Chambers AND PARTNERS

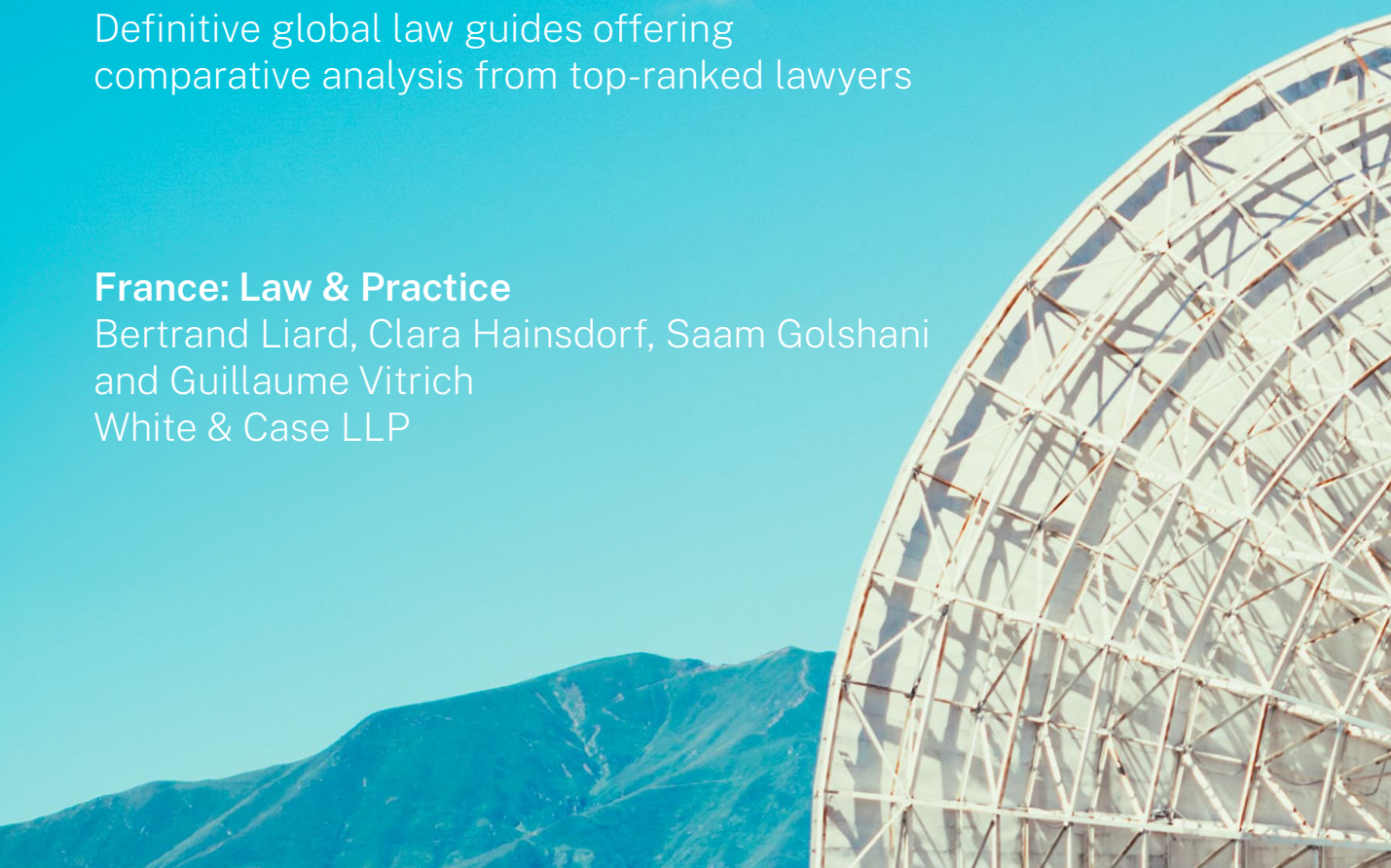
CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2024

