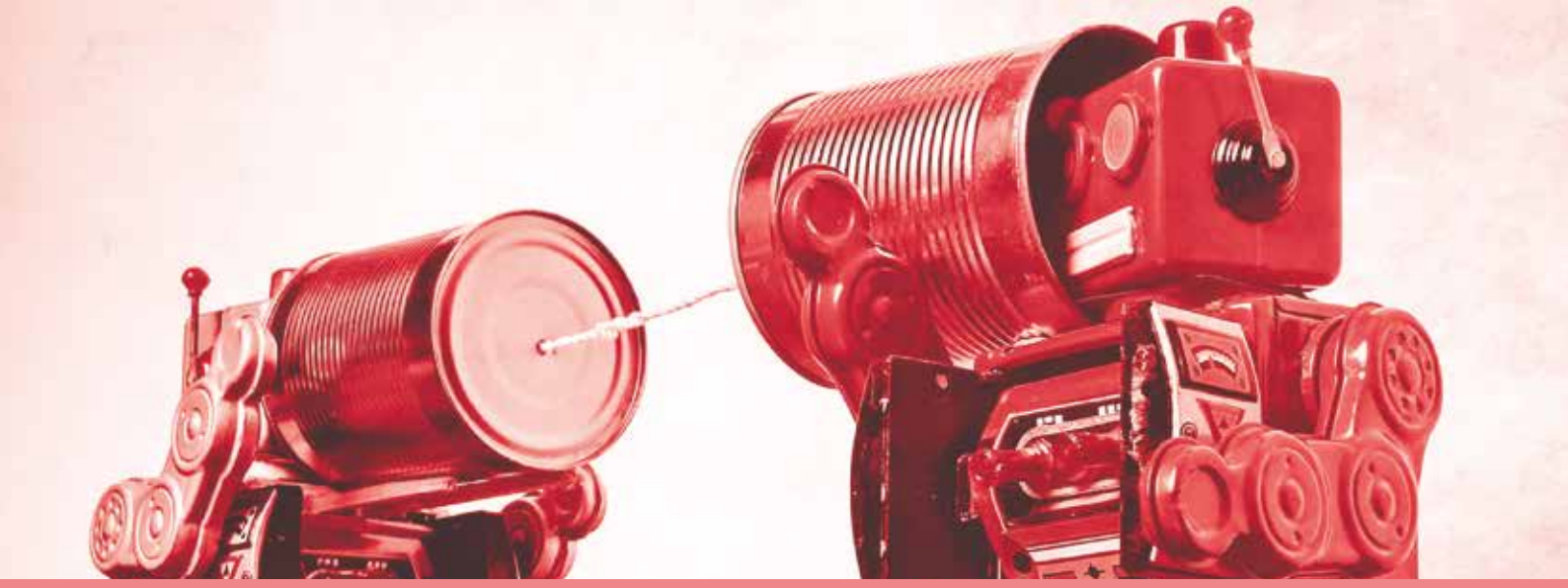

ICLG

The International Comparative Legal Guide to:

Telecoms, Media & Internet Laws & Regulations 2019

12th Edition

A practical cross-border insight into telecoms, media and internet laws and regulations

Published by Global Legal Group, with contributions from:

Arioli Law
Arnold & Porter
Ashurst Hong Kong
Attorneys-at-Law TRUST
Bagus Enrico & Partners
BEHRING
Bello, Gallardo, Bonequi y Garcia, S.C.
BTG Legal
Cairn Legal
CMS (UAE) LLP
D'LIGHT Law Group
Drew & Napier LLC
Fasken
Focaccia, Amaral, Pellon & Lamônica Advogados
Jingtian & Gongcheng
Kahale Abogados
Kalema Legal & Associates
Khaitan & Co
Mazanti-Andersen Korsø Jensen
MinterEllison
Monereo Meyer Abogados
Mori Hamada & Matsumoto
Nikolinakos – Lardas & Partners LLP
Pinsent Masons Germany LLP
Portolano Cavallo
Preiskel & Co LLP
Rato, Ling, Lei & Cortés – Advogados
RIAA Barker Gillette
Shearn Delamore & Co.
Tilleke & Gibbins
Ünsal Gündüz Attorneys at Law
Wilkinson Barker Knauer, LLP

MEF MOBILE ECOSYSTEM FORUM
glg global legal group

global legal group

Contributing Editor
Rob Bratby, Arnold & Porter

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Amy Norton

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Stephens & George
Print Group
November 2018

ISBN 978-1-912509-45-4
ISSN 2050-7607

Strategic Partners

General Chapters:

1	**European Digital Single Market: A Year in Review** – Rob Bratby, Arnold & Porter	1
2	**Re-Thinking Regulation** – Tim Cowen & Daniel Preiskel, Preiskel & Co LLP	4
3	**Liable *vs.* Accountable: How Criminal Use of Online Platforms and Social Media poses Challenges to Intermediary Protection in India** – Vikram Jeet Singh & Prashant Mara, BTG Legal	7

Country Question and Answer Chapters:

4	**Argentina**	Kahale Abogados: Roxana M. Kahale	10
5	**Australia**	MinterEllison: Anthony Borgese & Athena Chambers	16
6	**Belgium**	Cairn Legal: Guillaume Rue & Frédéric Paque	26
7	**Brazil**	Focaccia, Amaral, Pellon & Lamônica Advogados: Rafael Pellon	36
8	**Canada**	Fasken: Laurence J. E. Dunbar & Scott Prescott	43
9	**China**	Jingtian & Gongcheng: Chen Jinjin & Hu Ke	51
10	**Congo – D.R.**	Kalema Legal & Associates: Fulgence Kalema Bwatunda & Gabson Mukendi Kabuya	61
11	**Denmark**	Mazanti-Andersen Korsø Jensen: Hans Abildstrøm	68
12	**Finland**	Attorneys-at-Law TRUST: Jan Lindberg & Terhi Rekilä	75
13	**France**	BEHRING: Anne-Solène Gay	83
14	**Germany**	Pinsent Masons Germany LLP: Dr. Florian von Baum & Dr. Igor Barabash	94
15	**Greece**	Nikolinakos – Lardas & Partners LLP: Dr. Nikos Th. Nikolinakos & Dina Th. Kouvelou	104
16	**Hong Kong**	Ashurst Hong Kong: Joshua Cole & Hoi Tak Leung	115
17	**India**	Khaitan & Co: Harsh Walia	125
18	**Indonesia**	Bagus Enrico & Partners: Enrico Iskandar & Bimo Harimahesa	133
19	**Italy**	Portolano Cavallo: Ernesto Apa & Eleonora Curreli	141
20	**Japan**	Mori Hamada & Matsumoto: Hiromi Hayashi & Akira Marumo	149
21	**Korea**	D'LIGHT Law Group: Won H. Cho & Hye In Lee	157
22	**Macau**	Rato, Ling, Lei & Cortés – Advogados: Pedro Cortés & José Filipe Salreta	166
23	**Malaysia**	Shearn Delamore & Co.: Janet Toh	178
24	**Mexico**	Bello, Gallardo, Bonequi y Garcia, S.C.: Carlos Arturo Bello Hernández & Bernardo Martínez García	188
25	**Pakistan**	RIAA Barker Gillette: Mustafa Munir Ahmed & Shahrukh Iftikhar	198
26	**Singapore**	Drew & Napier LLC: Lim Chong Kin & Shawn Ting	209
27	**Spain**	Monereo Meyer Abogados: Consuelo Álvarez & Christian Krause	219
28	**Switzerland**	Arioli Law: Martina Arioli & Antonio Bernasconi	228
29	**Thailand**	Tilleke & Gibbins: David Duncan	235
30	**Turkey**	Ünsal Gündüz Attorneys at Law: Burçak Ünsal & Dr. Okan Gündüz	242
31	**United Arab Emirates**	CMS (UAE) LLP : Rob Flaws & Rachel Armstrong	250
32	**United Kingdom**	Arnold & Porter: Rob Bratby	256
33	**USA**	Wilkinson Barker Knauer, LLP: Brian W. Murray & Rachel S. Wolkowitz	263
34	**Vietnam**	Tilleke & Gibbins: Tu Ngoc Trinh & Waewpen Piemwichai	272

France

BEHRING

Anne-Solène Gay

1 Overview

1.1 Please describe the: (a) telecoms, including internet; and (b) audio-visual media distribution sectors in your jurisdiction, in particular by reference to each sector's: (i) annual revenue; and (ii) 3–5 most significant market participants.

