The State of Communication Privacy Law in Spain

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Griselda Casadellà (Eticas
Foundation)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Griselda Casadellà (Eticas Foundation)

EFF's Associate Director of Research, Gennie Gebhart edited this report. EFF's Engineering and Design Project Manager, Kim Carlson, along with EFF's Art Director, Hugh D' Andrade and EFF's Education & Design Lead, Soraya Okuda designed and formatted this report. EFF's engineers, Syd Young, Artemis Schatzkin, and Will Greenberg developed the revamped version of the Necessary & Proportionate website.

EFF would like to thank Luiza Rehder do Amaral, EFF Tecs-USP Fellow (2019) for her research and contributions to this report.

A publication of the Electronic Frontier Foundation, 2020.

JUNE 2020

INTRODUCTION

This report provides condensed information on the rules for government access to communication data in criminal investigations in Spain. It offers brief and straightforward answers on a set of relevant questions regarding when and under which conditions law enforcement authorities can gain access to users' communications data in criminal investigations as well as an overview of transparency obligations and practices.

This FAQ is intended for non-lawyers who want some general information about the legal framework for government access to data, but is not legal or technical advice.

The legal questions raised by this FAQ can be complex and the legal risks in any case will depend on the particular facts and on legal doctrines not necessarily mentioned here. This FAQ is meant to familiarize you with some of the principles involved, so that you can have a more effective discussion if and when you engage an attorney to help you with your particular circumstance.

DATA PROTECTION OVERVIEW

1. Is there a data protection law?

Yes, Spain is subject to the EU's Data Protection Reform package. This package contains the GDPR, the General Data Protection Regulation 2016/679, and Police Directive 2016/680 on the processing of personal data for authorities responsible for preventing, investigating, detecting, and prosecuting crimes. The GDPR, which entered into force on May 28, 2018, required the preparation of a new national law in each EU member state. In 2018, Spain adopted its new data protection law, Organic Law 3/2018[1] based upon the GDPR, and repealed the Organic Law 15/1999, which transposed the old Directive 95/46/CE. However, as Spain has not implemented the Police Directive yet, part of the repealed law remains in force with regards to personal data processing for law enforcement activities.[2]

2. Is there a data protection authority?

The Spanish Data Protection Agency was founded in 1994 and it is an independent body.

3. Does the data protection law apply to law enforcement activities?

Spain is subject to the EU's Data Protection Reform package, which contains the GDPR and the Police Directive 2016/680 on the processing of personal data for authorities responsible for preventing, investigating, detecting, and prosecuting crimes. Spain has not implemented the Police Directive 2016/680 yet. Still, provisions regarding law enforcement activities within the country's previous data protection law (Organic Law 15/1999) remain applicable to personal data processing in criminal investigation and prosecution.[3]

4. What are the criteria, if any, for the transfer of personal data to third countries under their data protection law?

Spanish data protection law follows the GDPR. The GDPR primarily applies to controllers and processors located in the European Economic Area (EEA) with some exceptions. However, the GDPR restricts the transfer of personal data outside the EEA unless the

[1] Data Protection Law - Organic Law 3/2018 (*Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*) https://boe.es/diario_boe/txt.php?id=BOE-A-2018-16673 (Spanish).
[2] See fourteenth additional provision (*disposición adicional decimocuarta*) and fourth transitional provision (*disposición transitoria cuarta*), Data Protection Law.
[3] Articles 22 to 24, and provisions that unfold them, Organic Law 15/1999 (*Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*), https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750 (Spanish)

third country guarantees an adequate level of personal data protection. Article 45 of the GDPR states that a transfer of personal data to a third country or an international organization may take place where the European Commission has decided that the third country, such as those outside the European Union, can ensure an adequate level of data protection. If the European Commission has approved a country's "adequacy" decision, the transfer of personal data from Spain to a third country can take place without the need for specific authorization.

