Legal 500
Country Comparative Guides 2025

France
TMT

Contributor

Joffe & Associés

Emilie de Vaucresson

Partner | edevaucresson@joffeassocies.com

Amanda Dubarry

Associate | adubarry@joffeassocies.com

Hanna-Marie Borten-Guary

Associate | hmbortenguary@joffeassocies.com

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

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

France: TMT

1. Software – How are proprietary rights in software and associated materials protected?

The French intellectual property code includes provisions on the protection of software in France. It applies to object code, source code and to the preparatory design material. French *droit d'auteur* arises automatically on creation of an original work. Pursuant to article L.131-2 of the French intellectual property code a software is original when it bears the mark of the personality of its author. In certain cases, software must be registered, especially when the software is made available to the public (article L.131-2 (2) of the French heritage code).

Not all aspects of software are protected by software specific regime in France: ideas, principles, methods, software features, algorithms cannot be protected as a materialisation of the idea is necessary for the work to be protected by French *droit d'auteur*.

Pursuant to Munich Convention of October 5, 1973, the object code of a software is not patentable is France. However, software features are patentable provided they solve a technical problem, in other words, when the standard conditions for patentability are met.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

The person who created the software owns the proprietary rights in the newly created software (article L.113-1 of the French intellectual property code). In the absence of any written assignment of intellectual property rights that complies with legal requirements of article L.131-3 of the French intellectual property code, the proprietary rights in newly created software would belong to the software developer or consultant who created it and not to the customer.

However, article L.113-9 of the French intellectual property code provides an exception for software created by employees as part of their duties or under the instructions of their employer: intellectual property rights on software are automatically vested in the employer.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

Liability for harm caused by software or computer systems is governed by general liability regime in France.

The French civil code includes provisions on liability for defective products, including software and computer systems. Under these provisions, producers can be held liable for damage caused by defects in their products.

Directive (EU) 2024/2853 of 23 October 2024 provides for a liability framework for defective products. It repeals the previous directive regulating that matter and extends definition of 'product' to include digital manufacturing files as well as software, excluding free and open-source software that is developed or supplied outside the course of a commercial activity (articles 2 and 4(1) of the directive). In addition, it extends the definition of 'damage' to include the destruction or corruption of data that are not used for professional purposes (article 6(1)(c) of the directive). In particular, this directive:

- provides that economic operators are not exempted from liability where the defectiveness of a product is due to (i) digital services that are integrated or interconnected with the product, (ii) software, including software updates or upgrades, (iii) a lack of software updates or upgrades necessary to maintain safety, when they are under the control of the product manufacturer (article 11(2));
- provides that relevant product safety requirements, including safety-relevant cybersecurity requirements, must be taken into account when assessing the defectiveness of a product (article 7(2)(f) of the directive);
- introduces an obligation to disclose evidence to remedy information asymmetry (article 9 of the directive); and
- alleviates the burden of proof by presuming the defectiveness of the product when the claimant faces excessive difficulties, in particular due to technical or scientific complexity, to prove the defectiveness of the product or the causal link between its defectiveness and the damage (article 10 of the directive).

The transposition of this directive into domestic law is scheduled for 9 December 2026.

On 11 February 2025, the European Commission announced the withdrawal of the proposal for a directive on the adaptation of rules on non-contractual civil liability to the field of artificial intelligence, commonly known as the 'AI Liability Directive'. The Commission justified the withdrawal of the directive by the fact that no foreseeable agreement would be reached.

4. Software – To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The French intellectual property code provides rules against software counterfeit (article L.335-2-1 of this code provides that software counterfeiting is punishable by three years' imprisonment and a fine of 300 000 euros). The French criminal code also criminalizes attacks on automated data processing systems (article L.323-1 and seq. of this code).

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

The provision of software by a supplier to customers is governed by the general principles of French contract law (as well as consumer protection law when customer is acting as a consumer).

At the European level, Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, along with Directive (EU) 2019/771 of 20 May 2019 on certain aspects concerning contracts for the sale of goods, have been transposed into French law by Ordinance No. 2021-1247 of 29 September 2021. The provisions of this ordinance specifically address contracts for the supply of digital content and digital services, aiming to enhance consumer protection.

Some provisions of the French consumer code are specific to software and digital products, such as information to be transmitted to consumer before any sales (articles L.111-1 and L.111-6 of the French consumer code), information to be mentioned in the agreement (article L.224-25-5 of the French consumer code) or the extension of the legal guarantee of conformity to digital products (articles L.224-25-12 et seq. of the French consumer code).

The new law No 2024-449 dated 21 May 2024 to secure the digital space ("SREN") transposes new EU regulations (Digital Services Act, Digital Market Act and Data Act) into French legislation. It contains specific provisions concerning cloud providers such as prohibition to charge data transfer fees that exceed the costs borne by the provider when switching providers, regulation of cloud credits or interoperability of cloud services.

The Data Act and the Data Governance Act significantly impact cloud technologies by enhancing data portability and interoperability and impose strict security and privacy requirements on cloud service providers to ensure that data is protected throughout its lifecycle.

Cloud service providers serving financial-sector clients must also comply with the EU 2022/2554 Digital Operational Resilience Act (DORA), which became fully applicable on 17 January 2025. Under DORA, they are required to ensure high standards of cybersecurity, operational resilience, incident reporting, data availability, and to include specific contractual clauses covering audit rights, performance metrics, termination conditions, and data portability.

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Yes, it is typical in France for a software vendor to cap its maximum financial liability to a professional customer in a software transaction. The cap must however be proportionate, as per article 1170 of the French civil code, which stipulates that any clause depriving the debtor's material obligation of its substance is deemed unwritten (i.e. the liability of the software vendor will not be capped) – See for example: Court of appeal of Limoges 15 June 2022 No 21/00432; court of appeal of Bordeaux, 17 November 2021, No 19/00215.

A market standard level for liability cap in B2B agreements can vary from 1 to 3 times the value of the contract. Monetary caps are prohibited in B2C agreements.

