

Access to telecommunication data is an essential and powerful investigative tool in criminal justice. At the same time, the interception of such data can seriously affect individual privacy. This is true not only with respect to content data but also with respect to traffic data. The legal instruments and provisions that allow the gathering of these data are primarily the traditional rules on the interception of telecommunication based on the cooperation duties of telecommunication providers. In addition, access to telecommunication data can also be granted by rules on remote forensic software, by search and seizure of – temporarily or permanently – stored data, and (especially in cases of traffic and subscriber data) by production orders demanding the delivery of stored data.

The rules governing these interception techniques vary considerably among the national legal orders. These differences are not only most interesting from the perspective of fundamental research in the area of comparative criminal law but also for practical reasons, such as identifying best practices and evaluating the scope of international cooperation.

This publication provides a comparative analysis dealing with the commonalities and differences of these rules on interception and other means of access to telecommunication data. It also includes country reports on the following European legal orders, which form the basis of this comparison: Belgium, Czech Republic, France, Germany, Spain, Sweden, and the United Kingdom.

ISBN 978-3-36113-796-2 (Max-Planck-Institut)
ISBN 978-3-428-15143-1 (Duncker & Humblot)



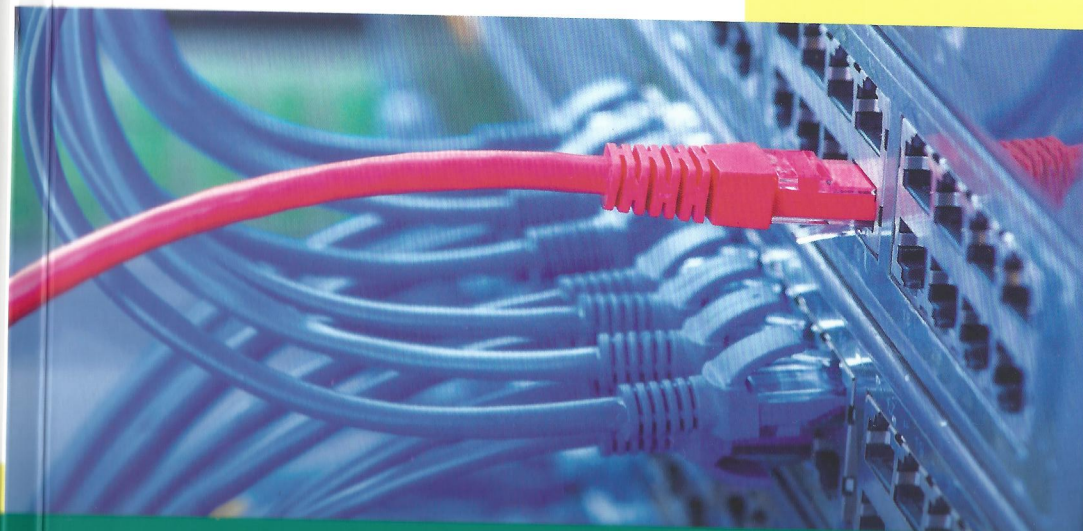
Ulrich Sieber / Nicolas von zur Mühlen (eds.)
**Access to Telecommunication
Data in Criminal Justice**

A Comparative Analysis of European Legal Orders

Schriftenreihe des Max-Planck-Instituts
für ausländisches und internationales
Strafrecht

Strafrechtliche Forschungsberichte
Herausgegeben von Ulrich Sieber

Band S 156



Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische
Daten sind im Internet über <<http://dnb.ddb.de>> abrufbar.

Alle Rechte vorbehalten

© 2016 Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.

c/o Max-Planck-Institut für ausländisches und internationales Strafrecht

Günterstalstraße 73, 79100 Freiburg i.Br.

<http://www.mpicc.de>

Vertrieb in Gemeinschaft mit Duncker & Humblot GmbH, Berlin

<http://www.duncker-humblot.de>

Umschlagbild: © istock.com/kynny

Druck: Stückle Druck und Verlag, Stückle-Straße 1, 77955 Ettenheim

Printed in Germany

ISSN 1860-0093

ISBN 978-3-86113-796-2 (Max-Planck-Institut)

ISBN 978-3-428-15143-1 (Duncker & Humblot)

Gedruckt auf alterungsbeständigem (säurefreiem) Papier

entsprechend ISO 9706 ☞

Schriftenreihe des Max-Planck-Instituts für
ausländisches und internationales Strafrecht

Strafrechtliche Forschungsberichte

Herausgegeben von Ulrich Sieber

Band S 156



Max-Planck-Institut für ausländisches
und internationales Strafrecht

Access to Telecommunication Data in Criminal Justice

A Comparative Analysis
of European Legal Orders

Ulrich Sieber • Nicolas von zur Mühlen (eds.)



Duncker & Humblot • Berlin

France*

National Rapporteur:
Estelle De Marco

* This report reflects legislation and case law as of April 2016.

Contents

I. Security Architecture and the Interception of Telecommunication	441
A. Law Enforcement Institutions and Public Authorities with Powers of Electronic Communications Interception	441
1. Legal regimes organising the interception and the collection of electronic communications	441
2. Powers for the interception of electronic communications	443
a) Law of penal procedure	443
b) Law of intelligence agencies	444
aa) Areas in question	444
bb) Legal provisions	445
c) Prevention of attacks on automated data processing systems	446
d) Prevention of terrorist acts	446
e) Customs Investigation Service	447
3. Responsibility for the technical performance of interception measures	447
4. Legitimacy of data transfers between security and law enforcement agencies	450
a) Separation of functions	450
b) Exchange of data between law enforcement authorities and intelligence agencies	450
aa) Passing on of data by law enforcement authorities to intelligence agencies	450
bb) Passing on of data by intelligence agencies to law enforcement authorities	451
B. Statistics on Electronic Communications Interception	451
II. Principles of Electronic Communications Interception in Constitutional and Criminal Procedural Law	452
A. Constitutional Safeguards of Electronic Communication	452
1. Areas of constitutional protection	452
a) Secrecy of telecommunication	453
b) Personal data protection	454
2. Proportionality of access to data	454
3. Consequences for the interception of telecommunication	456
4. Statutory protection of personal data	457

France	437
B. Powers in the Penal Procedure Code	458
1. Requirement of (reasonable) clarity for powers in the law of criminal procedure	458
2. Differentiation and classification of powers in the law of criminal procedure	458
III. Powers for Accessing Electronic Communication Data in the Law of Criminal Procedure	458
A. Overview	458
B. Interception of Content Data	458
1. Statutory provision	459
a) Correspondence interceptions	459
b) Remote data capture	461
c) Interception of the content of the information accessed by users of electronic communications operators' services	463
2. Scope of application	464
a) Object of interception and temporal limits of electronic communication	464
aa) Correspondence interception	464
bb) Remote data capture	466
cc) Interception of the content of the information accessed by users of electronic communications operators' services	466
b) Current matters of dispute	466
aa) Rules protecting correspondence before their reception by the recipient	466
bb) Direct access to mailboxes using their password	467
3. Special protection of confidential communication content	468
a) Privileged correspondence	468
b) Prohibition of transcription of certain types of correspondence	468
c) Privileged computer data within the framework of remote data capture	468
4. Execution of electronic communications interception	469
5. Duties of electronic communication service providers to cooperate	469
6. Formal prerequisites of interception orders	471
a) Competent authorities	471
aa) Correspondence interception	471
bb) Remote data capture	472
cc) Interception by service providers of the content of the information accessed by their users	472
b) Formal and substantive requirements for applications and orders	473

aa) Correspondence interceptions	473
bb) Remote data capture	473
cc) Interception by service providers of the content of the information accessed by their users	474
7. Validity of interception orders	474
a) Correspondence interception	474
aa) Maximum length of interception order	474
bb) Revocation of authorisations	475
b) Remote data capture	475
aa) Maximum length of interception order	475
bb) Revocation of authorisations	475
c) Interception by service providers of the content of the information accessed by their users	476
aa) Maximum length of interception order	476
bb) Revocation of authorisations	476
8. Duties to record, report, and destroy	476
a) Correspondence interception	476
b) Remote data capture	477
c) Interception by service providers of the content of the information accessed by their users	477
9. Notification duties, remedies and consequences	477
10. Confidentiality requirements	478
C. Collection and Retention of Traffic Data and Subscriber Data	478
1. Collection of traffic data and subscribers data	478
a) Relevant information and prerequisite of collection	478
aa) Requisition of traffic and connection data	478
bb) Remote access to stored data	479
cc) Access to subscribers lists	480
b) Duty of addressees to disclose information	480
c) Automated procedure of disclosure	480
2. Data retention	481
3. Location of mobile terminal device	482
D. Access to Stored Communication Data	482
1. Search and seizure of stored electronic communication data	482
2. Duties to cooperate: production and decryption orders	483
a) Duties to cooperate	483
b) Non application to the defendant	483
3. Power of judicial authorities to decrypt encrypted data that are necessary to ascertain the truth	484
E. Taking of Audio Recordings and Visual Images	486

IV. Use of Electronic Communication Data in Judicial Proceedings	486
A. Use of Electronic Communication Data in the Law of Criminal Procedure	487
1. Evidence produced by public authorities	487
2. Evidence produced by private parties	488
B. The Right for the Accused to Challenge the Probity of Intercepted Data	489
V. Exchange of Intercepted Electronic Communication Data between Foreign Countries	489
A. Legal Basis for Mutual Legal Assistance	489
1. General provisions	490
2. Provisions specific to cooperation between France and other EU Member States	491
B. Requirements and Procedure	492
1. Simplified exchange of information, implementing Decision 2006/960/JAI of 18 December 2006	492
a) General provisions	492
b) Requests for information issued by French services	493
c) Requests for information received by French services	493
2. Other provisions	495
Bibliography	496
List of Abbreviations	497

I. Security Architecture and the Interception of Telecommunication

A. Law Enforcement Institutions and Public Authorities with Powers of Electronic Communications Interception

Several legal regimes organise the interception and the collection of electronic communications under French law. However, comprehensive and updated statistics are not consistently available in all cases.

1. Legal regimes organising the interception and the collection of electronic communications

Under French law, electronic communications are defined as “emissions, transmissions or reception of signs, signals, writings, images or sounds, by electromagnetic means.”¹

The formula “electronic communications” has replaced the term “telecommunications” according to a law of 9 July 2004.² Therefore, where French law still mentions the term of “telecommunications,” this notion has to be understood as “electronic communications.”

The interception of electronic communications is not provided for as such. French law distinguishes between several types of communications, which may be intercepted or accessed by judicial institutions and/or administrative services following different kinds of procedures, mainly within the framework of the application of either (repressive) penal law, or State security law (which includes the prevention of terrorism, of organised crime, and of organised delinquency). Additionally, some traffic data may be accessed for the purpose of the prevention of attacks on automated data processing systems.

These types of communications and the legal regimes governing their interception or collection are the following:

- Electronic correspondence. These communications receive strong legal protection and may only be intercepted under strict conditions. Electronic correspondence interceptions are organised by repressive penal law and state security law.

¹ Art. L. 32-1 of the Post and Electronic Communications Code (PECC).

² Law n°2004-669 of 9 July 2004; see also Court of cassation, criminal chamber, 8 July 2015, available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4696

- Traffic and connection data. Several procedures allow the access to or the interception of a limited list of this kind of data under particular conditions:
 - Access to traffic and connection data retained by certain service providers is organised by repressive penal law and state security law. Additionally, access to these data may take place for the purposes of the prevention of terrorist acts and of the prevention of attacks on automated data processing systems.
 - Real time collection of these data on service providers' networks is organised for the prevention of terrorist acts only, by State security law n° 2015-912 of 24 July 2015 (entered into force October 2015³).
 - Direct collection of some of these data (including location data) by means of an intrusion into the computer system is organised by the above-mentioned State security law n° 2015-912 of 24 July 2015.
 - Geolocation of a person, a vehicle or an object, is organised by repressive penal law and the above-mentioned State security law n° 2015-912 of 24 July 2015.
- Other forms of private communications, as well as public communications, are not subject to specific intercept or access procedures. They may be collected within the framework of the application of the three following more general procedures:
 - The ordinary legal system governing search and seizure of information held by a third party, organised by repressive penal law;
 - A procedure that permits requiring from electronic communications operators the preservation of the content of the information accessed by their users, organised by repressive penal law;
 - A procedure allowing remote computer data capture, organised by repressive penal law and the above-mentioned State security law n° 2015-912 of 24 July 2015.
- Finally, all communications may be monitored at the service provider level for the purposes of real-time detection of "connections that may reveal a terrorist threat," as permitted by the above-mentioned State security law n° 2015-912, for the prevention of terrorism only.

³ Law n° 2015-912 of 24 July 2015 relating to intelligence, JORF n°0171 of 26 July 2015, p. 12735, text n°2; legislative dossier available at <http://www.senat.fr/dossier-legislatif/pjl14-424.html>. Its entry into force was scheduled the day after the publication of a decree nominating the President of a new established "National Commission for intelligence techniques control," which replaces the current "National Commission for security intercepts control." This Decree was published on 2 Oct. 2015 (Decree of 1 October 2015 on the composition of the National Commission for intelligence techniques control/*Décret du 1er octobre 2015 relatif à la composition de la Commission nationale de contrôle des techniques de renseignement*), JORF n°0228 of 2 Oct. 2015 p. 17882, text n°26.

2. Powers for the interception of electronic communications

Powers for the interception of electronic communications are different depending on the legal regime.

a) Law of penal procedure

Electronic correspondence may be intercepted in limited situations, following the procedure described in articles 100 to 100-7⁴ and article 706-95 of the Penal Procedure Code.

Traffic and connection data retained by service providers⁵ can be requisitioned according to articles 77-1-1 (preliminary investigation), 60-1 (flagrancy investigation) and 99-3 (investigation procedure conducted by an investigative judge) of the Penal Procedure Code.

Real-time geolocation of a person, a vehicle or an object, without the consent of this person or the owner of this vehicle or object, can be done in limited situations according to articles 230-32 to 230-44 of the Penal Procedure Code.

The ordinary legal system governing search and seizure of information held by a third party is set out in articles 76 to 76-3 (preliminary investigation), 56 to 59 (flagrancy investigation), 92 to 99-4 (investigation procedure conducted by an investigative judge), and 706-89 (in relation with a limited list of crime or misdemeanours) of the Penal Procedure Code.

The procedure that permits requiring the preservation of the content of the information accessed by their users by electronic communications operators is described in articles 77-1-2 (preliminary investigation), 60-2 (flagrancy investigation) and 99-4 (investigation procedure conducted by an investigative judge) of the Penal Procedure Code.

The procedure that allows remote computer data capture (in relation with a limited list of crime or misdemeanours) is described in articles 706-102-1 to 706-102-9 of the Penal Procedure Code.

⁴ These and the following articles are available in French language at <https://www.legifrance.gouv.fr/>

⁵ On the basis of art. L. 34-1 PECC and of art. 6 of the Law n°2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN").

b) *Law of intelligence agencies*aa) *Areas in question*

The following provisions may be used within the framework of the search for information by intelligence services and agents of several ministries listed by law and their implementing administrative acts, in the pursuit of a limited number of objectives.

Until October 2015 these objectives were:⁶ national security; safeguard of essentials elements of the French scientific and economic potential; prevention of terrorism; prevention of organised crime and organised delinquency; prevention of the reconstitution or of the preservation of disbanded groups.⁷

These objectives have been replaced by the search for information relating to the defence and promotion of the following “fundamental interests of the nation”:⁸

- National independence, territorial integrity, and national defence;
- Major interests of foreign policy, implementation of France’s European and International commitments, and prevention of any form of foreign interference;
- Major economic, industrial, and scientific interests of France;
- Prevention of terrorism;
- Prevention of:
 - attacks against the republican form of French institutions,
 - actions pursuing the reconstitution or the preservation of disbanded groups,⁹
 - collective violence likely to cause serious harm to public peace;
- Prevention of organised crime and delinquency;
- Prevention of proliferation of weapons for mass destruction.

It must also be noted that, despite the fact that the aforementioned objectives are theoretically the only ones that can justify the exercise of the exceptional measures described in the next subsection, French law requires that any (other) crime or misdemeanour discovered upon exercising these special powers is brought to the atten-

⁶ Former art. L. 241-2 Internal Security Code (ISC).