The European Commission takes into account the following elements when assessing the adequate level of privacy protection of a third country:

- The rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security, and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation;
- The existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules;
- The international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular concerning the protection of personal data.

Alternatively, a controller or processor may transfer personal data to a third country that does not comply with the adequacy requirements of Article 45(3) if the controller or processor provides appropriate safeguards. Article 46 describes appropriate safeguards. Some appropriate safeguards that do not require any specific authorization from a supervisory authority are: a legally binding and enforceable instrument between public authorities or bodies; binding corporate rules; and standard data protection clauses adopted by the Commission, among others.[4] Some other appropriate safeguards that require authorization from a competent supervisory authority are contractual clauses between the controller or processor and the controller, processor or recipient of the personal data in the third country or international organization; or provisions to be inserted into administrative arrangements between public authorities, which include enforceable and effective data subject rights.[5]

[4] Article 46 (2), Data Protection Law.
[5] Article 46 (3), Data Protection Law.

COMMUNICATIONS PRIVACY LAW

5. What's the legal authorization needed to access communications data?

Interception of communication

The Criminal Procedure Act *(Ley de Enjuiciamiento Criminal)* requires that the interception of communication be authorized by a judge *(juez de instrucción)*,[6] except in case of emergencies. A judge can request the interception either ex officio or following an initiative by the Judicial Police[7] or public prosecutor.[8]

Access to the content of communications and metadata

A judge can authorize requests to access the content of a communication and traffic data or data associated with the communication, either ex officio or following an initiative by the Judicial Police or public prosecutor.[9] The law defines traffic data or data associated with the communication to be any data generated as a result of electronic communication or a communication service.[10]

Devices or media that are subject to such intervention are the ones regularly or occasionally used by the person under investigation.[11] Additionally, access to the victim's devices or means of communication may also occur if there is a foreseeable severe risk to their life or physical integrity.[12] Finally, a judge (*juez de instrucción*) can authorize accessing the devices belonging to a third person as long as there is evidence that the person under investigation uses that device to transmit or receive information, or that the owner cooperates with the person under investigation in their illegal activities or if the owner benefits from their activity.[13]

[6] *Juez de instrucción* is a judge in charge of the initial phase of the criminal process, i.e. of the instruction phase.
[7] The Judicial Police assist the courts and the public prosecutor in the investigation of crimes and in the discovery and assurance of criminals. The Judicial Police include administrative public safety authorities responsible for prosecution of all crimes or special ones; employees of the security police, majors deputy and neighborhood mayors; chief officers and individuals of the civil guard, and any urban or rural police; personnel dependent on the Central Traffic Headquarters in charge of the technical investigation of accidents. To learn more about the Judicial Police, see article 547 of the Organic Law of the Judicial Branch (*Ley Orgánica del Poder Judicial)* and article 283 of the Criminal Procedure Law *(Ley de Enjuiciamiento Criminal)*.
[8] *See* article 588 bis a, b and c, article 579 (1), 588 ter a. Criminal Procedure Act, Royal Decree, September 14, 1882, and amendments. (*Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal y sus modificaciones posteriores*) https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).
[9] Article 588 bis b (1), article 588 ter b, Scope (*Ámbito*), Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).
[10] Article 588 ter b. Scope (*Ámbito*), Criminal Procedure Act.
[11] Article 588 ter b (1), Criminal Procedure Act.
[12] Artícle 588 ter b (2), Criminal Procedure Act.
[13] Artículo 588 ter c, Criminal Procedure Act.