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

France: Law & Practice

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



FRANCE

Law and Practice

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

Contents

1. Metaverse p.5
1.1 Laws and Regulation p.5

2. Digital Economy p.6
2.1 Key Challenges p.6

3. Cloud and Edge Computing p.7
3.1 Highly Regulated Industries and Data Protection p.7

4. Artificial Intelligence p.9
4.1 Liability, Data Protection, IP and Fundamental Rights p.9

5. Internet of Things p.12
5.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.12

6. Audio-Visual Media Services p.14
6.1 Requirements and Authorisation Procedures p.14

7. Telecommunications p.16
7.1 Scope of Regulation and Pre-marketing Requirements p.16

8. Challenges with Technology Agreements p.18
8.1 Legal Framework Challenges p.18

9. Trust Services and Digital Entities p.20
9.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.20

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

Authors

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

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

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

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

White & Case LLP

19, place Vendôme
75001
Paris
France

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

WHITE & CASE

1. Metaverse

1.1 Laws and Regulation

While there is no official definition for the metaverse and this is mostly a prospective subject, the notion is used to describe real-time online virtual worlds that are deeply immersive and often include 3D technologies and avatar representations of their users. The metaverse may also rely on other Web3 technologies such as cryptocurrencies and non-fungible tokens. It is sought to be used in a wide variety of areas such as gaming, arts, education, and professional and social activities. For the moment, the metaverse mostly raises challenges regarding data protection, intermediary services regulation and intellectual property.

The French Minister of Economy recently commissioned a report on the metaverse, which was published on 24 October 2022 and addresses some of the key legal considerations related to the metaverse.

Data Protection Implications

The metaverse is likely to raise personal data protection issues, as it will involve information relating to identified or identifiable individuals. Metaverse platforms that are either established in France or target data subjects in France will therefore have to comply with the General Data Protection Regulation (GDPR) and the French Data Protection Act of 1978 as amended.

The metaverse will generate an increase in personal data collection and subsequent data processing operations due, among other things, to virtual reality headsets and other biometric sensors used to render the user experience more immersive. This possibility will, however, have to be articulated with the data minimisation principle and the security obligation laid by Articles 5(1)(c) and 32 of the GDPR. Part of this personal data may also qualify as special category data under Article 9 of the GDPR and health data under the French Data Protection Act, resulting in the application of a more restrictive legal regime.

Data controllers will also have to find valid technical solutions to collect data subjects' freely given, specific, informed and unambiguous consent for processing operations that rely on such consent as a lawful basis.

Intermediary Services Regulation Implications

Metaverse platforms will likely qualify as intermediary services subject to the Confidence in the Digital Economy Act of 2004, the EU Digital Services Act and the EU Digital Market Act of 2022. Such platforms will therefore have specific obligations as well as a particular liability regime depending on their exact qualification under such laws and their average number of users.

Intellectual Property Implications

The metaverse is expected to display many elements that may be protected by intellectual property, such as copyright or trade marks; therefore, it will have to comply with the applicable intellectual property laws governing the permitted and prohibited uses of such elements.

On 30 September 2022, the French Higher Council for Literary and Artistic Property (*Conseil Supérieur de la Propriété Littéraire et Artistique* or CSPLA), an entity responsible for advising the Minister for Culture on intellectual property matters, published a report on the intellectual property implications of virtual reality and augmented reality. The CSPLA also recently announced the creation of a committee dedicated to the metaverse. Their report on the mat-

ter is expected to be published in July 2023 and firstly discussed in plenary session.

2. Digital Economy

2.1 Key Challenges

The rise of the digital economy has led to the adoption of numerous laws in France and the European Union in order to govern digital services, content regulation and digital markets.

