Chambers AND PARTNERS

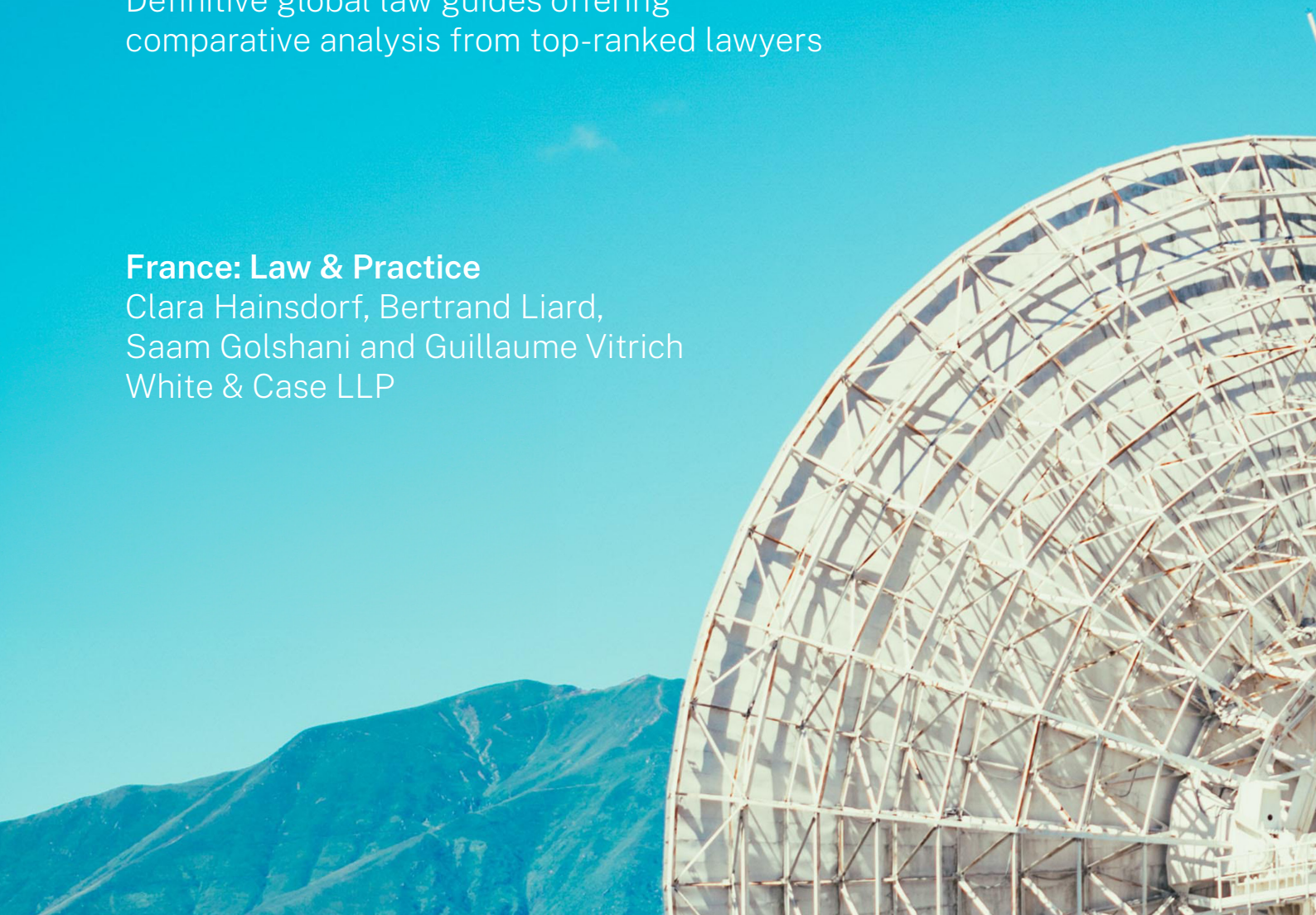
CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2026

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

France: Law & Practice

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



FRANCE

Law and Practice

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

Contents

White & Case LLP has 44 offices across 30 countries, making it a truly global law firm, uniquely positioned to help clients achieve their ambitions in today's G20 world. Not only is White & Case a pioneering international law firm but it is also one of the oldest US/UK law firms in France (opened in 1926), with a history of excellence. The Paris office has over 200 lawyers, including 59 partners, who work with some of the world's most respected banks and businesses, as well as start-up visionaries, governments and state-owned entities. Its TMT practice houses a large group of dedicated lawyers and offers deep experience across a wide range of technologies in areas including both hardware and software across a variety of applications, uses and deployment, such as data centres, analytics, communication infrastructure, on-premises and SaaS, embedded technologies, internet of things, security, privacy and data protection, semiconductors and more.

Authors

Clara Hainsdorf is a partner in White & Case's intellectual property and information technology department in Paris. She has extensive experience in ICT legal issues, including technology licences, e-commerce and complex commercial contracts. Clara specialises in privacy and data protection, advising on GDPR compliance, international data transfers and investigations. She is also an expert in AI law, focusing on algorithmic transparency and regulatory compliance, and is knowledgeable about the Digital Services Act and cybersecurity, assisting clients with content moderation and liability issues. A frequent speaker and author, she combines legal expertise with a forward-thinking approach to technology.

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

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

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

White & Case LLP

19, place Vendôme
75001
Paris
France

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

WHITE & CASE

1. Digital Economy

1.1 Legal Framework

Digital Services and Content Regulation

In light of the broad scope of application of the Digital Service Act (DSA), the inter-relationship of some of the national laws set out in this chapter with the DSA still needs to be clarified, particularly where national measures may overlap or diverge from EU-level obligations.

The liability of hosting providers, previously governed by Law No 2004-575 on Confidence in the Digital Economy (LCEN), is now regulated by the DSA, which generally came into effect on 17 February 2024 and is directly applicable in French law.

This new framework establishes harmonised due diligence obligations for providers of intermediary services, and gives regulators broad investigative and enforcement powers at both national and EU levels. However, the core principle of intermediary liability remains the same: hosting providers are not liable for user content unless they have actual knowledge of its illegal nature and fail to act promptly.

The French Consumer Code sets out the obligations that are applicable to online platforms in their relations with consumers (eg, pre-contractual duty to inform).

French Law No 2024-449 of 21 May 2024, known as *Sécurité et Régulation de l'Espace Numérique* or Security and Regulation of the Digital Space (SREN Law), aligns French legislation with EU regulations such as the DSA, the Data Governance Act (DGA) and the Digital Markets Act (DMA), focusing on online safety, misinformation and digital asset regulation. It affects cloud computing, interoperability and digital sovereignty.

Since the adoption of the SREN Law, several implementing decrees have further clarified its application, with the following examples.

- Decree No 2024-753 mandates online comparators, marketplaces and news aggregators to enhance transparency about ranking criteria, provider relationships, pricing and guarantees. Sponsored content must be labelled as "Ads".
- Decree No 2024-1255 sets out the procedures under which the *Autorité de régulation de la communication audiovisuelle et numérique* (ARCOM) may conduct investigations and inspections when enforcing the DSA.
- Decree No 2025-768 establishes a threshold of 10 million unique monthly visitors for certain obligations relating to the temporary retention of illegal content by online platform operators.
- Decree No 2025-9 designates the Directorate General for Competition Policy, Consumer Affairs and Fraud Control (DGCCRF) as a competent authority for monitoring compliance with the DSA by intermediary service providers.

Digital Markets Regulation

Digital markets are currently mostly regulated by general competition law.

The EU Regulation on platform-to-business relations (P2B Regulation) was adopted in 2019 to impose

transparency and fairness obligations on online intermediation services and online search engines used by business users to provide goods and services to consumers.

The DMA imposes a range of obligations on providers of core platform services, which are designated as "gatekeepers". An undertaking should be identified as a gatekeeper if it fulfils three qualitative criteria:

- it has a significant impact on the internal market;
- it provides a "core platform service" that serves as an important gateway for business users to reach end users; and
- it enjoys an entrenched and durable position in its operations, or is expected to enjoy such a position in the near future.

These three criteria are presumed to be satisfied if three quantitative thresholds are met, respectively:

- the undertaking has either an annual turnover above EUR7.5 billion in each of the last three financial years or market capitalisation or equivalent fair market value above EUR75 billion in the last financial year, and it provides the same core platform service in at least three member states of the European Union;
- the core platform service has at least 45 million monthly active end users or 10,000 active business users located or established in the EU; and
- this second threshold has been met in each of the last three financial years.

