy and protection of personal data. Following the CJEU decision of 6 October 2020 and of the Conseil d’Etat (French highest administrative court) of 21 April 2021, article 34-1 of the CPCE has been recently modified by the law n°2021-998 of 30 July 2021 relating to the prevention of terrorism and intelligence. The law aims to offer some limits and warranties to privacy rights by limiting the scope of the data that may be requested from operators, the retention periods obligations and compensation and control procedures. Time will tell if the new provisions will be welcomed positively.

Minors

The French legislator has set the minor consent age threshold at 15 years (Article 45 of the FDPA).

On 9 June 2021, the CNIL published its 8 recommendations “*to strengthen the protection of minors online*” and recommended that consent should be given by both the parents and children for online services provided to children under 15.

Health data

French law requires service providers who host personal health data collected in the context delivering preventive, diagnostic, and other health services, to obtain a specific certification issued by an accredited organization from the Ministry of Health (Article L.1111-8 of the Public Health Code) (HDS certification).

Digital death

Where the GDPR addresses the right of data subjects "to be forgotten" (Article 17), French regulation anticipated the question of digital death.

Law n°2016-1321 of 6 October 2016 for a Digital Republic has set up a legal framework allowing a data subject to anticipate the management of his/her personal data after his/her death, by leaving retention, deletion and disclosure instructions in relation to that data (Article 85 of the FDPA).

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

Cloud-based services are subject to different sectorial laws and regulations in France.

The "NIS" directive

Cloud computing service providers activities are explicitly covered by The Network and Information Security Directive, known as the "NIS" Directive, which is the first European text dedicated to improving cyber security at a European level. The directive was incorporated into French law with the adoption of French law 2018-133 of 26 February 2018 on various provisions for adaptation to European Union law.

This law requires operators of essential services and digital service providers, which include cloud computing companies, to conform with certain level of cybersecurity, essentially by adopting appropriate technical and organizational measures to prevent security incidents or, at least, to minimize their impact in order to ensure continuity of service.

The French text further imposes obligations to report certain incidents to the National Information Systems Security Authority (ANSSI), which is the national competent authority regarding cybersecurity. The ANSSI is also empowered to carry out controls, upon decision of the Prime Minister.

A proposal for a revised NIS directive was presented by the European Commission on 16 December 2020. This "NIS 2" Directive is expected to be definitively adopted in 2023 at the latest.

The GDPR and the Guide of conduct

Companies which offer data storage services usually act as data processor under the meaning of the GDPR. Consequently, they are required to comply with all the requirements arising from this status, particularly in their contractual relations with their clients, who generally act as controllers.

On 11 June 2021, the CNIL approved the first European code of conduct submitted by Cloud Infrastructure Service Providers Europe (CISPE) and dedicated to cloud infrastructure service providers (IaaS) located in the European Union.

This code includes:

- requirements regarding data protection;
- requirements about transparency of security measures;
- a governance project;
- an appendix listing technical and organizational best practices in the area of security;
- an appendix listing the control points for compliance with the code of conduct, with numerous recommendations on the documentation to be put in place;
- a template for notification of a security breach.

In accordance with the GDPR, codes of conduct are only binding on those parties who have adhered to them.

Health data hosting regulation (*HDS*)

As mentioned in our answer to question 12 above, health data hosting activity can only be implemented by a hosting service provider previously approved by the Ministry of Health, in accordance with Article L.1111-8 of the Public Health Code.

This system specifically aims at protecting the confidentiality, integrity and availability of patients' data.

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

French law sets out the legal value of the electronic signature in Articles 1366 and 1367 of the Civil Code.

The electronic signature consists of "*the use of a reliable*

identification process guaranteeing its link with the act to which it is attached" (Article 1367, paragraph 2 of the Civil Code).

The reliability of this process is presumed, until proven otherwise, provided (i) the electronic signature is created, (ii) the identity of the signatory is assured and (iii) the integrity of the act is guaranteed.