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's

liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

In negotiated software transaction, certain areas of liability can be subject to a separate enhanced cap, such as confidentiality, data protection, data security (including loss of data) or IPR infringement claims, generally based on specific insurance policies. With respect to breaches of applicable law or regulatory fines, it is generally not appropriate to negotiate an exclusion or limitation of liability as it could be considered as a material obligation of the software vendor. When gross negligence or wilful misconduct is proven, no limitation of liability can apply (article 1231-3 of French civil code).

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

Software escrow is quite common in France for the benefit of the software licensee, in particular (i) when the software vendor is a small company (with a risk of insolvency or bankruptcy); (ii) when the software is customized; or (iii) when the software is embedded by the customer in a solution made available to end users so that to guarantee the continuity of the service. It is less common for cloud-based software to offer licensee a possible access to source codes held in escrow. The Agency for the Protection of Programs (APP) is a French renowned escrow provider.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

Export of dual use items is subject to the EU Regulation No 2021/821 of 20 May 2021 setting up an EU regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. Dual-use items are include software that can be used for both civil and military purposes (e.g. encryption software, 3D simulation games or missile guidance or firing software). In France, a license for export of software classified as dual-use items outside the EU is delivered by the Service for dual-use items ("SBDU"). Non-compliance with legal requirements related to customs and export control is punishable in accordance with articles 410 et seq. of the French customs code.

10. IT Outsourcing – Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

No specific law governs IT outsourcing transactions in France.

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

In the event of a change in the legal status of the employer, in particular by sale, merger, transformation of the business or incorporation of the company, all employment contracts in force on the date of the change continue to exist between the new employer and the company's personnel (article L.1224-1 of the French labor code). As a consequence, when IT services provided by employees of a company are transferred to a third-party IT outsource provider, all concerned employees of said company will be automatically transferred to the provider if the transferred services constitute an autonomous economic entity (i.e an organized grouping of resources dedicated to a specific activity) (see Cour de Cassation, 23 January 23 No. 99-46.245).

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The principal laws that govern telecommunications networks and/or services in France are set out below (not exhaustive list):

- the French code of post and electronic communications ("CPCE");
- EU Directive No 2018/1972 establishing the European Electronic Communications Code, and transposed into

French law by Ordinance No 2021-650 of 26 May 2021;
- Law No 2021-1755 of 23 December 2021 for the reinforcement of the environmental regulation of the digital sector by ARCEP;
- Law No 2020-901 of 24 July 2020 to regulate marketing calls and prevent fraudulent calls;
- Law No 2019-486 of 22 May 2019 on the growth and transformation of companies, known as the "Pacte Law";
- Law No 2018-1021 of 23 November 2018 on changes in housing, land management and digital technology ("ELAN")
- Law No 2016-1321 of 7 October 2016 for a Digital Republic;
- Law No 2015-990 of 6 August 2015 for growth, activity and equal economic opportunities ("Macron Law");
- Law No 2014-344 of 17 March 2014 on consumer protection ("Hamon Law");
- Law No 2008-776 of 4 August 2008, on the modernization of the economy ("LME");
- Law No 2008-3 of 3 January 2008, on the development of competition in favour of consumers ("Chatel Law");
- Law No 2004-575 of 21 June 2004, on the confidence in digital economy ("LCEN").

The French authority for posts and electronic communications ("ARCEP") adopts decisions for all or some of the operators and publishes opinions to provide the sector with clarity or to guide stakeholders' behavior.

The purposes of the CPCE and other legislation applicable to telecommunications are:

- The regulation of the electronic communication sector to ensure fair competition and maintain market integrity, under the control of the ARCEP and the Competition Authority;
- Protection of consumers with confidentiality of communications and data, transparency, fair practices, or mechanisms for dispute resolution and service termination without penalties;
- Protection of net neutrality;
- Promotion of the development of digital infrastructure with support to digital transformation of businesses and public services;
- Environmental responsibility with obligation of transparency regarding environmental impact, promotion of eco-design, and encouraging recycling to foster sustainable practices in the digital sector.

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

Postal service providers providing domestic and cross-border mail services, except when these services are limited to domestic correspondence and do not include distribution, must obtain an authorisation from the French authority for posts and electronic communications ("ARCEP") (article L.3 of the French code of post and electronic communications ("CPCE")). This renewable but non-transferable authorisation is issued for a period of fifteen years (Article L.5-1 of the CPCE).

Electronic communications operators may carry out their activities freely, with the following exceptions (article L.32-1 of the CPCE):

- **Operators of Vital Importance ("OIV")**, designated as such by the relevant coordinating Ministries by virtue of their activity as operators of a public electronic communications network whose unavailability could significantly reduce the nation's war or economic potential, security or survivability (article L.1332-1 and seq. of the French Defence Code) must obtain an authorization from the Prime Minister for operating hardware or software devices enabling end-user terminals to connect to the mobile radio network, with the exception of fourth-generation and earlier generation networks, which, by virtue of their functions, pose a risk to the permanence, integrity, security, availability of the network, or to the confidentiality of transmitted messages and communications-related information. The authorisation is not required when operating devices installed at end users' premises or dedicated exclusively to an independent network, passive or non-configurable electronic devices, and non-specialised computer hardware devices incorporated into devices. The authorisation is granted for a maximum period of eight years and its renewal is subject to a renewal application, which must be submitted at least two months before the expiry of the current authorisation (article L.34-11 of the CPCE).
- **Operators establishing radio installations that use frequencies specifically assigned to their users** may be subject to the obtention of an authorisation from the ARCEP when this is necessary to avoid harmful interference, ensure the technical quality of the

service, preserve the efficient use of radio frequencies, or achieve one of the objectives of general interest mentioned in articles L.32-1 and L.42(III) of the CPCE (article L.41-1 of the CPCE). The ARCEP formalises a list of conditions in which the use of frequencies is subject to administrative authorisation (article L.42 of the CPCE). The initial duration of the authorisation is a minimum of fifteen years, except in certain cases listed in the CPCE, such as for experimental uses (article L.42-1 of the CPCE).