⁷ Art. L. 212-1 ISC lists exhaustively the categories of groups that must be disbanded by decree issued by the Council of Ministers (such as groups provoking armed events in the streets).

⁸ According to the new art. L. 811-3 ISC, created by Law n° 2015-912 of 24 July 2015 relating to intelligence, JORF n°0171 of 26 July 2015, p. 12735, text n°2; legislative dossier available at <http://www.senat.fr/dossier-legislatif/pjl14-424.html>. This article entered into force on 3 Oct. 2015 (see footnote n°3).

⁹ Art. L. 212-1 ISC. See footnote n°7 above.

tion of the public prosecutor (who has the discretion to take action on it), accompanied by related information.¹⁰

bb) *Legal provisions*

Electronic correspondence could be intercepted, until October 2015, following the procedure described in former articles L. 241-1 *et seq.* of the Internal Security Code. This procedure has been replaced by a new one that results from the law of 24 July 2015 (entered into force on 3 October 2015¹¹). This procedure is now described in articles L. 852-1 and L. 821-1 *et seq.* of the Internal Security Code.

Traffic and connection data¹² retained by service providers¹³ can be accessed according to articles L. 851-1 and L. 851-4 of the new Internal Security Code 5 (including access by “network solicitation” and “real-time transmission by operators”), corresponding to former articles L. 246-1 to L. 246-4 of the Internal Security Code.

¹⁰ Former art. L. 242-8 ISC (relating to correspondence intercepts) and current (from the 3 Oct. 2015) art. L. 811-2 of the latter Code (relating to all the measures described in the next subsection). These articles refer to art. 40 of the Penal Procedure Code (PPC), which in turn lays down this obligation.

¹¹ Law n° 2015-912 of 24 July 2015 relating to intelligence, *op. cit.*

¹² More precisely, data that may be accessed are more widely identified by law (in art. L. 851-1, former art. L. 246-1) as being “information or documents processed or stored by (ISP’s) networks or electronic communications services, including technical information relating to the identification of subscription or connection numbers to electronic communications services, to the census of all subscription numbers and connection numbers of a specified person, to the geolocation of terminal equipment used, and to a user’s communications regarding the list of called and calling numbers, the duration and date of communications.” The decree of application of the original provision (art. L. 246-1, created by Law n°2013-1168 of 18 Dec. 2013, art. 20), specified that these data are the ones, which are of a technical nature only and cannot relate to the content of communications that can be accessed by the judiciary for the repression of crimes (Decree n°2014-1576 of 24 Dec. 2014 – <http://www.legifrance.gouv.fr/eli/decret/2014/12/24/PRMD1422750D/jo>). The decree of application of the new law (Decree n° 2016-67 of 29 Jan. 2016) refers to the same data. It provides for an additional list of data that may be accessed by intelligence services or other Ministries, but only within the framework of administrative correspondence intercepts. It should be noted that the French Constitutional Council has recalled that traffic data that can be accessed for intelligence purposes cannot be related to the content of correspondence or to consulted information (Decision n°2015-713 DC, recital n° 55, <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc2015713dc.pdf> – press release: <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/communiqu-de-presse.144139.html>).

¹³ These data are retained on the basis of art. L. 34-1 PECC (relating to electronic communications operators and access providers) and of art. 6 of the Law n°2004-575 of 21 June 2004 regarding confidence in the digital economy, so-called LCEN (relating to access and hosting providers).

Direct collection of some of these data (connection data of a technical nature enabling the identification of terminal equipment or the identification of the subscription number of its user, as well as location data of terminal equipment) by means of an intrusion into the computer system is organised by the new article L. 851-6 of the Internal Security Code.

Real-time geolocation of a person, a vehicle or an object, without the consent of this person or the owner of this vehicle or object, is organised by the new article L. 851-5 of the Internal Security Code.

The procedure that allows remote computer data capture is organised by the new article L. 853-2 of the Internal Security Code.

Globally, the situations in which access to the types of data discussed above may take place are wider, persons who may access them are more numerous, accessed data are potentially more numerous, and safeguards in place are lower than those that govern the implementation of access to traffic and connection data by the judiciary for the purpose of the repression of penal infringements.

c) Prevention of attacks on automated data processing systems

Some limited traffic data, namely the identity, the postal address and the electronic address of users or owners of vulnerable, threatened or attacked information systems, retained by electronic communications operators,¹⁴ can be requisitioned according to article L. 2321-3 of the Defence Code, by authorised and sworn agents from the national authority for information systems, in order to alert these persons to the vulnerability or the compromise of their system.

d) Prevention of terrorist acts

All the measures described in the subsection relating to the law of intelligence agencies are applicable for the prevention of terrorist acts.

In addition, for the purpose of terrorism prevention only, there exists

- The possibility to implement on service providers' networks an automated processing aimed at detecting "connections that may reveal a terrorist threat," under new article L. 851-3 of the Internal Security Code.
- The possibility to request real time collection of traffic and connection data (relating to a person previously identified as presenting a threat) on service providers' networks, under new article L. 851-2 of the Internal Security Code.

¹⁴ On the basis of art. L. 34-1 PECC.

e) Customs Investigation Service

According to article 28-1 of the Penal Procedure Code, some specially nominated customs agents may be authorised to conduct judicial investigations in order to look for and report a limited list of infringements, including infringements to the customs Code. Within that framework, judicial procedures described in subsection a. above may be applicable.

In addition, the Decree n° 2015-1185 of 28 September 2015,¹⁵ adopted in order to apply Law n° 2015-912 includes the National Directorate for Custom Intelligence and Investigations (*Direction nationale du renseignement et des enquêtes douanières*) in the list of specialised intelligence services that are entitled to exercise the powers described in subsection b. above. This Directorate is an agency with national authority, within the General Directorate for customs and indirect rights, which itself rests with the Ministry of Finance.¹⁶

Moreover, according to the new article L. 811-4 of the Internal Security Code, a decree issued by the Council of State designates services other than intelligence services that may be authorised to exercise the powers granted to intelligence services as they have been detailed in subsection b. above, and these services may belong to customs services. The Decree n°2015-1639 of 11 December 2015¹⁷ did not designate services other than some services that belong to the Ministry of Defence and the Ministry of Interior. However, subsequent decrees might follow.¹⁸

3. Responsibility for the technical performance of interception measures

Under French law, the technical enforcement of interception and data collection measures follows certain rules:

- Regarding correspondence interceptions performed by the judiciary for the purpose of the repression of crimes and misdemeanours, the investigating judge or

¹⁵ Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement, JORF n°0225 du 29 septembre 2015 p. 17344, texte n°1.

¹⁶ <http://www.douane.gouv.fr/articles/a12574-la-direction-nationale-du-renseignement-et-des-enquetes-douanieres>.

¹⁷ Décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure, pris en application de l'art. L. 811-4 du Code de la sécurité intérieure, JORF n°0288 du 12 décembre 2015 p. 22978, texte n° 28.

¹⁸ Before the entry into force of Law n° 2015-912 of 24 July 2015 – therefore before the 3 Oct. 2015 – agents of the Ministry for economy, therefore possibly customs agents, could access traffic and connection data if individually appointed and duly authorised, for limited purposes listed in former art. 241-2 ISC (former art. 246-1 ISC created by art. 20 of Law n° 2013-1168 of 18 Dec. 2013). Correspondence intercept could also be authorised on the proposal of the Ministry in charge of customs (former art. L. 242-1 ISC).

the police officer appointed by this judge can require any qualified agent belonging to a service or organisation placed under the authority of the Ministry in charge of electronic communications, or any qualified agent belonging to an authorised electronic communications service provider, to perform the installation of an interception system.¹⁹

- Regarding remote computer data capture performed by the judiciary for the purpose of the repression of certain crimes and misdemeanours, the investigating judge or the police officer appointed by this judge can require any qualified agent belonging to a service, a unit or a body placed under the authority of the Ministry of Interior or the Ministry of Defence, and which list is established by decree, to perform the installation of the technical devices that enable data captures authorised by law.²⁰
- Regarding geolocation of a person, a vehicle or an object performed by the judiciary in certain situations, the investigating judge or the police officer appointed by this judge can require any qualified agent belonging to a service, a unit or a body placed under the authority of the Ministry of Interior (the list of which is established by decree), to perform the installation and of the removal of the technical device that enables geolocation as authorised by law.²¹
- Regarding search and seizures performed by the judiciary for the purpose of the repression of crimes and misdemeanours, where it is necessary to perform technical or scientific examinations, the public prosecutor or police officer (depending on the nature of the procedure – flagrancy or preliminary investigation) may call upon any qualified person.²² When the procedure is directed by an investigating judge, search and seizures are performed by this judge or the police officer appointed by this judge.²³
- Regarding intelligence gathering techniques (including the prevention of terrorism, organised crime and organised delinquency), Law n° 2015-912 states that the Prime Minister organises traceability of the execution of authorised techniques.²⁴

This law also states that all these techniques can only be implemented by agents individually appointed and authorised for the purpose.²⁵ This is repeated in the provision relating to the possibility of directly collecting some traffic and connection

¹⁹ Art. 100-3 PPC.

²⁰ Art. 706-102-6 PPC.

²¹ Art. 230-36 PPC.

²² Arts. 60 (flagrancy investigation), 77-1 (preliminary investigation) PPC.

²³ Art. 97 PPC.

²⁴ Art. L. 822-1 ISC.

²⁵ Art. L. 821 ISC.

data²⁶ by means of an intrusion into the computer system.²⁷ In addition, in that case, technical devices that are used for the purpose are recorded in a special register made available to the National Commission for the control of intelligence techniques.²⁸

The technical performance of the other intelligence gathering techniques is subject to two different procedures:

- Electronic correspondence intercepts,²⁹ administrative access to traffic and connection data,³⁰ administrative direct access to traffic and connection data using “network solicitation” and “real-time transmission by operators,”³¹ and concerning the prevention of terrorism only, real time collection of traffic and connection data³² and monitoring of service providers’ networks in order to detect “connections that may reveal a terrorist threat,”³³ can only be technically performed following the procedure described in article L. 871-6 of the Internal Security Code,³⁴ which takes over the provisions of the former article L. 242-9 of the Internal Security Code, which was relating to correspondences intercept only.³⁵ According to article L. 871-6, the above-mentioned measures can only be technically performed by qualified agents belonging to the organisation or the service provider in whose premises and installations the measure must be implemented. Regarding qualifications, only the technically competent agents who (1) have been employed for at least two years at the same electronic communications operator, and (2) have not been convicted or found guilty of any criminal offence recorded in bulletin n° 2 of their criminal records³⁶ are able to perform these tasks.
- Real-time geolocation of a person, a vehicle or an object, without the consent of this person or the owner of this vehicle or object,³⁷ and remote computer data

²⁶ Namely technical connection data enabling the identification of terminal equipment or the identification of the subscription number of its user, as well as location data of terminal equipment.

²⁷ Art. L. 851-6, II ISC.

²⁸ Art. L. 851-6, II ISC.

²⁹ Art. L. 852-1 ISC.

³⁰ Art. L. 851-1 ISC.

³¹ Art. L. 851-4 ISC.

³² Relating to a person previously identified as presenting a threat on service providers’ networks, art. L. 851-2 ISC.

³³ Art. L. 851-3 ISC.

³⁴ Created by art. 11 of Law n° 2015-912 of 24 July 2015.

³⁵ The only element that changes, beyond the fact that the procedure is extended to more numerous measures, is that the technical performance of these measures can only be performed by order of the Prime Minister, whereas such an order was the duty of the Ministry for electronic communications in former art. L. 242-9.

³⁶ Art. R 242-4 ISC; see also art. R. 242-6.

³⁷ Art. L. 851-5 ISC.

capture³⁸ can only be technically performed following the procedure described in the new article L. 853-3 of the Internal Security Code.³⁹ According to this article, entrance to a vehicle or to a private location can only be performed by agents individually appointed and authorised for the purpose, who belong to one of the services that may be authorised to use intelligence gathering techniques, the list of which is established by decree issued by the Council of State.⁴⁰

4. Legitimacy of data transfers between security and law enforcement agencies

Services in charge of the repression of criminal offences and services in charge of the prevention of terrorism and organised crime and delinquency are separated, and exchanges of data between these services constitute an exception.

a) Separation of functions

The repressive function and the intelligence function are separated, though some services exercising the first one and some services exercising the second one come under the control of the same ministry (Ministry of Interior). Moreover, most communications intercepts as defined above are performed under the control of an independent judge within the framework of crime repression, whereas they are performed under the control of an independent administrative authority within the framework of intelligence gathering.

b) Exchange of data between law enforcement authorities and intelligence agencies

No accessible general rule provides for the possibility of exchanging information between law enforcement authorities and intelligence agencies, except where a crime or a misdemeanours is discovered during the gathering of intelligence information.

aa) Passing on of data by law enforcement authorities to intelligence agencies

Law n° 2015-912 provides intelligence agencies with the same – and even wider – intercept capabilities as the judiciary, which renders global information exchange unnecessary (in addition, constraints on judges for the purpose of preserving fundamental rights are stronger).

³⁸ Art. L. 853-2 ISC.

³⁹ Created by art. 6 of Law n° 2015-912 of 24 July 2015.

⁴⁰ Art. L. 853-3, § 2 ISC.

bb) Passing on of data by intelligence agencies to law enforcement authorities

According to article 40 of the Penal Procedure Code, when an established authority, a public officer or a public servant learns, during the performance of their duties, of a crime or of a misdemeanour, they must give notice of it to the public prosecutor, and must provide this magistrate with any information, official records and other investigative acts relating to this crime or misdemeanour. The public prosecutor evaluates what further action should be taken in accordance with article 40-1 of the Penal Procedure Code.

B. Statistics on Electronic Communications Interception

Before the entry into force of law n° 2015-912, communication intercepts performed under intelligence law were subject to an annual report of the National Commission for the Control of Security Interceptions (*Commission nationale de contrôle des interceptions de sécurité*, CNCIS), which has been replaced in the new law by the National Commission for the Control of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement*, CNCTR).

According to the CNCIS in its report for the years 2013-2014,⁴¹ 6,182 correspondence intercepts were requested in 2013 (4,213 initial requests and 1,969 renewals), and 6,145 correspondence intercepts were requested in 2012 (4,022 initial requests and 2,123 renewals).⁴²

Moreover, in 2013, 324,243 requests of access to traffic data were issued for national security (71%), delinquency and organised crime prevention (22%), terrorism prevention (3%), protection of the economic and scientific potential (3%), and reconstitution of disbanded groups (1%). 315,792 of these requests were for identification, or requests regarding the history of an identifier or the identification of a cell. 5,451 measures consisting of traffic details (which are more intrusive) were also reviewed. 7% of the measures were refused and 10% were subject to referral for additional information prior to their validation. The number of requests that were met increased by 61% in comparison with 2012. This increase relates exclusively to identification measures.⁴³

Moreover, 36,712 additional requests (compared with 29,322 in 2012) were related to combatting terrorism. 34,366 were validated (compared with 26,563 in 2012). A percentage close to 65% was composed of requests for subscriber identification, and a percentage close to 35% was composed of requests for traffic de-

⁴¹ This report is available at <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000101.pdf>

⁴² See p. 80 of the report.

⁴³ See pp. 96 *et seq.* of the report.

tails. In 2013, 20% of these requests related to fixed telephony, 67% to mobile telephony, and 13% to Internet.⁴⁴

Regarding communications intercepts performed by the judiciary for the repression of crime and delinquency, less exact figures are known. In 2012, 35,000 telephone communications intercepts, 650,000 judicial requisitions of traffic data and 12,000 geolocations took place.⁴⁵

II. Principles of Electronic Communications Interception in Constitutional and Criminal Procedural Law

Constitutional principles frame the powers for interception and collection of electronic communications that are set out in the Penal Procedure Code.

A. Constitutional Safeguards of Electronic Communication

Constitutional safeguards of electronic communications have consequences for the description of the powers for intercepting or collecting electronic communications in the Penal Procedure Code, and are reflected in other legal texts.

1. Areas of constitutional protection

French constitutional safeguards do exist but do not refer explicitly to the protection of electronic communications.

The right to respect for private and family life is protected by the French Constitutional Council under “articles 2 and 4⁴⁶ of the French Human and Citizens Rights

⁴⁴ See p. 99 of the report.