According to the French Federation of Telecom Operators, in 2016, the telecommunications sector generated €40bn (*i.e.*, 1.8% of GDP) and the audio-visual media distribution sector generated €9bn (*i.e.*, 0.4% of GDP). The digital economy as a whole is estimated to have generated €75bn (*i.e.*, 3.4% of GDP).

Based on the ARCEP's (Electronic Communications and Postal Regulatory Authority, *Autorité de Régulation des Communications Electroniques et des Postes*) last annual report, the electronic communications services' retail market generated a €36.2bn turnover in 2017, and telecom operators employed about 112,700 people at the end of the year. Without including the price of spectrum acquisition, in 2017, investments made by telecom operators reached an historical record of €9.6bn as a result of a 7.5% increase from the previous year.

The main players in the telecom market are Orange (France Telecom), SFR (Altice), Bouygues Telecom and Free (Iliad).

The Internet infrastructure sector is controlled by the above-mentioned telecom operators, but OVH has developed successfully as a pure player in this segment.

The prevailing companies in the audio-visual media distribution sector are France Televisions, TF1, M6 and Canal+.

It should be noted that the audio-visual distribution sector is facing the emergence of new players, offering streaming and video on-demand services, such as Netflix or OCS (owned by Orange and Canal+). In the future, these new players may compete with the most significant market participants.

1.2 List the most important legislation which applies to the: (a) telecoms, including internet; and (b) audio-visual media distribution sectors in your jurisdiction.

The operation of electronic communications networks and the provision of electronic communications services are governed by the Postal and Electronic Communications Code (*Code des Postes et des Communications Electroniques – CPCE*), which was mainly based on the provisions of Law n°96-659 of 26 July 1996 regulating telecommunications, and then amended and notably enriched by Law n°2004-669 of 9 July 2004 on electronic communications, which transposed the new EU regulatory framework of 2002 ("Telecoms Package") into French law.

More recently, the telecom sector was impacted by the adoption of the following texts:

- Ordinance n°2014-329 of 12 March 2014 on the Digital Economy which restored the ARCEP's power to sanction following the French Constitutional Council ruling, which considered the previous provisions to be unconstitutional (Constitutional Council, Decision n°2013-331 QPC of 5 July 2013).
- Law n°2015-912 of 24 July 2015, relating to intelligence services which organise the control of technologies used by said services.
- Law n°2015-990 of 6 August 2015, to promote the economic growth, activity and equity economic opportunity (*Loi Macron*), includes provisions regarding electronic communications operators and Internet players.
- European Regulation 2015/2120 of 25 November 2015, laying down measures concerning open Internet access and roaming on public mobile communication networks, entered into force on 30 April 2016.

In 2016, France passed Law n°2016-1361 of 7 October 2016 for a "Digital Republic", which significantly impacted the French digital economy. This Law aims to strengthen consumer confidence in the Internet. It is also meant to increase competition between service providers by lowering entry barriers, notably by organising data portability. It also gives the telecom regulator the authority to oversee net neutrality and open Internet access.

Law n°86-1067 of 30 September 1986 on Freedom to Communicate forms the basis of audio-visual media distribution regulation. It was subsequently amended, notably by Law n°2004-669 of 9 July 2004 relating to electronic communication and audio-visual communications services, which expanded the objectives and strengthened the powers of the broadcasting authority, reviewed the broadcasting licensing regime and softened the anti-concentration provisions, and by Law n°2013-1028 of 15 November 2013, relating to the independence of French public service broadcasting.

General privacy and data protection rules are set by Law n°78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties, as subsequently amended by Law n°2004-801 of 6 August 2004 to implement the EU Directive of 24 October 1995, and more recently by Law n°2018-493 of 20 June 2018 relating to the protection of personal data. The said Law is the result of the implementation of the GDPR. Decree n°2018-687 adopted on 1 August 2018 is the last step for the complete transposition of the GDPR within the French legal system.

The Internet is more specifically governed by Law n°2009-669 of 12 June 2009 favouring the diffusion and protection of artistic creation on the Internet, which adapted for the Internet the standard legal protection of copyright for literary and artistic works set in the Intellectual Property Code, and by Law n°2004-575 of 21 June 2004 regarding Confidence in the Digital Economy ("*LCEN*").

1.3 List the government ministries, regulators, other agencies and major industry self-regulatory bodies which have a role in the regulation of the: (a) telecoms, including internet; and (b) audio-visual media distribution sectors in your jurisdiction.

The ARCEP is the independent government agency that oversees the electronic communications and postal services sector.

The Broadcasting Authority (*Conseil Supérieur de l'Audiovisuel – CSA*) is the state agency responsible for the audio-visual media distribution sector.

The question of whether to merge these two authorities was regularly discussed. However, this merger project has been ruled out for now in favour of closer cooperation.

The National Frequencies Agency (*Agence Nationale des Fréquences – ANFR*) ensures the planning, management and control of the use, including for private use, of the public domain radio frequencies. As such, the agency is in charge of allocating frequency bands to the ARCEP and the CSA for their allocation, respectively, to the telecom and broadcasting operators.

The Data Protection Authority (*Commission National de l'Informatique et des Libertés – CNIL*) controls automatic personal data processing and ensures the protection of personal data.

The High Authority for the Distribution of Works and the Protection of Copyright on the Internet (*Haute Autorité pour la diffusion des oeuvres et la protection des droits – HADOPI*) is dedicated to the protection of intellectual property rights on the Internet. HADOPI has been much challenged since it was created in 2009. Its dissolution is regularly under discussion, but the decision keeps being postponed.

The Competition Authority (*Autorité de la Concurrence – AdlC*) also plays a major role in the TMT sectors in the enforcement of general competition rules, and is notably in charge of sanctioning anticompetitive practices and controlling merger operations.

The government also plays an active part in the telecom, media and Internet sectors through the Ministry of Economy and Finance, notably the General Directorate for Competition Policy, Consumer Affairs and Fraud Control (*Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes – DGCCRF*), as well as through the *Secrétaire d'Etat* for the Digital Sector under the authority of the Minister of Economy and Finance, and through the Ministry of Culture and Communication, and notably the Department of Media and of Cultural Industries (*Direction Générale des Médias et des Industries Culturelles – DGMIC*).

1.4 In relation to the: (a) telecoms, including internet; and (b) audio-visual media distribution sectors: (i) have they been liberalised?; and (ii) are they open to foreign investment?

The telecoms and media distribution sectors are liberalised. By exception, the audio-visual media distribution market is subject to specific ownership restrictions designed to preserve media pluralism and competition. These restrictions prevent any single individual or legal entity from holding, directly or indirectly, more than 49% of the capital or the voting rights of a company that has an authorisation to provide a national terrestrial television service, where the average audience for television services (either digital or analogue) exceeds 8%. In addition, it is forbidden for any single individual or legal entity that already holds a national terrestrial television service, where the average audience for this service exceeds 8%, to, directly or indirectly, hold more than 33% of the capital or voting rights of a company that has an authorisation to provide a local terrestrial television service.