The designated gatekeepers under the DMA are subject to a list of ex ante obligations and prohibitions, most of which must be implemented within six months of their designation. The DSA takes a more comprehensive approach, encompassing a wider range of digital intermediary services and imposing requirements on very large online platforms and very large online search engines to address systemic risks associated with their operations.

On 6 March 2024, the new DMA regulatory framework came into effect for the first designated gatekeepers. This framework includes rules on interoperability and data sharing, and prohibits practices such as self-preference. The European Commission oversees its application and can impose fines of up to 10% of worldwide turnover for infringement (20% in case of repeat offence). At the time of writing, the European Commission has designated seven gatekeepers (Alphabet, Amazon, Apple, Booking.com, ByteDance, Meta and Microsoft) and 23 core platform services.

Under the DMA, gatekeepers must submit and regularly update a series of compliance reports detailing how they implement their obligations. They also had to publish independently audited reports on consumer profiling techniques, by 7 March 2025. The European Commission reviews these submissions to assess the effectiveness of the measures adopted.

The DGA, together with the Data Act, is part of the European Data Strategy presented by the European Commission in 2020. This strategy aims to develop a single data market by supporting responsible access, sharing and reuse, in compliance with EU values, and particularly the protection of personal data. The DGA entered into force on 24 September 2023, with a compliance obligation for entities providing data intermediation services no later than 24 September 2025. The regulation aims to promote the sharing of personal and non-personal data by setting up intermediation structures, and concerns all sectors of activity, public and private, without restriction given the nature of data.

It includes a framework facilitating the reuse of certain categories of protected public sector data (confidential commercial information, intellectual property, personal data), and regulates the provision and sharing of data services by imposing notification obligations (private as well as public) and compliance obligations on the operators of these services. It also develops a framework for the voluntary registration of entities that collect and process data provided for altruistic purposes.

Digital Omnibus

In November 2025, the European Commission introduced the so-called Digital Omnibus proposal, marking a significant step in its broader simplification agenda for EU digital regulation. The initiative aims to streamline and rationalise the existing digital legisla-

tive framework while preserving the EU's high standards of protection. It responds to repeated calls from the European Council, the European Parliament and market stakeholders to address the growing regulatory complexity resulting from the cumulative expansion of EU digital legislation over recent years.

At its core, the proposal seeks to better align and consolidate several existing digital instruments, particularly in the area of data regulation. According to the proposal, GDPR remains the cornerstone of personal data protection. However, it restructures and integrates overlapping provisions from the Free Flow of Non-Personal Data Regulation, the Open Data Directive and the Data Governance Act into a reinforced and more coherent Data Act framework. The objective is to eliminate overlaps, harmonise key concepts and reduce legal uncertainty for businesses operating across the single market, with the Commission anticipating meaningful compliance cost reductions over time.

A central innovation of the proposal is the creation of a single EU entry point for incident reporting. This mechanism would allow organisations to comply with multiple notification obligations under different legal frameworks, including NIS2, GDPR data breach notifications, the Digital Operational Resilience Act (DORA), the EU regulation on electronic identification and trust services for electronic transactions of 2014 (eIDAS) and the Critical Entities Resilience (CER) Directive, through a single interface. This approach is intended to substantially reduce administrative burdens while ensuring effective and timely information sharing with competent authorities.

The proposal also aims to strengthen the EU data economy by clarifying and streamlining data-sharing frameworks. It builds on existing concepts such as data intermediation services and data altruism, while reinforcing safeguards for confidential information and trade secrets in data-sharing scenarios. By integrating rules on the reuse of public sector data into the Data Act framework, the Omnibus proposal seeks to provide clearer and more consistent conditions for data access and reuse, including specific considerations for large market players and gatekeepers in support of fair competition.

In the field of personal data protection, the Digital Omnibus maintains GDPR's high level of protection while introducing targeted adjustments designed to simplify compliance, particularly for low-risk processing activities. These include the alignment of certain notification thresholds, clarification of administrative obligations, and the development of EU-level harmonised tools and templates for data protection impact assessments. The proposal also seeks to better align e-privacy consent mechanisms with GDPR principles, notably by supporting automated and machine-readable consent signals once relevant standards become available, with the aim of reducing so-called "consent fatigue".

1.2 Key Challenges

Digital Services and Content Regulation

A key legal challenge in France concerns the regulation of minors' access to social media and the management of harmful online content. French Law No 2023-566 of 7 July 2023 (Article 4) attempted to restrict access for children under 15 by requiring parental consent for registration and account retention, enabling parents to request the suspension of accounts, and imposing age verification obligations according to ARCOM and French Data Protection Authority (CNIL) standards, with penalties capped at 1% of global turnover. However, the European Commission found the law incompatible with EU legislation, notably the DSA and the E-Commerce Directive, due to overlaps in content moderation obligations, the inability of French authorities to enforce obligations on providers established outside France (contrary to Article 56 of the DSA), and unjustified restrictions on the free provision of information society services under Article 3 of the E-Commerce Directive (letter from the Commission dated 14 August 2023).

This tension illustrates the broader challenge for France of balancing national efforts to protect minors and regulate harmful content with the need to comply with EU rules – a challenge that has influenced subsequent provisions under the SREN Law to harmonise domestic requirements with European obligations.

Another key legal challenge in France relates to age verification and harmful content. The SREN Law introduces strict requirements for verifying the age of users,

particularly in relation to access to pornographic content, in line with broader EU objectives. ARCOM has issued technical standards for implementing these age checks, aiming to ensure that platforms deploy effective mechanisms without compromising user safety or privacy.

Legal challenges have already emerged, as questions remain regarding the practical enforcement of age verification obligations while respecting personal data protection and privacy rights. On 15 July 2025, the *Conseil d'État* rejected the request for a provisional suspension of the interministerial order establishing age verification measures, confirming that the ARCOM-enforced framework could remain in force. In response, some platforms have withdrawn from the French market. This highlights the ongoing tension between safeguarding minors and ensuring that regulatory requirements are feasible and proportionate for service providers.

1.3 Digital Economy Taxation

Traditional tax rules cannot adequately tax highly digitalised businesses without a traditional "bricks and mortar" presence. Because of the difficulty in achieving agreement on a multilateral level, France introduced a French digital services tax (DST) in 2019, covering online advertising, sales of user data and the use of digital platforms. The tax applies to resident and non-resident companies with a worldwide turnover exceeding EUR750 million and a French turnover exceeding EUR25 million. The 3% tax applies on gross revenues deriving from the provision of a digital interface, targeted advertising and the transmission of data about users for advertising purposes. In 2025, the French government proposed to increase the DST to 6%, starting in January 2026, reflecting its intent to capture more revenue from major digital companies. The French Constitutional Court confirmed the constitutionality of the DST in September 2025.

France's Finance Law for 2024 introduced a new "streaming music services tax", which came into effect on 1 January 2024. This 1.2% tax applies to both paid and free services providing access to recorded music and online music videos in France, levied on amounts exceeding EUR20 million.

Entities established outside of France may be subject to French value-added tax (VAT) obligations if they carry out transactions with customers located in France, including non-resident businesses offering digital products. The standard VAT rate in France is set at 20%. Businesses are required to register for VAT as soon as they make their first business-to-consumer (B2C) sale in France. In November 2024, EU member states unanimously agreed on the VAT in the Digital Age (ViDA) proposal, which seeks to update the EU VAT system with three main components:

- e-invoicing and digital reporting;
- platform economy; and
- single VAT registration.

The current lack of an internationally co-ordinated approach may lead to overlapping taxes, possible double taxation and the administrative burden of applying multiple digital taxes.

To ensure compliance with tax regulations, companies selling digital products and services must understand their obligations. They must:

- determine where they have obligations by cross-checking customer locations, product taxability and registration thresholds in each country;
- monitor tax exposure and register in exposed jurisdictions;
- identify transactions that require tax collection and apply the correct rates to those invoices;
- file tax returns;
- make payments; and
- keep records.

French tax law also introduces additional specific obligations for operators of online platforms that act as intermediaries, which must submit a user's activity report to the French tax authorities with data about the users.

1.4 Taxation of Digital Advertising

As mentioned in **1.3 Digital Economy Taxation**, DST is applied to revenues generated by certain digital services, including digital advertising platforms, and this mainly targets large companies.