⁴⁵ Club DJS, “Les écoutes judiciaires – Contributions au débat,” 1 April 2014, <http://www.droits-justice-et-securites.fr/2014/04/les-ecoutes-judiciaires/>; Franck Johannès, “Les écoutes judiciaires ont explosé depuis 2006,” 18 March 2014, *Le Monde*, http://www.lemonde.fr/societe/article/2014/03/18/les-ecoutes-judiciaires-ont-explose-depuis-2006_4384910_3224.html. Some publications evoke the number of 20,000 instead of 35,000 communication intercepts, see <http://www.senat.fr/leg/ppr13-422.html>. Some media evokes in addition 5,500,000 “additional services” such as access to detailed invoicing: see Franck Johannès, above [last accessed on 19 Sept. 2015].

⁴⁶ Art. 2: “The aim of every political association is the preservation of the natural and imprescriptible rights of Man. These rights are Liberty, Property, Safety and Resistance to Oppression”; Art. 4: “Liberty consists in being able to do anything that does not harm others: thus, the exercise of the natural rights of every man has no bounds other than those that ensure to the other members of society the enjoyment of these same rights. These bounds may be determined only by Law.” The Declaration is available in English on the

Declaration of 1789,⁴⁷ the latter Declaration being included in the so-called French “constitutionality bloc” (which has a constitutional value). The French Constitutional Council also protects some aspects of the right to respect for private life under the principle of personal freedom,⁴⁸ the guarantor of which is the Parliament, in accordance with article 34 of the Constitution.⁴⁹

a) Secrecy of telecommunication

The respect for private and family life includes the secrecy of correspondence⁵⁰ transmitted by means of electronic communications, and information consulted using an electronic communications network.⁵¹ It also includes the protection of connection and traffic technical data.⁵²

Constitutional Council website: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/cst2.pdf

⁴⁷ See, e.g., French Constitutional Council, Decision n° 2004-492 DC of 2 March 2004, J.O. 10 March 2004, p. 4637, recital n° 4; Decision n° 2005-532 DC of 19 Jan. 2006, recital n° 9.

⁴⁸ Other elements of personal freedom are, under French law, the freedom of movement, the right to not being arbitrarily arrested or sequestered, the right to be judged with all legal guarantees and the principle of inviolability of the home. See Jacques Robert et Jean Duffar, *Droits de l'homme et libertés fondamentales*, éd. Montchrestien, 7ème éd., 1999, p. 27; art. 136 PPC; Estelle De Marco, “Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux,” 4 June 2009, *Juricom.net*, p. 3, available at <http://www.juricom.net/uni/visu.php?ID=1133>

⁴⁹ The Constitutional Council considers that the refusal to take into consideration the right to respect of private life can be liable to hurt personal freedom: Decision n° 94-352 DC, 18 Jan. 1995, J.O. 21 Jan. 1995, p. 1154 and JCP 1995, II, 22 525, note *Frédérique Lafay*. The Council also analysed the implementation of technical mechanisms allowing picking-up, fixing or registering words or images without the consent of interested people, in the light of personal freedom: Decision n° 2004-492 DC, 2 March 2004, JORF 10 March 2004, p. 4637. The Council also extends the notion to some personal data filing systems: Decision n° 2004-492 DC, 2 March 2004, JORF 10 March 2004, p. 4637, § n° 64. On all these elements, see Estelle De Marco, “Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux”, *op. cit.* and Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT, n° 20. The French Constitution is available in English on the Constitutional Council website: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/constitution_anglais_juillet2008.pdf

⁵⁰ It also includes the “freedom” to correspond: see, e.g., Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT, n° 132 *et seq.*; Virginie Peltier, *Le secret des correspondances*, PU d'Aix-Marseille, 1999, p. 99 *et seq.*, n°119 *et seq.*; Pierre Kayser, *La protection de la vie privée par le droit*, PU d'Aix-Marseille/Economica, 3rd ed., 1995, especially pp. 11–12, p. 60.

⁵¹ See, e.g., French Constitutional Council, Decision n°2015-478 QPC of 24 July 2015, recital n° 10 *et seq.*

⁵² French Constitutional Council, Decision n°2005-532 DC of 19 Jan. 2006, recitals n° 9 to n° 21.

b) Personal data protection

In addition, the respect for private and family life includes the right to the protection of personal data, and more precisely "collection, recording, retention, consultation and communication of personal data."⁵³

2. Proportionality of access to data

According to the French Constitutional Council, limitations to the right to private and family life, which include, as already analysed, the protection of electronic communications and personal data, "must be justified by a reason in the public interest and implemented properly and in a manner proportionate to this end."⁵⁴ In other decisions, in relation to the preservation of the freedom of expression, the Council used a slightly different test that any limitation to this right must be necessary, adequate and proportionate to the aim pursued.⁵⁵

Overall, the meaning of these formulas is close to the notions of "necessity" and "proportionality" used by the European Court of Human Rights.⁵⁶ Indeed, in the words of a legal author, the French Constitutional Council seems to have "aligned its jurisprudence with the one of the E. Court H. R., since it performs a similar proportionality test, between general interests on the one hand and the limitation

⁵³ French Constitutional Council, Decision n° 2012-652 DC of 22 March 2012, recital n° 8; Decision n° 2013-681 DC of 5 Dec. 2013, recital n° 27; see also French Constitutional Council, Commentary on the Decision n° 2014-690 DC of 13 March 2014, p. 20.

⁵⁴ French Constitutional Council, Decision n° 2012-652 DC of 22 March 2012, recital n° 8; Decision n° 2013-681 DC of 5 Dec. 2013, recital n° 27; see also French Constitutional Council, Commentary on the Decision n° 2014-690 DC of 13 March 2014, p. 20, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2014690DCccc_690dc.pdf [last accessed on 18 Sept. 2015].

⁵⁵ See, e.g., French Constitutional Council, Decision 2009-580 DC of 10 June 2009, recital n° 15; Decision 2012-647 DC of 28 Feb. 2012, recital n° 5; Decision n° 2010-3 QPC of 28 May 2010, recital n° 6.

⁵⁶ The European Convention on Human Rights (ECHR) is in France of infra-constitutional but supra-legal force, even though the national law is subsequent to the Convention. Indeed, the Convention is directly integrated into the local system by the Constitution, as its art. 55 states that "Treaties or agreements duly ratified or approved shall, upon publication, prevail over Acts of Parliament, subject, with respect to each agreement or treaty, to its application by the other party" (the second part of the text does not receive application because the principle of reciprocity does not apply as regards the ECHR.). See Frédéric Sudre, "La dimension internationale et européenne des libertés et droits fondamentaux," in *Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, ed. Dalloz, 11th ed., 2005, p. 39, n° 68; Estelle De Marco and Cormac Callanan, in C. Callanan, M. Gercke, E. De Marco and H. Dries-Ziekenheiner, *Internet blocking – balancing cybercrime responses in democratic societies*, October 2009, n° 6.5.2.2, available at <http://www.aconite.com/blocking/study> (French version available at <http://juriscom.net/2010/05/rapport-filtrage-dinternet-equilibrer-les-responses-a-la-cybercriminalite-dans-une-societe-democratique-2/>) [last accessed on 18 Sept. 2015].

brought to a freedom on the other hand, based on the principle of separation of powers."⁵⁷

The Constitutional Council may verify the adequacy of the measure in relation with its aim,⁵⁸ the appropriateness of the resources allocated in pursuit of this aim (even though the Council considers that it is not its duty to verify if the aim could have been achieved using other means),⁵⁹ and the necessity to combat the issue that justifies the measure⁶⁰ (which are the three elements that compose the notion of "necessity" according to the European Court of Human Rights⁶¹).

Regarding proportionality in the strictest sense, and particularly in the area of the protection of the right to private life, the French Constitutional Council considers that it is the mission of the Parliament, on the basis of article 34 of the Constitution, to lay down the rules relating to fundamental safeguards that must be granted to individuals for the exercise of their public freedoms.⁶² In addition, the Constitutional Council generally verifies whether legal guarantees are adequate and sufficient.⁶³

⁵⁷ Olivier Dutheillet de Lamothe, "L'influence de la Cour européenne des droits de l'Homme sur le Conseil constitutionnel," 13 Feb. 2009, Conseil constitutionnel, visite du Président et d'une délégation de la Cour européenne des droits de l'homme au Conseil constitutionnel, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/pdf/Conseil/cedh_130209_odutheillet.pdf, p. 9. See also Estelle De Marco, *Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux*, 4 June 2009, p. 16, Juriscom.net, <http://juriscom.net/2009/06/hadopi-analyse-du-nouveau-mecanisme-de-prevention-de-la-contrefacon-a-la-lumiere-des-droits-et-libertes-fondamentaux/>

⁵⁸ See, e.g., French Constitutional Council, Decision n° 2009-599 DC of 29 Dec. 2009, recital n° 81; see also Valérie Goessel-Le Bihan, "Le contrôle de proportionnalité exercé par le Conseil constitutionnel, technique de protection des libertés publiques?" <http://juspoliticum.com/Le-controle-de-proportionnalite.html> [last accessed on 22 Sept. 2015].

⁵⁹ See, e.g., French Constitutional Council, Decision n° 2000-433 DC of 27 July 2000, recital n° 41; see also Valérie Goessel-Le Bihan, "Le contrôle de proportionnalité exercé par le Conseil constitutionnel, technique de protection des libertés publiques?", *op. cit.*

⁶⁰ See, e.g., French Constitutional Council, Decision 2009-580 DC of 10 June 2009, recital n° 13.

⁶¹ See, e.g., Estelle De Marco et al., *D3.3 – Legal recommendations*, Deliverable, ePOOLICE project (early Pursuit against Organized Crime Using Environmental Scanning, the Law and Intelligence Systems), project n° FP7-SEC-2012-312651, version 1.2 of 29 Aug. 2014 and version 1.3 of 10 Dec. 2014.

⁶² See, e.g., French Constitutional Council, Decision 2009-580 DC of 10 June 2009, recital n° 23, *op. cit.*

⁶³ See, e.g., French Constitutional Council, Decision n° 2013-681 DC of 5 Dec. 2013, recital n° 28; French Constitutional Council, Decision n° 2012-652 DC of 22 March 2012, recital n° 8; see also *La proportionnalité dans la jurisprudence constitutionnelle*, 5ème conférence des Chefs d'institution de l'Association des Cours constitutionnelles ayant en partage l'usage du français, 8–13 July 2008, p. 7, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/Bilan_2008/confV_accpuf_libre_ville_juillet2008.pdf

Among these legal guarantees or safeguards, lies the respect of the principle that offences and penalties must be defined by law. Other safeguards are the respect of the rights of the defence;⁶⁴ the limitation of the duration of the measure;⁶⁵ the limitation of the number of people who may suffer from the limitation;⁶⁶ the limitation and the definition of the purposes⁶⁷ and of the situations⁶⁸ in which the measure can be exercised; and the existence of an independent control of the implementation of the measure.⁶⁹ During these controls, the nature and sensitivity of data that may be collected are naturally also taken into account.⁷⁰

3. Consequences for the interception of telecommunication

The consequences of the Constitutional Council jurisprudence is that the law authorising the limitation of the right to private life must be necessary and proportionate, which implies that it provides for adequate safeguards. Otherwise, the Constitutional Council may declare the law unconstitutional, if the law is referred to it before it is enacted. The request must in this case be submitted by the President of the Republic, the Prime Minister, the President of one of the two Parliament's chambers, or by 60 members of the National Assembly or 60 members of the Senate.⁷¹

In addition, after the law is enacted, citizens can challenge the compliance of a law with the Constitution on the occasion of a trial. The judge must in this case, if the request is considered admissible and if criteria established by law are met,⁷² transmit the request to the Court of Cassation or to the Council of State (depending on the nature of the trial), which may transfer in turn the request to the Constitutional Council.⁷³

⁶⁴ See, e.g., French Constitutional Council, Decision 2009-580 DC of 10 June 2009, recital n° 14, *op. cit.*

⁶⁵ See, e.g., French Constitutional Council, Decision 2004-492 DC of 2 March 2004, recital n° 59; Decision n° 2013-681 DC of 5 Dec. 2013, recital n° 28.

⁶⁶ See, e.g., French Constitutional Council, Decision 2004-492 DC of 2 March 2004, recital n° 59, *op. cit.*; Decision n° 2012-652 of 22 March 2012, recital n° 10.

⁶⁷ See, e.g., French Constitutional Council, Decision n° 2012-652 of 22 March 2012, recital n° 10 *op. cit.*

⁶⁸ See, e.g., French Constitutional Council, Decision 2004-492 DC of 2 March 2004, recital n° 59, *op. cit.*; Decision n° 2013-681 DC of 5 Dec. 2013, recital n° 28.

⁶⁹ See, e.g., French Constitutional Council, Decision 2004-492 DC of 2 March 2004, recital n° 59, *op. cit.*

⁷⁰ See, e.g., French Constitutional Council, Decision n° 2012-652 of 22 March 2012, recitals n° 10 and n° 11, *op. cit.*

⁷¹ Art. 61 French Constitution.

⁷² These criteria are set out in the organic law n° 2009-1523 of 10 Dec. 2009.

⁷³ Art. 61-1 French Constitution. See also "Comment saisir le Conseil constitutionnel?," <http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/le-conseil->

4. Statutory protection of personal data

In addition to the constitutional protection, all private life aspects are protected by the French civil judge on the basis of article 9 of the civil Code and of article 8 of the European Convention on Human Rights (ECHR).⁷⁴ Moreover, some other legal provisions protect specific private life aspects or more generally personal or confidential data, such as the following:

- Correspondence (including electronic correspondence) is protected during transmission by articles 226-15 and 432-9 of the French Penal Code.⁷⁵
- The protection of personal data is organised by Law n° 78-17 of 6 January 1978 (last modified in 2015). Some of its provisions are subject to penal charges according to articles 226-16 to 226-24 of the French Penal Code. The principle of specified, explicit and legitimate purpose is declared in Article 6 of Law n° 78-17.
- Attacks on automated data processing systems are punished by articles 323-1 to 323-8 of the French Penal Code, last modified in 2015.⁷⁶

constitutionnel/la-saisine/comment-saisir-le-conseil-constitutionnel/-comment-saisir-le-conseil-constitutionnel.17421.html

⁷⁴ See, e.g., a case of annulment of a criminal procedural act consisting of the geolocation of the accused, because French law did not provide for a clear legal basis authorising such a procedural act and providing for adequate safeguards: Cass. crim., 22 October 2013, n°13-81945.

⁷⁵ Art. 226-15 French Penal Code (PC): "Maliciously opening, destroying, delaying or diverting of correspondence sent to a third party, whether or not it arrives at its destination, or fraudulently gaining knowledge of it, is punished by one year's imprisonment and a fine of € 45,000." "The same penalty applies to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by electronic means, or the setting up of a device designed to produce such interceptions." Art. 432-9: "Except where provided for by law, the ordering, committing or facilitation of the misappropriation, suppression or opening of correspondence, and the disclosure of the contents of such correspondence, by a person holding public authority or discharging a public service mission acting in the course of or on the occasion of his office or duty, is punished by three years' imprisonment and a fine of € 45,000."

The same penalties apply to the persons referred to under the previous paragraph, or to employees of electronic communication networks open to the public, or to employees of a supplier of telecommunication services, who, acting in the performing of their office, order, commit or facilitate, except where provided for by law, any interception or misappropriation of correspondence sent, transmitted or received by a means of telecommunication, or the use or the disclosure of its contents."

⁷⁶ An English version of these provisions that does not take into account the most recent legal modifications is available at http://www.legifrance.gouv.fr/content/download/1957/13715/version/4/file/Code_33.pdf. Most modifications are relating to penalties, which have been increased.

B. Powers in the Penal Procedure Code

As a result of constitutional principles, powers in the law of criminal procedure must be clearly defined by specific provisions.

1. Requirement of (reasonable) clarity for powers in the law of criminal procedure

As has been described in A above, the definition of coercive powers in criminal procedural law must be described by the law itself, and the principle "no crime without legal definition" is applicable under French law, meaning *inter alia* that criminal statutes must be defined precisely by the legislator before the commission of a criminal act can be assumed.

2. Differentiation and classification of powers in the law of criminal procedure

As a consequence, coercive powers in French criminal procedural law must be based on differentiated, precise, and specific provisions.

III. Powers for Accessing Electronic Communication Data in the Law of Criminal Procedure

Powers of accessing electronic communications, understood in a broad sense, cover powers relating to the interception of content data, including sounds and visual images, and to the collection and retention of technical connection and traffic data.

