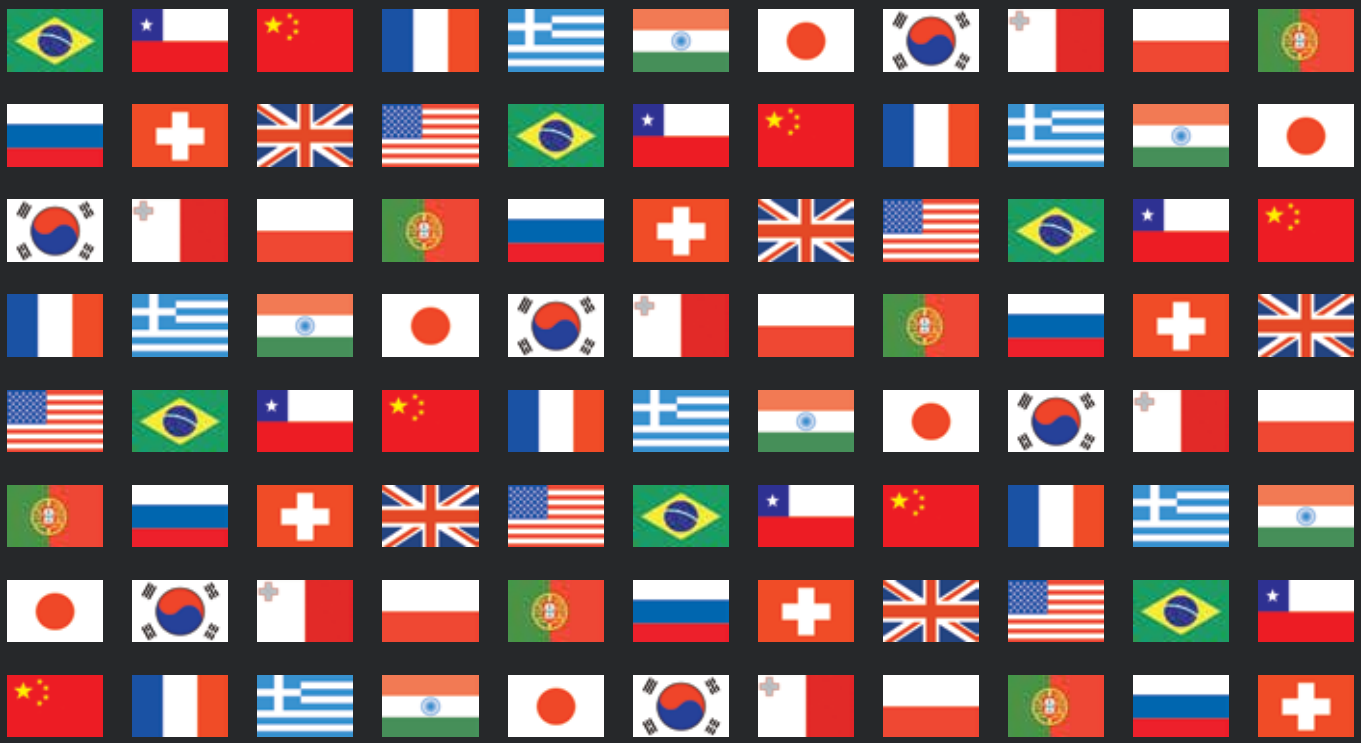
e-Commerce

Contributing editor
Robert Bond



2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

e-Commerce 2018

Contributing editor
Robert Bond
Bristows LLP

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2000
Fourteenth edition
ISSN 1473-0065

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

France

Bradley Joslove
Franklin

General

1 How can the government's attitude and approach to internet issues best be described?

The government appears to be well aware of the need for France to more fully embrace use of the internet in all sectors of the economy, but is frustrated that it cannot exercise the same level of control over what happens on the internet as it does over activities in the 'bricks and mortar' world.

With a view to promoting greater usage of the internet, the Hollande government announced a broadband plan for the development of high-speed broadband networks, entailing an investment of €20 billion to cover all of France with optic fibre by 2022. The Hollande government also wanted to accelerate development of French start-ups through another investment plan named the 'French Tech Mission'. Decree No. 2015-113 of 3 February 2015 created the Digital Agency that is notably in charge of managing the broadband plan and the French tech mission. Finally, the Digital Republic Law was adopted on 1 October 2016. The Law reforms the data protection legal framework, notably by the consecration of the right to be forgotten for minors, the introduction of a network neutrality principle in French law, the incitement to develop mobile networks, and the reinforcement of the opening up of data held by the public sector (open data) (see 'Update and trends').

As regards the repression of illicit uses of the internet, the Hollande government launched various public and private initiatives to combat jihadism and paedophilia. On 24 July 2015, the bill on intelligence was adopted to allow greater surveillance of the internet and electronic communications in general. This new legislation has been criticised by many as a sort of French 'Patriot Act'.

The recently elected French President Emmanuel Macron appears to want to build on the initiatives of the Hollande government and has announced a number of ambitious new initiatives with respect to the internet and the digital economy. Among these initiatives, we find the coverage of 100 per cent of the French territory by the 4G network, and the implementation of a specific regulatory and tax framework for e-business companies. At the European level, Macron undertakes to accelerate the digital market, to create a European venture capital fund dedicated to European start-ups, to renegotiate the Privacy Shield and to create a tax, at the European level, based on the turnover realised in the member states by the companies in the digital economy (sometimes called the 'Google tax').

Legislation

2 What legislation governs business on the internet?

The following laws and regulations, some of which have been codified, govern e-commerce:

- Law No. 78-17 of 6 January 1978, relating to data processing, data files and liberties (the Data Protection Law);
- Law No. 2000-230 of 13 March 2000, adapting the law of evidence to information technologies and introducing electronic signatures;
- Law No. 2004-575 of 21 June 2004, on confidence in the digital economy (the Digital Economy Law), that notably provides a legal liability framework regarding internet intermediaries;
- Law No. 2009-669 of 13 June 2009, in favour of the diffusion and the protection of creation on the internet, that created the High Authority for the Distribution of Creative Works and the Protection of Rights on the Internet;
- Law No. 2010-476 of 12 May 2010, introducing competition and regulation in the online gambling and gaming sector;
- Law No. 2014-344 of 17 March 2014, relating to consumers, improving pre-contractual information in favour of consumers for the conclusion of distant contracts and creating a 'French version' of the class action;
- the Order of 11 March 2015, on advertising price reductions to consumers;
- Law No. 2015-912 of 24 July 2015, concerning surveillance of the internet and electronic communications;
- Law No. 2015-990 of 6 August 2015, for economic growth and activity;
- Ordinance No. 2016-131 of 10 February 2016 reforming contracts law and the general rules on obligations;
- Law No. 2016-1321 of 7 October 2016 for a Digital Republic implementing new obligations of information for online platforms; and
- Decree No. 2017-126 of 9 February 2017 relating to intermediaries' reporting obligations in online advertising.

Regulatory bodies

3 Which regulatory bodies are responsible for the regulation of e-commerce, data protection and internet access tariffs and charges?