A specific tax applies to revenues generated by the broadcasting of advertising and sponsorship messages on video streaming. This tax is levied at a rate of 5.15% on the portion of pre-tax advertising income exceeding EUR100,000 received within a calendar year. The rate is raised to 15% for the portion of taxable advertising and sponsorship fees relating to access to pornographic content or incitement to violence on the audiovisual content access service. In cases where the platform is free of charge and hosts user-generated video content, allowing it to be shared and exchanged within communities of interest, the tax base is reduced by 66%. This reduction applies to streaming platforms that integrate social networking features, such as messaging services for users.

In France, all the specific taxation of digital advertising revenues must be liquidated, declared and paid to the *Direction générale des Finances publiques*.

To ensure compliance with tax law regarding digital advertising, companies must establish robust tax management and reporting systems. This includes the accurate collection of revenue data generated in each jurisdiction, the correct application of local taxes, and the timely submission of tax returns.

1.5 Consumer Protection

The French Consumer Code applies to the TMT sector and includes the new regulatory framework set by the DSA, the SREN Law and its implementing decree. Consumers benefit from several protections under this framework, including a legal guarantee of conformity (Articles L 217-4 to L 217-13 of the French Consumer Code) and a legal guarantee of hidden defects (Articles 1641 to 1648 of the French Civil Code).

Companies must include mandatory information on their websites to ensure consumers are aware of their rights. They must also comply with GDPR, which grants consumers enhanced rights of access, correction, deletion, restriction, objection and portability over their personal data. Companies must clearly inform users about how their data is used, especially for advertising purposes, and obtain explicit consent for the intended data processing, if needed.

To ensure that consumer rights are respected, companies must take the following steps:

- identify the applicable standards in the sector in which they operate and the specific regulations that apply thereto;
- follow best practices issued by authorities such as the CNIL, ARCOM or DGCCRF;
- adapt their processes to ensure compliance with these regulations;
- train their teams to raise awareness and ensure everyone understands and follows best practices and regulatory requirements; and
- conduct regular internal or external audits, to verify if they are applying the rules correctly and to correct any non-compliance.

The best practices to handle consumer disputes are to provide clear and comprehensive information to consumers, ensuring transparency while avoiding the disclosure of sensitive details, and to inform consumers about the possibility of resolving disputes amicably.

Companies should ensure access to efficient after-sales services to support consumer satisfaction. They must also implement the processes required by the Consumer Code, such as the right of withdrawal and easy termination procedures outlined by law. Furthermore, consumers are entitled to access a consumer mediator at no cost, to facilitate the amicable resolution of disputes with professionals. Access to consumer-specific mediation must be guaranteed by TMT companies.

Finally, companies need to establish internal processes to handle complaints promptly, such as offering a complaint form to address consumer issues.

1.6 The Role of Blockchain in the Digital Economy

Cryptocurrency significantly impacts the legal landscape of the TMT sector, both in France and in Europe. Enhanced anti-money laundering (AML) and counter-terrorist financing regulations require TMT companies involved in cryptocurrency activities to implement comprehensive know-your-customer and AML procedures, which are essential for preventing illegal activities and ensuring transaction integrity. The

integration of blockchain introduces new considerations for intellectual property rights and data security, requiring legal frameworks to evolve to address issues related to the ownership, distribution and protection of digital content and user data. The legal environment actively supports blockchain and smart contracts, fostering innovation and enabling new business models within the TMT sector.

The main legal challenge posed by cryptocurrency is smart contracts, which are self-executing contracts with terms written into code and stored on a blockchain. Their code-based structure complicates the interpretation of terms, potentially leading to unintended outcomes. Programming errors pose serious security and financial risks due to the irreversible nature of blockchain transactions.

Blockchain and crypto-assets are regulated under EU laws, which are technologically-neutral and refer to Distributed Ledger Technology (DLT). These rules apply to both DLT market infrastructure and crypto-assets.

DLT-based market infrastructure is governed by the general framework, which includes Directive 2014/65/EU (MiFID II) for multilateral trading facilities and Regulation No 909/2014 (CSDR) for central securities depositories. To promote DLT adoption, Regulation (EU) 2022/858 introduced the Pilot Regime, offering regulatory exemptions. This applies to DLT multilateral trading facilities, DLT settlement systems (DLT SSs) and combined DLT trading and settlement systems (DLT TSSs).

Alongside the general requirements, the Pilot Regime enforces transparency and cybersecurity requirements, such as publishing business plans, defining operational rules and implementing risk management procedures. It also allows DLT SSs and DLT TSSs to settle transactions in DLT-issued currency without using securities accounts or central bank money.

Since 2017, France's Ordinance No 2017-1674 has enabled the use of shared electronic registration systems (DEEP) for financial securities, granting them the same legal effect as traditional account registration.

Since 30 December 2024, crypto-assets in the EU have been governed by Regulation 2023/1114 (MiCA), which standardises rules for crypto-asset issuers to enhance consumer protection and financial stability. MiCA defines crypto-assets as digital representations of value or rights that can be transferred and stored using DLT.

MiCA identifies three categories of crypto-assets, as follows:

- e-money tokens (EMTs) are crypto-assets whose value is pegged to a single official currency;
- asset-referenced tokens (ARTs) are linked to other assets or rights; and
- all other crypto-assets fall into a separate category.

Issuers are required to publish a white paper, and only credit institutions or electronic money institutions are permitted to issue EMTs. Issuers of significant EMTs and ARTs must also comply with additional obligations related to liquidity and remuneration policies. NFTs, however, are explicitly excluded from MiCA's scope.

Since the regulation took effect, only authorised crypto-asset service providers are allowed to operate, subject to strict governance and transparency requirements. Existing providers may continue operating under national laws until July 2026 or until they receive MiCA authorisation.

Throughout 2025, France continued to adapt its national framework to the new EU-wide regulatory environment created by MiCA. On 21 February 2025, Decree No 2025-169 amended the *Code montaire et financier* to align domestic rules applicable to digital asset service providers (PSANs) with MiCA's requirements. Among other measures, providers must now pay a fixed annual fee of EUR10,000 when submitting a MiCA white paper.

The *Autorité des marchés financiers* (AMF) published new guidance in June 2025 to facilitate the transition from the previous French PSAN regime to the MiCA crypto-asset service provider regime. It confirmed that PSANs may continue operating until 1 July 2026 under

the French regime, provided they initiate the authorisation process in due time.

Further regulatory developments in 2025 reflect increased oversight at both EU and national levels. The AMF introduced Instruction DOC-2025-01, which sets out the format, content requirements and filing procedure for MiCA white papers relating to public offerings and admission to trading of crypt-assets. At the same time, several French regulators expressed concerns about "regulatory shopping" within the EU. France indicated that it may oppose the passporting of providers authorised in jurisdictions applying insufficiently strict supervision, highlighting a growing tension within the EU over the consistency of MiCA enforcement.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

Cloud Computing

CNIL defines cloud computing as the use of the memory and computing capabilities of computers and servers that are distributed around the world and are linked by a network. Applications and data are no longer located on a specific computer, but in a cloud with many interconnected remote servers.

Cloud computing service providers offer several deployment models, such as infrastructure as a service, software as a service or platform as a service. They allow a client to switch part or all its IT infrastructure and resources to the cloud, rather than managing it locally or internally. Under French law, there is no contractual law category related to cloud computing contracts; as such, they are subject to common French contract law.

The SREN Law imposes stringent security requirements on cloud service providers to protect hosted data. Providers must implement strong encryption protocols, conduct regular security audits and ensure the confidentiality of user data. They must also be transparent about the locations of their data centres and their data back-up and recovery policies. Particular attention should be given to the content of the contract, notably regarding data integrity and security, service level agreements (SLAs), the clear division of the responsibilities of each party, and compliance with data protection laws and regulations (Data Act, GDPR).

In addition, the termination of the contract should be anticipated, with the use of precise clauses such as notice periods, chain termination of contracts, reciprocal restitution and reversibility. In September 2025, the *Autorité de Régulation des Communications Électroniques, des Postes et de la Distribution de la Presse* (ARCEP) published recommendations on the implementation of SREN's interoperability requirements.

The Data Act, which became partly enforceable in September 2025, also brought significant changes to data access, portability and interoperability obligations. It prohibits unjustified fees for data transfer and requires cloud service providers to provide automated switching tools. It also sets strong requirements around the contractual allocation of liability and around the use of non-personal data generated by cloud-hosted products and services. These obligations apply directly in France and complement existing consumer and security obligations under national law.