Law n°2004-1343 of 9 December 2004 and Decree n°2005-1739 of 30 December 2005, which introduced new articles L.151-1 *et seq.* and R.153-1 *et seq.* in the Monetary and Financial Code, establishes that there are no restrictions on foreign ownership and investment in France.

However, if all restrictions have in principle been lifted, foreign investment in business sectors considered to be "sensitive" still requires prior authorisation. In accordance with article L.151-1 *et seq.* and article R.153-1 *et seq.* of the Monetary and Financial Code, the investor must submit a formal application to the French Ministry of Economy for prior authorisation. This authorisation is provided within two months from when the application is received by the French Ministry of Economy (a tacit agreement is assumed if no reply is received).

These restrictions apply when a foreign (EU or non-EU) investment is made in a strategic sector. Decree n°2014-479 of 14 May 2014 has expanded the list of sectors in which foreign investors must seek prior authorisation by the French Ministry of Economy. The list is broader for non-EU/EEA countries' investors than for EU or EEA Member States' investors, and now includes, for the latter type, activities deemed crucial to France's national interests (*i.e.*, relating to public order, public security and national defence), encryption and decryption, communications interception and activities relating to integrity, security and continuity of electronic communication services and networks.

Any transaction concluded in violation of these rules is null and void, and the investor is subject to criminal sanctions (five years' imprisonment and a fine amounting to twice the amount of the transaction).

Further, regulation also provides for specific restrictions on foreign investments in the media sector. Unless otherwise agreed in international agreements, a foreign investor may not acquire shares in a company holding a licence for a radio or television service in France and that uses radio frequencies, if this acquisition has directly or indirectly the effect of raising the share of capital or voting rights owned by foreign nationals to more than 20%.

2 Telecoms

General

2.1 Is your jurisdiction a member of the World Trade Organisation? Has your jurisdiction made commitments under the GATS regarding telecommunications and has your jurisdiction adopted and implemented the telecoms reference paper?

France has been a World Trade Organisation (WTO) member and a member of GATT since 1 January 1995. It is a Member State of the European Union and all EU Member States are WTO members, as is the EU in its own right.

The EU has made commitments regarding telecommunications relating to unfair competitive practices, interconnection, universal service, licences and the allocation of scarce resources (notably in the document entitled "GATS/SC/31.Suppl3").

The principles of the WTO telecoms reference paper have been implemented under French law.

2.2 How is the provision of telecoms (or electronic communications) networks and services regulated?

Telecoms activities are regulated under the CPCE.

The operation of public networks and the provision of electronic communication services to the public are subject to prior notification to the ARCEP. However, the use of radio frequencies and numbering resources is based on an authorisation regime, and therefore requires an individual licence to be granted by the ARCEP.

2.3 Who are the regulatory and competition law authorities in your jurisdiction? How are their roles differentiated? Are they independent from the government?

The telecom regulator ARCEP is in charge of the regulation of the postal and electronic communications sectors. It ensures the implementation of a universal service, defines *ex ante* regulations applicable to operators that have a significant market power on certain defined markets, is involved in defining the regulatory framework, allocates scare resources (radio spectrum and numbering), imposes sanctions in case of infringement of the sector-specific regulations, and settles disputes arising between operators.

The Competition Authority AdlC enforces general competition rules. It is the result of Law n°2008-776 of 4 August 2008 on the modernisation of the economy (*LME*), passed on 4 August 2008, which transformed the *Conseil de la Concurrence* into a new *Autorité de la Concurrence*. This reform created a single agency with strengthened powers and means. The Competition Authority carries out all activities of competition regulation (inquiries, antitrust activities, merger control, publication of opinions and recommendations).

The two authorities interact frequently, as each can solicit the other's opinion on the subjects of its competence. For example, when conducting market analysis to identify operators with significant market power in a relevant market, the ARCEP must solicit the opinion of the Competition Authority.

Also, both authorities provide opinions to the government.

The ARCEP and the Competition Authority are state agencies, but are independent from the government; this independence is statutory.

Alongside the ARCEP and the AdlC, the ANFR is a specialised regulatory body dedicated to spectrum management, as it is a scarce resource. It especially interacts with the ARCEP for spectrum matters, such as, for instance, 450 MHz PMR applications or LTE. The ANFR is in charge of the national spectrum plan and has the ability to negotiate at the CEPT and ITU level on behalf of the French government (see *infra* question 3).

2.4 Are decisions of the national regulatory authority able to be appealed? If so, to which court or body, and on what basis?

The ARCEP's administrative decisions are enforceable but can be appealed before the Administrative Supreme Court (*Conseil d'Etat*) for decisions made by the Executive Board, or before the Paris Administrative Court (*Tribunal Administratif de Paris*) for decisions made by the Chairman under his own powers.

The ARCEP's arbitration decisions relating to disputes can be appealed before the Court of Appeal of Paris (*Cour d'appel de Paris*). The chamber of Court specialised in regulation and competition litigation can cancel, confirm or amend the ARCEP's arbitration decisions. The decision of the Court of Appeal can be challenged before the Judicial Supreme Court (*Cour de cassation*).

Licences and Authorisations

2.5 What types of general and individual authorisations are used in your jurisdiction?

The French telecommunication sector is based on a general authorisation regime. According to article L.33-1 of the CPCE, the establishment and operation of networks open to the public and the provision of electronic communications services to the public are free, subject to prior notification to the ARCEP by filling in a form available on its website. No notification is required for the establishment and operation of internal or independent (dedicated Closed User Groups) networks.

Based on Law n°2015-990 of 6 August 2015 to promote economic growth, activity and economic opportunity (*Loi Macron*), the ARCEP is now entitled to force any actor which has infringed the notification obligation to compulsorily declare itself to the ARCEP.

By abrogating section VII of article 45 of Law n°86-1317 of 30 December 1986 (Finance Law for year 1987), article 27 of Law n°2015-1785 of 29 December 2015 (Finance Law for year 2016) withdrew provisions relating to the administrative tax owed by operators to the ARCEP.

Operators have to contribute to the financing of universal service. To this end, every year they have to declare their turnover of the previous year after deduction of access and interconnection revenues (article L.35-3 of the CPCE) and after deduction of €100 million (article R.20-39 of the CPCE).

The use of scarce resources (frequency and numbering) is subject to an individual authorisation, the number of which can be limited by the ARCEP and which can be granted through competitive procedures.

A bill is currently under review by the Parliament to supress the prior notification requirement.

2.6 Please summarise the main requirements of your jurisdiction's general authorisation.

The general authorisation to establish and operate networks open to the public and to provide electronic communications to the public is subject to a prior notification to the ARCEP, which is now completed online. Following the ARCEP's receipt of such notification, the applicant is eligible for certain rights and is bound by various obligations. The main requirements associated with the general authorisation are as follows:

- compliance to standards and specifications for the networks and services offered;
- quality and availability;
- compliance with regulations in respect of health and the environment, and occupation of the public domain;
- sharing of infrastructure and local roaming;
- interconnection and access;
- contribution to universal service and payment of taxes;
- compliance with public order and national defence imperatives;
- confidentiality and neutrality in respect of transmitted communications; and
- payment of an annual administration fee.

2.7 In relation to individual authorisations, please identify their subject matter, duration and ability to be transferred or traded. Are there restrictions on the change of control of the licensee?