- **Operators using radio equipment for the reception of signals transmitted on frequencies allocated by the Prime Minister**, pursuant to article L.41 of the CPCE, for the purposes of national defence or public safety, are subject to an authorisation from the ARCEP (article L.41-1 of the CPCE). The initial duration of the authorisation is a minimum of fifteen years, except in certain cases listed in the CPCE, such as for experimental uses (article L.42-1 of the CPCE).
- **Operators operating radio equipment operating on frequencies allocated to amateur and amateur satellite services** are subject to the possession of an operator's certificate and the use of a personal call sign issued by the National Frequency Agency ("ANFR") (article L.42-4 of the CPCE).
- **Operators wishing to be allocated a frequency relating to a satellite system** must address their request to the ANFR. The use of a frequency assignment for a satellite system, declared by France to the International Telecommunication Union, is subject to authorisation by the Minister responsible for electronic communications, after consultation with the ANFR. The authorisation may only be transferred with the agreement of the ANFR (article L.97-2 of the CPCE). It is granted for a period of twenty years, or less if it concerns an experimental system (article R.52-3-12 of the CPCE).
- **Operators of terrestrial radio or television service** must obtain an authorization from the French public authority responsible for regulating audiovisual and digital communications ("ARCOM") (Law n°86-1067 of the September 30, 1986, on freedom of communication ("Loi Léotard"). The authorisation may not exceed ten years. For analogue radio services, the authorisation may not exceed five years (article 28-1 of the Loi Léotard).

Except for specific cases (e.g., attribution of numbering resources, frequencies, characterization of certain market power or obligation to contribute to universal service charges) there are no general reporting or financial contribution requirements.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

The French code of post and electronic communications ("CPCE") imposes on electronic communications operators the obligation to delete or anonymise data, except in strictly defined circumstances (article L.34-1 of the CPCE). These exceptions include the storage, for limited periods, of certain categories of data for the purposes of criminal proceedings, preventing threats to public safety, safeguarding national security, billing, or network security. The article details the categories of data concerned (civil identity, subscription data, technical connection data, etc.), the purposes of retention, the maximum periods, and the conditions of access by the competent authorities. Article R.10-13 of the CPCE specifies the nature of the data that must be retained by operators, pursuant to article L.34-1 of the CPCE. It lists, in particular, information relating to the user's civil identity, subscription data, payment information, technical data enabling the source of the connection to be identified, as well as traffic and location data that may be retained by order of the Prime Minister. In addition, article L.33-1 of the CPCE provides that operators of electronic communications services are required to allow access by judicial authorities, the police and national gendarmerie, fire and rescue services, and emergency medical services, acting in the context of judicial missions or rescue operations, to their complete, unedited, and up-to-date lists of subscribers and users.

The CPCE is completed by specific regulation allowing law enforcement agencies, government bodies, and related organisation to access data. For instance:

- **French Criminal law** provides for the interception, the recording and transcription, authorised by a judge, of correspondence sent by electronic means for the purpose criminal proceedings (e.g., article 706-95 of the French Criminal Procedure Code ("CPP") for flagrante delicto investigation or preliminary investigation, Article 100 of the same code for criminal and correctional matters if the penalty incurred is equal to or greater than three years' imprisonment, or

article 706-102-1 of the CPP allowing for the capture of computer data in the context of crime and organised crime and delinquency). In the specific case of searches, judicial authorities may require any person likely to have knowledge of the measures applied to protect the data (e.g., encryption) that may be accessed during the search to provide them with the information necessary to access such data (article 57-1 of the CPP). Judicial authorities may also use "cryptography experts" to "decrypt" the information at their disposal (article 230-1 and seq. of the CPP).
- **The French Internal Security Code ("CSI")** provides for cases were the principles of privacy and confidentiality of correspondence may be infringed upon by public authorities, for intelligence purposes, in cases of public interest necessity provided for by law (article L.801-1 of the CSI). To this effect, article L.851-1 of the CSI organises the collection of information or documents processed or stored by electronic communications operators, including technical data relating to the identification of subscription or connection numbers, the location of terminal equipment, and a subscriber's communications. A department of the Prime Minister is responsible for collecting this data. Moreover, article L.852-1 of the CSI organises the interception of electronic communications that may reveal information relating to the defence and promotion of the fundamental interests of the Nation. This interception must be authorised.

The National Commission for the Control of Intelligence Techniques ("CNCTR") has permanent, complete, direct and immediate access to the information, documents or communication collected.

Finally, **Chapter V of Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data ("Data Act")** provides for rules aiming at making data, including the relevant metadata necessary to interpret and use those data, available to public sector bodies, the commission, the European Central Bank and Union bodies on the basis of exceptional need defined as (i) a public emergency where the data may not be obtained by alternative means in a timely and effective manner under equivalent conditions, or (ii) a situation where the lack of an identified specific non-personal data prevents the relevant body from fulfilling a specific task carried out in the public interest that has been explicitly provided for by law (e.g., official statistics or the mitigation of or recovery from a public emergency, or (iii) a situation where all the means to obtain such data have been exhausted. This Regulation applies from 12 September 2025.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

In France, the **French Standardisation Association ("AFNOR")** coordinates the development of standards in France across all sectors, including information and communication technologies, digital health and connected mobility. Other bodies, although they do not produce standards in the strict sense, work towards accompanying the development of such technologies:

- the **French National Cybersecurity Agency ("ANSSI")** develops security benchmarks;
- the **French authority for posts and electronic communications ("ARCEP")** is responsible for regulating the electronic communications and postal sectors, and in particular allocating frequency and numbering resources, prescribing soft laws such as guidelines or recommendations, issuing opinions on request to the government, parliament or other regulatory authorities.
- the **national commission for information technology and civil liberties ("CNI")** is responsible for ensuring protection of personal data and is in particular involved in any issues relating to processing of sensitive health data or connected and autonomous vehicles (e.g., data controllers may need to carry out a declaration of compliance or obtain an authorisation from the CNIL) or connected and autonomous vehicles (e.g., the CNIL created a 'compliance club' dedicated to connected vehicle and mobility stakeholders and is in the process of publishing a recommendation on the use of location data from connected vehicles);
- finally, **any certification body accredited by the French Accreditation Committee ("COFRAC")** (or equivalent at European level) may certify 'Health data host' (in French "*Hébergeur de données de santé*", or "HDS") an entity hosting health data collected in the field of health, in compliance with article L.1111-8 of the French public health code. The certificate is issued for a period of three years, and a surveillance audit is carried out every year. The French Digital Health Agency ("ANS") published French and English versions of its health data host certification framework requirements.