Access to retained metadata

Service providers must request a judicial authorization before handing over retained traffic data (either data kept by the company voluntarily, or compelled retention in compliance with Spanish data retention law) to the competent authorities.[14] When knowledge of this retained data is essential for the investigation, a competent judge may authorize requesting access from service providers, cross-reference the information with other data held by the provider, or require that "an intelligent data search" be made, if the data is specified, along with reasons that justify handing over the data.[15] A competent judge can authorize such an order either ex officio or following an initiative by the Judicial Police or public prosecutor.[16]

Access to subscriber data

The law refers to subscriber data as data that is necessary for the identification of users, terminals and connectivity devices, such as a computer or mobile phone.[17] Competent authorities can obtain the data without a court order in specific cases authorized by law:

- Identification of owners of terminals or connectivity devices: The law refers to two situations. The first case is when the Public Prosecutor's Office or the Judicial Police, in the exercise of their functions, seek to know who owns a telephone number or any other means of communication. In the opposite case, authorities need to know a telephone number or the identifying data of any means of communication associated with an individual (although the law may be interpreted to permit both a request based on a person's legal identity, and a request based on some other technical identifier). In both cases, the Act allows them to contact the service provider directly. Refusing such a request counts as a "crime of disobedience."[18]
- Identification of the devices by captured IMSI or IMEI: The Judicial Police may use "technological means" (*artificios técnicos*) that allow access to the IMSI or IMEI identifiers and, in general, any method that is capable of identifying the equipment or the SIM card used to access a telecommunications network. The "technological means" in question could be interpreted broadly to include IMSI catchers, cell site simulators, or even malware, as long as it is used to identify the equipment or the SIM card. Those powers are authorized only when it is not possible to obtain a certain subscriber number in any other way, and the subscriber details are indispensable for the investigation.[19]

[14] Article 588 ter j (1), Criminal Procedure Act.
[15] Article 588 ter j (2), Criminal Procedure Act https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).
[16] Article 588 bis a, b and c, article 579 (1), 588 ter a. Criminal Procedure Act.
[17] Criminal Procedure Act, Section 3rd. Access to the necessary data for the identification of users, terminals and connectivity devices (*Sección 3.ª Acceso a los datos necesarios para la identificación de usuarios, terminales y dispositivos de conectividad*)
[18] Article 588 ter m, Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).
[19] Article 588 ter l, Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).

Identification by IP addresses

As for identification of IP numbers, law enforcement authorities are not allowed to demand subscriber data from service providers directly. Instead, the Judicial Police can ask the investigating judge to order the provider to disclose identifying information (such as location and subscriber identity) about the user of an IP address used in the commission of a crime, in cases where the identity of those using the IP address or the location of the equipment or the device or any other personal identification is unknown.[20]

Location data

A competent judge may authorize the use of devices or any technical means to track a target in real time and to identify their location provided the measure is necessary and proportionate.[21] The authorization must specify the technical means to be used. This requirement is essential for the judge to assess the proportionality of the use of specific location tracking tools. Law enforcement agents may use this authority to request authorization for a wide variety of technologies, such as physical trackers or electronic surveillance methods like IMSI catchers. In our view, the proportionality requirement in the law means that judges should nonetheless not grant authorization for the use of IMSI catchers under this provision, since they inherently cannot meet the proportionality requirement.

Exceptionally, in urgent cases, when the investigation could be frustrated, the law authorizes that the tracking technology must be immediately put in place. In such cases, the Judicial Police may proceed but must notify the judicial authority as soon as possible, and no more than twenty-four hours later. The judicial authority must be able to approve the adopted measure or to agree its immediate cessation, discarding the data, within the same period.

6. What's the factual basis to access communications data?

Content and metadata

Judicial authorization for investigative measures (for example, the interception of communications or accessing content or traffic data) must comply with the principles of relevance, adequacy, exceptionality, necessity, and proportionality.[22] An investigative measure is proportionate when, taking into consideration the circumstances of the case, the sacrifice of the rights and interests of affected individuals does not exceed the benefit that its use will result in for the public interest and that of third parties.[23] The relevance principle requires that the measure must be related to the investigation of an

[20] Article 588 ter k, ter l, and ter m and article 588 ter e, Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).
[21] Article 588 quinquies b. Use of devices or technical means for tracking and location, Criminal Procedure Act.
[22] Article 588, bis a, 1, 2, 3, 4, 5, Criminal Procedure Act.
[23] Article 588, bis a, 5, Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).

actual crime, and technological investigative measures that lack an objective basis cannot be authorized.[24] The adequacy principle defines the objective and subjective scope of the investigative measure and its duration as defined by its usefulness.[25] Lastly, in applying the exceptionality and necessity principles, the judicial authorization should ensure (a) that there are no other less burdensome measures to fundamental rights, and the measure is useful for the investigation; and (b) that the discovery and ascertainment of the facts, the perpetrators, and/or f their whereabouts would be seriously hindered without the measure.[26]

Interception and access to traffic data are authorized only when the investigation is related to crimes punishable by a maximum of at least three years in prison, crimes committed within a criminal group or organization, terrorist offenses, or crimes committed through a computer or any other technology.

Subscriber data

As for the identification of users, terminals and connected devices, the law does not require a previous judicial authorization, provided it is necessary and proportionate as per Article 588 bis, a, 5, and Article 588, ter l, and ter m.

7. Which authorities have the legal capacity to request access to communications data?

The competent authorities authorized to access retained traffic data are: (i) the members of the security forces, when they perform Judicial Police functions; (ii) officials from customs surveillance directorate when they act as Judicial Police; and (iii) the National Intelligence Center in the course of security investigations on persons or entities.[27]

For interception: A judge can request the interception either ex officio or following an initiative by the Judicial Police or public prosecutor.[28]

8. Does the country have provisions about access to data in cases of emergency?

In cases of emergency, the interception of communications can be ordered, in an exceptional manner, by the Minister of Home Affairs (*ministro del interio*r) and the Secretary of State for Homeland Security. Those emergency powers are authorized when the investigations are related to armed gangs or terrorist crimes, and there are likely reasons that make the planned measure essential. In such emergency cases, the

[24] Article 588 bis a, 2, Criminal Procedure Act.
[25] Article 588 bis a, 3, Criminal Procedure Act.
[26] Article 588, bis a, 4, Criminal Procedure Act.
[27] Article 6, Mandatory Data Retention Act (*Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*) http://noticias.juridicas.com/base_datos/Admin/l25-2007.html (Spanish).
[28] Article 588 bis b, Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).

investigative measure must be brought before a competent judge within a maximum of 24 hours.[29] A legal justification must be made in writing to the relevant judge, who will revoke or confirm it, also with a reasoned opinion, within 72 hours from the time the order was issued.

9. Is there any data retention mandate?

The Mandatory Data Retention Act compels telecom operators to retain traffic data (who communicates with whom, for how long, from where).[30] The obligation to retain data extends to unsuccessful calls, those that have been made successfully but without an answer, or when there has been an intervention by any of the operators involved in the call.

The data retention obligation ceases twelve months after the date the communication occurred. The retention obligation can extend to specific data or categories of data for up to a maximum of two years or a minimum of six months. The judicial authorization must define which retained data must be transferred to the authorized authorities and must comply with the principles of necessity and proportionality, and all the requirements of the Criminal Procedure Act. The Act establishes sanctions for those who fail to retain data or do not retain data systematically.[31]

10. Are there any rules that authorize the use of malware?

A competent judge may authorize the use of identification data and codes, as well as the installation of software which allows, remotely via a telecommunications system, long-distance examination of the content of a computer, electronic device, information system, computer mass storage system or database without knowledge of its owner or user, as long as it is done in pursuit of the investigation of any of the following crimes: [32]

a) Crimes committed by organized criminal organizations,
b) Terrorist offenses,
c) Crimes against minors or persons adjudicated as having diminished capacity,
d) Crimes against the constitution,
e) Crimes of treason or related to national defense,
f) Crimes committed by means of computing systems or any other information, telecommunications, or communications service.

[29] Article 588 ter d3, Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).
[30] Mandatory data retention, Act 25/2007 (*Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones*). The 25/2007 Act provides a specific list of items that must be retained such as data needed to track and identify the origin of a communication, data needed to identify (i) the destination of a communication, (ii) the date, time and duration of a communication, (iii) the type of communication, (iv) the users' communication device or what is considered to be the communication equipment, (v) the location of mobile communication equipment.
http://noticias.juridicas.com/base_datos/Admin/l25-2007.html (Spanish).
[31] Article 9, Act 25/2007, http://noticias.juridicas.com/base_datos/Admin/l25-2007.html#a2 (Spanish).
[32] Article 588 septies a, Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish).

The court order authorizing the search shall specify:

a) The computers, electronic devices, information systems or components thereof, data storage media or databases, data, or other digital content that form the object of the measure.
b) The scope of the measure, the form in which the access and seizure of the data or files relevant to the case will be carried out, and the software by means of which control over the information will be maintained.
c) The agents authorized to carry out the measure.
d) If applicable, the authorization to make and retain copies of data.
e) The measures required for the preservation of the integrity of stored data, as well as for the inaccessibility and suppression of the same.

When the agents carrying out a remote search have reason to believe that the data sought is stored on a different information system or part thereof, they shall bring this fact to the attention of the judge, who may authorize an expansion of the scope of the search.

11. Is there any law that compels companies to provide direct access to their internal servers for law enforcement purposes?

We did not find any provision in the law that authorizes this kind of access in criminal investigations.

12. Does the law compel companies to assist law enforcement agencies in their investigations?

Spanish law mandates that a broad set of companies and persons provide investigating agents with the necessary assistance for carrying out interception orders (art. 588 ter e) and malware installation (art. 588 septies b). Likewise, those companies and persons are obliged to provide the necessary assistance so the collected data and information can be examined and understood. Those companies and persons are specified in Article 588 ter e which includes telecommunication service providers, telecommunication network access providers, or information society service providers, as well as every person who contributes in any way toward facilitating communications by telephone or any other telematic, logical, or virtual communication system. This provision is also extended to malware installation (art. 588 septies b), compelling any person who either is familiar with the functioning of an information system or knows the details of the system's security measures to turn over the information that is needed to ensure the success of the investigative process. All of the entities compelled to provide assistance in this way are required to keep these activities secret, and many be punished for "disobedience" if they fail to provide the assistance demanded.

TRANSPARENCY & COMMUNICATIONS PRIVACY

13. Does the State report on the number of requests to access communications data?

No.

14. Is there any legal limitation that prohibits companies from publishing transparency reports?

To the best of our knowledge, no normative framework prohibits companies from publishing statistical data on the number of data requests made by the state in criminal or national security matters.

15. Do telecommunication companies publish transparency reports?

- **Telefónica-Movistar** publishes yearly transparency reports.
- **Orange** published its latest transparency report in 2018 containing statistical information about interception and metadata/subscriber data requests in Spain. **Jazztel**, its Spanish subsidiary, doesn't publish more detailed local transparency reports.
- **Masmóvil** hasn't published any transparency reports.
- **Ono Vodafone** published its latest transparency report in 2016-2017.

16. Can companies notify users about States' data requests?

Investigative measures (such as the interception of communication. malware, location tracking or access of communication data are secret by default.[33] The obliged party carrying out the investigative measures must comply and is sworn to secrecy or risk committing a crime of disobedience.[34]

[33] Article 588 bis d, Criminal Procedure Act, https://www.boe.es/eli/es/rd/1882/09/14/(1)/con (Spanish) "La solicitud y las actuaciones posteriores relativas a la medida solicitada se sustanciarán en una pieza separada y secreta, sin necesidad de que se acuerde expresamente el secreto de la causa."
[34] Article 588 bis c 3 h, Criminal Procedure Act.