

THE TECHNOLOGY,
MEDIA AND
TELECOMMUNICATIONS
REVIEW

NINTH EDITION

Editor
John P Janka

THE LAWREVIEWS

THE
TECHNOLOGY,
MEDIA AND
TELECOMMUNICATIONS
REVIEW

NINTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in January 2019
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
John P Janka

THE LAWREVIEWS

PUBLISHER

Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER

Nick Barette

BUSINESS DEVELOPMENT MANAGERS

Thomas Lee, Joel Woods

SENIOR ACCOUNT MANAGERS

Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS

Sophie Emberson, Katie Hodgetts

PRODUCT MARKETING EXECUTIVE

Rebecca Mogridge

RESEARCH LEAD

Kieran Hansen

EDITORIAL COORDINATOR

Gavin Jordan

HEAD OF PRODUCTION

Adam Myers

PRODUCTION EDITOR

Anne Borthwick

SUBEDITOR

Martin Roach

CHIEF EXECUTIVE OFFICER

Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK
© 2018 Law Business Research Ltd
www.TheLawReviews.co.uk

No photocopying: copyright licences do not apply.

The information provided in this publication is general and may not apply in a specific situation, nor does it necessarily represent the views of authors' firms or their clients. Legal advice should always be sought before taking any legal action based on the information provided. The publishers accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of November 2018, be advised that this is a developing area.

Enquiries concerning reproduction should be sent to Law Business Research, at the address above.

Enquiries concerning editorial content should be directed
to the Publisher – tom.barnes@lbresearch.com

ISBN 978-1-912228-63-8

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

ADVAITA LEGAL

BAKER & MCKENZIE.WONG & LEOW

BIRD & BIRD

CLEARY GOTTlieb STEEN & HAMILTON LLP

CMS

COELHO RIBEIRO & ASSOCIADOS

ELVINGER HOSS PRUSSEN

HOGAN LOVELLS BSTL, SC

LATHAM & WATKINS LLP

LEE AND LI, ATTORNEYS-AT-LAW

NIEDERER KRAFT FREY LTD

PETILLION

PINHEIRO NETO ADVOGADOS

SORAINEN

URÍA MENÉNDEZ

WEBB HENDERSON

ZHONG LUN LAW FIRM

CONTENTS

PREFACE.....	vii
<i>John P Janka</i>	
LIST OF ABBREVIATIONS.....	ix
Chapter 1 AUSTRALIA.....	1
<i>Angus Henderson, Richard Dampney and Irene Halforty</i>	
Chapter 2 BELARUS.....	21
<i>Kirill Laptev</i>	
Chapter 3 BELGIUM.....	31
<i>Flip Petillion, Jan Janssen, Diégo Noesen and Alexander Heirwegh</i>	
Chapter 4 BRAZIL.....	43
<i>Raphael de Cunto and Beatriz Landi Laterza Figueiredo</i>	
Chapter 5 CHINA.....	55
<i>Jihong Chen</i>	
Chapter 6 ESTONIA.....	68
<i>Mihkel Miidla and Liisa Maria Kuuskmaa</i>	
Chapter 7 EU OVERVIEW.....	88
<i>Marco D'Ostuni, Gianluca Faella and Manuela Becchimanzi</i>	
Chapter 8 FRANCE.....	108
<i>Myria Saarinen and Jean-Luc Juban</i>	
Chapter 9 GERMANY.....	125
<i>Christian Engelhardt</i>	

Contents

Chapter 10	HONG KONG	138
	<i>Simon Powell and Chi Ho Kwan</i>	
Chapter 11	INDIA	155
	<i>Atul Dua and Anuradha</i>	
Chapter 12	ITALY	168
	<i>Marco D'Ostumi, Marco Zotta and Manuela Becchimanzi</i>	
Chapter 13	JAPAN	189
	<i>Hiroki Kobayashi, David Lai and Takaki Sato</i>	
Chapter 14	LATVIA	210
	<i>Andris Tauriņš and Madara Melņika</i>	
Chapter 15	LITHUANIA	226
	<i>Stasys Drazdauskas</i>	
Chapter 16	LUXEMBOURG	235
	<i>Linda Funck</i>	
Chapter 17	MEXICO	259
	<i>Federico Hernández Arroyo</i>	
Chapter 18	PORTUGAL	270
	<i>Jaime Medeiros, Carolina Ribeiro Santos and Ana Ramos Logrado</i>	
Chapter 19	RUSSIA	292
	<i>Maxim Boulba and Elena Andrianova</i>	
Chapter 20	SINGAPORE	303
	<i>Ken Chia and Daryl Seetoh</i>	
Chapter 21	SPAIN	327
	<i>Pablo González-Espejo</i>	
Chapter 22	SWITZERLAND	342
	<i>András Gurovits and Victor Stancescu</i>	

Contents

Chapter 23	TAIWAN.....	360
	<i>Patrick Marros Chu, Vick Chien and Sam Huang</i>	
Chapter 24	UNITED ARAB EMIRATES.....	370
	<i>David Bintliff, Cathal Flynn, Racheal Sanni, Shannon Rogers and Ayah Abdin</i>	
Chapter 25	UNITED KINGDOM.....	382
	<i>John D Colahan, Gail Crawford and Lisbeth Savill</i>	
Chapter 26	UNITED STATES.....	429
	<i>John P Janka, Matthew T Murchison and Michael H Herman</i>	
Appendix 1	ABOUT THE AUTHORS.....	449
Appendix 2	CONTRIBUTING LAW FIRMS' CONTACT DETAILS.....	467

PREFACE

This fully updated ninth edition of *The Technology, Media and Telecommunications Review* provides an overview of evolving legal constructs in 26 jurisdictions around the world. It is intended as a business-focused framework rather than a legal treatise, and provides a general overview for those interested in evolving law and policy in the rapidly changing TMT sector.

Broadband connectivity (regardless of the technology used) continues to drive law and policy in this sector. Next-generation wireless connectivity will be provided by a network of networks, with multiple technologies – both wired and wireless, using licensed and unlicensed spectrum – playing an integral role in delivering service to the end user. By way of example, free WiFi service in homes and businesses today carries the majority of the data that is transmitted to smartphones and wireless tablets that also rely on paid service from a wireless carrier. And wireless carriers otherwise rely on a variety of technologies to ultimately connect the customer to the internet or someone on the other end of the phone.

The disruptive effect of new technologies and new ways of connecting people and devices creates challenges around the world as regulators both seek to facilitate digital inclusion by encouraging the deployment of state-of-the-art communications infrastructure to all citizens, and also seek to use the limited radio spectrum more intensively than before. At the same time, technological innovation makes it commercially practical to use large segments of ‘higher’ parts of the radio spectrum for the first time. Moreover, the global nature of TMT companies requires them to engage on these issues in different ways than before.

