THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

EIGHTH EDITION

Editor
John P Janka

THE LAWREVIEWS

THE TECHNOLOGY MEDIA AND TELECOMMUNICATIONS REVIEW

EIGHTH EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in December 2017
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
John P Janka

THE LAWREVIEWS

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGERS
Thomas Lee, Joel Woods

ACCOUNT MANAGERS
Pere Aspinall, Sophie Emberson,
Laura Lynas, Jack Bagnall

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCHER
Arthur Hunter

EDITORIAL COORDINATOR
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Robbie Kelly

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-90-4

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

© 2017 Law Business Research Ltd

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC–PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW

THE CONSUMER FINANCE LAW REVIEW

THE INITIAL PUBLIC OFFERINGS REVIEW

THE CLASS ACTIONS LAW REVIEW

THE TRANSFER PRICING LAW REVIEW

THE BANKING LITIGATION LAW REVIEW

THE HEALTHCARE LAW REVIEW

THE PATENT LITIGATION LAW REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ABOU JAOUDE & ASSOCIATES LAW FIRM

ADVAITA LEGAL

BAKER & McKENZIE.WONG & LEOW

CLEARY GOTTLIEB STEEN & HAMILTON LLP

CMS

COELHO RIBEIRO & ASSOCIADOS

DNFP IN ASSOCIATION WITH HOGAN LOVELLS

ELVINGER HOSS PRUSSEN

HOGAN LOVELLS BSTL, SC

KT LAW ASSOCIATES

LATHAM & WATKINS LLP

LEE AND LI, ATTORNEYS-AT-LAW

NIEDERER KRAFT & FREY LTD

PINHEIRO NETO ADVOGADOS

UDO UDOMA & BELO-OSAGIE

ÜNSAL GÜNDÜZ

URÍA MENÉNDEZ

WEBB HENDERSON

WOLF THEISS

ZHONG LUN LAW FIRM

CONTENTS

PREFACE

This fully updated eighth 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 for both start-ups and established companies, as well as an overview for those interested in examining evolving law and policy in the rapidly changing TMT sector.

Broadband connectivity and wireless services continue to drive law and policy in this sector. The disruptive effect of new technologies and new ways of communicating creates challenges around the world as regulators seek to facilitate the deployment of state-of-the-art communications infrastructure to all citizens and also to use the limited radio spectrum more efficiently 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 compels them to address 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, create pressures on the existing spectrum environment. Regulators are being forced to both 'refarm' existing spectrum bands, so that new services and technologies can access spectrum previously set aside for businesses that either never developed or no longer have the same spectrum needs; and facilitate spectrum sharing 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 to be held in 2019. No doubt, this Conference will lead to changes in long-standing radio spectrum allocations that have not kept up with advances in technology, and it should also address the flexible ways that new technologies allow many different services to co-exist in the same segment of spectrum.

Legacy terrestrial telecommunications networks designed primarily for voice are being upgraded to support the broadband applications of tomorrow that will extend economic benefits, educational opportunities and medical services throughout the world. 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. Convergence, vertical integration and consolidation 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 are 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 the 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 developing 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 the 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 would like to take the opportunity to 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
October 2017

Chapter 6

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 2016 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 (radio frequencies 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 impose sanctions on operators in cases of breaches of specific regulations. Law

1 Myria Saarinen and Jean-Luc Juhan are partners at Latham & Watkins. This chapter was written with contributions from associates Oriane Fauré and Julie Brousseau.

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) ensures the protection of personal data. Automatic personal data processing systems must be declared to the CNIL. The CNIL also supervises compliance with the law by inspecting IT systems and applications, 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 four 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 radio frequencies requires a licence granted by ARCEP (Article L42-1 of the CPCE).

2 Article L 33-1 I of the CPCE.

Media

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

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 years[7] and a fine amounting to up to twice the amount of the transaction) are also applicable. A Decree of 14 May 2014[8] 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 electronic communications services.

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]

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.

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 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 is 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 radio frequencies 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]

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

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-sur-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.