The following regulatory bodies are responsible for the regulation of these activities:

- the Data Protection Authority (the CNIL) is an independent administrative organisation that controls and ensures compliance of personal data processing with the data protection law;
- the Electronic Communication and Postal Regulatory Authority is in charge of:
  - ensuring fair competition in the communications sector;
  - receiving the declaration of operators before the provision of regulated telecommunications services;
  - the management and attribution of frequencies and numbering resources;
  - regulation of tariffs;
  - supervising and financing the provision of the universal service; and
  - the resolution of disputes between operators;
- the High Authority for the distribution of creative works and protection of rights on the internet is dedicated to the protection of the interests of copyright holders on the internet and to the promotion and the development of legal offers of internet access to copyright-protected works;
- the General Directorate for Fair Trade, Consumers Affairs and Fraud Control is in charge of:
  - the fight against cartels and abuses of dominant positions;
  - the control of concentrations;
  - the fight against unfair trade practices;
  - the implementation of rules to ensure the provision of a loyal information to consumers on goods and services; and
  - the preservation of the physical safety and health of consumers;
- the Online Gambling Regulatory Authority, whose role is to:

- issue approvals to operators allowed to provide online gambling services;
- protect at-risk populations;
- fight against gambling addiction;
- ensure the safety and fairness of gaming operations;
- fight against illegal sites; and
- fight against fraud and money laundering; and

- the Advertising Regulation Authority is a self-regulatory body that produces general standards and influential but legally non-binding rules and recommendations on key advertising issues.

Jurisdiction

4 What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions or disputes in cases where the defendant is resident or provides goods or services from outside the jurisdiction?

There is no provision of French law dedicated to the determination of the jurisdiction for internet-related transactions or disputes. General principles of the Civil Procedure Code, the Consumer Code and rules of private international law are applied by French courts.

Regarding contractual relationships, the general rule is that the parties can freely choose the competent tribunal. If no jurisdiction is chosen by the parties, the court of the place of performance of the main obligations of the contract will have jurisdiction (ie, place where the goods are delivered or the services are provided).

In the case of a contract concluded by a consumer with a business that directs sales to the country in which the consumer is domiciled (ie, the location of the consumer's habitual residence), the consumer may sue the business in the courts of the country in which the consumer is domiciled or the country in which the business is domiciled. A clause requiring a consumer to exclusively bring suit (or be sued) before a foreign jurisdiction would be unenforceable.

In the context of non-contractual matters (tort), the court where the damage occurred will have jurisdiction. To determine where the damage occurred in internet-related disputes, some French courts have used the criterion of the simple accessibility of the website by French residents (eg, in certain defamation and copyright disputes, but only for damages that were incurred in that jurisdiction) and other courts have focused on the targeting of the French public (use of French language on the website, transactions payable in euros, etc).

New article 113-2-1 of the French Criminal Code, introduced by Law No. 2016-731 of 3 June 2016, provides that any crime or offence committed on the internet against a person residing in France falls under French criminal law and jurisdiction.

Contracting on the internet

5 Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?

The validity of electronic contracts is recognised under French law. The Civil Code states that to be legally formed and enforceable, electronic contracts must satisfy specific requirements.

In particular, the trader who, by electronic means, proposes the delivery of goods or the provision of services must make available the applicable contract terms in a way that allows their conservation and reproduction.

The offer must also state:

- the different steps to follow to conclude the contract by electronic means;
- the technical means allowing the user to identify and correct input errors before the conclusion of the contract;
- the languages offered for the conclusion of the contract;
- in case of archiving of the contract, the details of this archiving by the offeror and the conditions of access to the archived contract; and
- the ways of consulting by electronic means the trader and commercial rules by which the offeror has the intention to be bound.

The trader remains bound by the offer so long as it is available by electronic means.

For the valid conclusion of an electronic contract, a three-step procedure must be followed, in accordance with the provisions of the Civil Code (article 1369-5):

- the offeree selects the goods or services that he or she intends to buy;
- the offeree must be able to check the details of his or her order and the full price, and to correct any possible error (first click); and
- the offeree must confirm his or her order, thus expressing his or her acceptance, through a second click.

The offeror must acknowledge without undue delay and by electronic means the receipt of the electronic order. However, this requirement does not affect the validity of the contract concluded after the double-click procedure.

Contracts concluded between two traders can derogate from this double-click requirement. Furthermore, when contracts related to the supply of goods or services are exclusively concluded through an email exchange, these provisions do not have to be respected (article 1369-6 of the Civil Code).

6 Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?

The Civil Code governs electronic contracts in article 1125 et seq as well as article 1174 et seq, entitled 'contracts in electronic form'. Some of the key provisions are described in question 5.

In addition, the Consumer Code provides additional protection to consumers in business-to-consumer distance contracts. In particular, the consumer must be provided with specified categories of information prior to the conclusion of the contract in a 'clear and comprehensible manner' and after the conclusion of the contract, and at the latest at the time of delivery, 'in writing or in another durable medium'.

Finally, Law No. 2014-344 of 17 March 2014, relating to consumers, introduced a section in the Consumer Code entitled 'distance and off-premises contracts,' which heavily reinforced transparency in distance contracts by expanding the categories of information that must be provided to the consumer both before and after the conclusion of the contract. A list of the required information is provided for in articles L 121-17 and L 121-19 to L 121-19-3 of the Consumer Code.

7 How does the law recognise or define digital or e-signatures?

Article 1316-4 of the Civil Code provides that an electronic signature must authenticate the signatory and ensure the integrity of the signed document. An electronic signature results from the association of three essential elements: a document, an encryption technique and a certificate. The encryption and the certificate are essential for identifying the author and guaranteeing the authentication of the document. A common form of electronic signature is one produced using public key infrastructure technology, whereby a communication is encoded using the sender's private key, and decoded using a public key made available to the receiver in a digital certificate, which proves the authenticity and integrity of the communication.

The eIDAS Regulation No. 910/2014, which entered into force on 1 July 2016, implemented a common legal framework in the EU to ensure mutual recognition of e-signatures within member states and the reliability of e-signature certification tools.

The aforementioned Digital Republic Act allows the government to pass decrees in order to ensure that e-signatures are enforceable in real estate contracts, insurance contracts and consumer credit contracts.

8 Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?

There is no legislation requiring the storage of an electronic contract for a minimum period, except for contracts concluded between a consumer and a trader. Article L 134-2 of the Consumer Code provides that when an electronic contract has been entered into between a trader and a consumer with a price equal to or above €120 including VAT, the contract must be stored for 10 years. This period starts from the date of the signature of the contract, if the delivery of goods or the performance of the service is immediate, otherwise, the period will run from the effective date of the delivery or performance.

Security

9 What measures must be taken by companies or ISPs to guarantee the security of internet transactions? Is encryption mandatory?

French law does not prescribe the measures that ISPs or companies must implement to ensure the security of internet transactions (for example, encryption is not an obligation for ISPs). However, according to the Data Protection Law, when online operations involve the processing of personal data, the data controller must take appropriate measures to ensure the security of the data and to prevent data from being altered, damaged or accessed by unauthorised persons or for unauthorised purposes. While data controllers are free to choose the security means, the CNIL has issued recommended security measures.