A host of new demands, such as the developing internet of things, the need for broadband service to aeroplanes, vessels, motor vehicles and trains, and the general desire for faster and better mobile broadband service no matter where we go, all create pressures on the existing spectrum environment. Regulators are being forced to both ‘refarm’ existing spectrum bands and rewrite their licensing rules, so that new services and technologies can access spectrum previously set aside for other purposes that either never developed or no longer have the same spectrum needs. Regulators also are being forced to seek means for coexistence in the same spectrum between different services in ways previously not contemplated.

Many important issues are being studied as part of the preparation for the next World Radio-communication Conference (WRC) of the International Telecommunication Union (ITU), to be held in 2019. No doubt, this conference will lead to changes in some long-standing radio spectrum allocations. And the conference also may include some political spectrum allocations that are based on pressures brought by well-heeled industries, rather than logic or sound policy. Indeed, these pressures already exist around the world in decisions being made by national regulators outside of and before the WRC.

Legacy terrestrial telecommunications networks designed primarily for voice are being upgraded to support the broadband applications of tomorrow. As a result, many governments

are investing in or subsidising broadband networks to ensure that their citizens can participate in the global economy, and have universal access to the vital information, entertainment and educational services now delivered over broadband. Many governments are re-evaluating how to regulate broadband providers, whose networks have become essential to almost every citizen. However, many policymakers still have not solved the problem caused when their incumbent service providers fail to extend service to all of their citizens for business reasons – because those businesses deem ‘unprofitable’ those who are the hardest to serve. Curiously, policymakers sometimes exacerbate this failure by resorting to spectrum auctions to award the right to provide service in a given frequency band to the highest bidder, failing to require service availability to everyone in the auctioned area, and then making the auction winner the gatekeeper for anyone else who wants to use the same spectrum. Too often, decisions are based (explicitly or implicitly) on expected auction revenues, which consumers end up paying for in the end through higher costs of service. Far too infrequently do policymakers factor in the benefits of ensuring ubiquitous connectivity: new jobs, economic growth, security, social inclusion, and improvements in healthcare, education and food production, to name a few. Indeed, treating spectrum as a property right rather than as the valuable public resource it is often leads to perverse results in the marketplace.

Convergence, vertical integration and consolidation can also lead to increased focus on competition and, in some cases, to changes in the government bodies responsible for monitoring and managing competition in the TMT sector. Similarly, many global companies now are able to focus their regulatory activities outside their traditional home, and in jurisdictions that provide the most accommodating terms and conditions.

Changes in the TMT ecosystem, including increased opportunities to distribute video content over broadband networks, have led to policy focuses on issues such as network neutrality: the goal of providing some type of stability for the provision of the important communications services on which almost everyone relies, while also addressing the opportunities for mischief that can arise when market forces work unchecked. While the stated goals of that policy focus may be laudable, the way in which resulting law and regulation are implemented has profound effects on the balance of power in the sector, and also raises important questions about who should bear the burden of expanding broadband networks to accommodate capacity strains created by content providers and to facilitate their new businesses.

The following chapters describe these types of developments around the world, as well as the liberalisation of foreign ownership restrictions, efforts to ensure consumer privacy and data protection, and measures to ensure national security and facilitate law enforcement. Many tensions exist among the policy goals that underlie the resulting changes in law. Moreover, cultural and political considerations often drive different responses at the national and the regional level, even though the global TMT marketplace creates a common set of issues.

I thank all of the contributors for their insightful contributions to this publication, and I hope you will find this global survey a useful starting point in your review and analysis of these fascinating developments in the TMT sector.

John P Janka

Latham & Watkins LLP

Washington, DC

November 2018

FRANCE

*Myria Saarinen and Jean-Luc Juhan*¹

I OVERVIEW

The French regulatory framework is based on the historical distinction between telecoms and postal activities on the one hand, and radio and television activities on the other (sectors are still governed by separate legislation and by separate regulators). Amendments in the past 15 years reflect the progress and the convergence of electronic communications, media and technologies, and the liberalisation of the TMT sectors caused by the *de facto* competition between fixed telephony (a monopoly until 1998) and new technologies of terrestrial, satellite and internet networks. French law also mirrors the EU regulatory framework through the enactment of the three EU Telecoms Packages in 1996, 2002 and 2009, which have been transposed into French law.

The TMT sectors in France have been fully open to competition since 1 January 1998, and are characterised by the interactions of mandatory provisions originating from many sources and involving many actors (regulators, telecoms operators, and local, regional and national authorities). The TMT sectors are key to the French economy, and 2017 was once again an important year in many respects for these sectors' business.

II REGULATION

i The regulators

There are four specialist authorities involved in the regulation of technology, media and telecommunications in France:

- a ARCEP is an independent government agency that oversees the electronic communications and postal services sector. It ensures the implementation of a universal service, imposes requirements upon operators that exert a significant influence in the context of market analyses, participates in defining the regulatory framework, allocates finite resources (RFs and numbers), imposes sanctions, resolves disputes and delivers authorisations for postal activities.
- b The Superior Audiovisual Council (CSA) is the regulatory authority responsible for the audiovisual sector. The CSA sets rules on broadcasting content and allocates frequencies by granting licences to radio and television operators. It also settles disputes that may arise between TV channels and their distributors, and is empowered to

¹ Myria Saarinen and Jean-Luc Juhan are partners at Latham & Watkins. This chapter was written with contributions from associate Floriane Cruchet and trainees François Tréfois, Clara Giordano and Charlotte Guérin.

impose sanctions on operators in cases of breaches of specific regulations. Law No. 2013-1028 of 15 November 2013 relating to the independence of the French public broadcasting service has amended the legal nature of the CSA, its composition, the status and appointment procedure of its members and their powers.

- c The Data Protection Authority (CNIL) supervises compliance with data protection regulations, and is empowered to issue sanctions that range from warnings to fines.
- d The High Authority for the Distribution of Works and the Protection of Copyright on the Internet (HADOPI), which was established in 2009, is in charge of protecting intellectual property rights over works of art and literature on the internet.

These authorities may deliver opinions upon request by the government, Parliament or other independent administrative authorities such as the French Competition Authority (FCA), and also renders decisions and opinions that may have a structural impact on these sectors (except for HADOPI). The National Frequencies Agency is also an important agency responsible for managing frequency spectrum and planning its use (see Section IV).

The CSA and ARCEP are the two main regulators of the TMT sectors. Discussions about merging these entities at the time of the convergence or to limit the powers of ARCEP occurred regularly during the past few years, but such merger was finally given up. Instead, it was argued that the two regulators should work in closer cooperation on certain common subjects.

The prevailing regulatory regime in France regarding electronic communications is contained primarily in the Post and Electronic Communications Code (CPCE), and regarding audiovisual communications in Law No. 86-1067 of 30 September 1986 on Freedom to Communicate, as subsequently amended. The main piece of legislation governing the law applicable to data protection is Law No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties (1978 Data Protection Law), as subsequently amended. Intellectual property rights are governed by the Intellectual Property Code.

ii Regulated activities

Telecoms

Telecoms activities and related authorisations and licences are regulated under the CPCE.