In March 2022, the National Cybersecurity Agency for France (ANSSI) published version 3.2 of its certification framework for cloud service providers (SecNumCloud), to promote a protective digital environment in line with technical developments. The SecNumCloud identifies trusted cloud services and gives them a label that confirms they comply with the security and regulatory standards set out in the framework. In particular, the framework ensures that the cloud service provider and the respective data that they process are subject to European laws, in order not to undermine the level of protection provided by them. This framework continues to serve as the de facto standard for "trusted cloud" services.

Cybersecurity Implications

The NIS1 and NIS2 Directives apply to cloud services and aim to strengthen the security of networks and information systems.

NIS1 established security standards for Operators of Essential Services and Digital Service Providers, including cloud service providers, while enhancing co-operation among EU member states.

Building on NIS1, NIS2 was adopted in 2022 and expands its scope to cover more sectors and entities, addressing sophisticated cyber threats and formalising the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe). It introduces stricter cybersecurity requirements, requiring cloud service providers to implement enhanced risk management measures, adopt state-of-the-art cybersecurity practices, and ensure supply chain security. Significant security incidents must be reported within 24 hours, with follow-up reports submitted within 72 hours.

As of 2025, the transposition of NIS2 in France is underway but not yet fully completed. A draft law was adopted by the French Senate in March 2025 and is now proceeding through the legislative process. Certain obligations and compliance mechanisms remain uncertain until the implementing decrees are published.

In France, compliance also involves the SecNumCloud certification mentioned above, and participating in the European cloud certification scheme (EUCS), although the final contours of EUCS are still evolving.

The banking industry is subject to specific provisions regarding cloud computing. On 25 February 2019, the European Banking Authority (EBA) adopted new guidelines on outsourcing, which are still applicable, and include specific provisions regarding the following, for instance:

- the protection of confidentiality and personal or sensitive information; and
- the need to comply with all legal requirements relating to the protection of personal data, banking secrecy or confidentiality obligations concerning customer data.

The French supervisory authority for banks and insurance (the Prudential Supervision and Resolution Authority – ACPR) has published a notice to ensure that these guidelines are followed in France.

In accordance with NIS2 and these EBA guidelines, DORA entered into force on 17 January 2025. It creates a stricter regulatory framework than NIS2 for financial entities, which will have to ensure that they can withstand, respond to and recover from any serious operational disruption linked to information and communication technologies.

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

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

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

The 2022 version of the SecNumCloud also provides guarantees on data protection against non-EU legislation. The design of the data protection regulations is compliant with the requirements of the Schrems II ECJ ruling. CNIL even recommends the use of this stand-

ard for all data controllers who want to guarantee a high level of data protection.

To rebalance competition between the various players and strengthen the control of personal data by the data subjects, the DMA prohibits gatekeepers from engaging in certain practices without obtaining the end users' consent, including:

- combining personal data from the relevant core platform service with personal data from other services of the gatekeeper;
- cross-using personal data from the relevant core platform service in other services provided separately by the gatekeeper; and
- signing in end users to other services of the gatekeeper in order to combine personal data.

The DMA is also intended to regulate the access and use of the data provided or generated by core platform services, and to enhance the transparency obligations related to profiling practices.

To encourage internet users to be aware of the realities of risks on the sites they consult, the French Law of 3 March 2022 introduced a cyberscore. Effective since October 2023, websites must display a cybersecurity rating indicating their level of security and data-hosting safeguards. To obtain this cyberscore, companies must carry out audits with providers qualified by ANSSI.

Finally, the Cyber Resilience Act (CRA) is a new EU regulation that came into force on 10 December 2024 and aims to strengthen the cybersecurity of products with digital elements (both hardware and software). The CRA imposes obligations on manufacturers, importers, distributors and software publishers to:

- design products according to "security-by-design" and "security-by-default" principles;
- conduct risk assessments;
- document compliance;
- maintain security updates throughout the product life cycle; and
- remediate vulnerabilities without undue delay.

Because of its scope, not all cloud services are necessarily covered by the CRA; many typical cloud-only set-ups might remain entirely outside the CRA's obligations.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

AI Act

The AI Act was adopted on 21 May 2024 and aims to regulate the use of AI, ensuring it is safe, ethical and trustworthy. The European Artificial Intelligence Office was established to support its implementation.

The AI Act uses a risk-based approach, classifying AI systems into four categories.

- Unacceptable risk systems: banned due to harm to safety, fundamental rights or human dignity.
- High-risk systems: strictly regulated, requiring high standards for data quality, transparency, accountability and human oversight.
- Limited risk systems: subject to strict transparency rules.
- Minimal or no risk systems: not subject to regulation.

The AI Act entered into force on 1 August 2024. EU member states were required to identify the authorities and bodies responsible for protecting fundamental rights by 2 November 2024; in France, the designated authorities are DGCCRF, CNIL and the *Défenseur des droits*. Certain provisions of the Act became applicable on 2 February 2025, including the definitions of AI systems, governance obligations, and a list of AI uses deemed to pose unacceptable risks.

The next key phase occurred on 2 August 2025, when several critical provisions of the AI Act became enforceable, including the governance framework involving the AI Office, national authorities and the scientific panel. On the same date, the sanctions regime became operational, and general-purpose AI models placed on the market from 2 August 2025 were required to comply immediately, whereas models

already on the market before that date were given until 2 August 2027 to achieve compliance.

The AI Act will be fully applicable as of 2 August 2026. Non-compliance can result in significant fines of up to EUR35 million or 7% of annual turnover.

In November 2025, the European Commission also addressed AI within its broader Digital Omnibus simplification agenda (see **1.1 Legal Framework**). While the AI Act remains the cornerstone of the EU's risk-based framework for regulating artificial intelligence, the Digital Omnibus proposes targeted technical adjustments aimed at facilitating its practical implementation. In particular, the proposal seeks to better align the timing and scope of certain obligations with the availability of harmonised standards, guidance and conformity assessment tools, in order to reduce legal uncertainty for deployers and providers of AI systems.

The Commission's approach focuses on easing compliance for low-risk and smaller market players, including SMEs and small mid-caps, without weakening safeguards applicable to high-risk AI use cases. By clarifying interfaces between the AI Act and related digital legislation, and by streamlining reporting and administrative requirements, the Digital Omnibus aims to ensure that the EU's AI framework is both enforceable and innovation-friendly, supporting the uptake of trustworthy AI while preserving a high level of protection for fundamental rights and public interests.

Deepfakes

The SREN Law incorporates measures in the penal code to regulate deepfakes:

- Article 228-8 criminalises the use of deepfakes for disinformation, including private sharing, emphasising the need for "communication of content" for legal action; and
- Article 226-8-1 targets pornographic deepfakes, penalising their creation and distribution without consent, aiming to combat sexism and exploitation.

Draft legislation is under discussion to mandate AI-generated content labelling more broadly on social networks.

At the European level, the DSA requires online platforms to remove illegal content, including deepfakes, quickly after it has been reported. Platforms must put effective mechanisms in place to enable users and authorities to report such content in order to facilitate its removal.

Pursuant to Article 50 of the AI Act, deployers of an AI system that generates or manipulates images, audio or video content to create deepfakes must disclose that the content has been artificially generated or manipulated. This requirement does not apply when the use is legally authorised for the detection, prevention, investigation or prosecution of criminal offences. When the content is part of an evidently artistic, creative, satirical, fictional or similar work or programme, the transparency obligation is limited to appropriately disclosing the existence of such generated or manipulated content in a way that does not interfere with the display or enjoyment of the work.

Autonomous Vehicles

France has established an advanced regulatory framework to support the development of autonomous vehicles, emphasising safety, gradual adoption and public acceptance. According to Article R. 311-1 of the French Highway Code, autonomous vehicles are categorised into three levels of automation: partially, highly or fully automated. A French decree issued in July 2022 authorises the use of vehicles with driver delegation corresponding to Level 3, which means the car can operate autonomously under specific conditions.

The PACTE Law (2019) and the Mobility Orientation Law (2019) enable experimentation and regulatory adaptation for autonomous vehicles by providing a legal framework that supports technological innovation and the deployment of autonomous driving solutions. These laws facilitate the testing of self-driving vehicles on public roads under controlled conditions, ensuring safety while encouraging advancements in mobility technologies. They also allow for the gradual integration of autonomous vehicles into the transport

system by adapting existing regulations to accommodate new mobility models.

Data Protection

Big data projects must consider users' rights granted by GDPR, especially regarding purpose restriction and prior information, as users may not have been informed of unforeseen processing purposes when the data was collected.