10 As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?

Article 230-1 of the Criminal Procedure Code entitles judicial authorities to designate an expert to perform technical operations in order to make available encrypted information. Such authority may also require the disclosure of the decryption key if necessary.

Certification authorities are permitted, provided they file a prior declaration with the National Agency for the Security of Information Systems and comply with the regulatory regime governing their services.

Article 33 of the Digital Economy Law sets forth the liability regime for electronic certification service providers. They are liable for any prejudice caused to those who have relied reasonably on the certificates presented by them as qualified. However, their liability will only be incurred for wilful misconduct or negligence.

Article L 871-1 of the Internal Security Code obligates providers of encryption services to make decryption keys available to intelligence services.

Domain names

11 What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?

The attribution and management of domain names for the geographical areas of .fr (France), .pm (St Pierre and Miquelon), .re (Réunion Island), .tf (French Southern and Antarctic Territories), .wf (Wallis and Futuna) and .yt (Mayotte) are handled by the French Association for Internet Naming in Cooperation (AFNIC).

Only natural persons resident in the territory of the European Union and legal persons that have their registered office or principal place of business in the territory of one of the member states of the European Union may apply to register a domain name managed by the AFNIC through the intermediary of accredited registrars. Domain names are attributed on a first-to-file basis.

According to article L 45-2 of the Postal and Electronic Communications Code (CPCE), the registration or the renewal of a domain name may be refused, or the domain name removed if it:

- disrupts public policy or morality, or the rights guaranteed by the French constitution or French law;
- infringes intellectual property rights or personal rights, unless the applicant demonstrates a legitimate interest and acts in good faith; and
- is identical or similar to that of the French Republic, of a regional or local governmental authority, of an institution or a local or national public service, unless the applicant demonstrates a legitimate interest and acts in good faith.

As concerns the judicial procedures in order to guarantee the ownership of a domain name, AFNIC implemented two alternative dispute resolution procedures ('PARL expert' and 'SYRELI') in November 2011 and March 2016, available for physical persons and legal entities, in order to enable them to get a domain name back or to obtain its deletion.

12 Do domain names confer any additional rights beyond the rights that naturally vest in the domain name?

Domain names allow their holder to act on the ground of unfair competition if a trademark is subsequently registered and is likely to create confusion in the public's mind. In addition, article L 711-4 of the Intellectual Property Code provides that a sign may not be adopted as a trademark if it infringes earlier rights. Although domain names are not expressly mentioned in the code as earlier rights, case law usually considers that a domain name may constitute an earlier right enforceable against a subsequently deposited trademark if the domain name is effectively exploited.

13 Will ownership of a trademark assist in challenging a 'pirate' registration of a similar domain name?

It is highly recommended that the holder of a domain name register a sign identical or similar to the domain name as a trademark to facilitate action against a third party for cybersquatting (exact reproduction of the sign as a domain name) or for typosquatting (use of a similar sign as a domain name). In addition, article L 45-2 of the CPCE expressly provides that the registration or the renewal of a domain name may be refused or the domain name removed if it infringes intellectual property rights. Thus, the ownership of a prior trademark assists in challenging a subsequent 'pirate' registration of a similar domain name. In such case, the applicant of the similar domain name can only obtain the domain name if it proves that it has a legitimate interest to register the domain name and is acting in good faith.

Advertising

14 What rules govern advertising on the internet?

The Digital Economy Law specifically governs advertising accessible by online communication services. Article 20 provides that all advertising on the internet must be clearly identifiable as such and must clearly indicate the identity of the person on whose behalf the advertisement is created. Article 21 provides that email advertising (including promotional offers such as discounts, premiums or gifts, and competitions or promotional games) must be clearly and unequivocally identified. The conditions applicable to promotional offers or to the participation in competitions or promotional games proposed by email must be clearly stated and readily accessible. Furthermore, article 22 bans sending out direct marketing communications by an automated calling system, fax or email using the contact details of an individual who has not opted in to receive such direct communications (except to the advertiser's customers of similar products or services).

Law No. 93-122 of 29 January 1993, as amended in 2015, along with a 1994 Circular and Decree No. 2017-159 of 9 February 2017 (collectively, 'the Sapin Law') constitute the regulatory framework governing the purchase or sale, via an intermediary, of advertising space on any media or materials, including websites. The purpose of the Sapin Law is to bring more transparency into an area that had been plagued by kick-backs and collusion between media and intermediaries. When the Sapin Law applies, the parties must comply principally with the following obligations:

- Any purchase of advertising space is made by the intermediary as an agent of the advertiser and under a written agreement that specifies the services provided and the payment terms. The intermediary must act strictly on behalf of the advertiser and not on its own.
- Any discounts that the intermediary has been offered by the media owner must appear on the invoice to the advertiser, and those can be kept by the intermediary only with the advertiser's agreement. In addition, the invoice relating to the purchase of advertising space must be provided directly by the seller to the advertiser even if the advertiser does not directly pay the media owner. The intermediary has to be paid exclusively by the advertiser and in no event by the media owner.
- The advertiser must be made aware of and agree to any change affecting the display of the advertisement.
- The intermediary is required by law to report directly to the advertiser within one month of the display of the advertisement, detailing the conditions under which the services were performed. The Decree of 9 February 2017, which details the intermediary's reporting obligations for digital advertising, will come into force on 1 January 2018.

In addition, general laws governing advertising also apply to internet media. For example, misleading advertising may be constituted through online advertising.

Comparative advertising is also strictly regulated. Comparative advertising must be exact and objective and must not: permit the advertiser to unduly benefit from the notoriety attached to the trademark of a competitor; discredit or denigrate a trademark, trade name and other distinctive signs of a competitor; create confusion between the advertiser and a competitor, or between a trademark, trade name and other distinguishing signs of the advertiser and those of a competitor; or present goods or services as imitations or reproductions of goods, or services bearing a protected trademark or trade name.

The ARPP (the French advertising self-regulatory organisation) is a trade association that has issued a Digital Advertising and Marketing Code for its members. The key principles are:

- identification of advertising: marketing communications and advertising should be clearly distinguishable as such, whatever their form;
- protection of children and teenagers: advertising and marketing communications must not contain statements or visual elements that could harm psychologically, morally or physically children and teenagers. ARPP has also recommended the use of targeted information (such as age or date of birth, etc) in order to avoid children and teenagers from gaining access to inappropriate content which might harm them;
- taste and decency: all advertising and marketing communications should be decent and respect human dignity and be compliant with ARPP's 'Portrayal of Human Being' and 'Race, Religion and Ethnic' Codes;
- fair, truthful and honest advertising: all advertising and marketing communication must comply with the law and be fair, truthful and honest;
- user generated-content: when users are invited to create some content for advertising purposes, respect of these principles will have to be organised; and
- comfort of use: digital advertising and marketing communications must respect users' comfort, in particular by ensuring the weight, size, sound and the exposure time of the commercial.