Individual authorisations relate to the use of radio frequencies or numbering resources. The allocation decision defines the usage conditions, in particular the authorisation's duration. According to article L.42-1 (for spectrum) and article L.44 (for numbering resources) of the CPCE, their duration cannot exceed 20 years.

GSM mobile operators' licences were initially awarded for a period of 15 years, and were renewed in 2006 for the same duration. In June 2010, UMTS licences were granted for 20 years and, in December 2015, 700 MHz spectrum was allocated for 15 years.

Individual authorisations can be transferred subject to the transfer having received the ARCEP's approval (for spectrum allocated through a competitive procedure or used for a public service mission), or if the transfer was declared to the ARCEP (for spectrum allocated based on the rule of "first come, first served"). The ARCEP must take a decision within three months in the first case and within six weeks in the second case. In case of spectrum assignment, the benefiting operator has to fulfil all conditions imposed on the operator initially holding the licence, and take responsibility for all the commitments contracted by the former operator.

By way of derogation, certain frequencies can be assigned on the secondary market (see *infra* question 3.6).

Public and Private Works

2.8 Are there specific legal or administrative provisions dealing with access and/or securing or enforcing rights to public and private land in order to install telecommunications infrastructure?

According to article L.45-9 of the CPCE, public network operators have a right of way on public land roads and on public networks that are part of the public domain (for example, underground pipes), except for electronic and communications networks and infrastructure. This right is granted by a unilateral administrative authorisation (*permission de voirie*) provided by the public authority in charge of the public land in question.

Regarding other parts of public land, operators have to negotiate a right of way and to enter into a contract (*convention d'occupation du domaine public*) with the public authority in charge of the public land in question.

Public land occupation can give rise to the payment of fees that are capped by a decree. The competent authority will take a decision within two months from the request.

The competent authority is the authority in charge of managing the public land in question, *i.e.*, either the one which owns such public land or the one to which the management of such public land has been delegated (*i.e.*, another public entity or a private entity such as a concessionaire for, *e.g.*, highways).

Regarding private land occupation, operators of networks opened to the public benefit from easements on private properties, allowing network installation and operation.

Access and Interconnection

2.9 How is wholesale interconnection and access mandated? How are wholesale interconnection or access disputes resolved?

Public network operators have the obligation to negotiate with all other public network operators requesting access and interconnection. Operators are free in their negotiation on this subject. Access can only be refused if justified.

Technical and financial conditions of interconnection and access are agreed upon between the two operators and formalised by a private law agreement which may be transmitted to the ARCEP, upon request.

In case of dispute, the ARCEP can impose interconnection and access conditions on objective, transparent, non-discriminatory and proportionate grounds.

In accordance with article L.36-8 of the CPCE, the ARCEP has the competence to settle disputes in case of refusal of access or interconnection, failure of commercial negotiations, or disagreement on the conclusion or execution of an access or interconnection agreement to an electronic communications network.

The ARCEP has to render its decision within a maximum of six months from the referral by a declared operator and define the fair technical and tariff conditions for access and interconnection. In case of emergency, the ARCEP is entitled to adopt interim measures.

The ARCEP's decisions can be appealed before the Paris Court of Appeal.

2.10 Which operators are required to publish their standard interconnection contracts and/or prices?

Operators that are designated as having significant market power (SMP) in a specific market are required to publish a standard interconnection offer. The ARCEP conducts rounds of market analysis and then decides for each relevant market which operators have SMP. Currently, the fifth round of market analysis is valid until 2020.

2.11 Looking at fixed, mobile and other services, are charges for interconnection (e.g. switched services) and/or network access (e.g. wholesale leased lines) subject to price or cost regulation and, if so, how?

Only the charges for interconnection or network access of SMP operators can be subject to a price or cost regulation. The ARCEP conducts analysis of the markets and can impose various obligations on SMP operators, including cost-orientation of their tariffs regarding selected relevant markets, based on a long-run incremental cost model.

2.12 Are any operators subject to: (a) accounting separation; (b) functional separation; and/or (c) legal separation?

a) In France, the first accounting separation of France Telecom was set up by the regulatory authority from the opening of competition. It was broadened in 2006 by the ARCEP's Decision n°06-1007, further to the implementation of the new regulatory framework.

It requires France Telecom, now Orange, to distinguish, from an accounting point of view, its various activities in

accordance with the segmentation of the relevant markets and to make sure that its retail activities are consistent with the wholesale offers it produces, in conditions equivalent to those granted to alternative operators when they position themselves in the retail markets. This supply leans in particular on the formalisation of internal transfer protocols on which the regulator can exercise control.

b) In March 2011, the Competition Authority invited the ARCEP to begin preparatory work related to the possible functional unbundling of monopolistic activities of France Telecom from competitive activities, but the project was put aside.

c) No operator has been required to separate parts of its business into separate legal entities.

2.13 Describe the regulation applicable to high-speed broadband networks. On what terms are passive infrastructure (ducts and poles), copper networks, cable TV and/or fibre networks required to be made available? Are there any incentives or 'regulatory holidays'?

The regulatory framework considers high-speed and very high-speed broadband networks on a different basis.

- High-speed broadband networks are copper-based and therefore regulated through the unbundling of the local loop which belongs to Orange, as the incumbent operator. Ducts and related infrastructure are regulated by the ARCEP's decision n°2017-1488, adopted on 14 December 2017. Also, decision n°2017-1570 of 21 December 2017 is currently regulating tariffs until 2020.
- Very high-speed broadband networks are fibre-based, as the regulatory framework especially emphasises FTTH technology. The ARCEP therefore adopted a series of decisions setting up a nationwide roll-out plan dividing the territory into denser areas and less dense areas (*zones très denses – ZTD* and *zones moins denses – ZMD*). Decision n°2009-1106 of 22 December 2009 is the main regulation for both areas.

The incumbent operator is the only one with a copper local loop, and is subject to an obligation to give access to its local loop in the technical and tariff conditions defined in its reference offer, issued annually under the control of the ARCEP.

Cable operators are not subject to a local loop access obligation.

Regarding access to passive infrastructure and for very high-speed broadband, the CPCE sets forth specific rules. According to article L.34-8-2-1, infrastructure managers should grant access to any operator of very high-speed broadband networks formulating a reasonable request. Access conditions, especially financial, must be fair and reasonable, as the infrastructure manager shall cover its expenses. On the other hand, the access request can be denied only upon special motives, such as lack of capacity or national security.

Cable TV still has a hybrid regulatory status between telecommunications and media regulations.

There are no regulatory holidays for infrastructure access. However, where private initiative is not sustainable, the local government Code (*Code Général des Collectivités Territoriales – CGCT*) authorises local public entities to operate networks, under article L.14215-1.

Price and Consumer Regulation

2.14 Are retail price controls imposed on any operator in relation to fixed, mobile, or other services?

Universal service is the only service in which retail prices can be controlled. CPCE provisions require an operator to be designated as a universal service provider. Among specific obligations such as quality of service, universal service is based on solidarity. Therefore, the designated provider of universal service must offer adapted retail prices as specified in regulations. The current provider of universal service is Orange, as per an order of 2017 (*Arrêté du 27 november 2017 portant designation de l'opérateur chargé de fournir les prestations "raccordement" et "service téléphonique" de la composante du service universel prévue au 1° de l'article L.35-1 du CPCE*).

2.15 Is the provision of electronic communications services to consumers subject to any special rules (such as universal service) and if so, in what principal respects?

The Consumer Code sets a certain number of rules specific to the provision of electronic communication services to consumers (including the information obligation, minimum commitment period, reimbursement of advances and deposits) which were reinforced over time, notably by Law n°2008-3 of 3 January 2008 on competition and consumer protection (*Loi Chatel*), according to which technical assistance and customer care services cannot be premium-rated and the waiting time for connect-calls to those services should be free-of-charge, and which also sets strict rules regarding cancellation fees, notice periods for termination and maximum contract duration.