In April 2024, CNIL released practical guides to offer clear recommendations for developing AI systems and creating databases for AI training involving personal data. These guides focus solely on the development phase, not deployment, and are limited to data processing under GDPR. They are designed to assist professionals with both legal and technical backgrounds, including data protection officers, legal professionals and those with or without specific AI expertise.

In 2025, CNIL expanded this framework by publishing updated recommendations confirming that AI models trained on personal data may fall under GDPR due to their capacity to memorise such data. CNIL now requires developers to document how they determine whether GDPR applies, to justify the legal basis used (including the possible but strictly regulated use of "legitimate interest"), and to implement robust filtering, data minimisation and security measures throughout the training pipeline. CNIL is also preparing additional guidance to clarify the distribution of responsibilities among actors across the AI value chain and to provide sector-specific recommendations.

The European Commission's draft code of practice aims to guide providers of general-purpose AI models in their compliance with EU legislation. European Data Protection Supervisor (EDPS) Opinion 2024/48 criticises the lack of detail on transparency, data protection and systemic risk management. The EDPS recommends rigorous monitoring to ensure the protection of fundamental rights in the face of technological developments.

In 2023, the Council of the European Union adopted the Data Act, laying down harmonised rules for fair access to data and fair use thereof. It specifies who can access and use data generated within the EU in all economic sectors. It aims to:

- ensure fairness in the distribution of the value generated by data between players in the digital environment;
- stimulate the development of a competitive data market;
- open up opportunities for data-driven innovation; and
- make data more accessible to all.

The new regulation became applicable in September 2025. However, the requirements for simplified access to data for new products will only apply to connected products and related services placed on the market 32 months after the entry into force.

Responsibility/Liability

The EU has adopted the Product Liability Directive, which is to be implemented by the end of 2026. The directive modernises EU civil liability rules to address the digital environment, explicitly extending the notion of "product" to include software and AI systems. It deals with claims for harm caused by AI systems or the use of AI, adapting non-contractual civil liability rules to artificial intelligence. Under this directive, manufacturers or providers of defective AI systems that cause physical harm, property damage or data loss to individuals are liable without fault.

The directive complements the AI Act by creating a legal framework for civil liability related to AI systems, ensuring consumer trust and legal clarity for businesses. It aims to introduce a harmonised liability regime across the EU, and ensures claimants have effective avenues for compensation comparable to non-AI-related damage cases.

Intellectual Property

Many elements of AI systems may be protected by intellectual property rights (or assimilated), including content, algorithms under certain conditions, computer programs, models, robots, databases, etc. It is necessary to consider the type of protection appropriate for each element (patent, copyright if original and specific form for content, designs for robots, etc).

The protection of creations by AI is of particular interest. It is obvious that the intellectual property protection system is based on human creativity, which will render the works of AI difficult to protect. No related case law is evident in France but, in the *DABUS* case, the European Patent Office denied patent protection of an invention by AI on the grounds that no human was named as inventor.

There are workaround solutions, such as naming a physical person as inventor or author, but this does not fully solve the issue, and a legislative intervention seems necessary on this topic.

4. Internet of Things

4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Liability

Under French law, there is no specific legal framework applicable to liability for connected objects or connected robots; general liability rules will apply. A distinction must be made between contractual and extra-contractual liability. In addition, several liability regimes may apply, in particular defective products or the custody of the object.

For instance, if the manufacturer/producer of the connected objects does not respect its pre-contractual information as referred to in Article 1112-1 of the French Civil Code and Article L 111-1 et seq of the French Consumer Code regarding the substantial characteristics of connected objects, they could be held accountable for that omission. However, these regimes do not fully meet the challenges related to connected objects and artificial intelligence in general. It seems necessary either to adapt the existing regimes or to create a specifically adapted regime

For now, the forthcoming EU Product Liability Directive – which explicitly extends product liability rules to software and digital components, including connected objects – represents the most significant structural development, but it will not apply in France until its transposition deadline of December 2026. Until then, French courts remain bound by existing general regimes.

In 2024, France updated its drone regulations to align with European directives, introducing new classifications and stricter requirements. These changes aim to enhance safety and confidentiality while expanding drone usage for leisure and professional purposes. The regulations cover flight zones, training certificates and drone flight scenarios, providing a comprehensive framework for drone operations.

Data Protection

GDPR and standard data protection provisions also extend to the internet of things (IoT). Identifying data controllers and processors in IoT projects is challenging due to the interoperability and constant data exchange of connected devices. Beyond GDPR and French law, CNIL recommends conducting Data Protection Impact Assessments for IoT projects, to clarify processing purposes and legitimate methods. CNIL also provides guidelines to help data subjects using IoT devices protect themselves from associated risks.

Consent

In IoT devices, it is not always possible to request consent directly. Therefore, in order to implement GDPR requirements for consent, IoT manufacturers must find other ways to collect it.

Cybersecurity

The Cyber Resilience Act establishes mandatory cybersecurity standards for digital products and services within the EU, aiming to protect consumers and businesses from cybersecurity risks. Its main provisions will become enforceable from 11 December 2027. It mitigates risks associated with the increasing prevalence of connected devices and digital services, and ensures a harmonised cybersecurity framework that supports innovation while safeguarding consumers.

4.2 Compliance and Governance

The principal compliance challenge is dealing with the multiplicity of European regulations in the same industries (particularly TMT), as mentioned in **4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection**. There are also sector-specific regulations that apply to industries such as healthcare, environment and energy.

Companies must implement internal regulations, such as policies and codes of conduct, to ensure compliance with various obligations. They should develop processes to inform employees of their obligations and conduct regular audits for compliance. External information notices must be provided to potential clients, detailing mandatory consumer regulations like terms and conditions.

In 2021, ANSSI published a guide to IoT security recommendations, facilitating security analysis based on probable attack scenarios and offering recommendations to mitigate identified risks. In May 2025, ANSSI published a new document geared toward the industrial IoT context. It proposes a security architecture model (secure interconnection gateways, risk analysis, segmentation) to mitigate the elevated risks associated with IoT systems.

4.3 Data Sharing

Sharing the personal data of European residents with countries lacking an EU adequacy decision is generally not permitted, unless appropriate safeguards, as outlined in Article 46 of GDPR, are in place. These include binding corporate rules, standard contractual clauses, an approved code of conduct or an approved certification mechanism.

The Data Act, which entered into force on 12 September 2025, promotes fair access to and fair use of data across the EU, complementing the DGA. While the DGA establishes frameworks for voluntary data sharing, the Data Act mandates entities to make data accessible to other parties.

The DGA allows companies to reuse data held by public sector bodies, including "protected data", provided it is anonymised or does not infringe business secrecy or copyright. The Data Act introduces a new obligation to share data obtained through IoT devices and connected products with the user and third parties at the user's request. This means data previously exclusive to the IoT provider or manufacturer must be shared upon request.

These obligations also include providing clear pre-contractual information: before sale, users must be informed of the type of data generated, how it can be accessed or exported, where it is stored, and the possibilities for sharing.

The Data Act establishes rules for users, data holders and third parties regarding data-sharing requirements, applicable to those processing personal data. Its territorial scope is similar to GDPR, applying regardless of the location of manufacturers, providers and data holders. Non-EU-based manufacturers and providers must comply if their connected products or services are marketed within the EU, and data holders must follow the regulations if they make data available to EU recipients.

These regulations have a broad scope, potentially affecting any company that processes data. However, not all IoT data falls under the sharing obligation. Manufacturers or service providers can refuse to share specific data identified as trade secrets, but only in exceptional circumstances with a high likelihood of serious economic harm from disclosure. Such refusals must be based on objective criteria, substantiated in writing, and notified to the national competent authority.

The French regulation does not impose higher standards than the EU approach.

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

Audiovisual services traditionally cover TV, radio and on-demand audiovisual media services (AVMS). AVMS commonly include services such as video on demand (VOD), catch-up television and audio podcasts.

Audiovisual services are subject to Law 86-1067 of 30 September 1986 on the freedom of communication, and are regulated by ARCOM, an independent administrative authority (formerly CSA).

The requirements and associated procedures for providing an audiovisual service depend on the nature of the service. Procedurally, operators of on-demand audiovisual services must declare their service to ARCOM. The requirements for providing these ser-

vices vary based on the service type but include general obligations such as respecting individual dignity and privacy rights, and protecting minors. In addition, programmes must promote the French language, uphold public order and avoid inciting hatred or violence. There are additional cultural obligations for VOD and subscription-based streaming services, including mandatory contributions to the production of French works, based on catalogue size or revenue.