To become a telecoms operator, no specific licences or authorisations are required; the implementation and the operation of public networks and the supply of electronic communication services to the public is free, subject to prior notification to ARCEP (Articles L32-1 and L33-1 of the CPCE). Law No. 2015-990 of 6 August 2015 for the growth, activity and equality of economic opportunities (also known as the Macron Law) grants ARCEP the power to register on its own initiative any actor that infringed the notification obligation to declare itself to ARCEP.²

Conversely, the use of RFs requires a licence granted by ARCEP (Article L42-1 of the CPCE).

Media

Authorisations and licensing in the media sector are regulated under Law No. 86-1067 of 30 September 1986.

² Article L33-1 I of the CPCE.

Authorisations for private television and radio broadcasting on the hertz-based terrestrial frequencies are granted by the CSA following bid tenders and subject to the conclusion of an agreement with the CSA. The term of authorisations cannot exceed 10 years.³ Broadcasting services that are not subject to the CSA's authorisation – namely, those that are broadcast or distributed through a network that does not use frequencies allocated by the CSA (cable, satellite, ADSL, internet, telephony, etc.) – are nevertheless subject to a standard agreement or a declaration regime.⁴

iii Ownership and market access restrictions

General regulation of foreign investment

Since the entry into force of Law No. 2004-669 of 9 July 2004, discrimination of non-EU operators is prohibited, and they are subject to the same rights and obligations as EU and national operators.⁵ According to Article L151-1 et seq. of the French Monetary and Financial Code, when a foreign (EU or non-EU) investment is made in a strategic sector (such as security, public defence, cryptographics or interception of correspondence),⁶ the investor must submit a formal application dossier to the French Ministry of Economy for prior authorisation. Any transaction concluded without prior authorisation is null and void, and criminal sanctions (imprisonment of up to five years⁷ and a fine amounting to up to twice the amount of the transaction) are also applicable. A Decree of 14 May 2014⁸ expanded the list of sectors in which foreign investors must seek prior authorisation from the Ministry of Economy. In particular, the Decree has added to the regulated activities referred to in Article R153-2 of the French Monetary and Financial Code activities relating to the integrity, security and continuity of the operation of networks and ECSs.

Specific ownership restrictions applicable to the media sector

French regulations provide for media ownership restrictions to preserve media pluralism and competition. In particular, any single individual or legal entity cannot hold, directly or indirectly, more than 49 per cent 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 per cent. In addition, any single individual or legal entity that already holds a national terrestrial television service where the average audience for this service exceeds 8 per cent may not, directly or indirectly, hold more than 33 per cent of the capital or voting rights of a company that has an authorisation to provide a local terrestrial television service.⁹

Regulation of the media sector is currently evolving in reaction to a number of changes in French media ownership. As a consequence, French lawmakers adopted Law No. 2016-1524 of 14 November 2016, which amends the Law of 30 September 1986.¹⁰ Its purpose is to ensure freedom, independence and pluralism in media ownership, for example

3 See Articles 28 to 32 of the Law of 30 September 1986, which determine the CSA's allocation procedures.

4 Articles 33 to 34-5 of the Law of 30 September 1986.

5 Article L33-1 III of the CPCE.

6 Article R153-2 of the French Monetary and Financial Code.

7 Article L165-1 of the French Monetary and Financial Code.

8 Decree No. 2014-479 of 14 May 2014.

9 Articles 39-I and 39-III of the Law of 30 September 1986.

10 Law No. 2016-1524 of 14 November 2016 strengthening media freedom, independence and pluralism.

by requiring media outlets to provide yearly information on their capital ownership and governing bodies,¹¹ and reinforcing the powers of the CSA over French media governance with the creation of deontology committees.¹²

Regarding the radio sector, a single person cannot retain networks whose coverage exceeds 150 million inhabitants or 20 per cent of the aggregated potential audience.¹³ This regulation will, however, be subject to modification in the future, as it does not take into account local pluralism challenges. In this respect, a report was submitted to Parliament by the CSA in April 2014.¹⁴

Further, unless otherwise agreed in international agreements to which France is a party, a foreign national may not acquire shares in a company holding a licence for a radio or television service in France that uses RFs if this acquisition has the effect of raising (directly or indirectly) the share of capital or voting rights owned by foreign nationals to more than 20 per cent.¹⁵ Under the same circumstances, such licence cannot be granted to a company in which 20 per cent of the share capital or voting rights is owned (directly or indirectly) by foreign nationals.¹⁶ These provisions do not apply to service providers of which at least 80 per cent of the capital or voting rights are held by public radio broadcasters belonging to Council of Europe Member States, and of which at least 20 per cent is owned by one of the public companies mentioned in Article 44 of the Law of 30 September 1986.¹⁷ Specific rules restricting cross-media ownership also apply.¹⁸

iv Transfers of control and assignments

The general French merger control framework applies to the TMT sectors, without prejudice to the above-mentioned ownership restrictions and to specific provisions for the media sector. The merger control rules are enforced by the FCA.¹⁹

Regarding the telecoms and post sectors, the FCA must provide ARCEP with any referrals regarding merger control, and ARCEP can issue a non-binding opinion.²⁰

Regarding companies active in the radio or TV sector involved in a Phase II merger control procedure before the FCA, a non-binding opinion from the CSA is necessary.²¹

Any modification of the capital of companies authorised by the CSA to broadcast TV or radio services on a frequency is subject to the approval of the CSA.²²

11 Article 19 of the Law No. 2016-1524 of 14 November 2016.

12 Article 11 of the Law No. 2016-1524 of 14 November 2016.

13 Article 41 of the Law of 30 September 1986.

14 Available at www.csa.fr/Etudes-et-publications/Les-autres-rapports/Rapport-du-CSA-su-r-la-concentration-du-media-radiophonique.

15 Article 40 of the Law of 30 September 1986.

16 Article 14 of the Law of 14 November 2016.

17 Article 40 of the Law of 30 September 1986.

18 Article 41-1 to 41-2-1 of the Law of 30 September 1986.

19 For recent examples of mergers in the TMT sectors, see, e.g., FCA, Decision No. 17-DCC-76 of 13 June 2017, in which the FCA ruled on the acquisition of Group News Participations by SFR Group.

20 Article L36-10 of the CPCE.

21 Article 41-4 of the Law of 30 September 1986.

22 Article 42-3 of the Law of 30 September 1986.

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

Under the CPCE, ECSs other than voice telephony to the public may be provided freely.²³

As regards the ADSL network, and following local loop unbundling, alternative operators must be provided with direct access to the copper pair infrastructure of France Télécom-Orange, the historical operator. Therefore, as with traditional fixed telephony, DSL networks are subject to asymmetrical regulation.