In Europe, several bodies work towards creating technical

standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles:

- the **European Telecommunications Standards Institute ("ETSI")** produces standards for the information and communications technology industry;
- the **European Committee for Standardisation ("CEN")** is concerned with laying down technical specifications for goods and services in all fields, including healthcare, the digital society (e.g., artificial intelligence, smart grids), defence and security, etc. – it collaborates with the AFNOR for France;
- the **European Committee for Electrotechnical Standardisation ("CENELEC")** develops standards in the field of electrical goods; and
- the **European Union Agency for Cybersecurity ("ENISA")**, although it does not create standards, influences the technical and cybersecurity frameworks adopted in European standards.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Interoperability standards are a strategic lever for creating open ecosystems, ensuring competitiveness and building reliable, scalable and secure solutions.

The components of connected technologies are manufactured and sold by entities subject to different regulations and standards. Therefore, it is crucial for the stakeholders in this ecosystem to ensure that the technologies they use or wish to market are interoperable and reliable. In this context, the use of standardized norms (such as AFNOR or ISO), labels, or certifications applicable to the connected technologies sector allows stakeholders to share a common framework and then facilitate commercial relationships between them.

Decree No 2023-1271 of 27 December 2023, and its implementing order transpose into French law the European regulation requiring a common charger. From 28 December 2024 (26 April 2026 for computers), radio equipment must include a USB Type-C port as a common charger. Additionally, companies will be required to offer consumers the option to purchase the device and the charger separately, indicated by a pictogram. Manufacturers of equipment such as cell phones and smartphones, tablets, cameras, headphones and earphones, game consoles, speakers, e-readers, keyboards, computer mice, portable navigation systems, laptops must comply with these legal and technical standards.

In addition, **the Regulation (EU) 2023/2854 ("Data Act")** – applicable from 11 September 2025 – provides for enhanced interoperability requirements for data and IT systems to facilitate the transfer and use of data between different services and applications.

This regulation also provides obligations for manufacturers of connected products and providers of related services to share data generated by these products/services with users and third parties chosen by users. This regulation was introduced in response to the increase in the number and proliferation of connected products ("Internet of Things"), which has increased the volume of data and its potential value to consumers, businesses and society, and the willingness to give users full control over their data.

The Regulation (EU) 2024/2857 ("Cyber Resilience Act" or "CRA") – applicable from 11 December 2027, with the exception of the reporting obligations of manufacturers applicable from 11 September 2026 and the rules regarding the notification of conformity assessment bodies applicable from 11 June 2026 – provides for horizontal cybersecurity requirements for products with digital elements. Under this regulation, manufacturers must take into account changes in harmonised standards, European cybersecurity certification schemes or common specifications, by reference to which the conformity of the product with digital elements is declared or by application of which its conformity is verified. The conformity with essential cybersecurity requirements of this regulation will be presumed when products with digital elements and processes put in place by the manufacturer are in conformity with these standards (article 27 of the CRA).

Finally, **Regulation (EU) 2024/1689 ("Artificial Intelligence Act")** – applicable from 2 August 2026, with some exceptions moving forward the application date to February and August 2025 or pushing it to August 2027 – lays down harmonised rules on artificial intelligence. It imposes on providers of AI systems, including general-purpose AI systems, generating synthetic audio, image, video or text content, to ensure that their technical solutions are effective, interoperable, robust and reliable as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art, as may be reflected in relevant technical standards.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

The principal laws which govern the protection of personal data are set out below:

- Law No 78-17 of 6 January 1978, which regulates the protection of personal data (and its implementing decree No. 2019-536 of 29 May 2019);
- EU General Data Protection Regulation No 2016/679 ("GDPR"), adopted on 27 April 2016, and effective since 25 May 2018;
- Law No 2016-1321 of 7 October 2016 for a Digital Republic;
- EU Directive No 2016/680 of 27 April 2016 on the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data;
- EU Directive No 2002/58 of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive). This Directive was meant to be replaced by a new ePrivacy Regulation. Whose proposal was withdrawn in 2025. Legislators claimed that no agreement was expected, and that the proposal was outdated in view of some recent legislation in both the technological and the legislative landscape.

The CNIL and the European Data Protection Board (EDPB) issue opinions and guidelines on the application of data protection regulations and render binding decisions.

Although not dedicated to the protection of personal data, the rules set out in the Digital Governance Act (Regulation (EU) 2022/868) and the Data Act (Regulation (EU) 2023/2854) concern both personal and non-personal data. These regulations provide for their provisions to be compatible with existing data protection regulations, such as the GDPR.

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Pursuant to article 83 of the General Data Protection Regulation, the sanctions issued by the CNIL range from 10 million euros to 20 million euros, or, in case of undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In 2022, the CNIL's enforcement procedures were modified. In particular, a "simplified" procedure was created to deal with cases that do not present any particular difficulty. This procedure remains at the discretion of the CNIL president. The following criteria are taken into account when identifying these cases:

- the existence of similar previous decisions;
- previous decisions made by the restricted panel – the CNIL body responsible for imposing sanctions;
- the simplicity of the factual and legal issues to be decided.

The penalties that may be imposed are capped at a fine of up to 20,000 euros which may not be made public.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

In France, technology contracts typically refer to the GDPR due to its applicability within the European Union. References to external data protection regimes are not common, unless there is a specific international element in the contract.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

Cybersecurity law in France is governed by the following European and national legislation:

- **Law No. 88-19 of 5 January 1988, commonly referred to as the "Godfrain Law"**, introduced into the French Criminal Code a set of criminal offences related to automated data processing systems (*systèmes de traitement automatisé de données* – STAD). Codified in Articles 323-1 to 323-8 of the French Criminal Code, these provisions criminalise various forms of cyber misconduct, including unauthorised access to an automated data processing system (Article 323-1); remaining within such a system without right, after

gaining access unlawfully (also Article 323-1); obstructing or disrupting the operation of such a system (Article 323-2) or introducing, modifying, or deleting data in the system fraudulently (Article 323-3). Depending on the nature and severity of the offence, penalties range from two years' imprisonment and a €60,000 fine to up to ten years' imprisonment and a €300,000 fine, particularly when committed by an organized gang.
The Godfrain Law remains the foundational legal framework for prosecuting cybercrime such as hacking in France.