Digital Services and Content Regulation

Digital services and content regulation are currently mostly ruled by the Confidence in the Digital Economy Act of 2004 (*Loi pour la confiance dans l'économie numérique*), which transposed the EU Directive on electronic commerce of 2000 and has been frequently amended since its coming into force. The Confidence in the Digital Economy Act provides the legal regime for hosting services, including their particular civil and criminal liability regime and their obligations regarding content regulation. The French Consumer Code lays down the obligations that are applicable to online platforms in their relations with consumers (eg, pre-contractual duty to inform).

The applicable regime is currently evolving due to the recent entry into force of the EU Digital Services Act (DSA) of 2022. The DSA establishes an EU-wide set of rules for intermediary services, including online platforms, which imposes new obligations and requirements regarding the content they host, transmit and make available to the public. In this regard, the DSA empowers regulators with broad investigative and enforcement powers to deal with non-compliance at the national and EU level. The DSA will progressively enter into application until 17 February 2024. However, since 25 August 2023, the DSA must be respected by online platforms and search engines with more than 45 million monthly active users ("very large online platforms" and "very large online search engines") in the European Union (EU).

Digital Markets Regulation

Digital markets are currently mostly regulated by general competition law (merger control and prohibition of anti-competitive practices). The EU Regulation on platform-to-business relations (the "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.

More recently, the Digital Markets Act (DMA) was adopted on 14 September 2022 to regulate certain very large online platforms (gatekeepers), which are important gateways for business users to reach end users. The designated gatekeepers under the DMA will be subject to a list of ex ante obligations and prohibitions.

On 6 July 2023, the European Commission published the list of seven companies that have identified themselves as "gatekeepers". Attributed to digital platforms capitalised to more than EUR75 billion on the stock market or with a turnover of more than EUR7.5 billion in Europe, the concerned platforms will then have to comply with the new DMA regulatory framework by 6 March 2024.

Digital Governance Act

Like the Data Act, the Digital Governanace Act (DGA) is part of the European Data Strategy, presented by the European Commission in February 2020. This strategy aims to develop a single data market by supporting responsible access,

sharing and reuse, in compliance with EU values and in particular the protection of personal data.

The DGA was adopted in May 2022 and has been applicable since 24 September 2023, with a compliance obligation for entities providing data intermediation services by 24 September 2025 at the latest. The text 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 the data. It includes a framework facilitating the reuse of certain categories of protected public sector data (confidential commercial information, intellectual property, personal data); 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; and develops a framework for the voluntary registration of entities that collect and process data provided for altruistic purposes.

3. Cloud and Edge Computing

3.1 Highly Regulated Industries and Data Protection

Cloud Computing

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

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

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 provides the service providers with a label that confirms that the service provider complies 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 must be subject to European laws in order not to undermine the level of protection by them.

After the opinion of the French Competition Authority on the potentially anti-competitive practices of 29 June 2023 concerning the cloud computing companies, the French Parliament adopted the bill “Secure and Regulate the Digital Space” on 17 October 2023. This law makes provision for the interoperability of cloud services, the prohibition of data transfer fees and the time limitation of cloud credits, in particular to align with the provisions of the Data Act.

Cybersecurity Implications

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

To obtain a certification pursuant to the SecNumCloud, the service providers must comply with the security standards set out in the frame. Since 2019, France has been engaged in the creation of the European certification scheme for Cloud providers (EUCS). The new version of the SecNumCloud is designed to ensure a very high level of certification and works in the future as a reference.

Data Protection Implications

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

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

The new version of the SecNumCloud also provides guarantees on data protection against non-EU legislation. Of particular importance is herein the incorporation of the aftermath of the Schrems II ruling of the European Court of Justice. The design of the data protection regulations are compliant with the requirements of the Schrems II ruling. The French data protection authority, the CNIL, even recommends the use of this standard for all data controllers who want to guarantee a high level of data protection.

With the aim of rebalancing competition between the various players and strengthening the control of personal data by the data subjects, the DMA prohibits access controllers for certain practices including the use of cross-linking of personal data from the various services provided by the access controller and the registration of end users to other services of the access controller in order to combine their data, unless the end users consent. The DMA is also intended to condition the access and use of the data provided or generated but also to strengthen the transparency obligations on profiling practices.