The CPCE also organises specific protection such as the right to be listed or not in directories, and the right to a detailed invoice.

The Commission of Unfair Clauses regularly declares abusive clauses contained in the operators' general conditions.

More recently, Law n°2014-344 of 17 March 2014 (*Loi Hamon*) also affected the telecom sector, by setting limits to phone marketing and specific rules regarding portability, billing, information on value-added services, etc.

Numbering

2.16 How are telephone numbers and network identifying codes allocated and by whom?

The operators ask the ARCEP to award them numbering resources based on the National Numbering Plan (such as prefixes, short numbers and blocks of numbers) according to their needs. These operators can reserve such numbering resources, which are then given to each customer of the operator. In case of scarcity, the ARCEP may decide to limit the number of licences and to implement a call for the tender procedure. In case of absence of scarcity, the "first come, first served" rule applies.

2.17 Are there any special rules which govern the use of telephone numbers?

The ARCEP defines, manages and controls the National Numbering Plan, which awards the various types of numbers to the electronic communications services (fixed-line, mobile, and value-added services). The National Numbering Plan was reviewed in 2018 (decision n°2018-0881), which notably unified the existing regulations and set tighter restrictions on the use of numbering resources.

2.18 Are there any obligations requiring number portability?

Each operator has to answer to a portability request from a customer wishing to subscribe to an offer from another operator within a maximum of three working days for mobile phone operators (except for overseas territories). It is also a maximum of three working days for fixed operators (seven working days for the B2B segment).

3 Radio Spectrum

3.1 What authority regulates spectrum use?

Spectrum use is regulated by the ANFR which manages and provides spectrum resources for services (broadcasting, electronic communications services, defence, etc.).

The frequency bands assigned to these services are respectively awarded to the operators by the ARCEP and the CSA.

3.2 How is the use of radio spectrum authorised in your jurisdiction? What procedures are used to allocate spectrum between candidates – i.e. spectrum auctions, comparative 'beauty parades', etc.?

Frequency allocation depends on the nature of the frequencies. Pursuant to article L.42-2 of the CPCE, in case of scarcity, the ARCEP may decide to limit the number of licences and to implement a call for the tender procedure (comparative submission or auctioning). In case of absence of scarcity, the "first come, first served" rule applies.

3.3 Can the use of spectrum be made licence-exempt? If so, under what conditions?

In general, the use of frequencies requires an allocation decision issued by the ARCEP. Nevertheless, certain frequencies are exempted from authorisation of use, but have no guarantee against interference. This is notably the case of spectrum used by low power and small-range systems such as RFID, WiFi frequencies, anti-intrusion alarms, medical devices, etc.

The ARCEP can also decide, within the framework of an experimental procedure, to temporarily exempt certain technologies from frequencies authorisation of use.

The ARCEP also recently launched a regulatory "sandbox" which has the purpose of allowing companies to experiment with innovative services and applications in a lightened framework, particularly for spectrum licences.

3.4 If licence or other authorisation fees are payable for the use of radio frequency spectrum, how are these applied and calculated?

As spectrum is part of the public domain, the use of radio frequency spectrum gives rise to the payment of a fee, the amount of which is set by a ministerial decree, or by the allocation decision according to the frequency band used and the operator's expected profitability resulting from this use.

3.5 What happens to spectrum licences if there is a change of control of the licensee?

Any change of control must be declared to the ARCEP in order to allow it to verify that the conditions under which the spectrum licence was initially awarded are still respected.

3.6 Are spectrum licences able to be assigned, traded or sub-licensed and, if so, on what conditions?

This depends on the type of frequencies.

The transfer of spectrum licences is subject either to notification to the ARCEP, which may oppose it, or, when frequencies are used for public service missions or were granted within the framework of a selection process, to the prior approval of the ARCEP.

Ordinance n°2011-1012 of 24 August 2011 introduced a greater flexibility in spectrum assignment by giving the operators the ability to trade frequency licences on the secondary market. The list of frequency bands which can be traded was set by the Ministerial Order of 11 August 2006, pursuant to article L.42-3 of the CPCE and Decree n°2006-116 of 11 August 2006. The spectrum licence holder may transfer all of its rights and obligations to a third party for the entire remainder of the licence (full transfer), or only a portion of its rights and obligations (geographical region or frequencies).

Spectrum licences can be sub-licensed, subject to the ARCEP's prior approval. The ARCEP must make a decision within two months.

4 Cyber-security, Interception, Encryption and Data Retention

4.1 Describe the legal framework for cybersecurity.

The legal framework for cybersecurity is set out by:

- Law n°2013-1168 of 18 December 2013, stating legal requirements for the providers of critical infrastructure;
- Law n°2018-133 of 26 February 2018, implementing the provisions of the Directive concerning measures for a high common level of Security of Network and Information Systems (NIS Directive), of 6 July 2016;
- Decree of the *Conseil d'Etat* of 25 May 2018, concerning the security of network and information systems applicable to operators of essential services and to the digital service providers; and
- Decree of 13 June 2018 establishing the terms provided by articles 8, 11 and 20 of the above-mentioned Decree.

Furthermore, specific requirements relating to cybersecurity are stated by the Data Protection Law (articles 34 and 35) and by article D98-5-III of the CPCE.

In addition, article L.33-14 of the CPCE, created by Law n°2018-607 of 13 July 2018 on military programming, states that, for the purposes of security and defence of information systems, operators are authorised to install, on their networks, at their own expense and after informing the French National Cybersecurity Agency (*Agence Nationale de la Sécurité des Systèmes d'Information – ANSSI*), devices using technical markers in order to detect events affecting security. In the case of detection of such events, operators are not obliged to interrupt the attack but shall inform ANSSI without delay. Upon ANSSI's request, operators shall also inform their subscribers of the vulnerability of their information systems or the breaches they have suffered.

4.2 Describe the legal framework (including listing relevant legislation) which governs the ability of the state (police, security services, etc.) to obtain access to private communications.

The interception of electronic communications was instituted as part of the effort to fight serious crime and terrorism. In the context of an increased terrorism threat, this subject has become a major issue.

Regulation regarding the technical measures for lawful interception is the result of various successive legal texts. Regulation varies depending on the authority (either judicial or administrative) from which the interception operation originates.

See *infra* question 4.3 for the description of the administrative interception regulation.

4.3 Summarise the rules which require market participants to maintain call interception (wire-tap) capabilities. Does this cover: (i) traditional telephone calls; (ii) VoIP calls; (iii) emails; and (iv) any other forms of communications?

a) Regulation of judicial interceptions

Firstly, the interception of electronic communications can be ordered by judicial authorities pursuant to article 100 of the Criminal Procedure Code, resulting from article 2 of Law n°91-646 of 10 July 1991 regarding correspondence secrecy. Electronic communications which can be intercepted include voice, videoconferencing, mobile data (Short Message Service [SMS] and Multimedia Messaging Service [MMS]) as well as Internet data.

Secondly, connection data can be required through judicial requisitions issued based on articles n°60-2, 77-1-2 and 99-4 of the Criminal Procedure Code. Connection data which can be gathered include data retained by electronic communications operators pursuant to articles L.34-1 and R.10-12 to R.10-14 of the CPCE, and by hosting service providers and ISPs pursuant to article 6-11 of LCEN and Decree n°2011-219 of 25 February 2011.

Since the enactment of Law n°2011-267 of 14 March 2011 relating to domestic security (*LOPPSI*), it is also possible to capture in real-time keyboard entry data (via key loggers) and data displayed on the screen as part of the fight against serious crime and terrorism, upon authorisation of the examining magistrate.