- The **French Defence Code** ("FDC") imposes specific cybersecurity obligations on Operators of Vital Importance (OIVs) pursuant to Articles L.1332-1 et seq. These provisions mandate that OIVs implement robust security measures, including conducting regular security audits, promptly reporting security incidents, and maintaining active cooperation with the French National Cybersecurity Agency (ANSSI). Furthermore, under Articles L.2321-1 et seq. of the FDC, ANSSI is vested with the authority to oversee and safeguard the State's information systems. The agency is empowered to issue binding security regulations and technical guidelines to ensure appropriate protection standards. In executing its mandate, ANSSI may, subject to stringent confidentiality requirements, access specified data and systems—particularly those pertaining to national defence matters—to assess vulnerabilities and mitigate potential threats to France's digital infrastructure.
- Law **No 2024-449 of 21 May 2024 ("SREN")** aims to secure and regulate the digital space, extending cybersecurity obligations to online platforms, including hosting providers, messaging apps, and social media companies, requiring them to cooperate with national authorities in the event of cyber incident. It grants increased powers to ARCOM (the audiovisual and digital communication regulator) and ANSSI (France's cybersecurity agency) to detect, monitor, and respond to malicious digital activities, including phishing and the spread of harmful content.
- The **EU Cybersecurity Act**, formally Regulation (EU) 2019/881, in force since 27 June 2019, strengthens the EU's cybersecurity framework by giving ENISA (the EU Agency for Cybersecurity) a permanent mandate and enhanced responsibilities in supporting Member States and EU institutions. It also establishes a European cybersecurity certification framework for ICT products, services, and processes, aiming to harmonise certification schemes and increase trust in digital technologies. The regulation introduces three assurance levels—basic, substantial, and high—to reflect different risk profiles.
- The **EU Cyber Solidarity Act (Regulation 2025/38) (CSA)**, proposed by the European Commission in April 2023 and in force since 4 February 2025, strengthens the EU's collective cyber defence capacity. It establishes a European Cyber Shield through a network of national and cross-border Security Operations Centres (SOCs) to detect and respond to cyber threats. The Act also introduces a Cyber Emergency Mechanism for testing critical sector resilience, and a Cybersecurity Incident Review Mechanism for assessing major incidents, thereby reinforcing EU-wide coordination and preparedness.
- The **Cyber Resilience Act (CRA)** aims to ensure that digital products placed on the EU market are secure by design and remain so throughout their lifecycle. It introduces mandatory cybersecurity requirements for manufacturers, covering areas such as secure development, regular updates, and incident reporting. Products deemed critical must undergo third-party certification. Exemptions apply to sectors already covered by equivalent regulations, such as medical devices or vehicles. The Cyber Resilience Act entered into force on 10 December 2024. The main obligations introduced by the Act will apply from 11 December 2027.
- The **Digital Operational Resilience Act (DORA)** (**Regulation (EU) 2022/2554**) is in force since 17 January 2025. It establishes a harmonised cybersecurity framework for the financial sector, requiring banks, insurers, investment firms, and their ICT providers to manage and report cyber risks, ensure operational resilience, and test their digital defences.
- **EU Directive on Security of Network and Information Systems (NIS Directive / NIS2 Directive)** enhance cybersecurity across the EU by imposing security and incident reporting obligations on operators of essential services and digital service providers. NIS2 Directive that came into force in January 2023 replaces the original NIS Directive of 2016. The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the EU by ensuring.
  Specifically, it requires:
  - Member States to ensure national preparedness, including the establishment of a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.
  - Enhanced cooperation between EU countries, through the creation of a Cooperation Group to facilitate strategic coordination and information exchange.
  - A stronger cybersecurity culture in essential sectors such as energy, transport, water, banking,

healthcare, and digital infrastructure.
- Operators of essential services and key digital service providers (e.g., cloud services, search engines, online marketplaces) to implement risk management measures and to notify authorities of significant incidents.

In France, the transposition of this directive into national law is currently underway. The transposition of this directive into national law was expected by October 17, 2024, but has been delayed. A bill was adopted on first reading by the Senate on March 12, 2025, and is still pending approval by the Parliament.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

In the event of a breach of applicable cybersecurity laws, the maximum sanction that can be imposed by a regulator in France or under EU law depends on the regulatory framework and the sector concerned.

Notably, CNIL can impose fines of up to €20 million or 4% of global annual turnover under the GDPR when data security breaches occur.

Under NIS2, the ANSSI (France's national cybersecurity authority) may propose sanctions, with the maximum administrative fines reaching €10 million or 2% of global annual turnover for essential entities, and up to €7 million or 1.4% for important entities, whichever is higher.

Under Article L. 1332-7 of the French Defence Code, entities designated as Operators of Vital Importance (OIVs) that fail to comply with the cybersecurity obligations imposed under the national security framework may face administrative sanctions, such as financial penalties of up to €750,000 for legal entities.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

The EU Regulation No 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence ("EU AI Act") provides for the designation of a European Artificial Intelligence Board at the European level and of a national authority in each Member State to act as market surveillance authorities. These authorities and board shall be designated by 2 August 2025. The European Data Protection Board recommended that data protection authorities be designated as market surveillance authorities for high-risk AI systems in a statement dated 17 July 2024.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

The EU Regulation No 2024/1689 of 13 June 2024, in force since 1st August 2024, laying down harmonised rules on artificial intelligence ("EU AI Act") is the principal law that governs the provision, deployment and use of artificial intelligence on a risk-based approach. The EU AI Act defines the binding rules for an AI system which are proportionate to the level of risk it poses: AI systems with unacceptable risks are prohibited, high-risk systems will be subject to stringent obligations and conformity assessments, and certain AI systems will be required to meet transparency obligations.