As regards services, ISPs can operate freely and provide services, but they must file a declaration with ARCEP before commencing operations.²⁴ A failure to comply with this obligation constitutes a criminal offence.²⁵

More generally, ISPs must comply with the provisions of Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy governing e-commerce, encryption and liability of technical service providers, as subsequently amended. Law No. 2004-575 of 21 June 2004 also sets out a liability exemption regime for hosting service providers. They are not subject to a general obligation to monitor the information they transmit or store; nor are they obliged to look for facts or circumstances indicating illicit activity. Nevertheless, when the provider becomes aware that the data stored is obviously illicit, it has the obligation to remove the data or render their access impossible. In that respect, the question of the qualification as ‘host provider’ has been widely debated before French courts.²⁶

ii Universal service

The EU framework for universal services obligations, which defines universal services as the ‘minimum set of services of specified quality to which all end users have access, at an

23 Article L32-1 of the CPCE.

24 Article L33-1 of the CPCE.

25 Article L39 of the CPCE.

26 This issue now seems resolved regarding video-sharing sites: see, for instance, the judgment of the French Supreme Court (Cass civ 1ère, 17 February 2011, No. 09-67896, *Joyeux Noël*) in which the Supreme Court recognised a simple hosting status for Dailymotion. The Supreme Court ruled that host websites did not have to control *a priori* the content they host but need to ensure the content is not accessible once it has been reported as illegal (Cass Civ 1ère, 12 July 2012, No. 11-15165 and No. 11-15188, *Google and Aufeminin.com*). This issue is still to be debated with respect to online marketplaces such as eBay from which it follows that French courts, which are favouring a very factual analysis of the role of the services provider, will give significant importance to judges’ discretion. In that respect, see Cass Com, 3 May 2012, No. 11-10.507, *Christian Dior Couture*, No. 11-10.505, *Louis Vuitton Malletier* and No. 11-10.508, *Parfums Christian Dior*, in which the Supreme Court confirmed an earlier decision of the Paris Court of Appeals that did not consider eBay as a ‘host provider’, and therefore refused to apply the liability-exemption regime. See, in contrast, *Brocanteurs v. eBay*, Paris Court of Appeals, Pôle 5, ch 1, 4 April 2012, No. 10-00.878, in which second-hand and antique dealers accused eBay of encouraging illegal practices by providing individuals with the means to compete unfairly against professionals, and in which the Paris Court of Appeals considered eBay as a host provider able to benefit from the liability-exemption regime. The Court of Appeals based its decision on the fact that eBay had no knowledge or control of the adverts stored on its site. If the seller was asked to provide certain information, it was for the purpose of ensuring a more secure relationship between its users. The issue is also debated in the context of online forums. The Supreme Court ruled on 3 November 2015 that publishing directors are responsible for ‘personal contribution spaces’ from the moment they become aware of their content and must be held criminally liable for failing to take down defamatory comments (Cass Crim, 3 November 2015, No. 13-82645).

affordable price in the light of specific national conditions, without distorting competition',²⁷ has been implemented by Law No. 96-659 of 26 July 1996 and further strengthened by Law No. 2008-3 of 3 January 2008. Universal service is one of the three components of public service in the telecoms sector in France (the other two being the supply of mandatory services for electronic communications and general interest missions).

Obligations of the operator in charge of universal service are listed in Article L35-1 of the CPCE and fall into two main categories of services:

- a* telephone services: connection to an affordable public telephone network enabling end users to take charge of voice communications, facsimile communications and data communications at data rates that are sufficient to allow functional internet access and free emergency calls; and
- b* enquiry and directory services (either in printed or electronic versions).

These services must be rendered under tariff and technical conditions that take into consideration the difficulties faced by some users, such as users with low incomes, and that do not discriminate between users on the ground of their geographical location. Following calls for applications (one per category), the Minister in charge of electronic communications designates the operator or operators in charge of the universal service for a period of three years. France Télécom-Orange was designated as such until 2020.²⁸

Universal service currently only covers telephone provision and not information technologies. However, in Opinion No. 11-A-10 of 29 June 2011, the FCA considered that the reduced price policy (also called the 'social tariff') set up for telephone networks, pursuant to universal service rules might be extended to internet services even though the EU Telecoms Package does not expressly allow for the inclusion of such in the universal service. In the absence of regulation, France Télécom-Orange launched a 'social tariff' for multi-service offers (telephone and internet) on 9 February 2012.

ARCEP determines the cost of the universal service and, when it is necessary to finance it in the event that it represents an excessive burden for the operator in charge, ARCEP also determines the amount of the other operators' contributions to the financing of USOs through a sectoral fund. In principle, every operator contributes to the financing, with each contribution being calculated on the basis of the turnover achieved by the operators in their electronic communications activities.²⁹

iii Restrictions on the provision of service

Net neutrality is a growing policy concern in France. From the electronic communications regulator's standpoint, which focuses on the technical and economic conditions of traffic conveyance on the internet, the key question in the debate over net neutrality is how much control internet stakeholders can rightfully exert over the traffic. This implies examining operators' practices on their networks, as well as their relationships with some content and application providers.

The Digital Republic Law³⁰ recently introduced the principle of net neutrality into the national legal framework and grants ARCEP with new investigatory and sanctioning

27 Article 1(2) of Directive No. 2002/22/EC.

28 See Ministerial Order of 27 November 2017 designating Orange (JORF No. 0282 of 3 December 2017).

29 Article L35-3 of the CPCE.

30 Law No. 2016-1321 of 7 October 2016 for a Digital Republic.

powers to ensure compliance (see also Section VI.i).³¹ In particular, Arcep is now in charge of implementing net neutrality in accordance with Regulation No. 2015/2120 of 25 November 2015 establishing measures concerning open internet access.³² When Arcep identifies a risk of infringement by an operator, it can require said operator to comply ahead of time. The Digital Republic Law also reinforces the conditions under which the Minister in charge of electronic communications and Arcep can conduct an investigation.³³

Since the adoption of the Digital Republic Law, ARCEP has published a courtesy French translation of the guidelines for national regulatory authorities on the implementation of Regulation No. 2015/2120 of 25 November 2015, which the Body of European Regulators for Electronic Communications published on 30 August 2016.³⁴ In June 2018, for a second year, ARCEP also published its annual report on the state of the internet in France,³⁵ which identifies various threats that could undermine the internet's proper functioning and neutrality, and sets out the regulator's actions to contain these threats. This document addresses issues regarding data interconnection, the transition to IPv6,³⁶ the quality of fixed internet access, net neutrality and open platforms. Arcep issued in parallel a report devoted to the ways in which end user devices (mobiles and boxes) influence internet openness.³⁷

As to content, pursuant to the Law of 21 June 2004, ISPs have a purely technical role, and they do not have the general obligation to review the content they transmit or store. Nevertheless, when informed of unlawful information or activity, they must take prompt action to withdraw the relevant content, failing which their civil liability may be sought. Since 2009, HADOPI has been competent to address theft and piracy matters. It intervenes when requested to by regularly constituted bodies for professional defence that are entitled to institute legal proceedings to defend the interests entrusted to them under their statutes (e.g., SACEM), or by the public prosecutor. After several formal notices to an offender, the procedure may result in a €1,500 fine.³⁸

Finally, French e-consumers benefit from consumer law provisions and from specific regulations. In particular, they are protected against certain unsolicited communications via email if their consent has not been obtained prior to the use of their personal data. Moreover, consumers must be provided with valid means by which they may effectively request that such unsolicited communications cease.³⁹ In addition, Decree No. 2015-556 of 19 May 2015 provides for the implementation of an opposition list on which any consumer can add his

31 Articles 40 to 47 of Digital Republic Law.

32 Article 40 of Digital Republic Law.

33 Article 43 of Digital Republic Law.

34 Available at https://www.arcep.fr/fileadmin/uploads/tx_gspublication/2016-10-21-Lignes-directrice-s-NN-version-francaise.pdf.