The Digital Republic Act created a status for operators publishing consumers' ads on their website (consumer-to-consumer platforms mainly) and obligates them to identify which posts are advertisements, have been sponsored or for which their author had paid for a better indexing.

15 How is online advertising defined? Could online editorial content be caught by the rules governing advertising?

The term 'advertising' has been defined in the context of television as follows: '"(Television) advertising" means any form of announcement broadcast in return for payment or for any other consideration in order to promote the supply of goods or services, including those presented by their generic name, in connection with a trade, business, craft or profession or to ensure the trade promotion of a public or private company' (Decree No. 92-280 of 27 March 1992 on television advertising). In addition, Directive 2006/114/EC concerning misleading and comparative advertising defines advertising as 'the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services, including immoveable property, rights and obligations'. Finally, the notion has been defined by French courts as 'any means of information seeking to allow potential clients to form an opinion on the characteristics of the goods or service offered' (Crim, 14 October 1998, No. 98-80527).

Under French law, online editorial content could be caught by the rules governing advertising if it is identified as advertising or if it falls within the definition of advertising mentioned above.

16 Are there rules against misleading online advertising?

The general rules against misleading advertising apply to online advertising. A commercial practice is misleading when it creates confusion with another good or service, a trademark, a commercial name or any other distinctive sign of a competitor; when it is based on false allegations and concerns the existence, availability or nature of the good or service, its essential characteristics, its price and condition of sale, etc; and when the person who is responsible for its content is not clearly identifiable.

Articles L 511-5, L 511-20 and L 512-5 of the Consumer Code state that the agents of the Directorate-General for Fair Trading, Consumer Affairs and Fraud Prevention, those of the Directorate-General of Food of the Ministry of Agriculture and those of the Department of Metrology of the Ministry of Industry may require advertisers to make available to them any elements which substantiate their advertising claims, indications or presentations. As a result, advertisers should keep a record of these elements. Despite this rule, it is still up to the prosecution to prove that the advertising is misleading.

17 Are there any products or services that may not be advertised on the internet?

There are no rules specifically prohibiting advertisement of certain goods or services on the internet. General rules governing advertising will apply to the internet. Thus, various products may only be advertised in specific conditions. For example, the French Public Health Code prohibits all advertising for tobacco products, regardless of the medium used. In addition, a large number of specific regulations apply to advertisement on behalf of certain products or sectors: alcohol, automobiles, consumer credit, distance selling and discounts, electronic cigarettes, energy, environment, free credit, food products, gambling, health, job offers, life insurance, marriage agencies, medication, politics, premiums, prices, products and services presented as beneficial for health, real estate and real estate loans, repair service, telephone services, sweepstakes, tobacco, travel agencies and weapons.

18 What is the liability of content providers and parties that merely host the content, such as ISPs? Can any other parties be liable?

See question 20 for the liability of ISPs for content they host.

Also, French law requires telcos and hosting service providers (HSPs) to cooperate with judicial authorities to help identify individuals who have contributed to the creation of unlawful content. It requires ISPs and HSPs to keep data that enable the identification of users and to release them to prosecution authorities in case of legal proceedings. ISPs and HSPs must also have on their site a functionality that enables users to report content that constitutes child pornography, support for crimes against humanity, support of or provocation to commit terrorism, hate speech based on race, gender, sexual orientation or handicap. The function should be clearly visible. The website operator also has the obligation to report such prohibited content to the appropriate public authorities promptly upon becoming aware of it and publish the steps that it has taken to fight against such illicit activities.

Finally, article 34-1 of the CPCE requires telcos and ISPs to retain for one year certain categories of technical data (the IP address from which the content was created, the identifier assigned by the system to the content created, the type of content created, the date and time of creation, the name used by the author, etc) and deliver such data to judicial and authorised administrative authorities in conformity with the law.

Financial services

19 Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and, if so, by whom and how?

In France, the selling of financial services products to both consumers and traders via the internet is regulated by the Monetary Code. These regulations concern in particular public offers and direct marketing.

The selling of financial services products to consumers via the internet is also regulated by the Consumer Code, which notably creates a limited right of withdrawal for the consumer and contains detailed requirements as to the information that consumers must receive prior to contracting.

Defamation

20 Are ISPs liable for content displayed on their sites?

The liability regime of online intermediaries is a controversial and ever-evolving issue, as courts have taken various approaches concerning their liability for third-party content. The key to most decisions turns on whether the ISP is considered to be an HSP protected by a

special limited liability regime under French law or is considered to be something else (eg, a publisher).

An HSP is defined as an entity that provides (even without charge) with a view to public access by online communication services, the service of storage of signals, written documents, images, sounds or messages of any nature provided by the recipients of these services. An HSP is liable for the content stored on its website only if it was actually aware of the illicit character of the content or if it did not take down or prevent access to the illicit content promptly after becoming aware of its illicit character. In decision No. 2004-496 of 10 June 2004, the constitutional council clarified that the HSP cannot be held liable unless the user content was manifestly illegal or such user content had to be taken down as a result of a judicial decision. Child pornography, praise of crimes against humanity and incitement to racial hatred are specifically considered to be manifestly illicit.

21 Can an ISP shut down a web page containing defamatory material without court authorisation?

While an ISP does not have a general obligation to monitor third-party content on its site, it can shut down a web page containing defamatory material without court authorisation if it is granted such right in its contract with the third party or the defamatory nature of the content is manifest. In the latter case, it can in fact be held liable if it does not take down the content.

Intellectual property

22 Can a website owner link to third-party websites without permission?

Every act of communication of a work to the public has to be authorised by the copyright holder.

The Court of Justice of the European Union (CJEU) has recently clarified whether the linking to a third-party content could constitute an act of communication to the public requiring the authorisation of the author (*Svensson and Others*, C-466/12, 13 February 2014). In its decision, the court held that the provision of clickable links to a content protected by copyright must be considered as an act of communication. However, in the case in question, such act did not require the authorisation of the author since the communication was not made to a different public than the one targeted at the time of the initial communication. Indeed, access to the work was not subject to any restriction in that the public consisted of all potential visitors of the website. Therefore, visitors of the website where the link was displayed must be taken into account as being part of the initial targeted public. In consequence, since the work was not communicated to a new public, the authorisation to link to the content was not required.

Conversely, if the clickable link makes available a content whose access is limited, this act must be considered as a communication to a new public and therefore requires the authorisation of its author.

23 Can a website owner use third-party content on its website without permission from the third-party content provider? Could the potential consequences be civil in nature as well as criminal or regulatory?

Article L 122-4 of the Intellectual Property Code provides that any integral or partial representation or reproduction of a content protected by copyright without the author's prior consent is unlawful and may constitute an infringement. Thus, the third party's consent is required to use its content on a website.

However, the author's prior consent is not required for certain uses exhaustively set out by article L 122-5 of the French Intellectual Property Code: private and gratuitous performances carried out exclusively within the family circle, copies or reproductions strictly reserved for the private use of the copier and not intended for collective use, parody, pastiche, caricature, etc.