The harmonised rules laid down in the EU AI Act should apply across sectors and should be without prejudice to existing Union law, in particular on data protection, consumer protection, copyright, fundamental rights, employment and protection of workers, and product safety, to which this regulation is complementary.

In France, the CNIL has launched an AI Action Plan since May 2023, formally publishing two sets of recommendations in June 2024 and February 2025, covering topics such as the legal basis for training AI models (e.g., legitimate interest under Article 6 GDPR), transparency requirements, informing individuals about data in training sets, and integrating privacy-by-design principle.

At the EU level, the European Commission released the General Purpose AI Code of Practice in July 2025 to help providers of large language model applications comply with the AI Act's transparency and safety obligations. This voluntary code (non-binding) complements the regulation by offering practical guidance on best practice.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

The EU AI Act provides for specific legal requirements for

the provision, deployment and use of large language models (LLMs) and generative AI. Under article 53, providers must maintain detailed documentation of model architecture, training datasets, and performance, and must ensure copyright compliance and transparency to both national authorities and downstream users.

The French data protection authority (CNIL) is very active and provides guidelines and recommendations for the ethical and lawful use of AI. The CNIL has published sets of recommendations in June 2024 and February 2025, covering topics such as the legal basis for training AI models (e.g., legitimate interest under Article 6 GDPR), transparency requirements, informing individuals about data in training sets, and integrating privacy-by-design principle.

Beyond binding regulation, the European Commission issued the General-Purpose AI Code of Practice in July 2025, offering voluntary technical standards to fulfil transparency, copyright, and systemic-risk obligations under Articles 53 and 55 of the AI Act. The European Data Protection Board (EDPB) also published, in April 2025, a detailed report on the privacy risks associated with the use of LLM systems, proposing a comprehensive risk management methodology, including the identification, assessment and implementation of mitigation measures tailored to the requirements of the GDPR and the AI Regulation.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

In France, no legislation currently mandates the inclusion of clauses concerning artificial intelligence. However, the AI Act, although not directly addressing contract law, provides for the possibility for the AI Office of developing model terms for contracts between providers of high-risk AI systems and third parties that supply tools, services, components or processes that are used for or integrated into high-risk AI systems (EU AI Act, Article 25).

Regarding best practices, all contractual clauses should be considered in the context of artificial intelligence, particularly clauses related to liability, insurance, subcontracting, and security.

Additionally, the protection of personal data must be considered when developing, deploying or using AI systems. It is advisable to audit the AI systems in the light of GDPR in order to identify and analyse data flows, data processing and status (data controller/data processor) before updating GDPR documentation (such as register of processing activities, privacy policies, data protection impact assessment) and contracting in accordance with applicable requirements (e.g. data processing addendum of article 28, standard contractual clauses).

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

In France, intellectual property clauses are essential and common to all software and technology contracts. Therefore, it is crucial to include such clauses in the context of using AI systems to clarify the ownerships of the AI systems and/or of the outputs. In the absence of any written assignment of intellectual property rights that complies with legal requirements of article L.131-3 of the French intellectual property code, the proprietary rights in newly created software would belong to the software developer who created it and not to customer.

The protection of intellectual property rights must also be a key consideration for the co-contractors, concerning both data created by AI and third-party data that may be protected by intellectual property rights.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

Blockchain technology in France is governed by a combination of specific national laws and EU regulations such as Pacte Law, DLT regime Pilot and the GDPR.

- **The Regulation (EU) 2016/679 of 27 April 2016 ("GDPR")** applies to any technology or platform that processes personal data, including blockchain, if that technology is located in an EU Member State of it processes personal data of a resident of an EU Member State. It sets out principles for the lawful processing of personal data within the EU, ensuring data protection and privacy rights for individuals.
- **The Regulation (EU) 2022/858 of 30 May 2022 ("DLT**

Pilot Regime") aims to establish a specific regulatory framework to allow market infrastructures to experiment with the use of distributed ledger technology (DLT), such as blockchain, in a regulated and supervised environment. This regulation creates a regime in which market infrastructures can obtain exemptions from applicable financial regulation in order to be able to use DLT for the trading and settlement of securities transactions.
- **Regulation (EU) 2022/2554 of 14 December 2022 ("DORA")** does not govern blockchain technology as such, but it applies to a wide range of financial entities, including crypto-asset service providers. As such, entities operating in the blockchain sector should fall within the scope of DORA only when they qualify as regulated financial institutions, such as licensed crypto-asset service providers. These entities must comply with DORA's rules on ICT risk management, incident reporting, resilience testing, and contractual obligations with third-party ICT providers.

In addition, the European Data Protection Board adopted on 8 April 2025 guidelines 02/2025 on processing personal data through blockchain technologies. These guidelines highlight key GDPR compliance factors relevant to planned processing activities, while evaluating various architectural models of blockchain technologies and their impact on data processing.

Digital assets are regulated under several laws and EU regulations:

- **The 2019 PACTE Law** introduced a regulatory framework for Initial Coin Offerings (ICOs). ICO issuers can obtain a visa from the French Financial Markets Authority (*Autorité des Marchés Financiers, AMF*) which provides more credibility but is optional. This law also established the regime for Digital Asset Service Providers (DASPs). Digital asset service providers are required to register and obtain approval. The provisions of this law were supplemented by the DADDUE Law of 9 March 2023, which adds the mandatory enhanced registration for digital asset service providers. However, it should be noted that this French legislation has evolved with the implementation of the MiCA Regulation No 2023/1114, in force since30 December 2024.
- **The EU Regulation No 2023/1114 of 31 May 2023 ("MiCA")** defines a harmonized and specific regulatory framework for crypto assets. This regulation standardizes the legal framework applicable to players in this market, while also strengthening consumer and investor confidence. The stated objective of the European legislator is to create a secure environment to support the development of the crypto-asset sector within the European Union. The new obligations introduced by MiCA specifically aim to:
  - Increase transparency of the information provided to crypto-asset holders and investors: entities subject to MiCA will be required to publish a white paper containing essential information about the crypto-assets, such as the rights and risks involved; marketing communications will also be regulated.
  - Ensure market integrity: preventive measures target insider trading and market manipulation.