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]

III TELECOMMUNICATIONS AND INTERNET ACCESS

i Internet and internet protocol regulation

Under the CPCE, electronic communications services 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, 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 are 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]

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

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 Auféminin.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 fora.

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 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. France Télécom-Orange was designated as such until 2016. Therefore, a new call for applications was issued in January 2017, but no operator has been designated yet.

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 universal service obligations 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.[28]

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

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).

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

28 Article L35-3 of the CPCE.

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 Law[29] recently introduced the principle of net neutrality into the national legal framework and grants ARCEP with new investigatory and sanctioning powers to ensure compliance (see also Section VI.i).[30] 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.[31] 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.[32]

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.[33] In May 2017, ARCEP also published its first annual report on the state of the internet in France,[34] 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,[35] 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.[36]

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.[37]

Finally, French e-consumers benefit from consumer law provisions and from specific regulations. In particular, they are protected against certain unsolicited communications

29 Law No. 2016-1321 of 7 October 2016 for a Digital Republic (see Section VI.i).

30 Articles 40 to 47 of Digital Republic Law.

31 Article 40 of Digital Republic Law.

32 Article 43 of Digital Republic Law.

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

34 '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).

35 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.

36 '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).

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

via email if their consent has not been obtained prior to the use of their personal data.[38] 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 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

38 The CNIL is particularly attentive to the obligation of obtaining prior consent that is free, specific and informed. On 1 June 2015, the CNIL imposed a €15,000 fine on Prisma Media for not giving enough precise information regarding the nature of a newsletter to which its customers may subscribe.

39 See Article L34-5 of the CPCE.

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.

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 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 2016[48] 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

45 Article 20 IV of the LPM.

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.

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 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, 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.

IV SPECTRUM POLICY

i Development

The management of the entire French radio frequency 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.[54]

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 brands 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 ARCEP[55] or to notification to ARCEP, which may refuse the assignment under certain circumstances.[56] Another option available for operators is spectrum leasing, whereby the licence holder makes frequencies fully or partially available for a third party to operate.

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

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

54 Article L42-3 of the CPCE.

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

56 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,[57] and in December 2011, licences for the 800MHz were awarded to the same operators except Free Mobile,[58] 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. On 16 June 2017, ARCEP 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.[59]

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 3600–3800MHz, 10500–10625MHz, and 17300–17425MHz frequencies.[60] 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.[61]

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.

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

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

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

60 See ARCEP press release of 30 September 2015.

61 See ARCEP press release of 22 June 2017.

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.[62]

Private radio broadcasters must, in principle, dedicate at least 40 per cent of their musical programmes to French music.[63]

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.[64]

Advertising

Advertising is particularly regulated in television broadcasting.[65] 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

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

63 Article 28 2°-bis of the Law of 30 September 1986.

64 Article 56 of the Law of 4 August 2014.

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

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 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.[66]

VI THE YEAR IN REVIEW

i The Digital Republic Law

On 7 October 2016, the Digital Republic Law was promulgated by the President. This promulgation closes the legislative process commenced in December 2015, which was preceded by a public consultation initiated by the French Digital Council between October 2014 and February 2015, and which permitted the government to present its digital strategy in June 2015.

Structured around three titles (circulation of data and knowledge; protecting individuals in the digital society; universal access to data technology), the Law addresses a variety of subjects, which all aim to ensure a smooth digital transition. In essence, instead of creating a new legal framework, the Law broadens the existing legal structure.

In particular, the Digital Republic Law introduces, *inter alia*, the following innovations and amendments.[67]

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

67 The Digital Republic Law also strengthens the rights of data subjects (see Section VI.iii).

The strengthening of ARCEP's investigatory powers[68]

The Digital Republic Law notably extends the investigatory powers of ARCEP, enabling ARCEP to monitor the principle of net neutrality introduced by the Law. ARCEP may now carry out on-site investigations and seizures that expressly relate to electronic communications network operators, providers of online electronic communications services to the public and hosting infrastructure managers.