Additionally, in order to encourage internet users to know the realities of IT risks on the sites they consult, the French law of 3 March 2022 introduced a cyberscore. Effective since October 2023, the cyberscore will be displayed on web-

sites in order to warn the internet user of the security of the latter and the data hosted. To obtain this cyberscore, companies must carry out audits with providers qualified by the ANSSI.

Regulation in Specific Industries

The banking industry is subject to specific provisions regarding cloud computing. Indeed, on 25 February 2019, the European Banking Authority (EBA) adopted new guidelines on outsourcing. These guidelines include specific provisions – for instance, regarding:

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

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

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

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 concerning measures to ensure a high common level of cybersecurity throughout the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (the "SRI Directive 2"), creates a common regulatory framework to ensure a high level of cybersecurity across the Union, known as the NIS2. The directive requires EU member states to strengthen their cybersecurity capabilities and introduces cybersecurity risk management measures and reporting in critical sectors, as well as rules on co-operation, information sharing, supervision and enforcement. The Directive must be transposed into national law by 17 October 2024.

The rules should apply from 18 October 2024. The Directive applies mainly to medium and large entities operating in high-criticality sectors, which explicitly targets banking and financial infrastructures such as credit institutions, trading platform operators and central counterparties.

4. Artificial Intelligence

4.1 Liability, Data Protection, IP and Fundamental Rights

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

Big Data

Big data technologies have enabled emergence of AI, which requires both high computing power and large volumes of data to train and test models. Companies are now looking to integrate AI into their business processes and information systems. On issues such as image and voice recognition, AI innovations have reached an advanced level. Consequently, two major issues have arisen related to big data:

- the protection of personal data; and

- the reuse of public data with the phenomenon of "open data".

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

Data Protection

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

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

In 2022, the French Data Protection Authority (the CNIL) issued an online guidance on "AI: ensuring GDPR compliance". The CNIL recommends, among other things, to use data pseudonymisation or filtering/masking mechanisms when developing an AI system. In January 2023, the CNIL also announced the creation of an Artificial Intelligence Department dedicated to AI matters.

On October 2023, in order to clarify the rules applicable in AI, the CNIL published a first set of guidelines for the use of AI that complies with personal data protection requirements. These will be followed by two others, which will supplement them on other issues raised by the AI sector. Finally, in November 2023, the CNIL selected four AI projects aimed at improving public services. These winners will receive personalised support over a period of several months. The CNIL will also be advising four other projects that are also of interest in terms of data protection.

Responsibility/Liability

As AI can take decisions with a degree of autonomy, a key legal issue is responsibility/liability. As far as no legal regime is in place to deal with the liability of a robot or a machine that would act according to an autonomous AI process (autonomous cars, for example) in France, it is then necessary to look for the legal basis in the tort liability of Articles 1240 and seq of the French Civil Code, which states that any damage caused must be remedied by the person who

caused it. Regarding tort liability, French law sets out three conditions that need to be fulfilled for liability to be attributable to a party:

- fault;
- damage; and
- a causal link between the two.

The burden of proof lies with the claimant. However, this regime may not be adequate in that its application requires the presence of a legal personality.

In this context, the European Commission published a white paper on artificial intelligence in 2020 and by April 2021 it had issued a proposal for a new regulation on AI (Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence), for which the legislative process is still ongoing. The Commission bases its approach on the identification and framing of risks related to AI by creating categories (unacceptable risk, high risk and non-high risk) according to the fields of application concerned. Accordingly, AI categorised as having unacceptable risks would be prohibited. High-risk AI would be permitted subject to compliance with certain mandatory requirements and an ex-ante conformity assessment. For other non-high-risk AI systems, only limited transparency obligations would be imposed. In a press release published on 9 December 2023, the Council of the European Union claimed to have reached an agreement with the Parliament on the first AI rules in the world. The AI legislation harmonises rules for AI systems, ensuring they are safe and respect EU fundamental rights and values. The final text must now be formally adopted by the Council and the Parliament, as EU co-legislators. Finally, AI legislation is expected to apply from 2026.