35 2017 report: 'The state of internet in France', ARCEP report, May 2017 (available at ARCEP https://www.arcep.fr/uploads/tx_gspublication/State-Of-Internet-in-France-2017_may2017.pdf).

2018 report: 'The state of internet in France', ARCEP report, June 2018 (available at ARCEP https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2018_conf050618.pdf).

36 IPv6 is the most recent version of the Internet Protocol, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the internet. IPv6 has been developed to deal with the issue of IPv4 address exhaustion, and is intended to replace IPv4.

37 'End-user devices – Analysis of their influence on Internet Openness', ARCEP report, 30 May 2017 (available at https://www.arcep.fr/uploads/tx_gspublication/study-end-user-devices-internet-openness-may2017.pdf).

38 See Articles L331-25, L336-3 and R335-5 of the Intellectual Property Code.

39 See Article L34-5 of the CPCE.

or her name so that advertising material may not generally be sent to him or her.⁴⁰ The Decree joins a list of programmes in place to ensure consumer protection. With regard to phone-based advertising, new restrictions have been implemented since 1 June 2016 thanks to the designation of Opposetel, which is in charge of preventing unsolicited communications to consumers registered on an opposition list.⁴¹ The Bloctel service had over 2 million registered users two months after its launch. All telephone operators also have the obligation to offer their users the possibility to register on an opposition list.⁴²

iv Security

The past few years have seen increasing terrorist security threats, resulting in substantial changes in the legal framework regarding security in telecommunications.

Law No. 91-646 of 10 July 1991 concerning the secrecy of electronic communications, now codified in the Internal Security Code, provides that the Prime Minister may exceptionally authorise, for a maximum period of four months (renewable only upon a new decision), the interception of electronic communications in order to collect information relating to the defence of the nation or the safeguarding of elements that are key to France's scientific or economic capacity. In addition, pursuant to Law No. 2015-912 of 24 July 2015 (new Article L851-3 of the Internal Security Code) and only for the purpose of preventing terrorism, the Prime Minister may impose on providers of electronic communication services the obligation to implement an automated data-processing system for a maximum period of two months (renewable only upon a new decision) with the aim of detecting connections likely to reveal a terrorist threat. Article L851-2 of the Internal Security Code as amended by Law No. 2016-987 of 21 July 2016 provides that the administration is authorised, for prevention of terrorism, to collect real time connection data concerning individuals, beforehand identified, likely to be linked to a terrorist threat.⁴³

Further, Law No. 2013-1168 on Military Programming (LPM) introduced a new chapter in the Internal Security Code relating to administrative access to data connection, including real-time geolocation.⁴⁴ The new regime, which entered into force on 1 January 2015,⁴⁵ authorises the collection of 'information or documents' from operators as opposed to the collection of simply 'technical data'. In addition, access to data is exclusively administrative, namely without judicial control. Requests for implementing such measures are submitted by designated administrative agents to a 'chosen personality' appointed by the National Commission for the Control of Security Interceptions (CNCIS) upon the proposal of the Prime Minister. CNCIS is in charge of controlling (*a posteriori*) administrative agents' requests for using geolocation measures in the course of their investigation. The Minister

40 See Article L223-1 of the Consumer Code.

41 See Ministerial Order of 25 February 2016 designating SA Opposetel (JORF No. 0050 of 28 February 2016).

42 The red list service ensures that contact information will not be mentioned on user lists. The orange list service ensures that contact information will not be communicated to corporate entities with the goal of advertisement. The contact information remains available on universal directories made available to the public.

43 Initially, this article provided that the collection could be authorised against the individual's relatives. However, the Constitutional Council, in decision No. 2017-648 QPC of 4 August 2017, censored this provision because it infringes the balance between public security and right to privacy.

44 New Article L246-1 et seq. of the Internal Security Code introduced by Article 20 of the LPM.

45 Article 20 IV of the LPM.

for Internal Security, the Defence Minister and the Finance Minister can also issue direct requests for the implementation of real-time geolocation measures to the Prime Minister who, in this case, will directly grant authorisations.

Law No. 2014-1353 of 13 November 2014, implemented by Decree No. 2015-174 of 13 February 2015, also entitles the administrative authorities to request ISPs to prevent access to websites supporting terrorist ideologies or projects.⁴⁶ Additionally, laws linked to the state of emergency created extraordinary means of data search and seizure and expanded the provisions of Law No. 2014-1353.

In the context of the terrorism threat, the French legislator has amended the Criminal Proceedings Code to tackle organised crimes such as terrorism acts.⁴⁷ Law No. 2016-731 of 3 June 2016⁴⁸ allows police officers, with the authorisation and under the control of a judge, to access, remotely and without consent, the correspondences stored in electronic communications available through identification.⁴⁹ Police officers can also be authorised, by a judge and under his or her control, to use a technical disposal, such as an international mobile subscriber identity-catcher, to collect technical connection data to identify terminal equipment or users' subscription numbers as well as data regarding the location of the terminal equipment used.⁵⁰ This Law also extended some existing investigating powers to all organised crimes, such as the real-time collection of computer data without consent, in the context of both preliminary investigations and investigations of flagrancy.⁵¹

In addition to the general rules applicable to the protection of personal data laid down in the 1978 Data Protection Law, the CPCE provides specific rules pursuant to which operators must delete or preserve the anonymity of any traffic data relating to a communication as soon as it is complete.⁵² Exceptions are provided, however, in particular for the prevention of terrorism and in the pursuit of criminal offences.

Unauthorised access to automated data-processing systems is prohibited by Articles 323-1 to 323-7 of the French Penal Code. In addition, with regard to cyberattacks, Law No. 2011-267 on Performance Guidance for the Police and Security Services (LOPPSI 2) introduced a new offence of online identity theft in Article 226-4-1 of the French Penal Code and empowers police officers, upon judicial authorisation and only for a limited period, to

46 See Article 6-1 of Law No. 2004-575 of 21 June 2004 on Confidence in the Digital Economy as introduced by Article 12 of Law No. 2014-1353 of 13 November 2014 reinforcing regulations relating to the fight against terrorism.

47 However, the Constitutional Council established boundaries in the fight against terrorism regarding infringements of the freedom of communication. In Decision No. 2016-611 QPC of 10 February 2017, the Council considered as unconstitutional Article 421-2-5-2 of the French Criminal Code introduced by Law No. 2016-731 of 3 June 2016, which punishes any person who frequently accesses online public communication services conveying messages, images or representations that directly encourage the commission of terrorist acts or defend these acts when this service has the purpose of showing images or representations of these acts that consist of voluntary harm to life.