The strengthening of the CNIL's powers to sanction[69]

The Law amends in particular the escalation of sanctions in cases of breaches of the 1978 Data Protection Law and publication thereof. Now, the first level of sanction consists of a formal notice issued by the CNIL. If the identified breach cannot be cured within the framework of the formal notice process, the CNIL's restricted committee is now authorised to issue any sanctions (warnings, financial sanctions, injunctions to cease processing data). In addition, the amount of financial sanctions has significantly increased from €150,000 (up to €300,000 in cases of repeat offences) to €3 million.[70]

The deployment of high debit

The Digital Republic Law introduces the status of 'fibered areas'.[71] This status may be granted when the setting out and the operation of a fibre access network opened to mutualisation is sufficiently advanced in order to trigger measures that allow the transition towards high debit. The Law reinforces the role of ARCEP in the granting process. The Ministry of Economy sets the requirements and conditions of this status as well as the rights and obligations related thereto after the proposal of ARCEP, but the status is eventually granted by ARCEP.

ii The 'right to be forgotten'

On 13 May 2016, the Paris Court of First Instance[72] ordered Google to delete from its search results a link to a website accusing an individual of sexual offences against minors. The individual was identified by his name, address, job and name of his employer.

The judgment is of particular interest since few jurisdictions have so far ruled on the criteria to be taken into account to assess such kind of request since the European Court of Justice (ECJ) *Google Spain* ruling.[73]

More particularly, the Paris Court of First Instance rejected Google's arguments based not only on freedom of expression, but also on the qualification of whistle-blower, by applying the *Google Spain* ruling. As a reminder, in *Google Spain*, the ECJ ruled on questions referred by a Spanish court relating to the interpretation of Directive 95/46/EC[74] on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and its application to search engine activities. After having determined that

68 Article L32-4 of the CPCE as amended by the Digital Republic Law.

69 Article 45 of the 1978 Data Protection Law as amended by the Digital Republic Law.

70 Article 47 of the 1978 Data Protection Law as amended by the Digital Republic Law.

71 Article L.33-11 of the CPCE as amended by the Digital Republic Law.

72 Paris Court of First Instance, 13 May 2016, *M.X v. Google France and Google Inc*.

73 ECJ, 13 May 2014, *Google Spain SL and Google Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, C-131/12, ECLI:EU:C:2014:317.

74 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

search engines are data controllers in respect of their search results and that European data protection law applies to their processing of the data of EU citizens, even where they process the relevant data outside the EU, the ECJ found that a 'right to be forgotten' online applies to outdated and irrelevant data in search results unless there is a public interest in the data remaining available and even where the search results link to lawfully published content. In the case at hand, the Court of First Instance considered that first, the correctness of the information was not established and second, that the publication of such information was highly detrimental for the applicant's reputation, in particular as it was putting his job at risk.

The 'right to be forgotten' has also been taken into account in the Digital Republic Law with regards to post-mortem and minor's rights.

First, the 1978 Data Protection Law is supplemented by Article 40-1,[75] which introduces the concept of 'digital death' into French law. Under this new article, data subjects have a right to give instructions relating to the conservation, deletion and communication of their data after their death. All providers of online electronic communications services to the public will be required to inform users about what will happen to their data upon death, and allow users to choose whether their data will be transferred to a designated third party. Any contractual provision contained in general terms of use that limit these new prerogatives shall be deemed null and void. In the absence of instructions from the data subject, the rights in question may be exercised by their heirs, who notably have the right to initiate the closure of all of the deceased's user accounts.

Secondly, Article 40 of the 1978 Data Protection Law is supplemented by a new Section II,[76] which allows a data subject that has reached adulthood to request the deletion of his or her personal data that were collected when such person was still a minor. This supplement applies in particular to data collected in the context of the internet. However, this deletion right is not absolute and is limited by circumstances set forth in the law: for example, limits include exercising the right to freedom of expression and information, or complying with a legal obligation. In cases where data were provided to a third party (who is also a data controller), the data controller that was requested to delete the data must take reasonable measures, including technical measures, to inform such third parties.

iii The use of digital evidence before French courts

The use of digital evidence before French courts, that is to say any probative information stored or transmitted by digital means to establish the truth in a trial, has considerably increased in the past decade.[77]

In that respect, one of the main current issues is the use of data collected by employers against employees.