A. Overview

As explained in subsections I.A.1. and 2., the above-mentioned powers are subject to several procedures precisely described in the Penal Procedure Code.

B. Interception of Content Data

It has already been noted that the French Penal Procedure Code distinguishes between correspondence and other kinds of electronic data and communications. Correspondence can be intercepted following a specific procedure, whereas other pro-

cedures enable the interception of other type of communications (beyond the search and seizure procedure, which will be analysed later in this report).

These other procedures are the following: a procedure allowing remote data capture, and a procedure that requires electronic communications operators to preserve the content of the information accessed by their users.

1. Statutory provision

a) Correspondence interceptions

The interception of the content of electronic correspondence is set out in articles 100 to 100-7⁷⁷ and article 706-95 of the Penal Procedure Code.⁷⁸

Article 100:

For the investigation of felonies and misdemeanours, if the penalty incurred is equal to or in excess of two years' imprisonment, the investigating judge may order the interception, recording and transcription of correspondence transmitted by means of telecommunications where the requirements of the investigation call for it. Such operations are made under his authority and supervision.

The interception decision is made in writing. It is not a jurisdictional decision and cannot be appealed.

Article 100-1:

The order made pursuant to article 100 must include all the details identifying the link to be intercepted, the offence which justifies resorting to an interception, and the duration of this interception.

Article 100-2:

This decision can last for a maximum duration of four months. It may be extended only by following the same conditions as to form and duration.

Article 100-3:

The investigating judge or the judicial police officer appointed by him may require any qualified agent of a service or institution placed under the authority or supervision of the Minister in charge of telecommunications, or any qualified agent of a network operator or authorised purveyor of telecommunication services to set up an interception device.

Article 100-4:

The investigating judge or the judicial police officer appointed by him drafts an official record of both the interception and recording operations. This official record mentions the date and time when the operation started and ended.

The recordings are placed under closed official seals.

⁷⁷ An English translation of these articles taking into account modifications of the law up to 2005 is found at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf (Art. 100-5 was modified in 2010).

⁷⁸ An English translation of these articles taking into account modifications of the law up to 2005 is found at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf (Art. 706-95 was modified by a law of 2015).

Article 100-5:

The investigating judge or the judicial police officer appointed by him transcribes any correspondence which is useful for the discovery of the truth. An official record is made of these transcriptions. The transcription is attached to the case file.

Correspondence in a foreign language is transcribed into French with the assistance of an interpreter appointed for this purpose.

On penalty of nullity, no transcription may be made of any correspondence with an advocate relating to the exercise of the defendant's rights.

On penalty of nullity, no transcription may be made of any correspondence with a journalist allowing identifying a source in breach of Article 2 of the Law of 29 July 1881 on Freedom of the Press.

Article 100-6:

The recordings are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution.

An official record is made of the destruction.

Article 100-7:

No interception may be made on the telephone line of a member of Parliament or senator unless the president of the assembly he belongs to is informed of the interception by the investigating judge.

No interception may be made on a telephone line connecting the chambers or domicile of an advocate unless the president of the bar association is informed of this by the investigating judge.

No interception may be made on a telephone line connecting the chambers or domicile of a judge or prosecutor unless the president or the prosecutor general of the court with jurisdiction over the area in question is informed of this by the investigating judge.

The formalities set out by the present article are prescribed under penalty of nullity.

Article 706-95:

If the needs of a flagrancy inquiry or a preliminary inquiry into one of the offences within the scope of articles 706-73⁷⁹ and 706-73-1⁸⁰ justify this, the liberty and custody

⁷⁹ Art. 706-73 lists the following crimes and misdemeanours under the Penal Code unless otherwise stated: (1°) murder committed by an organised gang under 8° of article 221-4; (2°) torture and acts of barbarity committed by an organised gang contrary to article 222-4; (3°) felonies and misdemeanours relating to drug trafficking contrary to articles 222-34 to 222-40; (4°) felonies and misdemeanours relating to kidnapping and false imprisonment committed by an organised gang contrary to article 224-5-2; (5°) felonies and aggravated misdemeanours relating to human trafficking contrary to articles 225-4-2 to 225-4; (6°) felonies and aggravated misdemeanours relating to procuring contrary to articles 225-7 to 225-12; (7°) theft committed by an organised gang contrary to article 311-9; (9°) the felony of destroying, defacing or damaging property committed by an organised gang, contrary to article 322-8; (10°) felonies relating to counterfeiting contrary to articles 442-1 and 442-2; (11°) felonies and misdemeanours which constitute acts of terrorism contrary to articles 421-1 to 421-6; (12°) misdemeanours relating to weapons committed by an organised gang contrary to articles L. 2339-2, L. 2339-3, L. 2339-10, L. 2341-4, L. 2353-4 and L. 2353-5 of the Code of defence, or contrary to articles L. 317-2, L. 317-4, L. 317-7 of the internal security Code; (13°) misdemeanours in relation to the illegal entry, movement and residence of a foreigner in France committed by an organised gang, contrary to article L. 622-1 of the Code on the entry and residence for foreigners and on the right to asylum; (14°) money laundering misdemeanours contrary to articles 324-1 and 324-2, or

judge of the district court may, at the request of the district prosecutor, authorise the interception, recording or transcription of correspondence by telecommunication, under the provisions of paragraph two of article 100, article 100-1 and articles 100-3 to 100-7, for a maximum period of one month, renewable once under the same conditions of form and duration. These operations are carried out under the supervision of the liberty and custody judge.

For the application of the provisions of articles 100-3 to 100-5, the powers conferred on the investigating judge or the judicial police officer nominated by him are exercised by the district prosecutor or the judicial police officer appointed by him.

The liberty and custody judge who has authorised this interception is immediately informed by the district prosecutor of any actions carried out in accordance with the previous paragraph, including official records drafted pursuant to his authorisation, by way of the application of articles 100-4 and 100-5.

b) Remote data capture

Remote data capture is set out in articles 706-102-1 to 706-102-9 of the Penal Procedure Code.⁸¹

receiving stolen property contrary to articles 321-1 and 321-2, of the products, income and items resulting from the offences mentioned in 1° to 13°; (15°) membership of a conspiracy misdemeanours contrary to article 450-1, where the action aims to prepare one of the penal infringements mentioned in 1° to 14° and 17°; (16°) failure to justify resources corresponding to lifestyle misdemeanour contrary to article 321-6-1, when this misdemeanour is connected to one of the penal infringements listed in 1° to 15° and 17°; (17°) crime of hijacking of aircraft, ships or any other means of transport committed by an organised gang under article 224-6-1; (18°) crimes and misdemeanours sentenced to ten years of imprisonment contributing to proliferation of weapons of mass destruction and the means of delivering them under article 706-167; (19°) misdemeanours of mining or licensable substance holding without an authorisation or exploitation permit, accompanied by damage to the environment, committed by an organised gang, under article L. 512-2 of the mining Code, where it is related to one of the penal infringements mentioned in 1° to 17° of the current article; (20°) activities or employees concealment misdemeanour, misdemeanour of using the services of a person performing undeclared work, illegal subcontracting, illicit supply of workers, employment of foreign nationals without a work permit contrary to 1° and 3° of article L. 8221-1 and to articles L. 8221-3, L. 8221-5, L. 8224-1, L. 8224-2, L. 8231-1, L. 8234-1, L. 8234-2, L. 8241-1, L. 8243-1, L. 8243-2, L. 8251-1 et L. 8256-2 of the Labour Code. In addition, paragraph (8°) mentions aggravated felonies of extortion contrary to articles 312-6 and 312-7, but this paragraph has been declared unconstitutional and was removed from the penal procedure Code on 1st September 2015 (see Decision n° 2014-420/421 QPC of the Constitutional Council of 9 Oct. 2014, recital n° 25).

⁸⁰ Art. 706-73-1 lists the following crimes and misdemeanours under the Penal Code: (1°) offence of fraud committed by an organised gang under the last paragraph of article 313-2; (2°) misdemeanours listed in paragraph (20°) of article 706-73; (3°) money laundering misdemeanours contrary to articles 324-1 and 324-2, or receiving stolen property contrary to articles 321-1 and 321-2, of the products, income and items resulting from the offences mentioned in 1° and 2° of the current article; (4°) membership of a conspiracy misdemeanours contrary to article 450-1, where the action aims to prepare one of the penal infringements mentioned in 1° to 3° of the current article; (5°) failure to justify resources corresponding to lifestyle misdemeanour contrary to article 321-6-1, when this misdemeanour is in link with one of the penal infringements listed in 1° to 4° of the current article.

⁸¹ See note on English translation of these articles above.

Article 706-102-1:

For the investigation of crimes or offences coming within the scope of articles 706-73⁸² and 706-73-1,⁸³ and where the requirements of the investigation call for it, the investigating judge may, after having requested the opinion of the district prosecutor, authorise, by way of reasoned order, judicial police officers and agents that have been appointed by rogatory commission, to implement a technical device aiming to access computer data, in all places and without the consent of the concerned people, and to register, store and transmit those data, as they are displayed on the screen of the user of the computer system, or as they are typed by the user of the system, or as they are transmitted or received by audio-visual devices. These operations are carried out under the supervision of the investigating judge.

Article 706-102-2:

The decisions of the investigating judge, taken according to article 706-102-1, mention the penal infringement that justifies the operation, the exact location or the comprehensive description of the computer systems concerned and the duration of operations. The formalities set out by the present article are prescribed under penalty of nullity.

Article 706-102-3:

These decisions are valid for a maximum duration of four months. They may be extended, exceptionally and under the same conditions as to form and duration, where the investigation so requires.

The investigating judge may, at all times, require the interruption of operations.

Article 706-102-4:

Under penalty of nullity, these operations shall be limited to the investigation and identification of penal infringements mentioned in the authorisation of the investigating judge.

The fact that these operations reveal other penal infringements not mentioned in the investigating judge's decision is not a cause for nullity of incidental proceedings.

Article 706-102-5:

In order to implement the technical device mentioned in article 706-102-1, the investigating judge may authorise the introduction to a vehicle or to a private place, including outside the times mentioned in article 59 of the Penal Procedure Code,⁸⁴ without the knowledge or without the consent of the owner or of the possessor of the vehicle or of the occupier or of any person having a right to this vehicle or place. If the device must be introduced in a home before 6 am or after 9 pm, the authorisation must be delivered by the liberty and custody judge, on the special request of the investigating judge. These operations cannot pursue any other aim than implementing the technical device and are performed under the authority and supervision of the investigating judge. The current paragraph is also applicable to operations aimed at uninstalling the technical device that has been implemented according to article 706-102-1.

In order to implement this device, the investigating judge may also authorise the transmission of this device by means of an electronic communications network. These operations are performed under the authority and supervision of the investigating judge. The

⁸² See footnote n°79.

⁸³ See footnote n°80.

⁸⁴ Art. 59 states that, except where they are requested from within a building or in the exceptional cases provided for by law, searches and house visits may not be undertaken before 6 am or after 9 pm.

current paragraph is also applicable to operations aiming at uninstalling the technical device that has already been implemented.

The technical device mentioned in article 706-102-1 can neither be implemented in a computer system located in places covered by articles 56-1,⁸⁵ 56-2⁸⁶ and 56-3,⁸⁷ nor in the vehicle, the business premises or the home of people mentioned in article 100-7.

Article 706-102-6:

The investigating judge or the judicial police officer appointed by him may require any qualified agent of a service or unit or body placed under the authority or supervision of the Ministry of Interior or of the Ministry of Defence, a list of which is determined by means of a Decree, in order to install the device mentioned in article 706-102-1.

Article 706-102-7:

The investigating judge or the judicial police officer appointed by him drafts an official record of both the installation of the device mentioned in article 706-102-1 and the data capture operations. This official record mentions the date and time when the operation started and ended.

The recordings are placed under closed official seals.

Article 706-102-8:

The investigating judge or the judicial police officer appointed by him describes or transcribes, in an official record filed in the criminal case file, the data that are needed to ascertain the truth. No sequence relating to private life but that has no relation with penal infringements mentioned in the authorisation can be kept in the criminal case file.

Data in a foreign language are transcribed into French with the assistance of an interpreter appointed for this purpose.

Article 706-102-9:

The recordings of computer data are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution.

An official record is made of the destruction.

c) Interception of the content of the information accessed by users of electronic communications operators' services

The interception of the content of the information accessed by users of electronic communications operators' services is set out in articles 60-2 (flagrancy investigation), 77-1-2 (preliminary investigation), and 99-4 (investigation procedure conducted by an investigating judge) of the Penal Procedure Code.

Article 60-2, §2 et seq.:

A judicial police officer, intervening on the orders of a district prosecutor authorised in advance by a decree from the liberty and custody judge, may require telecommunications operators, particularly those mentioned in 1 of I of article 6 of Law no. 2004-575

⁸⁵ This article refers to business premises or the home of advocates.

⁸⁶ This article refers to business premises of media companies, audio-visual communication companies, online public communication companies, press agencies, to the professional vehicles of these companies and to journalists' home where the investigation is relating to this journalist's professional activities.

⁸⁷ This article refers to professional premises of doctors, notaries, or bailiffs.

of 21 June 2004 relating to confidence in the digital economy,⁸⁸ to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the text of the information consulted by persons using the services provided by the operators.

The organisations or persons to which this article applies must make the required information available as quickly as possible by means of telecommunication or computers.

Refusal to respond to such a request without a legitimate reason is punished by a fine of €3,750.

[...]

Article 77-1-2, §2 *et seq.*:

On the authorisation of the custody judge, given jurisdiction, to this end, by the district prosecutor, a police officer may carry out the measures provided for by the second paragraph of article 60-2.

The organisations or persons concerned make the required information available as quickly as possible, by means of telecommunication or computers.

Refusal to respond to such a request without a legitimate reason is punished subject to the provisions of the fourth paragraph of article 60-2.

Article 99-4, §2 *et seq.*:

With the express permission of the investigating judge, a judicial police officer may issue the demands provided for by the second paragraph of article 60-2.

The organisations or persons concerned must put the requisite information at their disposal by telecommunication or by use of computers as quickly as possible.

Refusal to respond to these demands without legitimate grounds is punished in accordance with the provisions of the fourth paragraph of article 60-2.

2. Scope of application

The object of interception and the temporal limits of electronic communications are subject to some matters of dispute.

a) *Object of interception and temporal limits of electronic communication*

The subject-matter of the interception and the temporal limits of the protection of electronic communications are different, depending on the procedure that is followed.

aa) Correspondence interception

In the above-mentioned provisions relating to correspondence interception, the subject-matter of the interception is correspondence transmitted by means of electronic communications.

⁸⁸ These persons are Internet access service providers.

The notion of "electronic correspondence," as well as the notion of "correspondence" more widely does not have any comprehensive legal definition.⁸⁹ Correspondence has been defined by the legal literature only, as being "personal and temporal communication, which allow interactivity, and which are addressed to determined and individualised persons."⁹⁰ This definition may be considered as applying to correspondence that is protected under the French Penal Code during the time of their transmission,⁹¹ and which may be subject to interceptions in compliance with the French Penal Procedure Code. Before and after transmission, correspondence may further receive the protection, as already mentioned in this report, of the French Civil Code, and it is in this case commonly referred to as "private correspondence." Since the definition of correspondence, according to the legal literature, applies to both the information medium and the information that is communicated,⁹² the notion of electronic correspondence is restricted to correspondence emitted, transmitted or received electromagnetically, in the form of signs, signals, writing, images or sounds.⁹³

As a consequence of this definition, the provisions that define electronic communications and the provisions of the French Penal Procedure Code relating to correspondence intercept, data that can be captured under the interception procedure is analogous to communication (voice and data) via landlines, and IP traffic of a person-to-person-communication.

Regarding the interception of other types of private communications, such as IP traffic between a person and an automated information system,⁹⁴ IP-traffic between a person's computer and their data storage in a cloud or other remote storage of data processing systems, and IP traffic between two independent computer systems (e.g., between an automated machine and its computer-based automated control centre), other procedures included in the Penal Procedure Code are more suitable,

⁸⁹ French law only evokes "private correspondence" in a negative way, within the provisions dedicated to public communications (Art. 1, IV, subparas. 3 and 4 of Law n°2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN"): "Public communication using electronic means shall mean any sign, signal, writing, image, sound or messages of all kinds, which are made available to the public by electronic means, and which have not the character of a private correspondence"; "Online public communication shall mean any transmission, on individual request, of digital data that have not the character of a private correspondence [...]."