48 Law No. 2016-731 of 3 June 2016 reinforcing the fight against organised crime and terrorism and their funding, and improving the efficiency and the protection of guarantees of criminal proceedings.

49 Articles 706-95-1 to 706-95-3 of the French Criminal Proceedings Code added by Article 2 of Law No. 2016-731 of 3 June 2016.

50 Articles 706-95-4 to 706-95-10 of the French Criminal Proceedings Code added by Article 3 of Law No. 2016-731 of 3 June 2016.

51 Article 706-102-1 of the French Criminal Proceedings Code amended by Article 5 of the Law No. 2016-731 of 3 June 2016.

52 See Articles L34-1 and D98-5 of the CPCE.

install software in order to observe, collect, record, save and transmit all the content displayed on a computer's screen. This helps with the detection of infringements, the collection of evidence and the search for criminals by facilitating the creation of police files and by organising their coordination. Cybersecurity threats are dealt by the National Agency for the Security of Information Systems (ANSSI), a branch of the Secretariat-General for Defence and National Security created in 2009.⁵³

In terms of personal data protection, LOPPSI 2 increases the instances where authorities may set up, transfer and record images on public roads, premises or facilities open to the public in order to protect the rights and freedom of individuals, and recognises that the CNIL has jurisdiction over the control of video protection systems.

With regard to the detection of cyberattacks, Law No. 2018-607 of 13 July 2018⁵⁴ created Article L33-14 of the CPCE that involves operators in the detection of cyberattacks. Pursuant to this article, electronic communications operators are entitled to use technical markers such as IP addresses to detect or prevent any potential threat that may affect the security of information systems of their subscribers. In this case, operators shall inform the ANSSI without delay.

IV SPECTRUM POLICY

i Development

The management of the entire French RF spectrum is entrusted to a state agency, the National Frequencies Agency. It apportions the available radio spectrum, the allocation of which is administered by governmental administrations (e.g., those of civil aviation, defence, space, the interior) and independent authorities (ARCEP and the CSA) (see Section II).

ii Flexible spectrum use

The trend towards greater flexibility in spectrum use is facilitated in France by the ability of operators to trade frequency licences, as introduced by Law No. 2004-669 of 9 July 2004.⁵⁵

The general terms of spectrum licence trading are defined by Decree No. 2006-1016 of 11 August 2006, and the list of frequency bands the licences of which could be traded are laid down by a Ministerial Order of 11 August 2006. A frequency database that provides information regarding the terms for spectrum trading in the different frequency bands open in the secondary market is publicly accessible. A 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 contained in the licence (e.g., geographical region or frequencies). The transfer of frequency licences is subject either to the prior approval of ARCEP⁵⁶ or to notification to ARCEP, which may refuse the assignment under certain circumstances.⁵⁷ Another option available for operators is spectrum leasing, whereby the licence holder makes frequencies fully or partially available for a third party to operate.

53 See Decree No. 2009-834 of 7 July 2009 as modified by Decree No. 2011-170 of 11 February 2011.

54 Law No. 2018-607 of 13 July 2018, Military Planning Law 2019–2025 (LPM).

55 Article L42-3 of the CPCE.

56 Article R20-44-9-2 of the CPCE.

57 Ibid.

Unlike in a sale, the original licence holder remains entirely responsible for complying with the obligations attached to the frequency licence. All frequency-leasing operations require the prior approval of ARCEP.

iii Broadband and next-generation mobile spectrum use

Until 2009, there were three 3G licence holders in France: Orange France, SFR and Bouygues Telecom. The fourth 3G mobile licence was awarded to Free Mobile on 17 December 2009.

In addition, spectrum in the 800MHz and 2.6GHz bands was allocated for the deployment of the ultra-high-speed 4G mobile network: in that respect, licences for the 2.6GHz frequency were awarded to Bouygues Telecom, Free Mobile, Orange France and SFR in September 2011,⁵⁸ and in December 2011, licences for the 800MHz were awarded to the same operators except Free Mobile,⁵⁹ which has instead been granted roaming rights in priority roll-out areas. New spectrum in the 700 and 800MHz bands was transferred in December 2015 to promote better network capacities in areas with low population density, but the transfer will only be made effective from October 2017 to June 2019. The French government launched a call for applications, to be sent before 2 October 2018, in order to reassign the 900MHz, 1,800MHz and 2.1GHz bands, whose authorisations will expire between 2021 and 2024.⁶⁰ As a result of an agreement reached between ARCEP, the French government and operators on 14 January 2018, the reassignment procedure will take into account operators' stated commitments to improve voice and data coverage in all territories, making regional development targets a priority.

On 16 June 2017, ARCEP had authorised Bouygues Telecom and SFR to deploy 4G networks in the 2.1GHz band, historically used by French mobile operators' 3G networks, to improve 4G speeds.⁶¹

Additionally, under ARCEP supervision, 5G deployment is being prepared, with network coverage estimated to begin in 2020. The European Union's public-private partnership between the European Commission and telecom industries, the 5G-PPP, which was launched on 1 July 2015, provides a framework for national 5G development. On 30 September 2015, ARCEP gave Orange authorisation to conduct initial tests for 5G in the city of Belfort until the end of 2016. The authorisation delivered to Orange tests three formerly unused spectrum ranges, namely the 3,600–3,800MHz, 10,500–10,625MHz, and 17,300–17,425MHz frequencies.⁶² ARCEP recently published a synopsis of the responses to its public consultation on 'New frequencies for superfast access in the regions, for businesses, 5G and innovation' launched on 6 January 2017.⁶³ Following said consultation, ARCEP now seeks to prepare 5G deployment in the 26GHz and 1.5GHz bands.⁶⁴ On 16 July 2018, the French government officially launched its 5G roadmap.⁶⁵ Three main goals have been announced: (1) launching of several 5G pilot programmes in various regions; (2) allocation of new 5G frequencies and ensuring a commercial rollout in at least one major city by 2020; and (3) provision of 5G coverage for main transport routes by 2025. Additionally,

58 ARCEP, Decision No. 2011-1080 of 22 September 2011.

59 ARCEP, Decision No. 2011-1510 of 22 December 2011.

60 See ARCEP press release of 2 August 2018.

61 ARCEP, Decisions No. 2017-0734 (*Bouygues Telecom*) and No. 2017-0735 (*SFR*) of 13 June 2017.

62 See ARCEP press release of 30 September 2015.

63 See ARCEP press release of 22 June 2017.

64 See ARCEP press release of 30 July 2018.

65 See: https://www.economie.gouv.fr/files/files/Actus2018/Feuille_de_route_5G-DEF.pdf.

four main working areas have been identified: (1) free-up and attribute RFs for the 5G network; (2) foster the development of new industrial uses; (3) accompany the deployment of 5G infrastructures; and (4) ensure transparency and dialogue on 5G deployments and the exposure of the public.

iv Spectrum auctions and fees

Spectrum auctions in the case of scarce resources

Pursuant to Article L42-2 of the CPCE, when scarce resources such as RF are at stake, ARCEP may decide to limit the number of licences, either through a call for applications or by auction. The government sets the terms and conditions governing these licensing selection procedures, and until now such proceedings have always been in the form of calls for applications.