The use of data loss prevention (DLP) in the termination of a contract

The development of cybercrime has led to the prevention of information leakage via DLP solutions (software allowing the identification, monitoring and protection of a company's information assets).

75 Article 63 of the Digital Republic Law.

76 Ibid.

77 In that respect, the possibility to submit such digital evidence has been introduced into French Law by Law No. 2000-230, in particular Article 1 now codified at 1366 of the French Civil Code.

In a decision of 12 May 2016,[78] the Paris Court of Appeals annulled the disciplinary dismissal of an employee who sent professional documents identified as 'confidential' from his workstation to his personal email address. The employer had discovered that his employee had sent emails to his personal address by using DLP software and submitted it to the Court to justify the dismissal. However, the Court of Appeals considered the use of this system in order to control the activity of employees constituted a 'change in the purpose of the control characterising a substantial change in the filtering and collection of information'. Therefore, this change of purpose required prior declaration of modification to the CNIL as the authority in charge of protecting personal data. In the absence of such declaration, the dismissal was considered illegal.

The use of emails collected in a professional email inbox as evidence by employers

Another question arises from the possibility for the employer to submit emails collected in a professional email inbox as evidence. In a decision issued by the French Supreme Court, the question was, in particular, whether an employer who provided his or her employee with a professional email address but did not comply with the obligation to declare it before the CNIL could use the emails found in the professional email inbox against his or her employee.

In a decision of 1 June 2017,[79] the French Supreme Court ruled that:

> *[...] the absence of a simplified declaration of a professional electronic messaging system which does not have individual control over the activity of employees, and is therefore not likely to infringe privacy or liberties [...] does not render illegal the production in court of the emails addressed by the employer or the employee whose author cannot be unaware that they are registered and kept by the computer system.*

The use of geolocation systems by employers

In the same vein, the Paris Court of Appeals ruled on 22 June 2017[80] that information on employees' working hours outside their working place, collected by means of a geolocation system, could not be used as evidence to justify the dismissal of employees, since such purpose (monitoring employees' working hours outside the working place) had not been declared to the CNIL and was not known by the employee.

iv The FCA fines a major French telecommunications operator for gun jumping

On 8 November 2016, the FCA imposed a fine of €80 million on Altice for merger control gun jumping in the context of the SFR and Virgin Mobile/OTL acquisitions by Altice in 2014.[81] Although Altice agreed to settle this case with the FCA – which resulted in a much lower fine than the initial fine – the fine still constitutes a record fine for gun-jumping violations.

Under French law, the parties to a transaction that meets the French merger control jurisdictional thresholds must notify that transaction to the FCA and are prohibited from

78 Paris Court of Appeals, 12 May 2016, Pôle 6, ch 9, No. 14/10477.

79 French Supreme Court, Cass soc, 1 June 2017, No. 15-23.522.

80 Paris Court of Appeals, 22 June 2016, Pôle 6, ch 6, No 13/11389.

81 FCA, Decision No. 16-D-24 of 8 November 2016 regarding the situation of the Altice group with regard to Section II of Article L.430-8 of the French Commercial Code.

completing the transaction before the FCA has given its clearance (the 'standstill obligation'). In particular, the standstill obligation means that the parties to the transaction must continue to act as independent businesses until clearance. In France, implementing notifiable transactions prior to clearance (including where such transactions have been notified but not yet cleared by the competition authorities – i.e., gun jumping) can be fined up to 5 per cent of the parties' French turnover.

In the present case, even though no shares or assets of the targeted entities had been transferred to Altice prior to the FCA's approval, the latter considered that Altice exercised a significant influence on its targets and had access to strategic information by, in particular, intervening in the operational management of SFR, starting the implementation of a coordinated strategy, exchanging strategic information such as data on SFR's recent business performance and starting managerial integration.

Appendix 1

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

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

ISBN 978-1-910813-90-4