⁹⁰ Estelle De Marco, *L'anonymat sur Internet et le droit*, thesis, Montpellier 1, 2005, ANRT, n° 637. See also Virginie Peltier, *Le secret des correspondances*, PU d'Aix-Marseille 1999.

⁹¹ Estelle De Marco, not. n° 641; Virginie Peltier.

⁹² Estelle De Marco; Virginie Peltier.

⁹³ As a consequence of the French legal definition of "electronic communications" which are "emissions, transmissions or reception of signs, signals, writings, images or sounds, by electro-magnetic means." Art. L. 32-1 PECC.

⁹⁴ Such as communication with a webserver while downloading a website.

such as the search and seizure procedure, the procedure enabling remote computer data capture and the special procedure that requires electronic communications operators to preserve the content of the information accessed by their users.

bb) Remote data capture

In the above-mentioned provisions relating to remote data capture, the subject-matter of the interception is any computer data exactly as it is displayed on the screen of the user of the computer system, or as it is typed by the user of the system, or as it is transmitted or received by audio-visual devices. As a consequence, the interception concerns all type of electronic and audio-visual communications, of a private and public nature.

cc) Interception of the content of the information accessed by users of electronic communications operators' services

In the above-mentioned provisions relating to this kind of interception, the subject-matter of the interception is the content of the information accessed by users. Therefore the interception covers public and private communications such as the information accessed during internet surfing.

b) Current matters of dispute

aa) Rules protecting correspondence before their reception by the recipient

One question is whether correspondence stored by a hosting provider, in a traditional mail box or on a social network, should be intercepted using the correspondence interception procedure or if they may be accessed via the search and seizure procedure.

A legal analysis performed in accordance with the doctrinal definition of correspondence and the principles enshrined in the decisions of both the French Constitutional Council and the European Court of Human Rights leads to the conclusion that no correspondence should be accessed outside the procedure set-up for correspondence interception, whatever its medium of transmission and its medium of storage, after they have been sent by the sender and before they have been received by the recipient.

Indeed, the penal protection of a correspondence (which imposes the use of the interception procedure if its content must be accessed for the purpose of criminal repression) begins when the message is sent, and ends "when the last piece of information has been received."⁹⁵ Such a reception must be understood as a reception

⁹⁵ Virginie Peltier, *op. cit.*, p. 471.

by the recipient, and not as reception in the medium of storage only, a medium which may be used to visualise the correspondence online, or to store the message until the recipient downloads it. The message stays therefore protected until the recipient opens it and decides to leave it stored on the server, or downloads it. This analysis, which is implied by the definition of correspondence, is also confirmed by Article 226-15 of the French Penal Code, which states that correspondence is protected whether or not it has "arrived at their destination." Such an analysis is also compatible with Recital n° 27 of Directive 2002/58/EC⁹⁶, transposed under French law, according to which "the exact moment of the completion of the transmission of a communication [...] may depend on the type of electronic communications service that is provided. [...] For electronic mail the transmission is completed as soon as the addressee collects the message, typically from the server of his service provider."⁹⁷

However, the Court of Cassation stated in a case of 8 July 2015⁹⁸ that emails may be seized in the mailbox hosted by the service provider, on the basis of a judicial search, without making a distinction between emails actually received by the recipient (and therefore opened by this recipient), and emails technically received by the hosting provider but not opened by the recipient. Indeed, the Court states that "collection, registration and transcription of correspondence sent or received by telecommunication means before the date of the written decision of correspondence interception taken by the investigating judge [...] must be performed in compliance with provisions regulating seizure."⁹⁹

This decision could be called into question in the future.

bb) Direct access to mailboxes using their password

As we will analyse later, the law concerning the retention of connection data (see III.C. below) imposes the retention of certain information provided at the time of the contract subscription or of the creation of the users' account, including – only where the provider usually collects such information – the password and the data that enable the modification or verification of this password, in its latest and updated form. Even if the interception procedure must in theory be used to access elec-

⁹⁶ Directive 2002/58/EC of 12 juillet 2002, J.O.C.E. n° L. 201 of 31 July 2002, p. 37.

⁹⁷ On the discussion see Estelle De Marco, *L'anonymat sur Internet et le droit*, *op. cit.*, n°641.

⁹⁸ Court of cassation, criminal chamber, 8 July 2015, available at http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4696

⁹⁹ Translated from French: "l'appréhension, l'enregistrement et la transcription de correspondances émises ou reçues par la voie des télécommunications antérieurement à la date de la décision écrite d'interception prise par le juge d'instruction [...] doivent être réalisés conformément aux dispositions légales relatives aux perquisitions."

tronic correspondence, access to passwords enables the access of these messages in practice.

3. Special protection of confidential communication content

Firstly, as has been mentioned above (III.B.1.), correspondence can only be intercepted under strict conditions when its sender or recipient practices certain occupations. Some types of correspondences are also protected against transcription. Secondly, remote data capture is not possible in certain places. Finally, the interception of the information accessed online may concern any person since no special protection is in place.

a) Privileged correspondence

Article 100-7 of the Penal Procedure Code provides special protection for the Parliament's members, advocates, judges and prosecutors. This article states that, under penalty of nullity,

- No interception may be made on the telephone line of a member of Parliament or senator unless the president of the assembly he belongs to is informed of the interception by the investigating judge;
- No interception may be made on a telephone line connecting the chambers or domicile of an advocate unless the president of the bar association is informed of this by the investigating judge; and
- No interception may be made on a telephone line connecting the chambers or domicile of a judge or prosecutor unless the president or the prosecutor general of the court with jurisdiction over the area in question is informed of this by the investigating judge.

b) Prohibition of transcription of certain types of correspondence

In addition to the rules described above, article 100-5 of the Penal Procedure Code states that, on penalty of nullity:

- No transcription may be made of any correspondence with an advocate relating to the exercise of the defendant's rights, and
- No transcription may be made of any correspondence with a journalist allowing identifying a source in breach of Article 2 of the Law of 29 July 1881 on freedom of the press.

c) Privileged computer data within the framework of remote data capture

Remote data capture cannot be performed:

- In the vehicle, the business premises or the home of members of Parliament, advocates, judges and prosecutors;
- In the business premises of media companies, audio-visual communication companies, online public communication companies, press agencies, in the professional vehicles of these companies;
- In a journalist's home;
- In the professional premises of doctors, notaries, or bailiffs.

4. Execution of electronic communications interception

As explained previously, according to Article 100-3 of the Penal Procedure Code, correspondence interception may be performed by any qualified agent belonging to a service or body placed under the authority of the Ministry in charge of electronic communications, or any qualified agent belonging to an authorised electronic communications service, if required by the investigating judge or the police officer appointed by this judge. The execution mode is determined by the investigative judge.

Regarding remote data capture, according to Article 706-102-6 of the Penal Procedure Code, the installation of the device that is necessary to perform data capture may be performed by any qualified agent belonging to a service or unit or body placed under the authority or supervision of the Ministry of Interior or of the Ministry of Defence and of which a list is determined by means of a decree.¹⁰⁰

Regarding finally the interception of the content of the information accessed by users of electronic communications operators' services, such an interception is required from electronic communication operators and internet access service providers, who must make the required information available as quickly as possible by means of telecommunication or computers.

5. Duties of electronic communication service providers to cooperate

French law includes some general provisions that recall the duty of electronic communications service providers¹⁰¹ – and more widely the duty of any citizen¹⁰² – to provide support to justice for the manifestation of the truth.

¹⁰⁰ This list is available in art. D15-1-6 PPC.

¹⁰¹ Art. L. 33-1, I, §§ 5, 6° and 7° PECC that "the setting up and the exploitation of electronic communications networks are subject to the respect for rules relating to [...] public order, national defence and public security requirements, including rules that are necessary to the setting up of communications intercepts required for public security purposes. Art. L. 32-1, II, § 7° also considers as a general objective (to be enforced by the Ministry for Electronic Communications and the regulatory authority) the respect by operators of the public order and of obligations of defence and public security.

More particularly, electronic communications operators¹⁰³ and internet access providers¹⁰⁴ must take without delay all appropriate measures to ensure the preservation of the text of the information consulted by persons using the services they provide, when they are required to do so according to article 60-2 of the Penal Procedure Code, and refusal to respond to such a request without a legitimate reason is punishable by a fine of €3,750.

Electronic communications operators have a general obligation, sometimes recalled by additional specific provisions relating to specific questions, to respect the rules relating to the protection of personal data,¹⁰⁵ the secrecy of correspondence,¹⁰⁶ and the confidentiality and neutrality of content transmitted using their networks.¹⁰⁷ These stakeholders are also obliged to ensure the integrity and the security of their networks.¹⁰⁸ French law does not provide for particular requirements for the transfer of content data following a judicial request, but these general principles do apply.

In addition, a decree plans the creation of a “judicial interceptions platform,” placed under the responsibility of the Ministry for Justice,¹⁰⁹ the purpose of which is to receive and store:

- The content of electronic communications intercepted on the basis of articles 74-2, 80-4, 100 to 100-7 and 706-95 of the Penal Procedure Code;

¹⁰² Art. 10 French Civil Code states: “Everyone is required to lend his aid to the court so that the truth may be revealed. He who, without legitimate reason, evades that obligation when it is legally required of him, may be compelled to comply with it, if need be on pain of a periodic penalty payment or of a civil fine, without prejudice to the right to recover damages”. See the English translation of the French Civil Code on Legifrance (the French public service for the dissemination of law) at <https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070721&dateTexte=20160929>

¹⁰³ Electronic communications operators are defined in art. L. 32, § 15° PECC as “natural or legal persons who exploit an electronic communications network opened to the public or who provide the public with an electronic communications service” (the notion of “provision” being understood here as the transmission of electronic communications on a network).

¹⁰⁴ Internet access providers are defined in art. 6, I, § 1 of Law 2004-575 of 21 June 2004 as “persons whose activity is to provide an access to online public communication services.”

¹⁰⁵ General rules are included in art. L. 32-1, II, § 6° PECC and in Law n°78-17 of 6 Jan. 1978. Specific obligations are, e.g., included in provisions relating to the retention of traffic data.

¹⁰⁶ The general rule is included in art. L. 32-1, II, § 6° PECC and in art. 226-15 Penal Code. Specific obligations are for example included in art. L. 32-3 PECC, in addition to art. 432-9 Penal Code which specifically sanctions correspondence violation where committed by electronic communications operators.

¹⁰⁷ General rules are included in art. L. 32-1, II, § 6° and L. 33-1, b) PECC. Specific obligations are, e.g., included in art. L. 32-3-3 of the same code.

¹⁰⁸ See, e.g., art. L. 33-1, a) PECC.

¹⁰⁹ Decree n°2014-1162 of 9 Oct. 2014, creating arts. R. 40-42 to R. 40-55 PPC.

- Data and information communicated by service providers within the framework of three procedures: the procedure for the interception of the content of the information accessed by users of electronic communications operators’ services (articles 60-2 §2 *et seq.*; 77-1-2 §2 *et seq.* and 99-4 §2 *et seq.* of the Penal Procedure Code), the procedure for requesting traffic and connection data (articles 60-1; 77-1-1 and 99-3 of the Penal Procedure Code), and the procedure for accessing, including remotely, information stored in computer and data processing systems (60-2, §1 and 5; 77-1-2 §1 and 99-4 §1 of the same Code).

This platform was not yet operational at the time of writing.¹¹⁰

6. Formal prerequisites of interception orders

As can be noted by reading statutory provisions relating to correspondence interceptions, remote data capture and interception of the content of the information accessed by the users of electronic communications networks, each of these procedures obeys different rules.

a) Competent authorities

aa) Correspondence interception

The principle is that correspondence interception must be ordered by the investigating judge, and the interception is made under his authority and supervision.

This order is issued by the initiative of the investigating judge, where the requirements of the investigation call for it, for the investigation of felonies and misdemeanours where the penalty incurred is equal to or in excess of two years imprisonment,¹¹¹ or if a person has disappeared.¹¹²

Moreover, the judge responsible for enforcing sentences can order such correspondence interception, for the same kinds of felonies and misdemeanours indicated above, where one or several reasonable grounds enable the belief that a person, having served his sentence, does not respect the prohibition written in the initial sentence, to contact certain persons or to be in certain areas.¹¹³ The judge responsible for enforcing sentences issues the order on his own initiative or, in some specific situations described by the penal Code, on the request of the district prosecutor.

¹¹⁰ See, e.g., Xavier Berne, “Ecoutes: la mise en place de la PNIJ avance doucement,” 14 Aug. 2015, available at <http://www.nextinpact.com/news/96181-ecoutes-mise-en-place-pnij-avance-doucement.htm>

¹¹¹ Art. 100 PPC.

¹¹² Art. 80-4 PPC.

¹¹³ Art. 709-1-3 PPC.

Additionally, the liberty and custody judge of the district Court may, where the requirements of the investigation call for it, on the request of the district prosecutor, order a correspondence intercept in the search for an escaping person. Correspondence interceptions are performed under the authority and supervision of this liberty and custody judge.¹¹⁴

The liberty and custody judge of the district Court may also order a correspondence interception, on the request of the district prosecutor, where the requirements of a flagrancy or preliminary investigation in relation with limited penal infringements¹¹⁵ call for it.¹¹⁶

bb) Remote data capture

The principle is that remote data capture must be ordered by the investigating judge for the investigation of specific crimes and misdemeanour exhaustively listed,¹¹⁷ after having requested the opinion of the district prosecutor. The measure is implemented and performed under his authority and supervision.

cc) Interception by service providers of the content of the information accessed by their users

During a flagrancy investigation, the preservation of the text of the information consulted by persons using their services may be requested by a judicial police officer, intervening on the orders of a district prosecutor authorised in advance by a decision from the liberty and custody judge.¹¹⁸

During a preliminary investigation, the preservation of this information may be requested by a judicial police officer, if authorised to do so by the liberty and custody judge. This authorisation is issued on the request of the district prosecutor.¹¹⁹

Where the investigation is conducted by an investigating judge, the preservation of this information may be requested by a judicial police officer, with the express permission of the investigating judge.¹²⁰

¹¹⁴ Art. 74-2 PPC.

¹¹⁵ See footnotes n°79 and n°80.

¹¹⁶ Art. 706-95 PPC.

¹¹⁷ See footnotes n°79 and n°80.

¹¹⁸ Art. 60-2 PPC.

¹¹⁹ Art. 77-1-2 PPC.

¹²⁰ Art. 99-4 PPC.

b) Formal and substantive requirements for applications and orders

Requirements for applications and orders differ depending on the procedure that is followed.

aa) Correspondence interceptions

Provisions that are specific to correspondence interceptions do not particularly regulate the form of the requests made by the district prosecutor to the competent judge.

Correspondence interception orders must be made in writing, must specify all the details identifying the link to be intercepted, the offence which justifies resorting to an interception and the duration of this interception, and must be justified according to the provisions recalled in subsection a. above, such as the situation where the requirements of the investigation call for it, or where there is grounds to believe that a person does not respect a prohibition on contacting certain persons (provisions which are supposed to ensure proportionality of the measure to the seriousness of the offence). They can only be issued in relation with the penal infringements listed in the texts that authorise the interception measure, also recalled above in subsection a. Within those limits, the Penal Procedure Code does not specify the persons (such as suspects, intermediaries or communication partners) who can be placed under surveillance. Nor does it require that less intrusive means must be first considered or tried.

bb) Remote data capture

Provisions that are specific to remote data capture do not particularly regulate the form of the opinion transmitted by the district prosecutor to the investigating judge.

The investigating judge may issue remote data capture orders only where the requirements of the investigation call for it, after having requested the opinion of the district prosecutor. Under penalty of nullity, remote data capture orders must be made in writing, must mention the penal infringement that justifies the operation, the exact location or the comprehensive description of concerned computer systems and the duration of operations. The penal infringement that justifies the operation must belong to the list set-up by articles 706-73 and 706-73-1 of the Penal Procedure Code.¹²¹ All these details are supposed to ensure proportionality of the measure to the seriousness of the offence. Within these limits, the Penal Procedure Code does not specify the persons who can be placed under surveillance, or require that less intrusive means must be first considered or tried.