TV and Radio Providers

ARCOM must grant authorisation to TV and radio providers using the network of assigned frequencies before they can provide their services. Private providers have to participate in a call for applications and be selected by ARCOM in order to be provided with an assigned frequency.

The provider must sign an agreement with ARCOM, outlining specific service rules based on coverage, advertising market share and competition compliance. ARCOM's authorisation can last up to ten years for TV services and five years for radio services, with the possibility of renewal up to two times without a new application process.

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

Finally, distributors of audiovisual services not using assigned frequencies must make a prior declaration before distribution. This declaration should include:

- the distributor's corporate form, name and head office address;
- a list of services;
- the service offer structure; and
- a letter of intent to conclude a distribution agreement for paid television services.

AVMS Providers

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

Companies With Online Video Channels With User-Generated Content

The revised Audiovisual Media Services Directive (AMSD) extends certain audiovisual rules to video-sharing services, such as YouTube. It was transposed in France by an ordinance dated 21 December 2020.

To be considered as a video-sharing service, the service must meet the following conditions:

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

Video-sharing services have specific obligations. Besides ensuring compliance with general content rules, ARCOM has additional powers, such as resolving disputes between users and providers and ensuring providers meet transparency obligations. ARCOM's powers have been reinforced in practice through increased co-ordination with the DSA framework and the extension of ARCOM's mandate to accessibility obligations applicable to audiovisual and online video services as of June 2025.

ARCOM's powers are limited to video-sharing platforms established in France, due to the country of origin principle. However, platforms from other EU states may still need to contribute to French cinematographic and audiovisual content production, despite being regulated by their home country. The classification of online video channels with user-generated content as AVMS must be assessed individually.

In this respect, the ECJ qualified the catalogue of videos proposed by an online press website with content

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

On 30 January 2024, in case C-255/21, the ECJ clarified that the term "messages broadcast by the television broadcaster regarding its own programmes" does not cover promotional messages for a radio station belonging to the same group as the television broadcaster, unless the programmes being promoted are distinct "audiovisual media services" and the television broadcaster assumes "editorial responsibility" for them.

In France, ARCOM has classified certain online video offerings as AVMS, including:

- radio station websites with video catalogues (CSA, 29 May 2013);
- company-operated YouTube channels (CSA, 9 November 2016); and
- YouTube channels of TV stations (CSA, 3 July 2019).

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

European Media Freedom Act

Since the adoption of the European Media Freedom Act (EMFA) in May 2024 and its full application across the EU as of 8 August 2025, the regulatory environment for media and audiovisual services has evolved substantially. The EMFA protects media pluralism and independence in the EU, complementing the AMSD, the DSA and the DMA. The EMFA is part of the EU's project to promote participation in democracy, to address fake news and disinformation and to support media freedom and pluralism. It shall ensure an easy cross-border operation of media in the EU internal market. Thus, the focus of this legislation lies on the independence (also in regard to stable funding) and transparency of media ownership.

The EMFA also regulates the protection of the independence of editors and the disclosure of conflicts. Furthermore, it created a new independent European Board for Media Services, which began operating in February 2025, with the goal of ensuring the consistent application of EU media law. Composed of representatives from national media regulators, the European Board for Media Services covers all media sectors, from audiovisual services to online platforms. Acting as a guardian of democracy, it supports the European Commission, promotes co-operation among regulators, and protects fundamental rights such as freedom of expression and media pluralism. The Media Board's priorities include:

- the promotion of European works;
- protection of minors;
- media literacy; and
- tackling disinformation.

Through independent, evidence-based advice, structured cross-border co-operation and stakeholder engagement, it contributes to a free, pluralistic, trustworthy and competitive media environment across the EU. The Media Board has already adopted its Rules of Procedure and work programme, and has begun issuing opinions on transactions and regulations.

Further measures the EMFA intends to implement include safeguards against espionage software, transparent state advertising and the new user right to customise their media offering. These new rules better protect editorial independence, media pluralism and journalistic sources, ensure transparency and fairness, and bring better co-operation of media authorities through the new European Board for Media Services.

For France and other member states, this means that the classification of online video services must now be considered not only under AMSD, but in the broader context of EMFA's systemic safeguards for editorial independence, media pluralism and transparency.

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

Local telecommunication rules traditionally apply to electronic communication networks (ECNs) and electronic communication services (ECSs) (Article L 32 of the French Postal and Electronic Communications Code, or CPCE). At an EU level, however, Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC Directive) has modified and updated the applicable framework. In France, the EECC Directive was transposed by Ordinance No 2021-650 of 26 May 2021.

The EECC Directive expands the definition of ECSs by including so-called "interpersonal communications services", defined as services normally provided for remuneration that enable 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 its recipients. Accordingly, and subject to the transposition ordinance of the EECC Directive, voice-over internet protocol (VoIP) and instant messaging fall under the new scope of the telecommunications rules. This was confirmed by Recital 15 of the EECC Directive, and is in line with the ECJ's previous ruling, which considered that SkypeOut offering a VoIP service constitutes an ECS (ECJ, 5 June 2019, C-142/18).The qualification of radio-frequency identification (RFID) as ECS remains unclear, as it is not specifically covered by the new scope of the telecommunications rules. However, ARCOM and ARCEP consider RFID technology as radio-electric installations, which can be used on certain frequencies only and with defined technical settings.

Furthermore, ARCEP proposed modifications to the national numbering plan in 2025, notably to restrict the use of short, highly surcharged numbers as identifiers of calling parties, in order to combat fraudulent practices and protect consumers.

Applicable Requirements

The declaratory regime for ECSs was abolished in 2021. The provision and establishment of ECNs are now unrestricted, but they must comply with the obligation to notify security incidents to ARCEP, net neutrality, interoperability of services, etc. Since 2024-2025, these security notification obligations have been reinforced in practice by the increasing convergence between telecoms regulation and cybersecurity regulation, notably in light of the application of the NIS2 Directive, which strengthens incident reporting and risk management duties for operators of essential and important digital services.

In France, every operator must pay an administrative tax under the conditions provided by the finance law. They must also pay an additional fee if they use a specific frequency or provide a specific numbering. As noted above, ARCEP has announced forthcoming reforms of the national numbering framework aimed at combatting large-scale fraud and abusive uses of premium rate and short numbers.

Providers of instant messaging are subject to stricter data protection law requirements regarding messages under Directive 2002/58 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive). The ePrivacy Directive notably obliges member states to ensure the confidentiality of communications and the related traffic data by means of an ECN or ECS through national legislation. For example, traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when no longer needed, pursuant to Article 6 of the ePrivacy Directive.

6.2 Net Neutrality Regulations

In France, net neutrality is governed by both EU regulations and national laws. The EU's Net Neutrality Regulation 2015 prohibits internet service providers (ISPs) from blocking, throttling or prioritising content, except in specific cases like network security or legal compliance. France has integrated these regulations into its national framework, with ARCEP overseeing enforcement.

A July 2025 judgment from the Court of Justice of the European Union (Case C-367/24) further confirmed

that "zero-rated" or tariff-bonus plans that impose traffic management restrictions (eg, reduced speed after a threshold) still violate the Net Neutrality Regulation when they discriminate against certain traffic categories.

Net neutrality continues to have a direct impact on TMT operators by requiring them to treat all internet traffic equally, preventing them from offering premium "fast lane" services for additional fees. This ensures fair competition, as ISPs cannot prioritise services like Netflix over smaller video platforms, but it also removes a potential revenue source for ISPs.

6.3 Emerging Technologies

Emerging technologies like 5G, IoT and AI are reshaping the legal landscape of TMT in France, requiring stringent regulatory compliance.

ARCEP oversees 5G deployment, while GDPR mandates strong data privacy and security measures. Intellectual property protection and clear liability contracts are crucial due to the complexities introduced by AI and IoT. Cybersecurity laws protect critical infrastructure, and competition laws ensure fair business practices. Consumer protection laws demand transparency and honesty, and environmental regulations like REACH aim to reduce the technological impact on the environment.

The EU AI Act entered into force on 1 August 2024, with application in stages:

- prohibited AI practices and AI literacy obligations applied from 2 February 2025; and
- rules for general-purpose AI (GPAI) models and governance became applicable on 2 August 2025.