Fees

Pursuant to Articles R20-31 to R20-44 of the CPCE, licensed operators contribute to the financing of the universal services.

V MEDIA

i Restrictions on the provision of service

Media are, in particular, subject to certain content requirements and restrictions.

Content requirements

At least 60 per cent of the audiovisual works and films broadcast by licensed television broadcasters must have been produced in the EU, and 40 per cent must have been produced originally in French.⁶⁶

Private radio broadcasters must, in principle, dedicate at least 40 per cent of their musical programmes to French music.⁶⁷

In addition, pursuant to Law No. 2014-873 of 4 August 2014 for genuine equality between women and men, audiovisual programmes have the duty to ensure fair representation of both women and men. Furthermore, audiovisual programmes and radio broadcasters must combat sexism by broadcasting specific programmes in this respect.⁶⁸

A draft law⁶⁹ with regard to ‘fake news’ is currently being debated before the French Parliament and suggests several measures in order to limit the impact of false information on the public election process. For instance, in the state of the discussions, the draft provides that certain operators of online platforms – in the context of public elections – should implement measures to combat the broadcasting of false information likely to trouble public order or alter polls’ reliability. They should implement easily accessible and visible systems that will allow users to report such false information, including when they are financed by third parties.

66 Articles 7 and 13 of Decree No. 90-66 of 17 January 1990.

67 Article 28 2^a-bis of the Law of 30 September 1986.

68 Article 56 of the Law of 4 August 2014.

69 The last draft published is draft law No. 1219 as amended regarding the fight against the manipulation of information.

Advertising

Advertising is particularly regulated in television broadcasting.⁷⁰ In particular, advertising must not disrupt the integrity of a film or programme, and there must be at least 20 minutes between two advertising slots. Films may not be interrupted by advertising that lasts more than six minutes.

Rules governing advertisements are stricter on public channels. In particular, since 2009, advertising is banned on public service broadcasting channels from 8pm to 6am. This prohibition does not, however, concern general-interest messages, generic advertising (for the consumption of fruits, dairy products, etc.) or sponsorships, which may continue to be broadcast.

In addition, some products are prohibited from being advertised, such as alcoholic beverages above a certain level of alcohol or tobacco products.

A new decree, Decree No. 2017-159 dated 9 February 2017, extended the media owners' transparency requirements in order to protect advertisers of digital advertisement. According to Article 2 of the Decree, the media owners have to provide advertisers with the date and place of diffusion of the advertisements; the global price of the advertising campaign; and the unitary price charged for each advertising space.

ii Internet-delivered video content

Internet video distribution refers to IPTV services, which can be classified into the three following main categories: live television, time-shifted programming and VOD.

For customers who cannot afford triple-play offers, access to video content is limited to the content of free channels. The regulatory framework for 'social' offers set by the Law of 4 August 2008 is only limited to mobile telephony offers, triple play offers being thus outside its scope. Following FCA Opinion No. 11-A-10 and in the absence of regulation, France Télécom-Orange launched a 'social tariff' for multi-service offers (telephone and internet) (see Section III.ii).

iii Mobile services

Mobile personal television, initiated in 2007, has suffered from substantial delays due to disagreements among operators and content providers on the applicable economic model and on how to finance the deployment of a new network.

Thus, on 8 April 2010, the CSA delivered authorisations to 16 channels (13 private channels selected by the CSA after a call for applications launched on 6 November 2007, together with three public channels selected by the government) for the broadcasting of personal mobile television services.

On 22 April 2010, TDF, a French company that provides radio and television transmission services, services for telecoms operators and other multimedia services, and Virgin Mobile signed an agreement under which TDF committed to develop the new network with up to 50 per cent coverage of the 'outdoor' population and 30 per cent of the 'indoor' population, with Virgin Mobile paying TDF a monthly per-customer fee using DVB-H, an airwave broadcasting format that does not allow interaction with the user. However, after Virgin Mobile's decision to withdraw from the project, TDF decided to end the agreement in January 2011, and in June 2011 announced that it no longer wished to be

70 Decree No. 92-280 of 27 March 1992.

the DVB-H operator in charge of mobile personal television. Following TDF's withdrawal, the CSA granted a two-month period to the selected channels to appoint a new operator in charge of mobile personal television. On 14 February 2012, no operator being appointed, the CSA acknowledged that the project was abandoned, and withdrew the authorisations it delivered to the 16 channels on 8 April 2010.⁷¹

VI THE YEAR IN REVIEW

i The 'blockchain' ordinance

On 9 December 2017, the French government published Ordinance No. 2017-1674 relating to the use of the blockchain technology for the record of the issuance and assignment of certain securities.

Pursuant to Article L211-3 of the French Monetary and Financial Code, securities must be recorded in an account (*compte-titres*) kept by the issuer of the titles or an intermediary. As of 1 July 2018, blockchain technology should be accepted as a parallel form of records for all transactions involving securities that are not listed, provided that the issuer of the securities formally accepts the use of such technology.

A decree, which has yet to be published, shall set out the conditions of this mechanism, including the technical requirements intended to ensure the security and inviolability of these transactions records.

The French government's ambition to put France in a leading position in financial innovation has been met with similar enthusiasm from the National Assembly, the latter having launched in January 2018 a fact-finding mission on blockchain technology.⁷²

In September 2018, the CNIL published first elements of analysis for stakeholders who want to develop blockchain technology in the context of processing of personal data.⁷³

ii The new data protection law

A new data protection law was enacted on 20 June 2018⁷⁴ to adapt 1978 Data Protection Law to the GDPR⁷⁵ and Directive (EU) 2016/680.⁷⁶ The enactment of the new law served to implement the derogations to the GDPR that apply to French residents, regardless of the data controller's country of establishment. Decree No. 2005-1309, supplementing the 1978 Data Protection Law implementing decree, was also amended to reflect the GDPR change by Decree No. 2018-687 of 1 August 2018.

71 CSA, Decision No. 2012-275 of 14 February 2012.

72 [http://www2.assemblee-nationale.fr/15/missions-d-information/missions-d-information-communes/chaines-de-blocs/\(block\)/47246](http://www2.assemblee-nationale.fr/15/missions-d-information/missions-d-information-communes/chaines-de-blocs/(block)/47246).

73 <https://www.cnil.fr/fr/blockchain-et-rgpd-quelles-solutions-pour-un-usage-responsable-en-presence-d-e-donnees-personnelles>.

74 Law No. 2018-493 of 20 June 2018 on the protection of personal data.

75 Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

76 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

However, further actions will be needed from the French government to pass an ordinance to overhaul the entire Law No. 78-17 to enhance comprehensibility of the act and to ensure the coherence of the French legislation on data protection.

The abolition of the existing authorisation regime

The prior filing requirements before the CNIL have been abolished with the exception of three types of processing activities: (1) certain types of processing of health data;⁷⁷ (2) certain types of processing activities carried out by the state in its exercise of public authority;⁷⁸ and (3) processing activities carried out by public or private persons which use the National Identification Number (i.e., the social security number).⁷⁹

The extended powers of the CNIL

Under this new law, the CNIL's advisory,⁸⁰ investigative⁸¹ and corrective⁸² powers have been enhanced.