On 28 September 2022, the European Commission (EC) adopted two proposals to adapt the liability rules to the digital age. First, the EC published a proposal to revise the Directive 85/374/EEC on liability for defective products to include a compensation for damages caused by products like robots, drones, smart home systems made unsafe by software update, AI or digital services such as software as well as cybersecurity vulnerabilities. Second, the EC published, on the same date, a proposal for an Artificial Intelligence Liability Directive (AILD) in order to adapt non-contractual civil liability rules to AI systems. It lays down consistent rules for aspects of non-contractual (tort) civil liability in connection with damage caused by or with the involvement of AI systems. A “presumption of causality” and a “right of access to evidence” are additional measures provided to consumers in complement to the Directive on defective products.

Intellectual Property

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

Of particular interest is the protection of creations by AI, since AI is already creating potential proprietary content, from works of art to algorithms and computer programs. It is obvious that the intellectual property protection system is based on human creativity, which will render the works of AI difficult to protect under the prevailing circumstances. No related case law is evident in France but, in the DABUS case, the European Patent Office denied patent protec-

tion 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.

Data Economy

Big data and the internet of things (IoT) have brought new challenges to consumers as well as to companies, but they have also brought new opportunities. The EC addressed data access, fairness in the digital environment, the stipulation of a competitive market and increasing opportunities for data-driven innovation by proposing new rules on who can use and access data generated in the EU across all economic sectors in February 2022 (the "Data Act"). The proposal for the Data Act includes:

- measures to allow users of a connected device to gain access to data generated by their devices and the ability to share such data with third parties;
- measures to balance the power between SMEs and big companies; and
- means for public sector bodies to access and use data held by the private sector if exceptional circumstances prevail.

On 27 November 2023, the Council of the European Union finally adopted the Data Act, laying down harmonised rules for fair access to and fair use of data. 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.

Following the formal adoption by the Council, the new Regulation will become applicable 20 months after its effective date. 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 date of entry into force of the Regulation.

5. Internet of Things

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

Liability

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

For instance, if the manufacturer/producer of the connected objects does not respect its pre-contractual information as referred to in Articles 1112-1 of the French Civil Code and Articles L 111-1 and seq of the French Consumer Code with regard to 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.

In December 2021, the French National Institute for Research in Digital Science and Technology (INRIA) published a white paper on the internet of things (IoT). It defines the scope of the IoT, its genesis and its current status, and it identifies the main societal, technical and scientific challenges.

It confirms that, at the present time, no specific regime is being developed for connected objects; these are only envisaged in relation to personal data. Indeed, the white paper highlights the "permanent tension between IoT data exploitability and IoT user privacy".

Data Protection

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

Beyond the obligations imposed by GDPR and French data protection law, the *Commission Nationale Informatique et Libertés* (the French authority enforcing data protection legislations) also recommends proceeding to Data Protection Impact Assessments when implementing IoT projects before processing personal data in order to highlight the purposes of the processing and the legitimate means of achieving them. It also provides guidelines to data subjects using connected objects to better protect themselves from the risks inherent to the use of IoT.

Consent

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

Cybersecurity

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

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

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

attacker to intercept the message containing the photo and replace it with another one.

On 15 September 2022, the European Commission proposed a regulation aiming to reinforce the security of hardware and software marketed in the European Union, and to protect consumers and businesses who purchase or use products or software with a digital component. This is the Cyber Resilience Act. At the end of November 2023, the Council and Parliament reached a provisional agreement, concerning manufacturers' responsibility in relation to product compliance, the vulnerability treatment process, or obligations in terms of product security transparency. In the same context, ANSSI published its recommendations on the security of connected objects, which, on the one hand, aim to realise an assessment of the security level by listing the potential threats that could be faced in this industry and, on the other hand, provide general technical recommendations to address those threats.