This directly affects TMT operators using AI for network optimisation, traffic management, fraud detection, content moderation or age verification, who must:

- classify their AI systems (prohibited/high-risk/limited-risk/GPAI);
- implement appropriate risk assessments, data-governance measures and human oversight; and
- ensure that fundamental rights impact is considered.

Companies must stay updated on legal changes, ensuring compliance across these areas while considering ethical implications.

7. Challenges With Technology Agreements

7.1 Legal Framework Challenges

Parties' Level of Expertise

Issues in IT service agreements often stem from late or incorrect fulfilment of contractual obligations, making the allocation of responsibilities crucial. Customers are often unfamiliar with the technology and rely on the service provider's obligation to advise and inform during both negotiation (Article 1112-1 of the Civil Code) and performance (Article 1104 of the Civil Code). This includes informing about the customer's needs and warning against unlawful or risky expectations, even refusing the contract if necessary. Customers must also collaborate with the provider.

Since 2016, French law protects against unfair clauses in pre-formulated standard agreements, including B2B contracts. If these terms create a significant imbalance, they may be deemed unfair and unenforceable, potentially invalidating the entire agreement if the clause is essential.

Liability of the Service Provider and Service Level

Providers may try to exclude or limit their liability by excluding indirect damages; such exclusion is authorised under French law, although providers will try to have a broad definition of "indirect damages" to include loss of data, loss of clients, breach of data privacy, etc. Unless these liability clauses deny the essential obligation of the provider, in which case they are prohibited, liability clauses (including the amount of the liability cap, if any) are often one of the key topics of the parties' service agreement negotiations.

However, because the parties may not have the same bargaining power, especially when customers are consumers or businesses with no IT expertise or when the product is complex or customised, those clauses may be more easily challenged and unenforceable. To better identify providers' contractual breach, customers would be advised to detail their needs as much as

possible and to set out clear specifications in terms of performance (eg, through a service level agreement) or in terms of timeframe (eg, including provision for liquidated damages).

To assess whether the service provider has complied with its obligations under IT service agreements, in particular its obligation to reach a specific result, the parties usually agree on service levels and a quality assurance plan. This implies the definition of key performance indicators and the payment of penalties if those indicators are not met. In June 2022, the French Supreme Court (1-6-2022 No 20-19.476) reiterated the importance of contractually stipulating the service provider's obligations in IT contracts. On this occasion, it ruled that a software deployment contract must be terminated to the detriment of the service provider if, being bound by an obligation of result, the latter was unable to resolve the blocking and recurring anomalies complained of by the customer.

Specific IT Service Agreements

In software licence agreements, a key issue is whether the licensee can repair or correct bugs themselves or through a third party, or if only the licensor can perform maintenance. French law typically allows licensors to retain the right to correct bugs, posing challenges for licensees without a maintenance agreement. When a licensee has both a licence and a maintenance agreement with the same provider, it is important to clarify whether the termination of one affects the other. Transitioning to new service providers requires a reversibility clause for a smooth transition. The Court of Justice of the European Union recently ruled that decompilation for bug fixing is lawful under certain conditions: necessity, lack of specific contractual provisions, and sole purpose of error correction (ECJ, 6 October 2021, C-13/20). Contracts should clearly regulate decompilation and maintenance terms.

Regulated Industries

A major challenge in technology agreements arises when providers contract with highly regulated industries. In France, sectors such as banking, insurance, healthcare, energy and critical infrastructure are subject to sector-specific supervision that directly shapes the content and negotiation of technology contracts.

- The banking and insurance sectors, supervised by the ACPR and the AMF, impose extensive contractual requirements on their IT, cloud and telecoms providers, including strict outsourcing rules, audit and access rights, data resilience obligations, and exit strategies under DORA, applicable since 2025.
- In the healthcare sector, technology agreements involving health data must comply with the certification regime for health data hosting and heightened confidentiality and security requirements under the supervision of CNIL.
- Telecoms, cloud and infrastructure providers are subject to sector-specific oversight by ARCEP and to reinforced cybersecurity obligations under the NIS2 framework where they qualify as "essential" or "important" entities.

These cumulative regulatory constraints can translate, at a contractual level, into heavier liability regimes, stricter service levels, mandatory cybersecurity clauses, enhanced audit rights and data localisation constraints, which can significantly complicate negotiations compared with technology agreements concluded in non-regulated sectors.

7.2 Service Agreements and Interconnection Agreements

A telecommunications service agreement should clearly define the parties, scope of services, pricing and payment terms. It should include SLAs with guaranteed performance and remedies for non-compliance, and should specify duration, renewal and termination conditions. Key provisions must address data privacy, security, liability limits, dispute resolution and force majeure. Equipment ownership and maintenance responsibilities, confidentiality clauses, legal compliance and signatures for legal enforceability are essential.

Companies should use competitive bidding to negotiate flexible pricing and ensure clear termination terms to minimise penalties. Favourable equipment terms should be sought, such as outright ownership or low-cost leasing. Engaging legal and technical experts ensures the agreement meets operational and regulatory requirements, and understanding their bargaining position aids successful negotiation.

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/ Digital Identity Schemes

Electronic signatures are governed by eIDAS and the French Civil Code.

Three categories of electronic signatures exist pursuant to eIDAS:

- advanced electronic signatures are those that meet the requirements set out in Article 26 of eIDAS;
- qualified electronic signatures are advanced electronic signatures that are created by a qualified electronic signature creation device and based on a qualified certificate for electronic signatures; and
- simple electronic signatures are those that are neither qualified nor advanced.

Article 25 (1) of eIDAS specifies that electronic signatures shall not be denied legal effect and admissibility as evidence in legal proceedings solely due to their electronic form or because they do not meet the requirements for qualified electronic signatures. Article 25 (2) of eIDAS indicates that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

Article 1367 of the French Civil Code indicates that an electronic signature must use a reliable identification process, guaranteeing its link with the document to which it is attached. Article 1 of Decree No 2017-1416 of 28 September 2017 further specifies that qualified electronic signatures under eIDAS are presumed to be reliable.

Further guidance on electronic signatures is available on the ANSSI website.

A major recent development is the entry into force of Regulation (EU) 2024/1183 on 20 May 2024, known as "eIDAS 2.0" or the European Digital Identity Wallet (EUDI-Wallet) framework. This new framework expands the scope of regulated trust services beyond traditional electronic signatures: it enshrines a universal, interoperable digital identity wallet recognised across the EU and supports a broader array of digital trust services, such as identity verification.

Article L 102 of the CPCE establishes the framework for electronic identification of online services in France and the presumption of reliability of electronic means of identification, and the procedures for their certification.

The security requirements applicable to these electronic means of identification are based on the provisions of eIDAS and the associated Implementing Regulation No 2015/1502. Decree No 2022-1004 of 15 July 2022 sets out the conditions for the certification by ANSSI of electronic identification means, as well as the specifications for establishing the presumption of reliability of these means. Further guidance on electronic identification is available on the ANSSI website.

9. Gaming Industry

9.1 Regulations

France's regulatory framework for the gaming industry emphasises consumer protection, copyright and age verification. A significant 2022 ruling from the Paris Court of Appeal requires game platforms targeting French consumers to comply with French regulations, emphasising fair and transparent terms. On 23 October 2024, the French Supreme Court ruled that digital games are complex works rather than simple computer programs, opposing digital game resale.

French regulations authorise horse betting, sports betting and online poker, but casino games and lotteries remain monopolised by *La Française des Jeux* (La FDJ). Influencer marketing in gaming is restricted to platforms that can exclude minors, under Law No 2023-451.

In 2024, the French legislature adopted the SREN Law, which for the first time introduces a regulated, experimental regime for digital games offering monetisable digital items (JONUM). As of 2025, operators of such games must declare their activity to the gambling regulator (*Autorité nationale des jeux*, or ANJ), implement robust age verification and comply with AML obligations if applicable; they may be subject to inspection and sanction if they fail to comply. This new regime does not automatically legalise all online casino games but creates a distinct legal category under

which some Web3/play-to-earn games may operate, albeit subject to tight regulatory scrutiny and pending implementing decrees.

The industry faces challenges in age verification, IP protection and compliance with consumer protection laws and GDPR.

9.2 Regulatory Bodies

The ANJ was created in 2020 as an independent administrative authority responsible for approving online gaming and betting operators. It has enhanced powers, the authority to sanction non-compliant operators, and a mandate to combat excessive gambling in casinos. In 2025, the ANJ issued three financial penalties against online gaming operators, ranging from EUR5,000 to EUR800,000.