In addition, an emergency procedure was created, whereby the CNIL's president is empowered to refer a case to the restricted committee when (1) a violation of the applicable data protection laws infringes upon public or individual liberties, human identity or human rights or (2) when the CNIL's president considers that a prompt intervention is necessary.⁸³

The derogations allowed by the GDPR, as adopted by the French legislator

Under the GDPR, the French legislator was entitled to adopt a number of derogations, applicable where the data subject's residence is in France.⁸⁴

The 1978 Data Protection Law now provides that a minor can consent alone to the processing of his or her data in relation to information society services upon reaching the age of 15.⁸⁵ Minors under this threshold may only give their consent after being duly authorised to do so by the holder of parental rights and, therefore, the lawfulness of the processing activity will require a double consent.

The new law also broadens the possibility to bring a class action in connection with non-compliance with the GDPR or Law No. 78-17.⁸⁶ The concerned data subjects will be entitled to claim compensation alongside an association accredited on a national scale and having the protection of privacy and personal data as its statutory purpose.

77 Article 54 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

78 Article 27 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

79 Article 22 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

80 Article 11 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

81 Articles 43 quinquies and 44 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

82 Articles 45 and 46 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

83 Article 46 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

84 Article 5-1 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

85 Article 7-1 of the Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

86 Article 43 ter of Law No. 78-17 of 6 January 2018 on information technology, data files and civil liberties.

iii The implementation of the Network and Information Security Directive

With regard to cybersecurity, the Network and Information Security Directive (NISD)⁸⁷ has been implemented into French law by Law No. 2018-133 of 26 February 2018 and Decree No. 2018-384 of 23 May 2018. This framework imposes an obligation in terms of security of network and information systems on two categories of entities: (1) the operators of essential services (OESs) and (2) digital service providers (DSPs).

The categories of services considered as essential services are listed in the appendix of Decree No. 2018-384 (e.g., payment services, insurance, services involving preventive medicine, diagnosis and healthcare, selling of electricity and gas). The prime minister can designate operators as an OES if they provide at least one of the services listed.⁸⁸ The operator is notified of the prime minister's intent to designate it as an OES and can formulate observations.⁸⁹ The first designations are expected in November 2018.

DSP are providers of cloud, online marketplace and search engine services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.⁹⁰

Nevertheless, the French implementing law excludes from its scope certain types of entities already subject to information system security regulations, such as operators for their activities related to the operation of ECNs or the provision of ECSs and providers of trust services for electronic transactions subject to Article 19 of Regulation 910/2014 dated 23 July 2014.⁹¹

Both OESs and DSPs shall appoint a representative in charge of the contact with the ANSSI.⁹² For DSPs, this representative acts in the name of the provider for compliance with its obligations set forth of the NSID framework.⁹³ DSPs shall keep an updated list of all networks and information systems necessary for the provision of their services within the European Union.⁹⁴

As regards security measures that should be implemented, OESs shall comply with security measures defined by the prime minister in a specific regulation (which has not been adopted to date).⁹⁵ DSPs shall ensure, based on the state of art, a level of security for all networks and information systems necessary for the provision of their services within the European Union appropriate to the existing risks.⁹⁶ DSPs shall refer to Article 2 of the Commission Implementing Regulation of 30 January 2018 for the security measures that should be implemented.⁹⁷ Documents attesting to this implementation should be made available to the ANSSI in case of control.⁹⁸

87 Directive No. 2016/1148 of 6 July 2016.

88 Article 3 of Decree No. 2018-384 dated 23 May 2018.

89 Article 3 of Decree No. 2018-384 dated 23 May 2018.

90 Article 10 of Law No. 2018-133 of 26 February 2018.

91 Article 2 of Law No. 2018-133 of 26 February 2018.

92 Articles 5 and 16 of Decree No. 2018-384 dated 23 May 2018.

93 Article 16 of Decree No. 2018-384 dated 23 May 2018.

94 Article 17 of Decree No. 2018-384 dated 23 May 2018.

95 Article 10 of Decree No. 2018-384 dated 23 May 2018.

96 Article 12 of Law No. 2018-133 of 26 February 2018.

97 Article 18 of Decree No. 2018-384 dated 23 May 2018.

98 Article 19 of Decree No. 2018-384 dated 23 May 2018.

Both OESs and DSPs shall report to the ANSSI, without delay, after becoming aware of any incident affecting networks and information systems that has or is likely to have a significant impact on the continuity of services.⁹⁹

Non-compliance with the obligations set forth in the NSID framework may be sanctioned with criminal fines ranging from €100,000 to €125,000 for OESs¹⁰⁰ and from €75,000 to €100,000 for DSPs.¹⁰¹

99 Articles 7 and 13 of Law No. 2018-133; Articles 11, 12, 20 and 21 of Decree No. 2018-384 dated 23 May 2018.

100 Article 9 of Law No. 2018-133 of 26 February 2018.

101 Article 15 of Law No. 2018-133 of 26 February 2018.

ABOUT THE AUTHORS

MYRIA SAARINEN

Latham & Watkins

Myria Saarinen is a partner in the Paris office of Latham & Watkins. She has extensive experience in IP and IT litigation, including internet and other technology-related disputes. She is very active in litigation relating to major industrial operations and is involved in a broad range of general commercial disputes.

She has developed specific expertise in the area of privacy and personal data, including advising clients on their trans-border data flows, handling claims raised by the French Data Protection Authority, and setting up training sessions on the personal data protection framework in general and on specific topics. She also has expertise in cross-border issues raised in connection with discovery or similar requests in France.

Ms Saarinen is named among leading practitioners in commercial litigation, data privacy and IT (*The Legal 500 Paris 2016/2017*, *Chambers Europe 2013*, *Chambers Global 2013*).

JEAN-LUC JUHAN

Latham & Watkins

Jean-Luc Juhan is a partner in the corporate department of the Paris office of Latham & Watkins.

His practice focuses on outsourcing and technology transactions, including business processes, information technology, telecommunications, systems and software procurement and integration. He also has extensive experience advising clients on all the commercial and legal aspects of technology development, licensing arrangements, web hosting, manufacturing, distribution, e-commerce, entertainment and technology joint ventures.

Mr Juhan is in particular cited in *Chambers Europe* and *The Legal 500 Paris*: the 'exceptional' Jean-Luc Juhan, 'whose negotiating skills and expertise are remarkable', is 'very sharp and down-to-earth' and has 'very good knowledge of the industry'; he advises high-profile French and international groups on large outsourcing, telecommunication and integration system projects.

LATHAM & WATKINS LLP

45 rue Saint-Dominique

75007 Paris

France

Tel: +33 1 4062 2000

Fax: +33 1 4062 2062

myria.saarinen@lw.com

jean-luc.juhan@lw.com

www.lw.com

Law
Business
Research

ISBN 978-1-912228-63-8