Decree n° 2017-1416 of September 28, 2017, issued for the implementation of Article 1367 of the Civil Code, specifies the conditions of the process allowing an electronic signature to benefit from this presumption of reliability, in accordance with the eIDAS (Electronic IDentification And Trust Services) Regulation n° 910/2014, which entered into force on 1 July 2016.

The eIDAS regulation clarified and standardized the legal framework for this technology at the European level.

The regulation has enshrined three different types of electronic signatures, which are each associated with a certain level of reliability:

- **Simple electronic signature:** This is a computer data attached or logically linked to other electronic data and used as an authentication method. It does not guarantee the identity of the signatory, but the content and time stamp of the document are assured.
- **Advanced Electronic Signature (AdES):** This AES must be generated by a reliable technical process to have a legal value and act as a signature ensuring the identity of a person and his adherence to the signed act. An advanced or secure electronic signature meets the following cumulative requirements:
    - it must be specific to the signatory;
    - it must be created by means that the signatory can keep under his exclusive control;
    - it must guarantee a link with the document to which it is attached such that any modification is detectable.
- **Qualified electronic Signature (QES):** This is an advanced electronic signature based on a qualified certificate and created by a secure electronic signature creation device. The legal effect of a qualified electronic signature is equivalent to that of a handwritten signature. The "qualified" electronic signature must fulfil a number of characteristics that are defined in the eIDAS regulation.

In France, the ANSSI ("*Agence nationale de la sécurité des systèmes d'information*") is the reference organization for electronic signatures.

ANSSI is in charge of the certification, which is recognized at the European level, of these qualified trust service providers (QTSPs) that can issue qualified certificates. The agency also identifies and controls such service providers to ensure their compliance with the eIDAS regulation.

The three types of signatures (simple, advanced and qualified) are admissible as evidence in court.

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

Article L. 1224-1 of the Employment Code provides that "*In the event of a change in the legal status of the employer, in particular by succession, sale, merger, transformation of the business, or incorporation of the company, all employment contracts in effect on the date of the change shall continue to exist between the new employer and the company's employees*."

According to consistent case law, this provision will apply and contracts will be continued with the new employer whenever the transferred activity constitutes an autonomous economic entity with its own staff, organization and specific resources.

Based on those criterion, French judges could extend the application of Article L. 1224-1 to other situations than those expressly listed, such as the total or partial transfer of a business or the partial contribution of assets.

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

In France, the liability regime applicable to AI is subject to a large debate insofar as there is no per se legal regime applicable only to AI to date but rather a set of limited initiatives.

The French legislator is indeed at an early stage of regulating AI devices. For instance, the French Law on Bioethics, voted on 29 June 2021, provides for several information obligations applicable to the manufacturer of AI devices but remains silent on the question of the liability regime.

A majority trend of the doctrine considers that AI liability should be governed by the civil liability regime. This

means that, depending of the situation, the developer of the solution, the producer or the importer of the device integrating an AI software could be considered liable in case of malfunction.

At a European level, following the resolutions on AI adopted by the European Parliament on 20 October 2020, the Commission proposed on 21 April 2021 a Regulation laying down harmonized rules on Artificial Intelligence (the "Artificial Intelligence Act").

The Artificial Intelligence Act proposal aims at setting harmonized rules for the development, placement on the market and use of AI systems in the Union following a proportionate risk-based approach.

Certain particularly harmful AI practices are prohibited as contravening Union values, while specific restrictions and safeguards are proposed for "high-risk AI systems" that pose significant risks to the health and safety or fundamental rights of persons.

As far as these "high-risk" systems are concerned, the proposal provides for a liability regime applicable to all actors of the AI tool: the provider, manufacturer of products integrating AI solutions, distributors, importers and even users of these AI solutions.

The European Parliament and the Member States will need to adopt the Commission's proposals by the ordinary legislative procedure. Once adopted, the regulation will be directly applicable across the EU.

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

a) obligations as to the maintenance of cybersecurity;

It would be difficult to draw up an exhaustive list of applicable provisions for maintaining cybersecurity in France.