¹²¹ See footnotes n°79 and n°80.

cc) Interception by service providers of the content of the information accessed by their users

Provisions that are specific to the interception of the content of the information accessed by users of electronic communications services do not regulate either the form of the requests made by the district prosecutor to the competent judge, or the order of this judge, or the requests made to internet service providers.

Content interception orders must be made in writing and must specify all the details identifying the link to be intercepted, the offence which justifies resorting to an interception as well as the duration of this interception. In addition, they must be justified according to the provisions recalled in subsection a. above, such as the situation where the requirements of the investigation call for it, or where there is one ground to believe that a person does not respect a prohibition to contact certain persons (provisions which are supposed to ensure proportionality of the measure to the seriousness of the offence). They can only be issued for the penal infringements listed in the texts that authorise the interception measure, also recalled above in subsection a.

Again, the Penal Procedure Code does not specify the persons (such as suspects, intermediaries or communication partners) who can be placed under surveillance or require that less intrusive means are considered or tried. The measure may be ordered in case of any penal infringement that justifies one of the three forms of judicial investigation set out under French law (flagrancy investigation, preliminary investigation or investigation procedure conducted by an investigating judge).

7. Validity of interception orders

Conditions for the validity of interception orders differ depending on the procedure that is followed.

a) Correspondence interception

aa) Maximum length of interception order

Correspondence interceptions ordered by the investigating judge, and by the judge responsible for enforcing sentences, must have a maximum duration of four months. The measure may be extended by following the same conditions as to form and duration. The Penal Procedure Code does not provide for a maximum of possible renewals.

Correspondence interceptions ordered by the liberty and custody judge of the district Court must have:

- A maximum duration of two months in the case of a search for an escaping person. In this situation, the measure may be extended by following the same condi-

tions as to form and duration, with a maximum duration of six months regarding misdemeanour (and with no limits regarding crimes).

- A maximum duration of one month in case of a flagrancy investigation or a preliminary investigation in relation with a restricted list of penal infringements.¹²² In this situation, the measure may be extended only once by following the same conditions as to form and duration.

bb) Revocation of authorisations

In all situations, any correspondence which is useful for the discovery of the truth is transcribed. The Penal Procedure Code does not require that the interception must be halted if it reveals information pointing to the commission of offences not anticipated or mentioned in the interception order. On the contrary, such information could be subject to the opening of a new investigation on the basis of article 40 of the Penal Procedure Code.¹²³

For the rest, the Penal Procedure Code is silent on the possibility for the competent judge to revoke his interception authorisation.

b) Remote data capture

aa) Maximum length of interception order

Remote data capture orders must have a maximum duration of four months. They may be extended, exceptionally and under the same conditions as to form and duration, where the investigation so requires.¹²⁴

bb) Revocation of authorisations

Only the data that are needed to ascertain the truth are described or transcribed, in an official record filed in the criminal case file, and no sequence relating to private life and that has no relation with penal infringements mentioned in the authorisation can be kept in the criminal case file.¹²⁵

Under penalty of nullity, operations shall be limited to the investigation and identification of penal infringements mentioned in the authorisation of the investi-

¹²² See footnotes n°79 and n°80.

¹²³ According to art. 40 PPC, "every constituted authority, every public officer or civil servant who, in the performance of his duties, has gained knowledge of the existence of a felony or of a misdemeanour is obliged to notify forthwith the district prosecutor of the offence and to transmit to this prosecutor any relevant information, official reports or documents". See the English translation of the French Penal Procedure Code noted above.

¹²⁴ Art. 706-102-3 PPC.

¹²⁵ Art. 706-102-8 PPC.

gating judge, but the fact that these operations reveal other penal infringements not mentioned in the investigating judge's decision is not a cause for nullity of incidental proceedings, as explicitly mentioned in article 706-102-4 of the Penal Procedure Code.

In addition, such information could be subject to the opening of a new investigation on the basis of article 40 of the Penal Procedure Code.¹²⁶

Finally, the investigating judge may, at all times, require the interruption of operations.¹²⁷

c) Interception by service providers of the content of the information accessed by their users

aa) Maximum length of interception order

The preservation of the text of the information consulted by persons using the services provided by the operators must not exceed one year.

bb) Revocation of authorisations

The Penal Procedure Code does not set out particular conditions regarding the specification, in the preservation authorisation and request, of the offence that justifies the request for information preservation. The Penal Procedure Code is also silent on the possibility for the competent judge to revoke his authorisation.

8. Duties to record, report, and destroy

Duties to record, report and destroy differ depending on the procedure that is followed.

a) Correspondence interception

Each interception and recording operation must be the object of the drafting of an official record, which must mention the date and time when the operation started and ended. Recordings are placed under closed official seals.¹²⁸ An official record is also made of any correspondence transcription, and attached to the case file.¹²⁹

¹²⁶ See footnote n°123.

¹²⁷ Art. 706-102-3 PPC.

¹²⁸ Art. 100-4 PPC.

¹²⁹ Art. 100-5 PPC.

Recordings are destroyed on the request of the district prosecutor or of the public prosecutor upon the expiry of the limitation period for prosecution. An official record is made of the destruction.¹³⁰

Reports of operations are addressed to the judge who authorised them.¹³¹

b) Remote data capture

The same procedure is followed as for correspondence interceptions, with similar rules on official seals,¹³² official records,¹³³ and destruction.¹³⁴ Reports of operations are addressed to the investigating judge.¹³⁵

c) Interception by service providers of the content of the information accessed by their users

The articles of the Penal Procedure Code that are specific to these kinds of interceptions do not regulate either the recording and reporting of operations, or the destruction of recordings.

9. Notification duties, remedies and consequences

Procedural efficiency implies the secrecy of interception measures.¹³⁶ Therefore, the accused can only have knowledge of their existence and results at the moment he is granted access to the entire procedural case file, this moment being determined by the Penal Procedure Code, depending on the nature of the procedure.¹³⁷

Procedural acts resulting from these measures can be annulled, especially where a substantive requirement laid down in the Penal Procedure Code has not been respected which has affected the interests of the concerned party, or where it is provided in the provision of the Penal Procedure Code related to the concerned measure.¹³⁸

¹³⁰ Art. 100-6 PPC.

¹³¹ Arts. 100, 74-2 and 706-95 PPC.

¹³² Art. 706-102-7 PPC.

¹³³ Art. 706-102-8 PPC.

¹³⁴ Art. 706-102-9 PPC.

¹³⁵ Arts. 706-102-1 and 706-102-5 PPC.

¹³⁶ See, e.g., Jacques Beaume, *Rapport sur la procédure pénale*, July 2014, p. 43 available at <http://www.justice.gouv.fr/publication/rap-beaume-2014.pdf>

¹³⁷ See mainly arts. 393, 278, and 279 PPC.

¹³⁸ See mainly arts. 170, 171 and 385 PPC.

For example, as we analysed it, the penalty of nullity is the consequence of a correspondence interception that takes place without respecting the requirements surrounding the implementation of such a measure on the line of a protected person (such as advocates or journalists) mentioned in articles 100-5 and 100-7 of the Penal Procedure Code.

10. Confidentiality requirements

Any person who provides support to the investigation must keep his or her support measure confidential, including internet service providers. Any violation of this obligation of professional secrecy may incur a penal sanction under articles 226-13 and 226-14 of the Penal Procedure Code.¹³⁹

C. Collection and Retention of Traffic Data and Subscriber Data

Several provisions regulate the collection of traffic and subscriber data, data retention and the location of mobile terminal devices.

1. Collection of traffic data and subscribers data

a) *Relevant information and prerequisite of collection*

aa) Requisition of traffic and connection data

Traffic and connection data retained by service providers can be requisitioned according to articles 77-1-1 (preliminary investigation), 60-1 (flagrancy investigation) and 99-3 (investigation procedure, conducted by an investigative judge) of the Penal Procedure Code.

Article 60-1:

The district prosecutor or a judicial police officer may, by any means, order any person, establishment or organisation, whether public or private, or any public services likely to possess any documents relevant to the inquiry in progress, including those produced from a computer system or a personal data processing system, to provide them with these documents, including in digital format. Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance. [...]

[...], failure to respond to such an order as quickly as possible is punished by a fine of €3,570. [...]

Article 77-1-1:

The district prosecutor or on his authorisation a judicial police officer, may, by any means, order any person, establishment or organisation, whether public or private, or

¹³⁹ Art. 11 PPC.

any public services liable to possess any documents relevant to the inquiry in progress, including those produced from a computer system or a personal data processing system, to provide them with these documents, including in digital format. Without legitimate grounds, the duty of professional secrecy cannot be given as a reason for non-compliance with this order. [...]

Where there is no response to these orders, the provisions of the second paragraph of article 60-1 are applicable. [...]

Article 99-3:

An investigating judge or judicial police officer delegated by him may, by any means, order any person, establishment or organisation, whether public or private, or any public services liable to possess any documents relevant to the investigation, including those produced from a computer system or a personal data processing system, to provide them with these documents, including in digital format. Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance with such an order. [...]

Where the person does not respond to this order, the provisions of the second paragraph of article 60-1 are applicable.

[...]

bb) Remote access to stored data

In addition, the first paragraphs of articles 60-2, 77-1-2 and 99-4 of the same Code organise the possibility to access, including remotely, information stored in computer and data processing systems:

Article 60-2, §1:

At the request of a judicial police officer, who can intervene by means of telecommunications or computers, public organisations or private legal persons, with the exception of those set out in the second paragraph of article 8, II, 3° and in article 67, 2° of Law no. 78-17 of 6 January 1978 relating to computers, databases and liberties,¹⁴⁰ must make available information helpful for the discovery of the truth, with the exception of information the secrecy of which is protected by statute, where it is stored in one or more computer or data processing systems that they administer.

Article 60-2, §5:

A Decree of the Council of State made on the advice of the National Commission for Data Protection determines the categories of organisation covered by the first paragraph, and also the methods for examining, transmitting and processing the required information.¹⁴¹

Article 77-1-2, §1:

On the authorisation of the district prosecutor, a judicial police officer may carry out the measures provided for by the first paragraph of article 60-2.

¹⁴⁰ These persons are the members of a non-profit association or entity of a philosophical, political, religious or trade-union character, the persons who have regular contacts with such association or entity within the framework of its activities (art. 8, II, 3°, § 2 of Law n°78-17), and professional journalists (art. 67, 2° of Law n° 78-17).

¹⁴¹ Decree n°2008-150 of 19 Feb. 2008, creating arts. R. 15-33-67 to R. 15-33-75 PPC.

Article 99-4, §1:

Where necessary to carry out a rogatory commission, a judicial police officer may issue the demands provided for by the first paragraph of article 60-2.

cc) Access to subscribers lists

Finally, article L. 33-1, V of the Post and Electronic Communications Code requires electronic communications operators to enable access by the judiciary, the national police, the national gendarmerie, fire and rescue services, and emergency services, when these services act within the framework of their respective judicial or rescue missions, to the comprehensive, unredacted and updated list of their users and subscribers.

b) Duty of addressees to disclose information

Internet access service providers and hosting providers who do not retain connection data according to article 6 of the Law n° 2004-275, or answer a communication request from the judiciary, may be punished by one year imprisonment and a fine of €75,000.¹⁴²

Electronic communications operators and internet access service providers who do not retain traffic data within the conditions laid down by law (including not anonymising these data when required by law) may be punished by one year imprisonment and a fine of €75,000.¹⁴³ Non-disclosure is punished by article 60-1 of the Penal Procedure Code.

Article 60-1 is also applicable to the non-disclosure of users and subscribers lists.

c) Automated procedure of disclosure

The procedure to be followed to access information remotely, on the basis of article 60-2, §1 of the Penal Procedure Code, is described in articles R. 15-33-67 to R. 15-33-75 of the Penal Procedure Code. Article R. 15-33-72 notably provides that technical arrangements for requesting and transmitting the data are defined in an agreement between the Ministry for Justice and, depending on the situation, the Ministry of interior or the Ministry of Budget, with each organisation or legal person liable for communicating data under article 60-1 of the Penal Procedure Code.¹⁴⁴

¹⁴² Art. 6, VI of Law n°2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN").

¹⁴³ Art. L. 39-3 PECC.

¹⁴⁴ The comprehensive list of the categories of concerned legal persons is included in art. R. 15-33-68 PPC.

2. Data retention

The obligations of internet services providers to retain traffic and connection data are laid down in article L. 34-1 of the post and electronic communications Code (retention of traffic data by operators and internet access providers) and article 6, II of the Law n° 2004-575 (retention of connection data by internet access providers and hosting providers)¹⁴⁵.

Data to be retained are specified in two decrees:

- Decree 2006-358 of 24 March 2004, which creates articles R. 10-12 *et seq.* of the post and electronic communications Code, issued under article L. 34-1 of the same Code;
- Decree 2011-219 of 25 February 2011, issued under article 6 of Law n° 2004-575.

Traffic data to be retained (for a duration of one year) under article L. 34-1 of the Post and Electronic Communications Code, in order to identify and prosecute penal infringements, according to article R. 10-13 of the same Code, are the following technical data:

- Information enabling the identification of the user;
- Data relating to terminal communication equipment used;
- Technical specifications and date, time and duration of each communication;
- Data relating to complementary services requested or used and their providers;
- Data enabling the identification of the recipients of the communication.

In addition to these data, for telephony activities, the operator must retain data that enable the identification of the origin and the location of the communication.

Connection data to be retained (for a duration of one year) under article 6 of Law n° 2004-575 according to Decree n° 2011-219, are once again only technical data, excluding other types of information (such as names, passwords, etc.) if such data are not usually collected. These data include – notably – the following:

- The identifier of the connection;
- The identifier attributed to the subscriber;
- The identifier of the terminal used for the purpose of the connection, when providers access such information;
- The dates and times at which the connection begins and ends;
- The specifications of the line of the subscriber;
- Certain information provided at the time of the contract subscription or of the creation of the users' account, including – only where the provider usually col-

¹⁴⁵ Law n°2004-575 of 21 June 2004 regarding confidence in the digital economy (called "LCEN").

lects such information – the password and the data that enables the modification or verification of this password, in their latest and updated form.

3. Location of mobile terminal device

Real-time geolocation of a person, a vehicle or an object, without the consent of this person or the owner of this vehicle or object, can be done in limited situations according to articles 230-32 to 230-44 of the Penal Procedure Code.

To reach this aim, according to article 230-32, any technical means may be used.

D. Access to Stored Communication Data

In addition to the procedures already studied that enable the access of certain kinds of stored communication data, French law authorises search and seizure, accompanied by a duty to cooperate.

1. Search and seizure of stored electronic communication data

Search and seizure of information held by a third party is set out in articles 76 to 76-3 (preliminary investigation), 56 to 59 (flagrancy investigation), 92 to 99-4 (investigation procedure conducted by an investigative judge), and 706-89 (in relation with a limited list of crime or misdemeanours) of the Penal Procedure Code.

This general procedure is applicable to stored electronic communication data. As already explained previously in this report, it is supposed to apply to the content of private correspondence – where such correspondence is involved – only before it is sent or after it has been received, which should be understood as receipt by the recipient himself and not the services of the hosting provider only.

Safeguards and requirements are different from those surrounding the interception of correspondence and remote access to data, since the privacy limitation is in this case considered lower. For example, the procedure of search and seizure can be used within the framework of any investigation, and is not limited to the investigation of certain kinds of penal infringements only. Safeguards include the drafting of an official report of the search, the initiation of steps that are necessary to ensure the observance of professional secrecy and the defendant's rights, the inventory and placement under official seals of any document or article seized, a restriction of access to consulted documents and information to the police officer who carries out the search and potential qualified persons requisitioned to help him, and the presence, during search and seizure, of the person in whose domicile the search is made or of two witnesses. In addition, certain categories of persons are more particularly protected.

2. Duties to cooperate: production and decryption orders

A duty to cooperate is set out in relation with the search and seizure procedure, and non-cooperation is punished by the Penal Code. However, these provisions do not apply to the defendant, who only risks an increase of the sentence in case he or she is found guilty.

a) Duties to cooperate

During search and seizure, judicial police officers may, by any means, request any person who may be aware of the security measures applied in order to protect the data that can be accessed during the search, or who may supply them with the information that is necessary to access to these data. Failure to respond to this request at the earliest opportunity is punishable by a fine of €3,750, except for some particularly protected people to whom such a sanction does not apply (advocates, media companies, audio-visual communication companies, online public communication companies, press agencies, journalists, doctors, notaries, bailiffs).¹⁴⁶ This provision is applicable to requests for the decryption of seized documents.

In addition, the Penal Code punishes some refusals to cooperate.

Article 432-15-2 (as last modified by law n° 2001-1062) states:

A penalty of three years' imprisonment and a fine of €45,000 are incurred by anyone who, having the key to decipher an encrypted message which may have been used to prepare, facilitate or commit a felony or a misdemeanour, refuses to disclose that key to the judicial authorities or to operate it following instructions issued by the judicial authorities under of title II and III of Book I of the Code of penal procedure.

Where the refusal was made where the disclosure of the key or its operation would have prevented the commission of a felony or a misdemeanour or would have limited its consequences, the penalty is increased to five years' imprisonment and a fine of €75,000.

b) Non application to the defendant

These provisions are not applicable to the defendant, in accordance with the principle of prohibition of self-incrimination. Doctrine and practitioners agree on that issue, even if no court decision seems to have been issued on that particular question.¹⁴⁷

However, a defendant who refused to cooperate could be punished more severely if found guilty, on the basis of article 132-79 of the Penal Code.

¹⁴⁶ Art. 57-1 PPC.

¹⁴⁷ See, e.g., Camille Polloni, "Si la police le demande, est-on obligé de donner son mot de passe?", 5 Feb. 2015, Rue 89, available at <http://rue89.nouvelobs.com/2015/02/05/si-police-demande-est-oblige-donner-mot-passe-257509>. This press article includes the interview of advocates and National Gendarmerie representatives.

Article 132-79 (inserted and last modified by Law n° 2004-575):

Where a means of encryption, in the sense of article 29 of act no. 2004-575 of 21 June 2004 used to ensure confidentiality in the digital economy has been used to prepare or commit a felony or a misdemeanour, or to facilitate the preparation of commission of a felony or a misdemeanour, the maximum prison sentence incurred is raised as follows:

1° where the offence is punished by thirty years' imprisonment, this is increased to life imprisonment;

2° where the offence is punished by twenty years' imprisonment, this is increased to thirty;

3° where the offence is punished by fifteen years' imprisonment, this is increased to twenty;

4° where the offence is punished by ten years' imprisonment, this is increased to fifteen;

5° where the offence is punished by seven years' imprisonment, this is increased to ten;

6° where the offence is punished by five years' imprisonment, this is increased to seven;

7° where the offence is punished by a maximum of three years' imprisonment, this is doubled.

The provisions of the present article are, however, not applicable to the perpetrator of or the accomplice to an offence who, at the request of the judicial or administrative authorities, has provided them with an unencrypted version of the coded messages and the secret keys necessary to decipher them.

3. Power of judicial authorities to decrypt encrypted data that are necessary to ascertain the truth

Articles 230-1 to 230-5 of the Penal Procedure Code provide for the possibility for judicial authorities to decrypt encrypted data that are necessary to ascertain the truth.¹⁴⁸

Article 230-1 (inserted by Law no. 2001-1062 of 15 November 2001 art. 30 Official Journal of 16 November 2001); (Act no. 2004-575 of 21 June 2004 art. 38 Official Journal of 22 June 2004) (Modified by Law n°2014-1353 of 13 November 2014):

Without prejudice to the provisions of articles 60, 77-1 and 156, where it appears that data seized or obtained during the course of the inquiry or investigation has been altered, preventing access to or understanding of the information in clear that it contains, or where it appears that these data are protected by an authentication mechanism, the district prosecutor, the investigating jurisdiction, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court seized of the case may appoint any qualified legal or natural person to carry out the technical operations necessary to obtain access to this information, to obtain a readable version of this information, and also, where a method of encryption has been used, the secret key for decoding it, if this appears necessary.

¹⁴⁸ The following articles correspond to the translation proposed by Legifrance, and modified by the author of the current report in order to take into account most recent modifications made to these articles by Law n° 2014-1353 of 13 Nov. 2014.

If the person thus appointed is a legal person, his legal representative submits for the approval of the district prosecutor, the judicial police officer or the court seized of the case the name of the natural person or persons who, within this legal person and under its name, will carry out the technical operations mentioned in the first paragraph. Unless these persons are registered on a list provided for by article 157, the persons thus nominated swears the oath provided for by the second paragraph of article 60 and by article 160, in writing.

If the penalty applicable to the offence is of at least two years' imprisonment and the needs of the inquiry or investigation justify this, the district prosecutor, the investigating jurisdiction, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court seized of the case may order the use of means protected by National Defence secrecy, following procedures laid down by the present chapter.

Article 230-2 (inserted by Law no. 2001-1062 of 15 November 2001 article 30 Official Journal of 16 November 2001) (Modified by Law n°2014-1353 of 13 November 2014):

Where the district prosecutor, the investigating court, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court in charge of the case decide to use, for the procedures mentioned in article 230-1, means protected by official State secrecy, the written submission must be sent to a technical organisation subject to the obligations of National Defence secrecy and designated for this purpose by Decree, along with the medium containing the data to be deciphered or a copy of it. This submission fixes the time limit in which these deciphering procedures must be carried out. The time limit may be extended under the same conditions or form. At any time, the district prosecutor, the investigating court, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court which is in charge of the case or which has requisitioned the technical organisation, may order the interruption of these prescribed procedures.

Data protected in the interests of national security may only be passed on under the conditions provided for by law n 98-567 of 8th July 1998 establishing the Advisory Commission for National Defence Secrecy.

Article 230-3 (inserted by Law no. 2001-1062 of 15 November 2001 art. 30 Official Journal of 16 November 2001) (Modified by Law n°2014-1353 of 13 November 2014):

As soon as the procedures have been completed, or as soon as it becomes clear that the procedures are technically impossible, or at the expiry of the time limit prescribed, or when an interruption order is received from the district prosecutor, the investigating court, the judicial police officer authorised by the district prosecutor or by the investigating judge, or the trial court in charge of the case, the results obtained and the documents received are returned by the head of the technical organisation to the author of the request. Subject to the obligations of National Defence secrecy, the results are accompanied by technical instructions enabling them to be understood and used, as well as by a statement drawn up by the head of the technical organisation, which attests to the genuineness of the results.

The facts thus obtained are recorded in an official record marking their receipt and are added to the case file of the proceedings.

Article 230-4 (inserted by Law no. 2001-1062 of 15 November 2001 art. 30 Official Journal of 16 November 2001) (Modified by Law n°2014-1353 of 13 November 2014):

Judicial decisions taken pursuant to the present chapter do not have judicial status and are not subject to appeal.

Article 230-5 (inserted by Law no. 2001-1062 of 15 November 2001 art. 30 Official Journal of 16 November 2001) (Modified by Law n°2014-1353 of 13 November 2014)

Without prejudice to any obligations relating to National Defence secrecy, officials to whom requests are made under the provisions of the present chapter are obliged to bring their support to justice.

E. Taking of Audio Recordings and Visual Images

In addition to the above-mentioned procedures, article 706-96 of the Penal Procedure Code authorises, in certain situations, the installation a technical device designed to hear, preserve, transmit or record words spoken by any person or persons in a private or confidential context, in private or public places or vehicles, or the images of any person or persons in a private place, without the consent of the persons concerned. These procedures are carried out under the authority and supervision of the investigating judge.¹⁴⁹

This procedure is not properly speaking a procedure that enables the interception of electronic communications, but may have such an interception as a result, notably through the recording of private images.

IV. Use of Electronic Communication Data in Judicial Proceedings

France applies the rule of evidence by all means,¹⁵⁰ subject to lawfulness and fairness, as long as this evidence can be discussed among the parties following the principle that both sides must be heard, in such a way that the right to a fair hearing is upheld).

¹⁴⁹ This paragraph is available in English at http://www.legifrance.gouv.fr/content/download/1957/13715/version/4/file/Code_33.pdf. However, the entire provision translated in the above-mentioned document has not been updated (the provision was last amended by Law n°2015-993).

¹⁵⁰ See notably art. 427 PPC. Production of evidence is regulated in arts. 427 to 457 PPC (in relation to misdemeanours) and in arts. 306 *et seq.* and 323 to 346 PPC (in relation to crimes).

A. Use of Electronic Communication Data in the Law of Criminal Procedure

Since evidence can be established by any means, electronic communication data are admissible in Justice in the same way as other proof, to the extent that their collection and the way they are presented before the court comply with legal rules and a principle of fairness.

Indeed, evidence must be collected in compliance with law,¹⁵¹ since rules of procedure are established in order to preserve the rights of the defence.¹⁵² A police record has probative value only if its form complies with requirements and if its author acted in the performance of their duties, on an issue falling within the scope of their responsibilities, and if they have reported what they have seen, heard, or noticed personally.¹⁵³

Moreover, the principle of fairness of evidence was established by the *Cour de cassation* (the French Supreme Court), as a condition for the exercise of the rights of the defence, and, more generally, as condition for a fair trial.¹⁵⁴

However, these requirements of lawfulness and of fairness are more strictly enforced in relation to evidence produced by the public authority (or by a private party on the instructions of the public authority), in comparison with evidence produced by a private party.

1. Evidence produced by public authorities

Evidence produced by public authorities may be the result of certain positive acts, but it must not be the result of acts that conduced the author to commit a penal infringement, in other words these acts must not have provoked or incited the commission of the penal infringement that is being proven.¹⁵⁵ More widely, the

¹⁵¹ Art. 427 PPC.

¹⁵² Pascal Lemoine, "La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)," *Cour de cassation annual report 2004*, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2004_173/deuxieme_partie_tudes_documents_176/tudes_diverses_179/travers_quelques_6401.html#n_20_

¹⁵³ Art. 429 PPC.

¹⁵⁴ Pascal Lemoine, "La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)," *op. cit.*

¹⁵⁵ Cass. crim., 27 Feb. 1996, "Schuller" court case, bull. crim. 1996, n° 93; JCP 96, ed. G, II-22629, note M.-L. Rassat; D. 96, p. 346, note Ch. Guéry; Cass. crim., 11 May 2006, pourvoi n°05-84.837, bull. crim. 2006, n°132; see Pascal Lemoine, *op. cit.* See also *Cour de cassation, rapport annuel 2012, La preuve*, Livre 3, partie 4, Titre 2, Chapitre 2 – Admissibilité des modes de preuve, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2012_4571/livre_3_etude_preuve_4578/partie_4_administration_preuve_4589/principes_gouvernant_4591/admissibilite_modes_26241.html

Cour de cassation rejects evidence obtained by fraudulent means.¹⁵⁶ Evidence thus obtained will be declared inadmissible,¹⁵⁷ and may even result in the nullity of proceedings.¹⁵⁸

However, the *Cour de cassation* does accept provocations that are not at the origin of the penal infringement, but which enable the infringement to be proven.¹⁵⁹

2. Evidence produced by private parties

The criminal chamber of the *Cour de cassation* considers that the judge does not have the power, based on articles 427 *et seq.* of the Penal Procedure Code, to reject evidence obtained by a party for the sole reason that this evidence has been unlawfully obtained.¹⁶⁰ Therefore, illegal and unfair means of proof are accepted by French courts, where the evidence is provided by a private party, especially where the way the evidence has been collected was justified by the necessity of proving a fact and the impossibility of proving it otherwise.¹⁶¹

The judge must in such a case appreciate the probative value of the evidence.¹⁶²

However, lawfulness and fairness is required where the private party who produces the evidence has acted in collaboration with public authority agents (under their instructions or with their assistance).¹⁶³

¹⁵⁶ Cass. crim., 28 Oct. 1991, bull. crim., n° 381; JCP, 1991.II.21704, note J. Pannier.

¹⁵⁷ Cass. crim., 9 Aug. 2006, n° 06-83.219, bull. crim. 2006, n° 202; Cass. crim., 7 Feb. 2007, pourvoi n° 06-87.753, bull. crim. 2007, n° 37; Cass. crim., 4 June 2008, pourvoi n° 08-81.045, bull. crim. 2008, n° 141; see *Cour de cassation*, rapport annuel 2012, *La preuve*, *op. cit.*

¹⁵⁸ Cass. crim., 27 Feb. 1996, bull. crim. 1996, n° 93.

¹⁵⁹ Cass. crim., 30 April 1998, pourvoi n° 97-85.747, bull. crim. 1998, n° 147; Cass. crim., 8 June 2005, pourvoi n° 05-82.012, bull. crim. 2005, n° 173; Cass. crim., 16 Jan. 2008, pourvoi n° 07-87.633, bull. crim. 2008, n° 14; see *Cour de cassation*, rapport annuel 2012, *La preuve*, *op. cit.*

¹⁶⁰ Cass. crim. 15 June 1993: bull. crim., n° 210 6 April 1993, JCP 1993, II, 22144, note M.-L. Rassat; see Pascal Lemoine, "La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)," *op. cit.*

¹⁶¹ Cass. crim., 31 Jan. 2007, pourvoi n° 06-82.383, bull. crim. 2007, n° 27. See *Cour de cassation*, rapport annuel 2012, *La preuve*, *op. cit.*

¹⁶² Cass. crim., 15 June 1993, pourvoi n° 92-82.509, bull. crim. 1993, n° 210; Cass. crim., 6 April 1994, pourvoi n° 93-82.717, bull. crim. 1994, n° 136; see *Cour de cassation*, rapport annuel 2012, *La preuve*, *op. cit.*

¹⁶³ Ex. Cass. crim., 11 May 2006, pourvoi n° 05-84.837, bull. crim. 2006, n° 132. See *Cour de cassation*, rapport annuel 2012, *La preuve*, *op. cit.*

B. The Right for the Accused to Challenge the Probity of Intercepted Data

The *Cour de cassation* does accept the admissibility of some proof obtained by illicit or unfair means under the strict condition that such proof does not entail a breach of the rights of defence. As a consequence, the Court verifies that the produced evidence has been submitted to a debate between the parties.¹⁶⁴

Indeed, the principle that both parties must be heard is set out in the Penal Procedure Code,¹⁶⁵ which implies that each of the parties can access the evidence produced by the other parties and has the time and the right to challenge this evidence. Therefore, the accused is entitled to challenge the means used and the procedure that has been followed in order to intercept electronic communications.

Proof to the contrary can in principle be established by any means, unless the law states otherwise, which is the case in very few matters. For example, where police records have been established by police officers or agents who received from a special legal provision the power of recording misdemeanours through police records, evidence to the contrary can only be produced in writing or by testimony.¹⁶⁶ Moreover, some special laws set out that some particular official records are considered to be valid proof until specific proceedings are launched to challenge the authenticity of facts.¹⁶⁷ Finally, written proof cannot result from correspondence between the accused and their attorney-at-law,¹⁶⁸ and the court can always order a forensic examination, if deemed necessary.¹⁶⁹

V. Exchange of Intercepted Electronic Communication Data between Foreign Countries

A. Legal Basis for Mutual Legal Assistance

International judicial cooperation is regulated by articles 694 *et seq.* of the Penal Procedure Code. These provisions apply in the absence of any international convention or bilateral treaty stipulating otherwise.

¹⁶⁴ See *Cour de cassation*, rapport annuel 2012, *La preuve*, *op. cit.*

¹⁶⁵ See, e.g., art. 427 PPC.

¹⁶⁶ Art. 431 PPC.

¹⁶⁷ Art. 432 PPC.

¹⁶⁸ Art. 433 PPC.

¹⁶⁹ Arts. 434, 310 PPC.

Within the limits of the provisions of these articles, which are detailed below, and within the limits of the powers for accessing electronic communications set out in the French Penal Procedure Code, mutual legal assistance may enable real-time access to electronic communication data.

1. General provisions

Article 694:¹⁷⁰

In the absence of any international conventions stipulating otherwise:

1° Requests for mutual assistance coming from French judicial authorities and addressed to foreign judicial authorities are sent through the intermediary of the Minister of Justice. The enforcement documents are sent to the authorities of the requesting State through the same channels.

2° Requests for judicial assistance coming from foreign judicial authorities are sent through diplomatic channels. The enforcement documents are sent to the authorities of the requesting State through the same channels.

In urgent cases, requests for mutual assistance sought by the French or foreign authorities may be directly sent to the authorities of the State who are competent to enforce them. The transmission of the enforcement documents to the authorities of the requested State is carried out in the same way and under the same conditions. However, unless there is an international convention stipulating otherwise, requests for judicial assistance coming from foreign judicial authorities and addressed to the French judicial authorities must be the subject of an opinion sent through diplomatic channels by the foreign government concerned.

Article 694-1:

In urgent cases, requests for judicial assistance coming from foreign judicial authorities are sent, according to the distinctions set out in article 694-2, to the district prosecutor or the investigating judge of the territorially competent district court. They may also be sent to these judges through the intermediary of the prosecutor general.

If the district prosecutor receives a request for judicial assistance directly from a foreign authority which may only be executed by the investigating judge, he sends it to the latter to be carried out, or seizes the prosecutor general in the case provided for by article 694-4.

Before executing a request for judicial assistance of which he has directly be seized, the investigating judge immediately sends this to the district prosecutor for his opinion.

Article 694-2:

Requests for judicial assistance coming from foreign judicial authorities are executed by the district prosecutor or by judicial police officers or agents nominated for this purpose by this prosecutor.

They are executed by the investigating judge or judicial police officers acting in the context of a rogatory letter where they require particular procedural acts which may not be ordered or executed in the course of a preparatory investigation.

¹⁷⁰ See the English translation of the French Penal Procedure Code proposed by Legifrance at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf (arts. 694 to 694-4 in this document correspond to their current version. Further articles have mostly been modified since the translation has been done).

Article 694-3:

Requests for judicial assistance coming from foreign judicial authorities are executed according to the procedural rules provided for by the present Code.

However, if the request for judicial assistance specifies this, it is executed in accordance with the procedural rules indicated by the competent authorities of the requesting State, on the condition, under penalty of nullity, that these rules do not reduce the rights of the parties or the procedural guarantees provided for by the present Code. Where the request for judicial assistance may not be executed in accordance with the stipulations of the requesting State, the competent French authorities immediately inform the authorities of the requesting State and indicate under which conditions the request may be executed. The competent French authorities and those of the requesting State may agree on the outcome of this request later on, where appropriate by subjecting it to the aforesaid conditions.

The irregularity of the sending of the request for judicial assistance may not constitute grounds for nullity of the acts executed in enforcing this request.

Article 694-4:

If the enforcement of a request for judicial assistance coming from a foreign judicial authority is liable to threaten public order or the fundamental interests of the nation, the district prosecutor seized of this request in accordance with the third paragraph of article 694-1 sends this to the prosecutor general who decides, if appropriate, to seize the Minister of Justice and gives, where applicable, notice of this reference to the investigating judge.

If he is seized, the Minister of Justice informs the authority which made the request, if appropriate, that no action, total or partial, may be taken in relation to the request. This information is communicated to the judicial authority concerned and blocks the enforcement of the request for judicial assistance or the return of the enforcement documents.

2. Provisions specific to cooperation between France and other EU Member States

Article 695-1:

Unless a foreign convention stipulates otherwise, and subject to the provisions of article 694-4, requests for judicial assistance are sent and enforcement documents returned directly between the judicial authorities territorially competent to issue and enforce them, in accordance with the provisions of articles 694-1 to 694-3.

Article 695-2:

Where there is need to carry out, in the context of a French prosecution, either complex inquiries involving the mobilisation of extensive resources and which concern other member states or where several member states are carrying out inquiries into offences which call for coordinated and concerted action between the member states concerned, with the prior agreement of the Minister of Justice and the consent of the member state or states concerned, the competent judicial authority may create a joint investigation team.

Foreign agents seconded by another member state to a joint investigation team may, within the limits of the powers conferred on them by their role, and under the supervision of the competent judicial authorities, have as their mission, as appropriate, over the whole of the national territory:

1° the establishment of any felonies, misdemeanours or petty offences, and to record these in an official record, if necessary in the forms provided for by the law of their state;

2° the reception of the official reports of any statements made to them by any person liable to provide information on the facts in question, if necessary in the forms provided for by the law of their state;

3° the secondment of French judicial police officers in the exercise of their duties;

4° the carrying out of any surveillance and, if they are authorised for this purpose, infiltration, under the conditions provided for by articles 706-81 onwards, and which is necessary for the application of articles 694-7 and 694-8.

Foreign officers attached to a joint investigation team may carry out these missions subject to the consent of the member state which has implemented their secondment.

These officers may only carry out the operations for which they have been designated. None of the powers which are the preserve of the French judicial police officer who is in charge of the team may be delegated to them.

The original copy of the official records which they prepare, and which must be drafted or translated into French, is attached to the case file.

Article 695-3:

In the context of a joint investigation team, French judicial police officers and agents attached to a joint investigation team may carry out operations ordered by the head of the team, over the whole of the territory of the State in which they are operating, within the limit of the powers conferred on them by the present Code.

Their tasks are defined by the authorities of the Member State competent to direct the joint investigation team in the territory where the team is working.

They may receive statements and record offences in the forms provided for by the present Code, subject to the consent of the State in whose territory they are operating.

B. Requirements and Procedure

1. Simplified exchange of information, implementing Decision 2006/960/JAI of 18 December 2006

The simplified exchange of information, implementing Decision 2006/960/JAI of 18 December 2006, is regulated in articles 695-9-31 to 695-9-49.

a) General provisions

Article 695-9-31 authorises National police and gendarmerie services and certain custom services to exchange, with competent services of another Member State, information that is at their disposal, in the aim of preventing a penal infringement, of collecting evidence in relation with a penal infringement or of searching for perpetrators of a penal infringement, either they detain it or they can access it, especially through the consultation of a data processing system, without making it necessary to take or ask for a requisition measure or another coercive measure.

Article 695-9-32 sets out that exchanged information is confidential, which must be guaranteed by its means of transmission and of storage.

b) Requests for information issued by French services

Articles 695-9-33 to 695-9-36:

When reasons exist to assume that a Member state holds information described in article 695-9-31 that is useful in order to prevent a penal infringement, or that is useful to investigations aiming at establishing evidence of a penal infringement or to search for its perpetrators, services and units mentioned in article 695-9-31 may request the transmission of this information from the relevant services of this State. The request for transmission must provide the reasons on which they base their assumption that this information is in the possession of these services, and must mention the purposes of the request for information, and, when this information is related to an identified individual, it must mention the link between this person and the purposes of the request (article 695-9-33).

Obtained information cannot be used as evidence without the agreement of the Member State that has transmitted it (article 695-9-34). This information cannot be used for other purposes (purposes other than those mentioned in the request) without the agreement of the Member State that has transmitted it, unless they may prevent a clear and immediate danger for public security (article 695-9-35). These provisions do not prevent the possibility for relevant authorities to control the modalities of processing and storage of transmitted information (article 695-9-35). If the transmitting State asks for it, the service or unit that obtained the information informs the relevant service of this State about the use that has been made of this information (article 695-9-36).

c) Requests for information received by French services

Articles 695-9-37 to 695-9-47:

Services and units mentioned in article 695-9-31 transmit, when requested so by relevant services of an EU member State, the information mentioned in the same article and that is useful in order to prevent a penal infringement, or that is useful to investigations aiming at establishing evidence of a penal infringement or to search for its perpetrators (article 695-9-37).

If the information mentioned in article 695-9-31 may be useful to another Member State to prevent one of the penal infringements mentioned in article 695-23¹⁷¹ and punished by at least three years of imprisonment, or if this information may be useful to this other member State in order to conduct investigations aiming at establishing evidence of such a penal infringement or to search for its perpetrators, the service or unit that holds this information transmits it to this other Member State without the need of having received a corresponding request (article 695-9-38).

When this information is initially transmitted by another Member State on the basis of the framework decision 2006/960/JAI, it may only be transmitted to another Member State following the conditions imposed by the first transmitting Member State. When this information is initially transmitted by another Member State on a basis other than

¹⁷¹ Art. 695-23 lists several penal infringements including (non-exhaustively) participation in a criminal organisation, terrorism, human trafficking, child pornography and sexual exploitation of children, cybercrime.

the framework decision 2006/960/JAI, or by a non-EU Member State, it may only be transmitted to another Member State with the agreement of the first transmitting State and under the conditions imposed by this State, in all the situations where France must respect these principles according to an International agreement (article 695-9-39).

Information can only be transmitted, to the relevant services of the Member State that requested it, with the authorisation of a judge, each time such an authorisation is mandatory under French law in order to access this same information or to transmit this same information to a judicial police service or unit. The request for authorisation is addressed to the relevant judge by the service or unit to which the information is requested. Elements of an ongoing penal procedure can only be transmitted with the authorisation of the investigating court in charge of the case, or with the authorisation of the public prosecutor when the trial court has been seized (article 695-9-40).

Services or units mentioned in article 695-9-31 cannot refuse to communicate information requested by a Member State, unless reasons exist to think that such communication:

- could be prejudicial to the fundamental interests of the State in terms of National security;
- could be prejudicial to ongoing investigations in penal matters or would jeopardise people's security;
- or would be clearly disproportionate or pointless in relation to the purposes for which the information has been requested (article 695-9-41).

Services or units mentioned in article 695-9-31 may refuse to transmit requested information when it relates to a penal infringement punished in France by a year or less of imprisonment and when they consider that the information is not of sufficient interest to justify the constraints attached to its transmission (article 695-9-42).

On the occasion of the transmission of the information, the service or unit mentioned in article 695-9-31 indicates to the receiving service the conditions of use of the information. Each time it deems it is necessary, it may ask the receiving service to provide information about the use that has been made of the transmitted information (article 695-9-43).

Where information has been transmitted by a service or unit mentioned in article 695-9-31 to the relevant service of a Member State and where the latter considers transmitting it to another State or using it for another purpose than the one for which the transmission was permitted, the service or unit that made the original transmission is competent to consider whether the new transmission or the new use should be authorised, on the request of the receiving State, and, if needed, to determine the conditions of it (article 695-9-44).

Information transmitted by the service or unit mentioned in article 695-9-31 may be used by the receiving service as evidence, unless it was otherwise stipulated on the occasion of its transmission (article 695-9-45).

Information transmitted by the service or unit mentioned in article 695-9-31 to the relevant service of a Member State is also transmitted to the Eurojust and Europol units, to the extent it relates to a penal infringement falling within their mandate (article 695-9-46).

Contact points to whose requests for transmission of information can be addressed by relevant services of Member States are nominated by order of the Ministry for Justice, of the Ministry of interiors and of the Ministry responsible for the budget (article 695-9-47).

Application of previous provisions to certain States that are not members of the European Union (articles 695-9-48 and 695-9-49)

Articles 695-9-31 to 695-9-47 are applicable to the exchange of information mentioned in article 695-9-31 between services and units mentioned in the latter article and relevant services from States which are not members of the EU but which are associated

with the implementation, the application and the development of the Schengen *acquis* (article 695-9-48).

Modalities of application of articles 695-9-31 to 695-9-48 are determined by a Decree issued by the Council of State (article 695-9-49).

2. Other provisions

Other provisions, not detailed or reproduced in this report, are related to Eurojust (articles 695-4 to 695-7), to the national members of Eurojust (articles 695-8 to 695-9), and to the issue and execution of orders freezing property or evidence under the European Union framework decision of 22 July 2003 (articles 695-9-1 to 695-9-30).¹⁷²

¹⁷² Arts. 695-9-1 to 695-9-9 and arts. 695-9-14, 695-9-18, and 695-9-26 can be read in their current version in the Legifrance translation available at http://www.legifrance.gouv.fr/content/download/1958/13719/version/3/file/Code_34.pdf. The other articles have been modified since 2005 (i.e., since this translation has been performed).

Bibliography*

- Beaume, Jacques, Rapport sur la procédure pénale, July 2014, p. 43, available at <http://www.justice.gouv.fr/publication/rap-beaume-2014.pdf>
- Chefs d'institution de l'Association des Cours constitutionnelles ayant en partage l'usage du français, "La proportionnalité dans la jurisprudence constitutionnelle," 5ème conférence, 8–13 July 2008, p. 7, available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/Bilan_2008/confV_accpuf_libreville_juillet2008.pdf
- Commission nationale de contrôle des interceptions de sécurité, CNCIS, report for the years 2013–2014, <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000101.pdf>
- Cour de cassation, rapport annuel 2012, *La preuve*, Livre 3, partie 4, Titre 2, Chapitre 2 – Admissibilité des modes de preuve, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2012_4571/livre_3_etude_preuve_4578/partie_4_administration_preuve_4589/principes_gouvernant_4591/admissibilite_modes_26241.html
- De Marco, Estelle, "Analyse du nouveau mécanisme de prévention de la contrefaçon à la lumière des droits et libertés fondamentaux," 4 June 2009, Juriscom.net, <http://www.juriscom.net/uni/visu.php?ID=1133>
- *L'anonymat sur Internet et le droit*. Thesis, Montpellier 1, 2005, ANRT.
- De Marco, Estelle et al., *D3.3 – Legal recommendations*, Deliverable, ePOOLICE project (early Pursuit against Organized Crime Using Environmental Scanning, the Law and Intelligence Systems), project n° FP7-SEC-2012-312651, version 1.2 of 29 August 2014 and version 1.3 of 10 December 2014.
- De Marco, Estelle/Callanan, Cormac, in: C. Callanan/M. Gercke/E. De Marco/H. Dries-Ziekenheiner, *Internet blocking – balancing cybercrime responses in democratic societies*, October 2009, n° 6.5.2.2, available at <http://www.aconite.com/blocking/study> (French version available at <http://juriscom.net/2010/05/rapport-filtrage-dinternet-equi-librer-les-reponses-a-la-cybercriminalite-dans-une-societe-democratique-2/>)
- Dutheillet de Lamothe, Olivier, "L'influence de la Cour européenne des droits de l'Homme sur le Conseil constitutionnel, 13 février 2009, Conseil constitutionnel, visite du Président et d'une délégation de la Cour européenne des droits de l'homme au Conseil constitutionnel, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/pdf/Conseil/cedh_130209_odutheillet.pdf
- Goesel-Le Bihan, Valérie, "Le contrôle de proportionnalité exercé par le Conseil constitutionnel, technique de protection des libertés publiques?", <http://juspoliticum.com/Le-controle-de-proportionnalite.html>

- Kayser, Pierre, *La protection de la vie privée par le droit*. 3rd ed. PU d'Aix-Marseille/Economica 1995.
- Lafay, Frédérique, note under Decision of the Constitutional Council n° 94-352 DC, 18 January 1995, J.O. 21 January 1995, p. 1154 and JCP 1995, II, 22525.
- Lemoine, Pascal, "La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)," Cour de cassation annual report 2004, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2004_173/deuxieme_partie_tudes_documents_176/tudes_diverses_179/travers_quelques_6401.html
- Peltier, Virginie, *Le secret des correspondances*. PU d'Aix-Marseille 1999.
- Rassat, Michèle-Laure, note under Cass. crim., 15 June 1993: bull. crim., n° 210. 6 April 1993, JCP 1993, II, 22144.
- note under Cass. crim., 27 February 1996, "Schuller" court case, bull. crim. 1996, n° 93; JCP 1996, ed. G, II, 22629.
- Robert, Jacques/Duffar, Jean, *Droits de l'homme et libertés fondamentales*. 7th ed. Montchrestien 1999, p. 27.
- Sudre, Frédéric, "La dimension internationale et européenne des libertés et droits fondamentaux." In: Rémy Cabrillac/Marie-Anne Frison-Roche/Thierry Revet (dir.), *Libertés et droits fondamentaux*. 11th ed. Dalloz 2005.

List of Abbreviations

bull. crim.	Bulletin de la Cour de Cassation, chambre criminelle (reports of the Court of Cassation's decisions, criminal chamber)
Cass. crim.	Cour de Cassation, chambre criminelle (Criminal Chamber of the Court of Cassation)
CNCIS	Commission nationale de contrôle des interceptions de sécurité (National Commission for the Control of Security Interceptions)
CNCTR	Commission nationale de contrôle des techniques de renseignement (National Commission for the Control of Intelligence Techniques)
D.	Recueil Dalloz (law journal)
dir.	sous la direction (edited by)
DJS	Droits, Justice et Sécurités (laws, justice and securities)
E. Court H. R.	European Court of Human Rights
ECTHR	European Convention on Human Rights
IP	Internet Protocol

* All URLs were last accessed in 10/2016.

ISC	Internal Security Code
JCP	La semaine juridique (law journal)
JCP. ed. G	La semaine juridique édition générale (law journal, general edition)
J.O.	Journal Officiel (official gazette of the French Republic)
JORF	Journal officiel de la République française (official gazette of the French Republic)
PC	Penal Code
PECC	Post and Electronic Communications Code
PPC	Penal Procedure Code