6. Audio-Visual Media Services

6.1 Requirements and Authorisation Procedures

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

Audio-visual services are subject to the Law 86-1067 of 30 September 1986 on the freedom of communication and regulated by an independent administrative authority, the *Autorité de régulation de la communication audiovisuelle et numérique* (Arcom since 1 January 2022, formerly CSA).

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

For TV and Radio Providers

The 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 the Arcom in order to be provided with an assigned frequency. The applications must be presented by the provider of the services, and must notably contain the general and technical characteristics of the service, the forecasts of expenditure and income and the composition of the applicant's shares, governing bodies and assets.

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

For other services provided without using the assigned frequencies, the applicable procedure will depend on the service. As a principle, such

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

For AVMS Providers

AVMS must be declared to the 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.

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

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

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

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

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

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

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

Specifically, regarding the possibility for online video channels with user-generated content

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

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

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

European Media Freedom Act

The European Commission adopted in September 2022 a proposal for the European Media Freedom Act to protect media pluralism and independence in the EU. It builds on the revised Audiovisual Media Services Directive, the Digital Services Act, and the Digital Markets Act. The European Media Freedom Act 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. The Act 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) as well as on the transparency of media ownership. The Act also regulates the protection of independence of editors and the disclosure of conflicts. The Act furthermore creates a new independent European Board for Media Services to act as a watchdog for media freedom. Further measures the legislation wants to implement are safeguards against espionage software, transparent state advertising and the new user right to customise their media offer.

On 15 December 2023, the European Parliament and the Council reached a political agreement on the European Media Freedom Act. These new rules will better protect editorial independence, media pluralism, ensure transparency and fairness, and bring better co-operation of media authorities through a new European Media Board. The political agreement is now subject to formal approval by the European Parliament and the Council.

7. Telecommunications

7.1 Scope of Regulation and Pre-marketing Requirements

Local telecommunications rules traditionally apply to electronic communication networks (ECNs) and electronic communication services

(ECSs) (Article L 32 of the French Postal and Electronic Communications Code).

At an EU level, however, the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (the "EECC Directive") modified and updated the applicable framework. In France, the EECC Directive was transposed by Ordinance No 2021-650 of 26 May 2021 in application of Article 38 of Law No 2020-1508 of 3 December 2020.

Importantly, the EECC Directive expands the definition of ECSs by including so-called "interpersonal communications services", defined as services normally provided for remuneration that enable direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipients. Accordingly, and subject to the transposition ordinance of the EECC Directive, voice-over internet protocol (VoIP) and instant messaging falls under the new scope of the telecommunications rules. This was confirmed by Recital 15 of the EECC Directive, and is in line with 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, the French telecommunication authority (*Autorité de Régulation des Communications Électroniques et des Postes* or ARCEP) considers RFID technology as radio-electric installations, which can be used on certain frequencies only and with defined technical settings.

Applicable Requirements

The declaratory regime for ECSs has been abolished by Ordinance No 2021-650 of 26 May 2021. The provision and the establishment of ECNs is now free subject to compliance with rules laid down in Article L 33-1 of the French Postal and Electronic Communications Code (obligation to notify security incidents to ARCEP, net neutrality, interoperability of services, etc).

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

Providers of instant messaging are subject to stricter data protection law requirements with regard to messages under the Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "ePrivacy Directive"). This Directive notably obliges member states to ensure the confidentiality of communications and the related traffic data by means of an ECN or ECS through national legislation. 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 with regard to Article 6 of the ePrivacy Directive.