The following key laws and regulations are worth mentioning:

- The FDPA: Article 32 imposes a number of obligations in relation to security to data controllers and processors;
- The CPCE: In particular, Article L33-1 which imposes on undertakings establishing and operating networks open to the public and providing electronic communications services to the public a general obligation to ensure the security of networks and services;
- Law n° 2018-133 of 26 February 2018, transposing the "NIS" Directive, supplemented by Decree n° 2018-384 of 23 May 2018 and the Order of 14 September 2018, which together impose obligations of security on operators of critical essential services and digital service providers (*question 13 of the present Guide*);
- Law n° 2016-1321 of 6 October 2016 for a Digital Republic, amended by Law n° 2018-493 of 20 June 2018 transposing the GDPR;
- The European Cybersecurity Act (Regulation (EU) 2019/881) of 17 April 2019, of direct application in the Member States, strengthening the EU Agency for cybersecurity (ENISA) and establishing a cybersecurity certification framework for products and services;
- Law n° 2001-1062 of 15 November 2001 on daily security and Law n° 2003-239 of 18 March 2003 on homeland security;
- Law n° 2014-1353 of 13 November 2014 on strengthening the provisions relating to the fight against terrorism;
- Law n° 2016-731 of 3 June 2016 strengthening the fight against organized crime, terrorism and their financing, and improving the effectiveness and guarantees of criminal procedure
- Law n°2011-267 of 14 March 2011 of orientation and programming for the performance of internal security;
- Law n° 2004-204 of 9 March 2004 adapting the justice system to changes in crime;
- Law n° 2006-961 of 1 August 2006 on copyright and related rights in the information society.

b) the criminality of hacking/DDOS attacks?

Articles 323-1 et seq. of the French Criminal Code sanction various types of cyber-attacks, including hacking and DDOS attacks but other cybercrimes such as phishing, identify theft, possession of software to commit cybercrime.

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

The technology that will probably cause the most legal change in France in the near future is artificial intelligence, in particular in view of the upcoming

adoption of the European Artificial Intelligence Act (*see question 12 of this Guide*).

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

The restrictions on personal data transfers overseas can raise commercial difficulties for companies (*see question 10 of this Guide*).

It is particularly challenging for those who wish to export data to the United States, considering the recent decision of the Court of Justice of the European Union which invalidated the "Privacy Shield" mechanism on which many of such transfers were previously based ("*Schrems II*" case of 16 July 2020).

On 18 June 2021, the EDPB adopted its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, which provides for some practical guidelines to assist data exporters in assessing the effectiveness of the different transfer tools of Chapter V of the GDPR and in determining which supplementary measures should be applied.

To summarize the EDPB' position based on these recommendations, there is no general prohibition on transferring data to the United States, but such operation remains problematic. In order to comply with the requirements of the GDPR, an analysis of the scope of application of the US laws and a verification of the practices of the recipient of the data is necessary, which is complex to say the least. It is to hope that the European authority will be able to define clearer and more pragmatic solutions for data exporters in the future.

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

France provides a fairly comprehensive legislative framework in the digital domain, providing for high standards in terms of consumer protection, developing the open data, and with a particular concern for green transformation, which can be perceived as restrictive from foreign countries.

This framework depends partly of the European legislator, France being subject to the respect of the requirements of harmonization of the legislations of the Member States.

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

The French authorities take the subject of artificial intelligence very seriously.

As an illustration of the legal framework for AI in France is Decree n° 2020-356 of 27 March 2020, which created an automated processing of personal data called "DataJust".

The purpose of the DataJust processing is to develop, for a period of two years, an algorithmic system for identifying, by type of injury:

- the amounts requested and offered by the parties to a dispute;
- the amounts awarded to victims in compensation for their personal injury in court decisions rendered on appeal by administrative courts and civil courts.

Moreover, the CNIL quickly addressed the issue following the initiative of the European Commission, publishing on 18 June 2021, along with its European counterparts and the European Data Protection Board, an opinion on the proposed European Artificial Intelligence Act.

Contributors

Elisabeth Marrache
Partner
elisabeth.marrache@marrache-avocat.fr

Fréderique Allier
Associate
frederique.allier@marrache-avocat.fr