ARCOM also acts as France's Digital Services Coordinator under the DSA. This significantly strengthens ARCOM's role in policing gaming-related advertising, sponsored content and influencer behaviour, especially where minors may be exposed. It can issue warnings or sanctions for non-compliance with digital content laws.

DGCCRF ensures fair commercial practices, focusing on consumer protection, and regulates practices around loot boxes, microtransactions and advertising transparency.

At the European level, the EU Commission ensures responsible operation of the video game industry through the DSA, GDPR and the Unfair Commercial Practices Directive, while fostering innovation and cultural impact. The PEGI rating system provides age ratings and content warnings for consumers and parents.

The French Competition Authority also plays a significant role, having fined Sony group companies EUR13.5 million in 2023 for abuses of dominant position in the market for PlayStation 4 video game controllers.

9.3 Intellectual Property

Game developers in France face several IP challenges, including ensuring originality for copyright protection, securing trade marks amidst conflicts, and managing third-party content licences. Patents for game technology are hard to secure, and enforcing IP rights against online piracy is challenging. Clear contracts are crucial to avoid IP ownership disputes with employees or contractors.

For digital and virtual assets, key considerations include ensuring originality, defining ownership and managing licensing terms to prevent unauthorised use. Creators must guard against unauthorised copying and potential infringement on shareable platforms.

Trade mark laws protect brand names, logos and distinctive marks in virtual goods and services, preventing consumer confusion and safeguarding brand identity. User-generated content complicates IP rights, as users retain copyright, but platforms may claim usage rights through terms of service, leading to ownership and commercial use disputes.

Meanwhile, the EU's updated approach to virtual worlds and AI-generated content underscores the continuing uncertainty over authorship, originality and exploitation rights when works combine human and machine-generated elements.

10. Social Media

10.1 Laws and Regulations for Social Media

The Law of 7 July 2023 aimed to regulate access by minors under the age of 15 to social media platforms through a system of mandatory parental consent for account creation and retention, but never entered into force. In a letter dated 14 August 2023, the European Commission considered the law to be incompatible with EU law, in particular because of its overlap with the DSA in terms of content moderation obligations, the breach of the country-of-origin principle under Article 56 of the DSA (by asserting jurisdiction over providers established outside France), the violation of the EU standstill period, and the unjustified restriction on the freedom to provide information society services under Article 3 of the E-Commerce Directive. As a result, the law remained inoperative.

Nevertheless, new legislative proposals have been introduced in France in 2025 to regulate minors' access to social media. The *Conseil d'État* reviewed a draft bill aimed at protecting minors from the risks of social media use and drafted an opinion on 13 January 2026. The *Conseil* acknowledged documented scientific evidence of harms associated with excessive screen and social media use among children. It stressed that the bill should clearly define key terms such as "online platform" and "social network service", using definitions from EU digital law, to ensure legal clarity and respect for EU competencies. However, the *Conseil d'État* considers that, as it is, the proposed law does not strike a balanced reconciliation between the best interests of the child and the fundamental rights of those holding parental authority.

The placement of cookies and subsequent processing of data is governed by GDPR and the ePrivacy Directive, which mandates explicit and informed consent for non-essential cookies. Users must have the option to accept or refuse non-essential cookies on equal terms. In December 2023, CNIL fined Yahoo EMEA Limited EUR10 million for failing to respect the choice of internet users to refuse cookies on its "Yahoo.com" website and for not allowing users of its "Yahoo! Mail" messaging service to freely withdraw their consent to cookies. CNIL further intensified its enforcement action in September 2025, issuing additional sanctions against Shein and Google for failure to comply with cookie consent and withdrawal requirements.

Platforms must navigate whether/when to expeditiously remove illegal content under LCEN, the DSA and the SREN Law, as mentioned in **1.2 Key Challenges**, while balancing free speech and avoiding over-moderation. Intellectual property compliance involves managing copyright issues on user-generated content without implementing overly restrictive measures. Frequent data breaches necessitate GDPR-compliant responses, and transparency obligations under the DSA and GDPR pose legal and competitive challenges.

Since 1 January 2025, the French tax authorities have extended the scope of their efforts to combat fraud. Thanks to a new decree, tax officials, like customs officers, can collect and analyse public data published on social networks such as Facebook, Instagram and LinkedIn.

10.2 Regulatory and Compliance Issues

There is no one specific regulatory body for social media. CNIL is the authority responsible for ensuring the protection of personal data and privacy rights, while ARCOM regulates content moderation, hate speech and online safety, DGCCRF monitors consumer protection, and the European Commission is in charge of enforcing various European regulations.

CNIL can impose fines of up to 4% of global turnover for GDPR violations and mandate corrective measures. ARCOM can issue warnings, fines or sanctions for failing to remove illegal content within required deadlines. DGCCRF can conduct investigations, impose fines and enforce fair practices. The European Commission imposes penalties of up to 6% of global turnover under the DSA and up to 10% of global turnover under the DMA in cases of infringement.

On 27 June 2024, ARCOM, CNIL and DGCCRF signed a tripartite agreement to co-ordinate the implementation of the DSA. The agreement formalises co-operation commitments, notably in terms of sharing information on investigations and handling user complaints. It also provides a framework for the designation of trusted flaggers, whose selection is overseen by ARCOM with the advice of CNIL and DGCCRF.

On 31 December 2021, CNIL imposed a fine of EUR150 million on Google LLC and Google Ireland Limited for inadequate cookie policies. The committee also ordered the companies to ensure that users of google.fr and youtube.com in France could refuse cookies as easily as they could accept them, giving them three months to comply.

In 2022, ARCOM alleged that Twitter was not complying with its obligations to combat hate speech and illegal content online, identifying significant shortcomings in the moderation and removal of such content. Consequently, ARCOM issued a formal notice to Twitter.

The French tax authorities have initiated several tax adjustments against social networks.

11. Data Privacy and Cybersecurity

11.1 Data Privacy in Telecommunications

In France, telecom providers are subject to the general EU GDPR and the *Loi informatique et libertés* (French Data Protection Act), but also to sector-specific rules in the CPCE, particularly Article L34-1, which governs the processing and retention of traffic and location data for providers of publicly available electronic communications services. These provisions, read together with the ePrivacy regime, impose strict limits on retention periods and require data to be kept no longer than necessary for billing, network security or the investigation of serious offences. Telecom operators must also notify personal data breaches to CNIL.

In parallel, the NIS2 Directive treats many telecom and cloud operators as "essential" or "important" entities, requiring stricter cybersecurity, third-party risk management and incident reporting, with significant impact on network and data governance practices.

Telecom operators are also at the centre of lawful interception and data retention obligations, and are obliged under the CPCE to retain certain connection data for law enforcement purposes. Operators therefore operate at a tight intersection between mandatory co-operation with law enforcement and the duty to respect confidentiality of communications.

Third-party vendors and cloud service providers now play a central role in telecom data processing chains, which raises additional compliance requirements around processor due diligence, data processing agreements, shared security responsibilities and reversibility. In 2025, ARCEP issued recommendations on cloud interoperability and portability, which directly affects how telecommunication systems architect their infrastructure and contracts with cloud partners.

Overall, the main challenge for telecom companies in 2025 is to reconcile these overlapping regimes into a coherent compliance framework that still allows them to innovate in services and network technologies while preserving user trust.

11.2 Cybersecurity in Digital Media and Streaming Services

In France, digital media and streaming services sit at the crossroads of GDPR, the French Data Protection Act and the ePrivacy directive (for cookies/trackers on websites, apps, connected TVs), plus platform-specific duties under the DSA and emerging NIS2 cybersecurity rules. Their primary legal and operational challenges are:

- collecting valid, granular consent for tracking and personalised recommendations across devices;
- enforcing data minimisation on extremely rich usage logs (eg, viewing history, watch-time); and
- handling user rights (access, deletion, objection, portability) at scale in real time.

Online safety rules also bite directly on streaming: under France's SREN Law and ARCOM's age verification reference framework, adult content streaming sites must deploy privacy-preserving age verification, a regime upheld by the *Conseil d'État* in July 2025 and now extended to some EU-based sites. This has forced parts of the industry to temporarily block access in France and redesign identity and access control flows.

Overall, digital media and streaming providers must treat privacy and security as structural design constraints:

- consent, tracking and user rights tooling must be monitored;
- ad-tech and analytics integrations must be tightly governed; and
- cybersecurity/online safety obligations must be contractually pushed down their technology stack, while still preserving enough flexibility to innovate in personalisation and cross-device experiences.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com