Furthermore, subject to clear attribution (name of the author and of the source), the content may be submitted to analyses or be subject to short quotations where justified by the critical, polemic, educational, scientific or informative nature of the work in which the content is incorporated. The same solution is provided for press reviews, dissemination, even in their entirety, through the press or by broadcasting, as current news, of speeches intended for the public made in political, administrative, judicial or academic gatherings, as well as in public meetings of a political nature and at official ceremonies.

It is also permitted to reproduce works of graphic or three-dimensional art intended to appear in the catalogue of a judicial sale held in France for the exclusive purpose of relaying current news.

Public establishments, such as libraries, museums and archives, may also reproduce and represent works as long as they do not use the content for profit. As concerns re-use of databases, see question 48.

Infringement is both a criminal offence and a tort. The author may choose to bring an action before the civil court to obtain:

- a specific prohibition of further infringement;
- compensation for the damage suffered;
- recall from the market, destruction or confiscation for the benefit of the victim, of the infringing items or the equipment predominantly used for their manufacture;
- any appropriate measure to make the judgment public; and
- the precautionary seizure of the capital assets, real estate of the alleged infringer and the blocking of its bank accounts.

Or the author might bring an action before the criminal court so that criminal sanctions be applied against the counterfeiter such as:

- three years of imprisonment and a fine of €300,000;
- the total or partial, permanent or temporary closure of the establishment that has served for the commission of the offence;
- the confiscation for the benefit of the victim of the infringing items or the equipment predominantly used for their manufacture; and
- at the cost of the convicted person, the posting of the judgment.

24 Can a website owner exploit the software used for a website by licensing the software to third parties?

According to article L 122-6 of the Intellectual Property Code, the right to exploit a software program belongs to its author. Thus, the two following situations may be envisaged:

- the website owner is also the author of the software: in this case, it can freely license the software to a third party; and
- the website owner is not the author of the software: no exploitation of the software is possible without the prior consent of the author. A contract with a freelance website creator does not assign any intellectual property rights in the software used for a website unless the agreement contains a specific provision effecting that assignment.

25 Are any liabilities incurred by links to third-party websites?

Depending on the facts of the case, a website owner who links to a third-party website could be held liable for unfair competition, copyright infringement or passing-off. Criminal liability may also be incurred if the link directs to illicit content (child pornography or pornographic or violent messages if the message may be seen by minors).

French case law also considers that a website owner who intentionally links to a third-party website that offers counterfeit works facilitates the commission of the infraction and thus can be found guilty of complicity to counterfeiting by provision of means under article L 121-7 of the Criminal Code.

A judgment by the CJEU (*GS Media*, C-160-15, 8 September 2016)) affirms that professionals referencing hyperlinks for profit are not presumed to act in good faith and thus must verify that the hyperlinks they propose on their website do not refer to pages infringing any intellectual property rights.

26 Is video content online regulated in the same way as TV content or is there a separate regime?

Video content online is not regulated in the same way as TV content since in France there is a separate regime: video content online is defined as 'online public communication service' whereas TV content is identified as 'audiovisual communications service'. The obligations of each service are different. Audiovisual communications services must, for instance, respect the rules concerning the chronology of media programming, reserve a certain percentage of the programming time for European works, and respect political pluralism.

27 Do authorities have the power to carry out dawn raids and issue freezing injunctions in connection with IP infringement?

In case of infringement seizure procedures, authorities have the power to carry out dawn raids and issue freezing injunctions.

28 What civil remedies are available to IP owners? Do they include search orders and freezing injunctions?

In addition to obtaining damages and the cessation of the infringing acts, it is possible to seek seizure and confiscation of:

- all copies of the infringing item;
- all or part of the receipts obtained from the infringement and the equipment specifically used for the infringement; and
- the precautionary seizure of the capital assets, real estate of the alleged infringer and the blocking of his or her bank accounts.

Data protection and privacy

29 How does the law in your jurisdiction define 'personal data'?

Personal data means any information relating to a natural person who is or can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to him. In order to determine whether a person is identifiable, all the means that the data controller or any other person uses or may have access to should be taken into consideration.

IP addresses have recently been deemed to constitute personal data in certain circumstances (see 'Update and trends' for more on this topic).

Article 8 of the French Data Protection Law defines sensitive personal data as 'personal data that reveals, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or which concern their health or sexual life'.

In principle, the collection and processing of sensitive data is prohibited. This prohibition does not apply to:

- processing for which the data subject has given his or her express consent;
- processing necessary for the protection of human life;
- processing carried out by an association or any other non-profit-seeking religious, philosophical, political or trade union body;
- processing that relates to personal data that the data subject has made public;
- processing that is necessary for the purposes of preventive medicine, medical diagnosis, provision of healthcare or statistical processing;
- processing carried out by the National Institute of Statistics and Economic Studies (INSEE);
- processing necessary for medical research;
- processing that is necessary for the establishment, exercise or defence of a legal claim; and
- processing justified by the public interest and authorised by the CNIL.

Subject to the approval of the CNIL, the prohibition also does not apply to sensitive data that will, within a short period of time, be subject to an anonymisation procedure that the CNIL has approved. Finally, this prohibition does not include the processing of personal data carried out for the sole purpose of literary and artistic expression and professional journalism.

If through anonymisation or similar techniques the data is anonymised in such a way that the data subject is no longer identifiable, then French data protection law would no longer apply to that data.

30 Do parties involved in the processing of personal data, such as website owners, have to register with any regulator to process personal data?

Any processing of personal data in France must be declared to the CNIL by the data controller before it is implemented. The standard declaration is quite long and detailed. One notification is required per 'purpose' (eg, human resources, CRM) of data processing. However, the CNIL has developed simplified norms for certain common categories of data processing. If a company complies with such norms, it can simply sign a certification of compliance and send it to the CNIL.

In addition, for certain types of processing considered as sensitive, authorisation must be obtained from the CNIL (eg, processing of sensitive data, or transfer of personal data to a country outside of the European Economic Area that has not been determined to provide an 'adequate level' of protection).

Finally, notifications and requests of authorisation with the CNIL are not required when a company has appointed a data protection officer (DPO) in conformity with the law. At present, a data protection officer is not compulsory in France, but that will change when the General Data Protection Regulation (GDPR) enters into force on 25 May 2018. The GDPR broadly provides that DPOs must be nominated by corporations if its core activities entail (i) the regular and systematic monitoring of data subjects on a large scale, or (ii) the processing on a large scale or special categories of personal data (race, politics, religion, health, etc) or personal data relating to criminal offences. The GDPR permits member state law to expand on the requirement to appoint a DPO.

The selling of personal data to a third party is permitted if the data subjects have been clearly and expressly informed of the possibility of the sale of the data and have given their prior express consent.

31 Could data protection laws and regulatory powers apply to organisations or individuals resident outside of the jurisdiction?

French data protection law may apply to foreign organisations or individuals. According to article 5 of the French Data Protection Law, French law is applicable when: the processing is carried out in the context of the activities of an establishment of the controller on French territory; or the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on French territory, unless such equipment is used only for purposes of transit.

Pursuant to the judgment of the CJEU in *Google Spain and Google* (C-131/12, 13 May 2014), European data protection law can apply to a processing of personal data carried out by an organisation resident outside of the European Union if that organisation processes personal data of EU residents within the context of the operations of an establishment (eg, subsidiary) in the European Union.

Furthermore, on 1 October 2015, the CJEU released an important judgment (*Weltimmo*, C-230-14) considering that data protection legislation of a member state may be applied to a foreign company (including within another EU member state) which exercises in that state, through stable arrangements, a real and effective activity, since the concept of 'establishment' extends to any real and effective activity, even a minimal one. The presence of only one representative can, in some circumstances, suffice to constitute an establishment.

On the question of jurisdiction, the *Weltimmo* decision distinguished between investigative and sanctioning powers. While the CNIL has the power to investigate a complaint by local data subjects irrespective of the applicable law, it only has powers to impose penalties if the applicable law is French law.

Finally, the Article 29 Working Party has taken the position that placing cookies on the computers of users can trigger the application of the second criterion mentioned above.

The GDPR codifies the *Google Spain* and *Weltimmo* decisions and will apply EU data protection law directly to data processors as well. In addition, the GDPR applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU where the processing activities are related to (i) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU (ie, targeting); or (ii) the monitoring of their behaviour as far as their behaviour takes place within the EU. The GDPR sets out criteria to determine whether EU residents are being targeted: use of language and currency of targeted member state(s); possibility of ordering goods and services in the local language; and mentioning of customers in the EU.

32 Is personal data processed on the basis of customer consent or other grounds? What is the commonly adopted mechanism for obtaining customer consent or establishing the other grounds for processing?

Processing of personal data must have received the consent of the data subject or must meet one of the following conditions:

- compliance with any legal obligation to which the data controller is subject;
- the protection of the data subject's life;
- the performance of a public service mission entrusted to the data controller or the data recipient;
- the performance of either a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract; and
- the pursuit of the data controller's or the data recipient's legitimate interest, provided this is not incompatible with the interests or the fundamental rights and liberties of the data subject.

Under French law, consent must be a freely given, specific and informed indication of the data subject's wishes by which they signify their agreement to the processing of personal data (eg, checked box that is not pre-selected). Companies must obtain the individual's prior consent ('opt-in' requirements).

33 May a party involved in the processing of personal data, such as a website provider, sell personal data to third parties, such as personal data about website users?

The selling of personal data to a third party is permitted if data subjects have been clearly and expressly informed of the possibility of the sale of the data and if they have given their prior express consent. If not, the seller may be subject to criminal prosecution:

A judgment of 25 June 2013 by the French Supreme Court has ruled that a sale of a database with personal data is void if the database is not registered with the CNIL.

In addition to the data privacy rules mentioned above, general principles of law apply to the sale or licensing of the personal data.

34 If a website owner is intending to profile its customer base to carry out targeted advertising on its website or other websites visited by its customers, is this regulated in your jurisdiction?

The analysis of a user's behaviour on the internet in order to target advertising is regulated under French data protection law and is subject to the prior notification of said user who must be able to easily and promptly refuse this analysis.

The European Directive 2009/136/EC, implemented in France by the ordinance of 24 August 2011 relating to electronic communications, has set up new cookie rules based on an opt-in approach. However, the user's express prior consent is not required for specific types of 'technical cookies' whose exclusive purpose is to enable or facilitate electronic communication or are strictly necessary for the provision of an online communication service at the express request of the user.

The CNIL has made several rulings concerning profiling. The CNIL considers that there is profiling when the processing enables the data controller to singularise a person even if the latter is not directly identified, but rather indirectly identified by his or her computer. This finding therefore triggers the application of the reinforced consent requirement (ie, explicit consent based on full, clear and easily accessible information on the specific purposes of the profiling).

The GDPR gives a definition of the profiling as 'the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance' (article 4.4). The concerned person has the right not to be subject to a decision only based on this profiling, except under specific conditions (article 22). As to personal data, a person concerned by profiling also has all the other rights recognised by the GDPR.

35 Does your jurisdiction have data breach notification or other cybersecurity laws specific to e-commerce?

In accordance with Directive 2009/136/EC, as transposed in Ordinance 2011-1012 of 24 August 2011 and in Decree No. 2012-436 of 30 March 2012, public network service providers (such as Orange, Free, Numericable-SFR or Bouygues) must notify the CNIL without delay of any personal data breach that occurs in connection with the provision of an electronic communication service. Where such a personal data breach might impact a subscriber's or an individual's personal data or privacy, the service provider must also notify that person without delay, unless the CNIL determines that adequate protective measures have been implemented (for example, as a result of encryption) and that the personal data breach is assessed by the CNIL as not being material. Public network operators must also maintain an inventory of data breaches.

36 Does your jurisdiction recognise or regulate the 'right to be forgotten'?

The Digital Republic Act introduced, in its article 63, the right to require those offering information society services to delete personal data of persons who were minors at the time of their collection.

In addition, in a high-profile ruling delivered on 13 May 2014, the CJEU held that a web user may directly request a search engine to remove from its index links to web pages lawfully published by third parties and containing personal information about him or her. The CJEU therefore affirmed a 'right to be forgotten' on the grounds that initially lawful processing of accurate data may, in the course of time, become incompatible with the data protection legislation where, having regard to all the circumstances of the case, the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in light of the time that has elapsed.

Pursuant to that decision, the French courts and the CNIL have also recognised and applied a right to be forgotten. For instance, by an interim order dated 19 December 2014, the Tribunal de Grande Instance of Paris ordered Google Inc to dereference links on the basis of the right to be forgotten enshrined in the CJEU *Costeja* decision. Similarly, by a deliberation dated 21 May 2015, the CNIL put Google on notice to dereference several results from its search engine. The CNIL expressly asked that the de-indexation be carried out on all extensions (.com, .uk, etc) of the search engine. Google refused to implement the CNIL request on non-EU sites. As a result, in a decision handed down on 10 March 2016, the CNIL imposed a €100,000 fine on Google. Finally, the GDPR (article 17) states, in pertinent part, that a person is entitled to obtain from the data controller the erasure of his or her personal data on any of the following grounds: (i) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (ii) the data subject withdraws his or her consent on which the processing is based and there are no other legal grounds for processing; (iii) the data subject objects to the processing and there is no overriding legitimate grounds for the processing; (iv) the data has been unlawfully processed; (v) the data has to be erased to comply with applicable regulation; and (vi) the personal data has been processed to provide information society services to minors.

37 What regulations and guidance are there for email and other distance marketing?

Under French law, unsolicited distance marketing is forbidden. According to articles L 34-5 of the CPCE and L 121-20-5 of the Consumer Code, email marketing is subject to prior consent of the recipient. There are two exceptions to this rule: if the prospective customer is already a client of the company and if the prospecting relates to comparable products and services provided by the same legal entity; and if the prospecting is not commercial (but charitable, for example).

In both cases, the person must be informed at the time of collecting that his or her email address may be used for direct marketing, and must be able to object simply and free of charge to such use. The CNIL declared that the person concerned must have expressed his or her prior consent through a 'positive act' (eg, ticking a box).

Rules are different for professionals. A professional must only be informed that his or her email address may be used for direct marketing and must be able to object free of charge to such uses. Besides, professionals can only be solicited for products and services related to their professional activities.

38 What rights and remedies do individuals have in relation to the processing of their personal data? Are these rights limited to citizens or do they extend to foreign individuals?

Data subjects may exercise their rights of access, rectification, opposition (and right to be forgotten since the CJEU decision of 13 May 2014). They also have a right to be informed of the identity of the data controller, the purpose of the processing, whether the information collected is required or optional, the consequences for failing to respond, the recipients of the information, the subject's rights, the person responsible for enforcing the rights and the projected transfers of the data.

In case of violation of their rights, they can bring legal action based on:

- civil law (articles 1382 and 9 of the Civil Code);
- employment law (article L 1222-4 of the Labour Code provides that 'no personal information about an employee may be collected by a device that has not previously been brought to the employee's attention'); and
- criminal law (Law No. 78-17 of 6 January 1978 provides in article 50 that '[v]iolations of the provisions of this Law are defined and punishable under articles 226-16 to 226-24 of the Criminal Code').

The CNIL may also receive and investigate complaints and ensure that the processing of personal data is implemented in accordance with the provisions of the Data Protection Law.

The CNIL may issue a warning to a data controller failing to comply with the obligations of the Data Protection Law. The Chair of the Commission may also serve a formal order to comply on said data controller to cease the non-compliance within a given deadline. Should the data controller fail to comply with the notice, the Restricted CNIL may pronounce the following sanctions, after due hearing of the parties:

- fines of up to €3 million;
- an injunction to cease the processing, or a withdrawal of authorisation; and
- the CNIL may publicise the sanctions.

Under the GDPR, competent authorities will be entitled to assess fines up to the higher of €10 million or 2 per cent of a company's global turnover, in case of certain breaches of data protection laws, and up to €20 million or 4 per cent of the company's global turnover in case of breaches of the basic principles of data collection or violation of data subjects' rights.

These rights and remedies may extend to foreign individuals if French law is applicable (see question 31).

Taxation

39 Is the sale of online products subject to taxation?

VAT treatment depends on the nature of the services, the geographical location of both the recipient and the provider, and the status of the client: trader or non-professional.

Downloading of software is classified as the purchasing of a service.

The place of taxation for services is set out in article 259 and 259 B of the Tax Code and is summarised in the following table:

	Place of establishment of the provider	Status and place of establishment of the recipient	Place of taxation
Articles 259 and 259 B of the Tax Code	France	Recipient is not a trader – France	France
		Recipient is not a trader –EU member state	Not taxable in France
		Recipient is a trader – France	France
		Recipient is a trader –EU member state	Not taxable in France
		Other country	Not taxable in France
	EU member state or other country	Recipient is not a trader – France	Taxable in France
		Recipient is a trader – France	France

40 What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?

As a general rule, companies are subject to corporate tax in France on the business performed in France. However, placing servers outside France is not necessarily sufficient to consider that the business is conducted outside France from a French tax perspective.

41 When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?

The company should register for VAT in the state where it is established. Domestic internet sales are subject to French VAT under normal conditions. The standard rate is 20 per cent. An intermediary rate of 10 per cent applies to certain goods and services such as hosting, passenger transport, museums, waste treatment, etc.

Another rate of 5.5 per cent applies to food products, books, gas and electricity, live entertainment, movie theatres, etc.

Finally, a 2.5 per cent rate applies to reimbursable medications, licence fees for new digital channels, etc.

42 If an offshore company is used to supply goods over the internet, how will returns be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?

Returning goods to an onshore retail outlet of an offshore company may raise the question of a permanent establishment (PE) in France. In most international tax treaties, a goods depot in France is not considered as a PE in France insofar as the establishment solely supports activities, such as research, advertising or the provision of information. If the French outlet of the foreign offshore company renders after sale services, it is advisable to check the PE definition in the concerned tax treaty because this could, in some cases, be sufficient to characterise a PE.

Gambling

43 Is it permissible to operate an online betting or gaming business from the jurisdiction?

Law No. 2010-476 of 12 May 2010 introducing competition and regulation in the online gambling and gaming sector has opened up horse race betting and sports event betting (both mutual and fixed-odds) as well as club games, which are defined as 'pooled games based on luck and skill in which a player, after the intervention of chance, decides, upon observing the other players' behaviour, on a strategy that is likely to modify his expected winnings'. In view of this law, it is now permissible to operate online betting or gaming services, provided that the operator has obtained a licence to carry out its activities from the Regulatory Authority of online games (ARJEL). This licence is granted for a five-year period.

This law does not apply to games that are based solely on chance, such as lotteries and slot machines, which remain under the monopoly of the state and licensed casinos.

44 Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?

Adult residents may use online casinos and betting websites. However, online gambling operators must prevent the participation of minors, persons who have been banned from gambling and games of chance, and those who have been excluded at their own request. Online gamblers must provide their identity, age, email, physical address and payment account – the gambling operator must also ensure that the player is a natural person.

There are no laws making it illegal for a simple player to place bets on an illegal gambling website. However, one could not exclude the possibility that such gamblers could be found guilty of complicity in illegal bookmaking.

Outsourcing

45 What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?

The provision of services on an outsourced basis notably raises the following legal difficulties:

- regarding labour law, the outsourcing operation may lead to the application of article L 1224-1 of the French Labour Code, which provides that when an autonomous economic entity is transferred, the labour contracts are transferred with it to the transferee;
- regarding intellectual property issues, the transfer may require the transmission of licences or applications. The software licence entered into between the licensor and the transferor may prohibit

Update and trends

Dynamic IP addresses may qualify as personal data

There is a growing trend to consider IP addresses as personal data.

In its judgment dated 29 October 2016 (*Patrick Breyer v Federal Republic of Germany*, C-582/14), the CJEU was called upon to rule on whether an IP address held by a website operator qualifies as personal data if that operator is able to access additional information held by a third party (in this instance, internet access providers) enabling it to identify the data subject. The CJEU held that an IP address, whether dynamic or static, constitutes personal data if the person collecting it has the legal means to obtain additional information from a third party that enables it to identify the data subject.

In a strict interpretation of the regulation related to data privacy, the Civil Chamber of the French High Court has considered that an IP address is personal data outright (decision dated 3 November 2016).

Finally, the GDPR, which will enter into effect on 25 May 2018, is interpreted by some as treating IP addresses as personal data: 'Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.' (Whereas No. 30 of the GDPR).

Information security at the heart of French and EU regulations

In 2016, a series of regulations were enacted to reinforce the information security obligations of tech companies.

First, the European Union published the eIDAS Regulation (No. 910/2014) dated 23 July 2016, establishing security standards based on electronic signatures, electronic seals, electronic time stamps and mechanisms for issuing qualified certificates so that they have the same legal value as paper documents.

Then, the NIS Directive (EU) 2016/1148 of 6 July laid down the requirements to be met by (i) operators of services designated as 'essential' by the member states (banks, energy companies, etc) and (ii) digital service providers (platforms, cloud service providers, etc). In particular, these companies will have to take appropriate measures to prevent risks, mitigate the impact of any incidents and notify the relevant authorities of those that have 'an actual adverse effect on the security of network and information systems'.

Finally, on 8 December 2016, the French cybersecurity watchdog (ANSSI) published a security standard applicable to cloud service providers and called 'SecNumCloud'. For their security system to achieve 'Essential Level' certification (which is the minimum certification level, an 'Advanced Level' is soon to be published), cloud service providers will have to meet access control, identity management, encryption, operational security and incident management requirements. In particular, they will be required to host and process data within the European Union.

The GDPR

The General Data Protection Regulation No. 2016/679 of 27 April 2016 (GDPR), replacing the 1995 Directive as of 25 May 2018, will dramatically reshape the rules governing the protection of personal data in the European Union.

On the one hand, it has increased the rights of individual data subjects, in particular by introducing the rights to data portability and erasure, and by establishing special protections for minors. On the other hand, it has simplified administrative procedures for controllers by drastically reducing filing requirements and, for controllers active in several EU countries, by introducing a 'one-stop shop' whereby such controllers only need to directly deal with a single national supervisory authority.

In exchange for the simplification of administrative formalities, the regulation encourages the sector to regulate itself and imposes new obligations on businesses ('privacy by design', accountability, reporting security breaches, direct liability of data processors, etc).

European lawmakers have made data protection more effective in several ways. First, violators of the GDPR may face fines of up to 4 per cent of their worldwide revenue. Second, data subjects will have enhanced means to enforce their rights. Finally, the territorial scope of the GDPR will be much wider: beyond the existing criterion (any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union), it will also apply to any processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to (i) the offering of goods or services to such data subjects in the Union, whether or not a payment is required ('targeting'); or (ii) the monitoring of their behaviour provided it takes place within the Union ('monitoring') (more information on the extraterritorial application of the data privacy laws can be found in question 31).

The e-Privacy Regulation

Assuming the current draft e-Privacy Regulation will be adopted as is, it will lead to several changes regarding communication data and the use of cookies. It would enter into force on the same day as the GDPR (25 May 2018). One of the main expected changes is the scope of the regulation. In the future, all communication services and terminal equipment would be subject to the obligation related to users' privacy such as for instance, over-the-top services (Whatsapp, Skype, Facebook Messenger, etc).

As regards communication data, the regulation distinguishes metadata from communication content. Metadata can only be processed with the user's consent or if it is necessary (i) to meet mandatory quality of service requirements, (ii) for a billing purpose, or (iii) for detecting and stopping fraudulent or abusive use of electronic communications. The communication content may be processed only (i) for the provision of specific content, (ii) when the user has given his or her consent to the processing, and (iii) the provision of the service cannot be fulfilled without the processing of such content. All these data must be erased or made anonymous as soon as they are no longer needed for the purpose of the transmission or after the period during which a bill may be lawfully challenged.

The control of cookies will be eased by the regulation. Whereas today, consent to use of cookies is obtained by means of banners, under the ePrivacy Regulation service providers will merely need to give users the option, via web browser settings, to prevent the placement of cookies on their terminal devices. This choice must be renewed every six months and the user must have the possibility to withdraw his or her consent at any time.

Finally, the regulation contains provisions concerning direct marketing that are already in force in France: opt-in is the principle, but opt-out will be sufficient for direct marketing if (i) the users are informed of the use made of their data at the time of their collection, and (ii) the marketing concerns only products or services similar to those already provided by the marketer.

the assignment to the transferee without the express consent of the licensor; and

- regarding personal data transfers, notably when the transferee is established outside the European Union, the data protection legal framework may also challenge the realisation of the operation.

Particular care should be given to the drafting of the outsourcing contract. The following elements must notably be taken into consideration: the definition of the concerned services; the definition of expected service levels; the definition of liabilities that may be incurred and indemnities; and the applicable law and jurisdiction in case of dispute.

For international outsourcing deals, careful tax planning is necessary to reduce the tax burden resulting from the VAT and withholding tax rules.

46 What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?

Article L 1224-1 of the French Labour Code has often been applied to outsourcing transactions. This legal provision, as interpreted by the French courts, provides that in the event of the transfer of an 'autonomous economic entity having conserved its identity', all the work contracts of the employees dedicated to that activity are automatically transferred to the transferee. This is the case if the transferred activity constitutes 'an organised grouping of persons and tangible or intangible property permitting the exercise of an economic activity that pursues its own objectives'. These broad principles have been applied in a rather inconsistent manner by the French courts. The new employer can only change the terms and conditions of employment of transferred

contracts for necessary reasons. In case of modification of the contractual conditions, an employee is entitled to challenge the employer for unfair dismissal when the modification cannot be justified.

Any outsourcing transaction by a French company that has an impact on the organisation of the work force or on employment requires prior consultation of the works councils and the health and safety committees.

Online publishing

47 When would a website provider be liable for mistakes in information that it provides online? Can it avoid liability?

The applicable regime depends on the website provider's exact role in the publication of the content. If it supervises or edits the content, it may be classified as a publisher and, as such, would be liable for mistakes in information that it provides. If the website provider acts simply as a hosting service provider, it would benefit from the limited liability regime set out by the Digital Economy Law (see question 20).

The Digital Economy Law requires publishers to nominate a publication manager, who is liable for press infractions committed through the provision of information on the website. However, Law No. 2009-669 of 13 June 2009 in favour of the diffusion and the protection of creation on the internet limits the liability of the publication manager for content posted by users on the website: the publication manager will only be liable if he or she was actually aware of the illicit character of the content or if he or she did not take down the illicit content promptly after becoming aware of its illicit character.

The website provider can also provide limitations of liability for mistakes in information published on the website in the website user agreement.

48 If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?

The French Intellectual Property Code defines databases as collections of independent works, data or other materials arranged in a systematic or methodical way and capable of being individually accessed by electronic or any other means. The database's author enjoys copyright on its creation if the database satisfies the condition of originality. The author can prohibit reuse or representation of his or her creation under specific conditions common to any intellectual creation.

The database's producer also benefits from a sui generis right if it justifies substantial investments in the creation of the database. Thus, the producer can prohibit the extraction of all or a substantial part, qualitatively or quantitatively, of the contents of a database and the reuse, by making available to the public all or a substantial part, qualitatively or quantitatively, of the contents of a database.

Moreover, the CJEU has recently held that the creator of a database who is not protected by copyright, due to lack of originality, nor by the sui generis right of a producer, failing to prove substantial investment, could set contractual limits to its commercial use by third parties (*Ryanair*, C-30/14, 15 January 2015).

FRANKLIN LAW FIRM

Bradley Joslove **bjoslove@franklin-paris.com**

26 Avenue Kléber
75116 Paris
France

Tel: +33 1 45 02 79 00
Fax: +33 1 45 02 79 01
www.franklin-paris.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

e-Commerce
ISSN 1473-0065

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law