MiCA replaces existing national frameworks, including the French PACTE law of May 22, 2019, which had established a specific regime for public offerings of tokens (Initial Coin Offerings or ICOs) and digital asset service providers (DASPs).

An ordinance (*Ordonnance n° 2024 936 of 15 October 2024)* adapted national law (notably the Monetary and Financial Code) to align with the EU's MiCA regulation. A decree, (*Décret n° 2025 169 of 21 February 2025)*, clarified registration procedures, financial contributions to the AMF, and transitional provisions.

French registered PSANs (*Prestataires de Services sur Actifs Numériques*) (i.e., Digital Asset Service Providers offering services such as crypto-asset custody, trading, or exchange) registered under the 2019 PACTE law may continue operating until 1 July 2026, allowing time to obtain MiCA-compliant authorization as CAPs (Crypto-Asset Service Providers).

- **The EU Regulation No 2024/1624 of 31 May 2024** on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. It considers notably notaries, lawyers and other independent legal professionals, where they participate, whether by acting on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning managing of client crypto-assets or opening crypto-assets accounts.
- **The EU Directive No 2018/843 ("AMLD V")**, which has been transposed into French law, includes provisions applicable to cryptocurrency exchanges and wallet providers, requiring them to implement robust AML/CTF measures.

28. Search Engines and Marketplaces – Please

summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

The principal laws that govern search engines and marketplaces are set out below:

- **Law No 2004-575 of 21 June 2004, on the confidence in digital economy ("LCEN")** (which transposes the Directive on Electronic Commerce (2000/31/EC) governs e-commerce and online service providers in France and was amended by the SREN law. The aim of the LCEN is to establish trust and security in the digital economy by imposing obligations on online service providers, such as defining the responsibility of online service providers for third-party content, requiring hosting providers to promptly remove illegal content as soon as they become aware of it, and requiring platforms to provide clear identification and contact information.
- **Law No 2016-1321 of 7 October 2016 for a Digital Republic** regulates the circulation of data and increases user's rights. As a matter of example, search engines have to inform users of criteria used to rank results. It also imposes that online marketplaces treat offers in a non-discriminatory manner.
- **The General Data Protection Regulation (2016/679) ("GDPR")** applies to search engines and marketplaces, which are located in the EU Member States or process personal data of EU Member States residents. The GDPR provides some obligations to ensure users' privacy and control over their personal data.
- **The EU Regulation No 2019/1150 of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services ("P2B")** ensures that business users of online intermediation services and corporate website users in relation to online search engines are granted appropriate transparency, fairness and effective redress possibilities. Platforms must be transparent about their terms and conditions, including product rankings. In addition, companies must have internal complaint handling mechanisms and access to mediators to resolve disputes.
- **The EU Regulation No 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector ("DMA")** aims to prohibit practices such as "self-preferencing" (favoring one's own services) and abusive use of user data. Furthermore, the DMA forces gatekeepers to allow their services to be interoperable with those of third parties and offer greater transparency about their operations.
- **The EU Regulation No 2022/2065 of 19 October 2022 on a single market for digital services ("DSA")** establishes rules for liability and control of providers of intermediary services (i.e. hosting services, mere conduit services and caching services). In particular these providers must have mechanisms in place to remove illegal content promptly upon notification and provide transparency reports on content moderation practices. In addition, they have to provide information on targeted advertising, including the targeting criteria used, and to protect consumers from counterfeit goods and scams on marketplaces. Larger platforms have specific obligations, such as conducting risk assessments and allowing audits by authorities.
- **Law No 2023-451 of 9 June 2023** regulates commercial influence and combats abuses by influencers on social media. In particular, it imposes moderation and verification obligations on platforms hosting sponsored content.
- **Law No 2024-449 of 21 May 2024 ("SREN")** aims at securing and regulating the digital space. The main measures of this law aim at protecting minors against access to pornographic websites, reinforcing sanctions for the publication of heinous and illegal content as well as fighting against disinformation. It also introduces a cybersecurity certification for operators of online platforms and of search engines offering services to the general public (article L.111-7-3 of the French consumer code).
- **The EU Regulation No 2024/1689 of 13 June 2024 lays down harmonised rules on artificial intelligence ("Artificial Intelligence Act")**. Providers and deployers of certain AI systems, and in particular providers of very large online platforms and very large online search engines are required to assess the systemic risks arising from the design, operation and use of their service using AI and are required to take appropriate mitigation measures. In particular, they are subject to obligations relating to the dissemination of content that has been generated or manipulated by AI, and must especially identify and mitigate the risk of actual or foreseeable negative effects on democratic processes, public debate and electoral processes, including through disinformation.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

Social media platforms and online platforms are governed by several key laws and regulations aimed at protecting users, combating illegal content, and ensuring

platform accountability:

- The social media, as data controller, must comply with the GDPR (General Data Protection Regulation (GDPR)). The goal is to enhance privacy rights and data security for the user.
- The Digital Services Act (DSA) and Digital Markets Act (DMA) shall apply, under certain conditions to social media. The DSA aims to combat illegal content online such as hate speech and disinformation and regulate online advertising practice.
- The DMA targets gatekeepers (Alphabet Inc., Amazon.com Inc., Apple Inc., Booking, ByteDance Ltd., Meta Platforms Inc., Microsoft Corporation) with specific rules to prevent unfair practices, promote competition, and enhance consumer choice and control over their data. The DSA, under Article 28, requires online platforms accessible to minors to implement appropriate and proportionate measures to ensure a high level of privacy protection. It also prohibits profiling-based advertising targeting minors when the platform has reasonable certainty that the user is underage.
- Law No 2022-300 of 2 March 2022 aimed at strengthening parental control over Internet access media requires all Internet-accessible terminals marketed in France to incorporate a free, accessible and comprehensible parental control system. This obligation has been fully applicable since 13 July 2024.
- Law No 2023-451 of 9 June 2023 defines a legal framework for influencers on social networks when they have a commercial activity in order to combat fraudulent or misleading practices. Promotion of specific products is prohibited (health, finance, sports betting, nicotine). After the letter sent by the European commission notifying that this law was not compatible with the DSA, the French government published a draft ordinance on 3 July 2024 which amends this law on influencers and has been transmitted to the European commission.
- Law No 2023-566 of 7 July 2023 establishes a digital majority (in France, this age is 15) and aims to combat online hate. Failure by an online social networking service provider to comply with these obligations is punishable by a fine not exceeding 1% of its worldwide sales for the previous financial year. However, it has not yet come into force, as the implementing decree has not yet been published. It could also remain a dead letter, as the European Commission felt that it was likely to contravene the Digital Services Act (DSA) by introducing stricter or more detailed requirements in areas regulated at European level.
- Law No. 2024-120 of 19 February 2024 aims to protect children's image rights by regulating “sharenting", the practice by which parents post photos or videos of their children on social media. The provisions of the French Civil Code (article 373-2-6 if the French Civil Code) allow the family court judge to intervene and prohibit one parent from sharing online content if there is a disagreement between the two parents regarding its publication.
- Law No 2024-449 of 21 May 2024 aims at securing and regulating the digital space. It introduces a cybersecurity certification for operators of online platforms and of search engines offering services to the general public (article L.111-7-3 of the French consumer code). It requires online platform operators to subject themselves to a cybersecurity audit, carried out by third parties qualified by the French National Cybersecurity Agency (“ANSSI") and covering the security and location of the data hosted on their platform, and their own security. The ‘cyber-score' resulting from the audit must be presented to the consumer in a legible, clear and comprehensible manner and accompanied with a visual based on a colour scheme.
- Article 227-24 of the French Criminal Code and Law of 21 June 2004(LCEN), updated by Law of 21 May 2024 (SREN), aims to protect minors from online pornographic content. The French audiovisual and digital regulator (ARCOM) is the key authority tasked with enforcing these regulations. On 9 October 2024, the French regulatory authority for audiovisual and digital communication (ARCOM) issued a reference framework establishing the minimum technical requirements for age verification systems. A simple age declaration is no longer sufficient. An arrêté issued on 26 February 2025 specifically designated several services, including Pornhub, YouPorn, RedTube, and xHamster, compelling them to comply with these obligations. On 15 July 2025, the Conseil d'État confirmed the immediate application of this arrêté, rejecting a suspension request.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

Under the DSA, ARCOM may impose administrative fines of up to 6% of a platform's global annual turnover for serious or repeated breaches of its obligations (e.g., failure to address illegal content, perform risk assessments, or ensure user protection), in accordance with Article 74 of the DSA.

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

No French or EU law currently regulates "spatial computing" per se.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

The upcoming European Quantum Act (proposal expected 2026), which is part of the EU's quantum strategy adopted in July 2025, aims to build a robust quantum ecosystem in the EU by supporting research, production of hardware (e.g. quantum chips), and secure infrastructures.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

France does not have dedicated laws for data centres per se, but several regulations apply to them under environmental and energy framework such as:

- **Law No 2021-1485 of 15 November 2021 ("REEN")** aims to reduce the environmental impact of digital technologies in France by promoting a more sustainable and responsible digital sector. This act promotes energy-efficient data centres by linking environmental conditions to tax benefits and requiring operators to publish key environmental indicators.
- **Law No 2025-391 of 30 April 2025 ("DDADUE")** transposes the revised EU Energy Efficiency Directive (DEE/EED) of 20 September 2023. It creates Articles L. 236 1 to L. 236 3 in the French Energy Code, requiring data centres ≥ 500 kW to publicly report annual energy and environmental performance, and for those ≥ 1 MW to utilise waste heat, unless exempted. After a formal public notice, the General Directorate of Energy and Climate (DGEC) may impose administrative fines of up to €50,000 per data centre for non-compliance with energy reporting and waste heat obligations. (article L236-3 of the French Energy Code).
- **A draft economic simplification law (*Projet de loi de simplification de la vie économique*)** in France proposes granting large data centres the status of "major national interest projects", enabling faster permitting, simplified environmental procedures, and accelerated grid connection.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

1. **Artificial Intelligence (AI):** France is likely to enhance its regulatory framework for AI, focusing on ethical guidelines, accountability, and transparency. Expect new laws addressing AI's impact on employment, privacy, and safety, with measures to mitigate biases and ensure responsible AI deployment in sectors like defense, healthcare, transportation, agricultural sector and public administration. Expect early case law on algorithmic discrimination or liability (e.g. in employment or insurance).
2. **Digital Services and Platforms Regulation**: there could be increased scrutiny and regulation of digital platforms and big tech companies operating in France especially in the perspective of the 2027 presidential election. Anticipate stricter rules on content moderation, and consumer protection, potentially aligning with EU directives such as the Digital Services Act (DSA) and Digital Markets Act (DMA. In addition, as a result of the Data Governance Act (DGA) and the Data Act, new platforms for sharing data for different purposes (business, general interest, etc.) should emerge.

Regulation of large online platforms could also be part of France's digital sovereignty strategy (e.g., strengthening the national enforcement of the DSA and DMA, particularly on issues such as foreign influence).

3. **New technology and ecology (environmental sustainability)**: France could enact new laws in order to promote green technologies, the use of technology for climate data collection, analysis, and monitoring. We can expect a possible emergence of a "green by design" principle in digital services as well as dedicated clauses in IT outsourcing and cloud agreements.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Environmental commitments are not common in technology contracts. However, there is a growing recognition of the importance of environmental considerations. Companies are increasingly looking to integrate sustainability goals into their contractual relationships. Companies subject to ESG reporting requirements (e.g., under the Corporate Sustainability Reporting Directive (Directive (EU) 2022/2464), entered into force on 5 January 2023 and transposed into French law by Ordinance No. 2023 1142 of 6 December 2023) can impose their internal codes of conduct or supplier charters on their subcontractors, including IT service providers. These codes of conduct often include environmental commitments. Even if they are not negotiated in the body of the contract, these obligations are often included by reference.

Contributors

Emilie de Vaucresson
Partner
edevaucresson@joffeassocies.com

Amanda Dubarry
Associate
adubarry@joffeassocies.com

Hanna-Marie Borten-Guary
Associate
hmbortenguary@joffeassocies.com