However, these provisions proved to be largely insufficient as they did not address VoIP.

Law n°2014-1353 of 13 November 2014, strengthening anti-terrorism provisions, addressed this shortcoming by introducing the right to also capture data sent to or issued from peripheral audio-visual devices (article 706-102-1 of the Criminal Procedure Code). This regulation was designed to give the possibility of monitoring the private conversations of Skype users.

However, article 226-3 of the Criminal Code prevented this new provision from being implemented, as technologies allowing for such capture were still banned as a result of the Ministerial Order of 4 July 2012, which had not been amended to consider this new provision. The new regulation was completed when the Ministerial Order of 17 July 2015 added to the list of authorised technologies – technologies allowing for the capture of data sent to or issued from peripheral audio-visual devices.

As a result, electronic communication services such as VoIP services are now subject to interceptions through the implementation of spyware.

In order to improve judicial interception capacity, responsiveness and security, the information system for the management of judicial interceptions (*Système de Transmission d'Interceptions Judiciaires – STIJ*), authorised by Decree n°2007-1145 of 30 July 2007, was replaced by a new centralised management platform (*Plate-forme Nationale des Interceptions Judiciaires – PNIJ*) instituted by Decree n°2014-1162 of 9 October 2014.

More recently, Law n°2016-731 of 3 June 2016 reinforcing efforts to fight against organised crime and terrorism provided additional investigative powers to magistrates, notably by allowing the use of technical devices to directly capture connection data necessary for the terminal equipment or the user subscription number (IMSI catcher). In addition, data access is not limited to data displayed on the screen or that are sent to or issued from peripheral audio-visual devices, but now includes data stored on the user IT system.

Interception decisions are taken for a maximum duration of four months, and can be renewed without exceeding one year (two years when in relation to major infringements).

b) Regulation of administrative interceptions

Used without any legal basis before 1991, administrative interceptions – like judicial ones – were regulated by Law n°91-646 of 10 July 1991, after France was condemned by the European Court of Human Rights (CEDH, 24 April 1990, *Huvig and Kruslin c/ France*), which provided that they could be implemented subject to a decision of the Prime Minister under the control of an independent authority (*CNCIS*). Law n°2004-669 of 9 July 2004 extended the scope of these interceptions beyond telephony interceptions to include all electronic communications.

Law n°2006-64 of 23 January 2006 providing for anti-terrorism measures allowed police forces to access electronic communication services, the access to which was initially restricted to judicial authorities. This data includes all data retained by electronic communications operators pursuant to articles L.34-1 and R.10-12 to R.10-14 of the CPCE, and by ISPs and hosting service providers pursuant to article 6-11 of LCEN and Decree n°2011-219 of 25 February 2011.

Law n°2013-1168 of 18 December 2013 on military programming (*LPM*) gave various state agencies the right to access Internet users' communications data, including the data issuer, data recipient, time of the communications, websites visited and real time geolocation outside of any judicial proceeding.

Law n°2015-912 of 24 July 2015, relating to intelligence, reinforced the anti-terrorism legal arsenal by legalising and providing a legal framework for practices implemented by intelligence services (namely, *Direction Générale de la Sécurité Extérieure – DGSE*, *Direction de la Protection et de la Sécurité de la Défense – DPSD*, *Direction du Renseignement Militaire – DRM*, *Direction Générale de la Sécurité Intérieure – DGSI*, *Direction Nationale du Renseignement et des Enquêtes Douanières* and *Tracfin*).

The said law sets out the conditions of broad administrative surveillance by granting intelligence services the right to use various technologies, such as online correspondences' administrative interceptions, IMSI catchers and device geolocation.

Furthermore, the said law enforces the use of "black boxes" within Internet service providers and telecoms operators' networks, aiming at collecting suspicious connection data in order to detect a terrorist threat (article L.851-3 of the Domestic Security Code). Although this text gave rise to strong reactions, these provisions were validated by the Constitutional Council (decision n°2012-713 DC of 23 July 2015).

As the implementation of black boxes may result in mass surveillance, this provision was very controversial and considered by numerous commentators as an infringement of the private life rights of French citizens; "black boxes" would analyse the metadata

of all communications (the origin or recipient of a message, IP address of a visited website, and connection duration).

To date, the government announced that "*only data concerning suspicious people will be stored. All other data will be immediately destroyed*".

There were many opponents of this law, including several associations as well as the French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés – CNIL*), and, more recently, the Office of the United Nations High Commissioner for Human Rights (OHCHR), which stated that it was "*worried about wide intrusive powers*" granted to intelligence services.

Following censorship of the international surveillance provisions by the Constitutional Council, the French Parliament adopted complementary legal provisions by passing Law n°2015-1556 of 30 November 2015, relating to the surveillance of international electronic communications.

c) Obligations incumbent upon operators

To comply with these interception obligations, operators have to fulfil the following obligations:

- to retain certain data pursuant to articles L.34-1 and R.10-12 to R.10-14 of the CPCE (see *infra* question 4.6);
- to put in place all necessary means to enforce interceptions requested under Law n°91-646 of 10 July 1991 (article D.98-7 III of the CPCE); and
- to appoint qualified personnel to conduct interception operations in compliance with Decree n°93-119 of 28 January 1993.

The use of technologies such as spyware and IMSI catchers does not require any action to be taken by the operators. In contrast, the implementation of black boxes should be the responsibility of the operators.

4.4 How does the state intercept communications for a particular individual?

Before resorting to surveillance technologies, intelligence services must obtain the prior authorisation of the Prime Minister granted after the opinion of the National Commission of Control of Intelligence Techniques (*Commission Nationale de Contrôle des Techniques de Renseignement – CNCTR*) (the derogation for "operational urgency" to this principle was censored by the Constitutional Council). The use of these technologies is subject to a "strict proportionality test".

See *supra* question 4.3 for the description of the administrative interception regulation.

4.5 Describe the rules governing the use of encryption and the circumstances when encryption keys need to be provided to the state.

Pursuant to article 30 of Law n°2004-575 of 21 June 2004, the use of encryption means on the French territory is free.

However, unless exempted based on Appendix I of Decree n°2007-663 of 2 May 2007, and Category 5 Part 2 of Appendix I of Commission Delegated Regulation (EU) No 1382/2014 of 22 October 2014, the supply, import and export of cryptology means in and from France are subject to a prior declaration or a prior authorisation of the French National Cybersecurity Agency (*ANSSI*), depending on the technical functionalities and commercial operation (provision or import) which are based on Decree n°2007-663 of 2 May 2007.

The export of encryption means can also fall under the regulation of dual-use items, and can require in certain cases a prior authorisation from the Ministry of Industry through its Dual-Use Items Department (*Service des Biens à Double Usage – SBDU*). By exception, export is free for encryption means used for consumer purposes that are certified as "*grand public*" by ANSSI, through the process set out by Decree n°2007-663 of 2 May 2007 (no ANSSI export authorisation and no SBDU licence).

These formalities are specified by the Ministerial Order of 29 January 2015. They are incumbent upon the provider of the encryption means.

In addition, pursuant to article 230-1 of the Criminal Procedure Code, certain magistrates can request encryption/decryption keys to be provided if necessary for the investigation. Infringement of this obligation is punishable by imprisonment of up to three years and a €270,000 fine (article 434-15-2 of the Criminal Code); this sanction can be brought up to five years' imprisonment and a €450,000 fine, if complying to the obligation could have avoided a crime being committed or could have mitigated its consequences.

The use of encryption means can also fall under foreign ownership restrictions (see *supra* question 1.4).