8. Challenges with Technology Agreements

8.1 Legal Framework Challenges

Parties' Level of Expertise

Most issues arising from information technology (IT) service agreements relate to late or wrong performance of the parties' respective contractual obligations. Given the technical aspect of an IT service agreement, the allocation of responsibilities between the parties is key. In many instances, customers are not very familiar with the technology supplied by the service provider, which is therefore subject to an obligation of advice and information during the negotiation (Article 1112-1 of the Civil Code) and the performance of the agreement (Article 1104 of the Civil Code). This obligation implies:

- an obligation to provide information (the service provider must inform itself about the customer's needs and wishes); and
- an obligation to warn (eg, in the event the service provider considers that the customer's expectations are unlawful or risky, it has a duty to inform the customer and may even refuse to contract with the customer on this basis).

As for the customer, it has a duty to collaborate with the service provider.

Furthermore, in 2016, French law extended the protection against unfair clauses to all pre-formulated standard agreements (*contrat d'adhésion*), including B2B agreements. Some IT service agreements may qualify as such pre-formulated standard agreements provided customers cannot negotiate their content. The terms of these agreements may be considered unfair if they create a significant imbalance between the rights and obligations of the parties. As a consequence, the unfair clauses may be deemed unwritten and therefore unenforceable. If the unenforceable clause is essential, then the IT service agreement as a whole may also be unenforceable.

Liability of the Service Provider

One of the main challenges in IT services agreements is to assess the existence and the extent of the provider's liability, as providers usually tend to impose an exclusion or a limitation of liability clause. It is thus strongly recommended to clearly indicate whether providers are subject to a performance obligation (where the provider must reach a specific result) or an obligation of best efforts.

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. In order to better identify providers' contractual breach, customers would be advised to detail their needs as much as possible and to set out clear specifications in terms of performance (eg, through a service level agreement) or in terms of timeframe (eg, including provision for liquidated damages). On 23 November 2018 (No 15/19053), the Paris

Court of Appeal handed down a decision confirming that, when an IT project involves the integration of software, an obligation of result cannot be imposed on the service provider, unless otherwise stipulated in the contract (in this case, the customer was claiming an obligation of result with regard to the installation of the software proposed by the service provider), since the success of the project largely depends on the active collaboration of the customer at each stage of its implementation.

Service Level

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

Changes in the Economic Situation of the Parties

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

Specific IT Service Agreements

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

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

In relation to bug fixing by decompilation, the Court of Justice of the European Union recently held, concerning a licensee who had decompiled a part of a software in order to disable a defective function, that such decompilation was lawful. The Court also stated that decompilation must be subject to a certain number of conditions (necessity, absence of specific contractual provisions, decompilation for the sole purpose of error correction). It therefore seems appropriate to regulate decompilation for the purpose of error correction through the contract, as well as through the maintenance terms implemented by the editor (CJEU, 6 October 2021, C-13/20).

9. Trust Services and Digital Entities

9.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Electronic Signatures

Electronic signatures are governed by the EU regulation on electronic identification and trust services for electronic transactions of 2014 (the "eIDAS Regulation") and the French Civil Code.

Three categories of electronic signatures exist pursuant to the eIDAS Regulation. Advanced electronic signatures are electronic signatures that meet the requirements set out in Article 26 of the eIDAS Regulation. 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. Simple electronic signatures are electronic signatures that are neither qualified nor advanced.

Article 25(1) of the eIDAS Regulation 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 (non-discrimination principle). Article 25(2) of the eIDAS Regulation indicates that a qualified electronic signature shall have the equivalent legal effect of a handwritten signature (functional equivalence principle).

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 the eIDAS Regulation are presumed to be reliable.

Further guidance on electronic signatures is available on the website of the French National Cybersecurity Agency (*Agence nationale de la sécurité des systèmes d'information* or ANSSI).

Electronic Identification

Article L 102 of the French Postal and Electronic Communications Code establishes the framework for electronic identification to online services in France as well as 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 the eIDAS Regulation 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, including a reference of security requirements of 11 August 2022.

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 Katie.Burrington@chambers.com