4.6 What data are telecoms or internet infrastructure operators obliged to retain and for how long?

The French government instituted an obligation of retention of data relating to electronic communications (Daily Safety Law n°2001-1062 of 15 November 2001), codified under article L.34-1 of the CPCE. On a purely exceptional basis, operators were authorised to keep this data for one year for billing needs and for the purposes of research and infringements proceedings. A new exception was created by Law n°2003-239 of 18 March 2003 (*Home Safety Law*) which made these provisions perennial, while they were supposed to last only until December 2003.

In 2006, the new French Anti-Terror Act (Law n°2006-64 of 23 January 2006) extended the provisions concerning retention data in two ways. Firstly, not only the judicial authority but also the police forces may access the retained data. Secondly, data retention obligations now apply to Internet cafés, hotels, restaurants, and more generally to any person or organisation providing Internet access, free or for a fee, as a main or side activity. These provisions were lastly completed by Law n°2013-1168 of 18 December 2013 on military programming (*LPM*).

Decree n°358-2006 of 26 March 2006, on electronic communications data retention, and Decree n°2012-436 of 30 March 2012 specified the retention and anonymisation obligations of traffic data which are incumbent upon operators, pursuant to articles L.34-1 III and IV of the CPCE.

According to article R.10-13 of the CPCE, operators must retain the following data:

- user identification data;
- the terminal equipment used to make the communication;
- the technical characteristics, date, time and duration of each communication;
- any associated services requested or used by the user, and the suppliers of those services;
- the recipient of the communication; and
- for telephony services (in addition to the above), geolocation data.

Retention of content is strictly forbidden (article L.34.1 VI of the CPCE).

The data must be retained by the operator for 12 months (article R.10-13 III of the CPCE).

These data retention obligations apply to all ECN operators and all ECS providers.

Costs incurred by operators are reimbursed by the state.

Failing to comply with data retention obligations is punishable by up to one years' imprisonment and a €75,000 fine (article L.39-3 of the CPCE).

5 Distribution of Audio-Visual Media

5.1 How is the distribution of audio-visual media regulated in your jurisdiction?

The distribution of audio-visual media is regulated by Law n°86-1067 of 30 September 1986 on Communication Freedom under the supervision of the CSA.

This regulation applies to both radio and television, and provides as a core principle that "*any communication to the public via electronic means is free*" (article 1 of Law n°86-1067).

However, this communication freedom is restricted by various obligations imposed on audio-visual media companies from the public and private sectors, such as:

- child protection (article 15 of Law n°86-1067);
- advertising, teleshopping and sponsorship (Decree n°92-280 of 27 March 1992);
- product placement (article 14-1 inserted by Law n°2009-258 of 5 March 2009);
- film works broadcasting quotas (Decree n°90-66 of 17 January 1990); and
- French songs broadcasting (Law n°94-88 of 1 February 1994).

Public audio-visual media dsitribution companies are subject to additional rules, notably in terms of programmes to be broadcast and advertising.

5.2 Is content regulation (including advertising, as well as editorial) different for content broadcast via traditional distribution platforms as opposed to content delivered over the internet or other platforms? Please describe the main differences.

Pursuant to article 2 of Law n°86-1067 of 30 September 1986, modified by Law n°2009-258 of 5 March 2009:

- "*A television service or a communication service to the public via electronic means, means a service intended to be simultaneously received by the whole public or by a category of the public and for which the program is comprised of emissions including sounds*"; and
- "*An on-demand audio-visual media service means any communication service to the public via electronic means, allowing for programs viewing at the moment chosen by the user and upon its request […]*".

No differentiation is made between traditional broadcasting and broadcasting over the Internet (*e.g.*, on-demand video services, on-demand audio-visual services and catch-up TV).

5.3 Describe the different types of licences for the distribution of audio-visual media and their key obligations.

The formalities of audio-visual media broadcasting, using frequencies assigned by the CSA, differ according to whether the operator falls within the public or private sector.

Private companies are subject to the CSA's prior authorisation to operate television or radio services. Key obligations are then formalised in a contract entered into between the CSA and the company which has been granted the authorisation to operate.

Public sector companies (public TV channels, namely channels of the group France Télévisions, Arte, LCP, Assemblée Nationale and Public Sénat and the three public radio stations, namely Radio France, Réseau France Outre-mer and Radio France Internationale) are not subject to the CSA's prior authorisation, but must draft specification requirements (*cahier des charges*) taking into account the obligations resulting from the public missions assigned to them, notably regarding education and culture, and submit them to the CSA. They are also bound by the terms of the contracts signed with the government with regards to their goals and means (*contrats d'objectifs et de moyens*).

Distributors of audio-visual media services that do not use frequencies assigned by the CSA (satellite, cable, Internet, ADSL) are only subject to prior notification to the CSA.

5.4 Are licences assignable? If not, what rules apply? Are there restrictions on change of control of the licensee?

The CSA can withdraw any authorisation in case of substantial changes to the conditions according to which the authorisation was initially granted (share capital, executive bodies, financing arrangements, etc.).

The CSA can agree to an assignment of the authorisation if the assignee is the legal person controlling or controlled by the initial holder.

6 Internet Infrastructure

6.1 How have the courts interpreted and applied any defences (e.g. 'mere conduit' or 'common carrier') available to protect telecommunications operators and/or internet service providers from liability for content carried over their networks?

Article L.32-3-3 of the CPCE protects telecommunications operators and ISPs from both civil and criminal liability for content carried over their networks, by stating that they cannot be held liable save if: *(i)* they requested the communication; *(ii)* they selected the addressee of the communication; or *(iii)* they selected or modified the transmitted content.

The courts have, on several occasions, exonerated telecom operators and ISPs from all liability in respect of content. However, ISPs can, to a certain extent, be under the obligation to restrain access to certain websites (see *infra* question 6.4).

6.2 Are telecommunications operators and/or internet service providers under any obligations (i.e. to provide information, inform customers, disconnect customers) to assist content owners whose rights may be infringed by means of file-sharing or other activities?

France was an early adopter of a graduated response approach, understanding it as a way to protect artistic creation. In 2007, the Minister of Culture ordered a report regarding online copyright protection, which led to an agreement signed by copyright holders as well as network operators.

This report led to the enactment of Law n°2009-669 of 12 June 2009 aiming to promote broadcasting and protection on the Internet (*Loi*

Création et Internet), which created an independent administrative authority: the Supreme Authority for the Broadcasting of Works and the Protection of Rights on the Internet – HADOPI.

In cooperation with ISPs, HADOPI is in charge of identifying online copyright infringers and to implement a graduated response (codified under L.331-12 *et seq.* of the Intellectual Property Code).

Firstly, HADOPI requires ISPs to send warning notices to online copyright infringers. Secondly, if the same Internet user continues its illegal downloading activities after six months, HADOPI shall send a warning email and a registered letter. In case of repeated infringement after this second warning, HADOPI shall transfer the files of repeated infringers to criminal courts for prosecution.

If the Internet user is prosecuted by criminal courts for copyright infringement, the judge will be empowered to pronounce a complementary penalty, which may lead to the suspension of the infringer's Internet access as well as the imposition of a range of criminal penalties. Article 7 of Law n°2009-1311, regarding penal protection of intellectual property, foresees that the judge may pronounce the suspension of the Internet access for a maximum of one year. During such suspension, the subscriber is still under the obligation to pay their Internet subscription.

Pursuant to this law, ISPs are also under the obligation to provide their subscribers with customers' contracts containing specific information on various subjects, such as:

- the obligation of vigilance which is incumbent upon the subscriber;
- the existence of legal content offers;
- the means of securing connections;
- the criminal and civil penalties incurred in case of copyright violation; and
- the threat posed by unlawful copying practices to the artistic creation and the cultural sector's economic sustainability.

6.3 Are there any 'net neutrality' requirements? Are telecommunications operators and/or internet service providers able to differentially charge and/or block different types of traffic over their networks?

Pursuant to article L.32-1 of the CPCE, the ARCEP must ensure "*that no discrimination exists, under analogous circumstances, in the relationship between the operators and providers of publicly available online electronic communication services in traffic routing and access to these services*" and "*end users' ability to access and distribute information and to access the applications and services of their choice*".

In the context of this mission, the ARCEP issued a series of recommendations for ISPs in 2010 and in 2012. In 2011, a Parliamentary report concluded with concrete proposals for legislative provisions and recommended that net neutrality become a political objective in France, as did the *Conseil National du Numérique*.

The European Regulation (EU) 2015/2120 of 25 November 2015, laying down measures concerning open Internet access, entered into force on 30 April 2016.

The text introduces the guiding principles of open Internet access and net neutrality into European legislation: on the one hand, equal and non-discriminatory treatment of Internet traffic; and on the other hand, all end users' (*i.e.*, consumers and content providers) rights to distribute and to access the information and content of their choice.

The text provides for the following rules:

- Reasonable traffic management by ISPs is acceptable in only a limited number of circumstances, and must not be based on commercial considerations.
- ISPs are prohibited from degrading or blocking traffic (or certain categories of traffic), except under clearly defined circumstances. These practices are justifiable in only a small number of instances: to comply with court orders; to protect the integrity or security of the network; or to prevent impending network congestion that occurs temporarily and under exceptional circumstances.
- In addition to providing Internet access, ISPs can offer services that need to be transmitted in an optimised fashion to meet certain specific requirements, provided that these practices do not have a negative impact on the availability or general quality of Internet access services.
- ISPs' commercial practices are now subject to scrutiny, notably their promotion of bundled online services. The national regulator has the right to monitor the features of these products.
- Operators are subject to strengthened transparency obligations. These pertain in particular to providing more detailed information in customers' contracts: the possible impact of traffic management techniques used by the ISPs; the concrete impact of the (traffic, speed, etc.) caps or allowances attached to the plan; and information on connection speeds, etc.

Within nine months of the Regulation entering into force, the Body of European Regulators for Electronic Communications (BEREC) must "*issue guidelines for the implementation of the obligations of national regulatory authorities*" under article 5.3 of the Regulation, to set out the concrete implementing procedures for the Regulation. The guidelines will ensure that the principles contained in the Regulation are implemented in a harmonious way across the European Union. The ARCEP actively contributed to the work done by the BEREC to prepare these guidelines.

On 6 June 2016, the BEREC launched a public consultation on draft guidelines which aim to support the national regulator in monitoring net neutrality.

The BEREC's guidelines are still to be adopted.

Law n°2016-1321 of 7 October 2016 formally introduced net neutrality in the CPCE, giving to the ARCEP the authority to ensure net neutrality and oversee open Internet access.

6.4 Are telecommunications operators and/or internet service providers under any obligations to block access to certain sites or content? Are consumer VPN services regulated or blocked?

Law n°2004-575 of 21 June 2004 (*LCEN*) provides that ISPs cannot be subject to any general monitoring obligation. Content suspension and access can only be decided by courts under specific circumstances. As an example, Orange, Bouygues Telecom, SFR and Free were recently ordered to prevent access from France to the music downloading website T411 (TGI Paris, 2 April 2015).

However, telecommunications operators and/or ISPs may be under obligations to block access to certain sites or content under specific circumstances, such as:

- Terrorism:
  - Law n°2014-1353 of 13 November 2014 for strengthening anti-terrorism provisions increased criminal sanctions for apology of terrorism on the Internet, and authorised the blocking of Internet sites "*encouraging or making apologist arguments for terrorism actions*".

- Law n°2016-731 of 3 June 2016 for strengthening the fight against organised crime, terrorism and its funding, and improving the efficiency and warranties of criminal procedure, creates a criminal offence for the obstruction of blocking websites encouraging or making apologist arguments for acts of terrorism.

- Child pornography:
  - Since the enactment of Law n°2011-267 of 14 March 2011 (*LOPPSI*), websites obviously publishing child pornography can be blocked by ISPs upon request of the administrative authority in charge, the Central Office of Anti-Criminality Committed with Information and Communication Technologies (*Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication – OCLCTIC*).
  - If the pornographic nature of the content is not "*obvious*", the administrative authority can bring the matter before the judicial authority.
- Online gambling:
  - Law n°2004-575 of 21 June 2004 (*LCEN*) provides that ISPs cannot be subject to any general monitoring obligation. Temporary monitoring obligations can only be decided by judicial courts under specific circumstances.
  - However, all ISPs must prevent online access to gambling services that have not been granted an authorisation by the Online Gambling Authority (*Autorité de Régulation des Jeux en Ligne – ARJEL*), in order to prevent French residents from gambling on blacklisted sites.

Decree n°2015-253 of 4 March 2015, for the delisting of websites encouraging acts of terrorism or broadcasting child pornography, provides for the delisting of illicit websites through a purely administrative procedure which does not require any judicial decision. In accordance with these new provisions, the OCLCTIC directly addresses to search engines the URL links of the websites to be delisted. Search engine companies then have 48 hours to make the search results disappear and operate the delisting. The Decree also specifies the conditions under which expenditure resulting from the search engines' obligation to delist may be supported by the government.

By contrast, hosting service providers are subject to a broader liability if they were actually aware of the illegal character of content, and did not act promptly to withdraw this content or make access to it impossible (article L.32-3-4 of the CPCE and article 6 of LCEN).

As for consumer VPN services, they are neither regulated nor blocked for the time being.

Anne-Solène Gay
BEHRING
10, rue de Presbourg
75116 Paris
France

Tel: +33 1 53 64 70 00
Email: asgay@behring.fr
URL: www.behring.fr

Attorney at law of the Paris Bar since 1997, Anne-Solène Gay has developed expertise in telecommunications, space activities, IT and IP.

Anne-Solène advises governments and regulators as well as telecom operators on regulatory and transactional matters. Anne-Solène has notably provided legal assistance in liberalisation processes, the granting of licences, the privatisation of operators, the restructuring of incumbent operators and the adjustment of the regulatory framework applicable to the telecommunications and information technology sector. Anne-Solène also advises companies acting in emerging technologies sectors on regulatory and IT matters.

Prior to establishing BEHRING law firm, Anne-Solène practised law with various international law firms (Jeantet & Associés and Bird & Bird) in Paris and London. Anne-Solène worked on a wide range of projects.

International legal directories (*Chambers & Partners* and *The Legal 500*) name her every year as one of the leading lawyers in TMT (telecoms, media and technologies) in France.

BEHRING
société d'avocats

BEHRING is a law firm specialising in telecommunications, space activities, IT and IP.

The firm was founded by Anne-Solène Gay, a leading legal expert on these issues for 20 years.

Highly knowledgeable in the industrial sectors in which our clients are involved, BEHRING's legal team provides crucial assistance for the many challenges our clients face during their business development.

BEHRING serves as regular counsel to French and foreign companies, start-ups, SMEs and large industrial groups. The firm helps various companies in both the service and manufacturing sectors, particularly in supporting technology and regulated activities. BEHRING also advises on issues related to innovation and intellectual property rights.

BEHRING supports its clients for contractual and regulatory matters, both in France and abroad, notably in Africa, Asia and North America.

Thanks to its expertise and global practice, BEHRING is regularly awarded in international rankings, such as *The Legal 500* and *Chambers & Partners*.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk