Report

This part of the EDPL hosts reports in which our correspondents keep readers abreast of various national data protection developments in Europe, as well as on the most recent questions in different privacy policy areas. The Reports are organised in cooperation with the Institute of European Media Law (EMR) in Saarbrücken (www.emr.sbg.de) of which the Reports Editor Mark D. Cole is Director for Academic Affairs. If you are interested in contributing or would like to comment, please contact him at mark.cole@uni.lu.

Spain


Juan José González López and Julio Pérez Gil*

Organic Law 13/2015 of 5 October 2015, amending the Spanish Criminal Procedure Law in order to strengthen procedural guarantees and regulate technology-related investigation measures, has made a remarkable improvement to the now century-old code governing Spanish criminal procedure called the Ley de Enjuiciamiento Criminal (Criminal Procedure Law, hereinafter CPL). An answer has thus been provided to an often-heard cry from jurisprudential, police and academic circles calling for a number of criminal investigation measures to be regulated with sufficient clarity, precision and predictability, since they make use of the new technologies and affect fundamental rights.¹ The latter include the right to protection of personal data as set out in Article 18.4 of the Spanish Constitution (SC).

I. The amendment of the Criminal Procedure Law

The ‘technology-related investigation measures’ referred to in the amendment include various proceedings for obtaining sources of evidence that come to be regulated in Chapter IV et seq of Heading VIII in Book II of the CPL: interception of telephone and telematic communications, obtaining and recording oral communications through the use of electronic devices, the use of devices for image monitoring, localisation and capture, the searching of mass data storage devices and remote searches performed on computer equipment.² A feature that is common to all of them is the use of instruments or interference

---

¹ Given the extent of the doctrine that has concerned itself with these types of measures (although not all cases are discussed with the same degree of intensity), we cite the following by way of example: Juan José González López, ‘Intervención de comunicaciones: nuevos desafíos, nuevos límites’ in Julio Pérez Gil (ed), El proceso penal en la sociedad de la información (La Ley 2012), 109-172, for communications interception; Jesús Martínez Ruiz, Límites jurídicos de las grabaciones de la imagen y el sonido (Bosch 2004) 364, for recordings of direct oral communications; J. Pérez Gil, ‘Los datos sobre localización geográfica en la investigación penal’ in Ernesto Pedraz Penalva (ed), Protección de datos y proceso penal (La Ley 2010), 307-354, for monitoring measures; José Francisco Echeverría Guriñi, ‘Videovigilancia y su eficacia en el proceso penal’ in Pérez Gil (ed), El proceso penal en la sociedad de la información (La Ley 2012), 267-310, for video surveillance; J. González López, ‘Utilización en el proceso penal de datos vinculados a las comunicaciones electrónicas recopilados sin indicios de comisión delictiva’ in E Pedraz Penalva (ed), Protección de datos..., 355-430; for the search of devices used by the new technologies; and J C Ortiz Pradillo, ‘Nuevas medidas tecnológicas de investigación criminal para la obtención de prueba electrónica’ in J Pérez Gil (ed), El proceso penal..., 279-304, for remote searches.

² The Explanatory Memorandum also appears to include the seizure and opening of written and telegraphic correspondence (arts 579 and 579.bis of the CPL).
with devices that use the new technologies and, what is most relevant to our analysis, involve a qualified processing of personal data.

All the measures outlined here can be considered to fall within the scope of the right to protection of personal data. However, extension of this right in the regulation introduced by Organic Law 13/2015, if it is regulated at all, is not clear, let alone coherent. For example, in some cases, the attention it merits becomes blurred in the attention paid to other fundamental rights (right to secrecy of communications, in the case of interception of telephone and telematic communications; privacy, in the case of obtaining and recording of direct oral communications and use of devices or technical resources for monitoring and localisation), while in other cases, it is doubtful whether regulation of the measure has been carried out in consideration of this right. That appears to result from the absence of a comprehensive analysis of its implications in criminal investigations, in addition - in the case of Organic Law 13/2015 - to the influence that the regulation of interception of communications has on the package of measures that are governed by the Law.3

II. The New Measures Introduced

1. Interception and Monitoring of Communications

As regards the interception of communications, Organic Law 13/2015 incorporates a number of jurisprudential requirements for the adoption and enforcement of the measure.4 Given the reinforced protection that the right to secrecy of communications is afforded in Spanish law (subject, in its limitations, to jurisdictional authorisation by constitutional mandate in Article 18.3), the guarantees that are required from the viewpoint of the right to protection of personal data are subsumed in those laid down for restricting the right to secrecy of communications. The fact remains, however, that the doctrine stating that this right is limited to the communication in hand has, albeit hesitantly, gradually predominated, leaving the gathering of data linked to electronic communications, but prior or subsequent to that communication, outside its scope of application.5 This is the meaning that can be sensed in the regulation in two different sections that are integrated into Chapter V itself, which is devoted to ‘The interception of telephone and telematic communications’. On the one hand, the ‘Incorporation into the processing of electronic traffic or associated data’ is regulated and on the other hand, we find the regulation of ‘Access to the data necessary for identifying users, connectivity terminals and devices’, which does not even involve interception in the strict sense of the word.

In relation to the ‘obtaining and recording of oral communications through the use of electronic devices’, it must be emphasised that the Law overrides a prior restrictive view. As a result of the discussion whether or not privacy was possible in public spaces, the requirement for judicial authorisation had become limited to closed spaces. We can, however, see in the regulation of the ‘obtaining of images in public places or spaces’ (Article 588.quinquies.a of the CPL) that the requirements proposed with regard to obtaining of oral communications (jurisdictionality, proportionality) are more stringent since they respond to the more restrictive application of fundamental rights to sound than to image. This reasoning might make sense from the viewpoint of privacy (although not necessarily: an image may reveal much more private information than a conversation), but not when considering image and sound as personal data. The fact that the Law is based on privacy and not on the protection of personal data also explains why it excludes the obtaining of images in public spaces from being subject to judicial authorisation and that, on the other hand, obtaining them in closed spaces requires judicial authorisation (which is also apparent from Article 588 bis.1 of the CPL).

The Law’s focus on privacy also leads to a blurring of the requirements for adopting the measures. Thus, the use of monitoring devices (beacons, for example) is subject to judicial authorisation, while monitoring involving the obtaining of images is not, because apparently it is not considered so intrusive. The truth is, however, that from the viewpoint of the right to

---

3 A clear example of this is the provision for ‘jurisdiction’ contained in art 588 bis.1 of the CPL, to be found in the chapter devoted to ‘rules that are common’ to all technology-related investigation measures, that is later objected to by some of them.

4 The analysis made in Fiscalía General del Estado, ‘Circular 1/2013, sobre pautas en relación con la diligencia de intervención de las comunicaciones telefónicas’ (11 January 2013) is of great interest in this respect.

5 A recent example of this is Supreme Court Judgment (Criminal Division) 31/2015 of 27 May 2015.
protection of personal data, both types of action are, in principle (we shall be qualifying this later on) comparable (i.e., a data collection) and from the viewpoint of the right to privacy it is very doubtful that control over location is a less serious matter than control over image. What is more, and in relation to monitoring devices, the Law does not make any distinction whatsoever as to the source of the information, in other words, whether it is obtained through the use of specific devices for generating it or from interference with data processed for other purposes. The latter is precisely what happens in the case of electronic communications, the subsumption of which under Article 588.quinquies.b is apparent from the fact that this provision’s third paragraph provides for the duty of electronic communications service providers to cooperate in facilitating compliance with court decisions ordering monitoring to be implemented. Thus, the different intensity of the interference that results depending on whether the data has or has not been processed previously, is avoided.

2. Searching of Mass Data Storage Devices

The amendment also includes the ‘searching of mass data storage devices’ (Chapter VIII) and ‘remote searches on computer equipment’, the latter being subject to much stricter requirements than the former, owing to the more serious nature of the interference, as it is conducted without the knowledge of their registered holder or user (Chapter IX, Article 588.quinquies.a.1 of the CPL). Both measures are designed to cover automated data processing devices, which, in the opinion of the Agencia Española de Protección de Datos (Spanish Data Protection Agency) and in jurisprudence, are covered by the right to protection of personal data. The regulation is, however, applied regardless of the type of information, which does not necessarily have to be of a personal nature (although it would be hard to rule out a priori the possibility that this category of data is found among the content). This would appear to indicate that the legal basis for the regulation is not the right to protection of personal data, but another fundamental right or manifestation of privacy in the broadest sense of the word. This seems to be related to what has been called in Germany the ‘fundamental right to the guarantee of confidentiality and integrity of computer equipment’ (‘Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität Informationstechnischer Systeme’).

III. Lack of Rules Concerning Data Transfer

The neglect of the right to protection of personal data that we have been discussing here finds its clearest manifestation in an omission: generally speaking, the transfer of personal data for criminal investigation purposes is not regulated. It is true that there is provision for certain manifestations of what might be qualified as data transfer or, at least, as an interference the seriousness of which is comparable with that, but this is done in a disconnected way since it falls within the ambit of other investigative measures laid down in the CPL. In this respect, the following needs to be pointed out:

- Three different norms regulate a further three types of data transfer: a) that of ‘data present in automated files of service providers’ (Article 588.ter.j of the CPL), b) that of data permitting identification and location of the connected terminal or device and identification of the suspect (Article 588.ter.k of the CPL) and c) the supply of data requested for identifying registered holders or connectivity terminals or devices (Article 588.ter.m of the CPL). All these measures involve a data transfer and what they have in
common is that they are related to electronic communications and are directed at the providers of such services. They are regulated in different articles since they are linked to different fields: a) the first is related to the generalised retention of data provided for in Law 25/2007 of 18 October 2007 on the retention of data relating to electronic communications and public communications networks (Data Retention Law, hereinafter DRL); b) the second is connected to ‘cyber patrolling’ or the obtaining of the IP address upon a formal complaint or a chance discovery on the web; c) the third one is linked to a kind of general clause on obtaining what can be identified as ‘subscriber or user data’. Judicial authorisation is required, in practice, in all three cases, which satisfies jurisprudential requirements in this regard. The legal basis for such requirement is, however, unclear. In the first case, it finds support in the DRL (whose Article 7 calls for judicial authorisation) and in a Resolution adopted by the non-jurisdictional Plenary Session of the Supreme Court (Criminal Chamber) of 23 February 2010. Yet in the second and third cases the legal basis lies in the different judgments that have called for such authorisation under the influence of the foregoing, and therefore in view of the right to the confidentiality of communications, which is not limited to ongoing communications.

- Transfer is, as noted above, confined to what has been obtained from the electronic communications service providers, so that what can be collected from other subjects, including the owner of the information, is not regulated;
- Use of the ‘IMSI-catcher’ is also inserted by the amending law and regulated by the amending law (Article 588.1 of the CPL). However, its different significance from the viewpoint of the right to protection of personal data is not specified (this had certainly been noticed by jurisprudence). Although this aspect has been reflected in its regulation, jurisdictional authorisation is not required.
- Access to or transfer of personal data is only regulated when the processing is automated (computerised), and so in the case of transfer of non-automated data it is necessary to resort to the general regulations governing data protection (Organic Law 15/1999 of 13 December 1999 on the Protection of Personal Data, and its regulations). Moreover, the legal provision only refers to occasions when access or transfer occurs through seizure or remote access without consent (by an unknown individual);
- Due to the above, the access system is individualised, depending on the medium, and used in specific circumstances (with the exception of access occurring in the framework of communications interception). This could be construed as meaning that measures such as data monitoring in real time or at programmed intervals, which are highly useful in relation to bank data, for example, are dispensed with.

**IV. Lack of Data Subjects’ Rights**

While everything stated thus far remains relevant, the part where the disregard or outright non-application of the right to protection of personal data is most apparent is that concerning the absence of provisions relating to data subjects’ rights regarding the information collected and its retention. For example, the regulation governing communications interception devotes one precept to access by the parties to the recordings and by persons participating in the intercepted communications (Article 588.1 of the CPL) and another one to safeguards concerning the storage or retention of the intercept material (Article 588.2 of the CPL). On the other hand, in the remaining measures, only partial, non-systematic attention is paid to aspects linked with the protection of personal data once the measure has been adopted. The use of information obtained in a different proceeding, coincidental discoveries (Article 588.2 of the CPL with reference to Article 579.2) and the destruction of records (Article 588.2 of the CPL) is regulated in the provisions that are common to all technology-related investigation measures (Chapter IV). These provisions are applicable to all measures, but when we examine the specific regulation of each of them, it can be seen

---

12 Regarding this distinction, see J J González López, *Los datos de tráfico de las comunicaciones electrónicas en el proceso penal* (La Ley 2007), 293 et seq. Referring to the LCD (Data Retention Law) whose constitutionality has not, with specific exceptions, been placed in doubt, despite the European Union Court of Justice (Grand Chamber) Judgment of 8 April 2014.

13 ‘Judicial authorisation is necessary in order for electronic communications or public communications network service providers to transfer the data generated or processed for that purpose. That is why the Office of the Public Prosecutor will require such authorisation in order to obtain from the operators the retained data specified in art. 3 of Law 25/2007 of 18 October.’

14 Eg, the Supreme Court (Criminal Division) Judgment of 18 March 2010.

that the exercise of rights by the owners of the information is totally absent. The need to establish conditions of authenticity is only set out in some of them, this being entrusted to the judicial authority in the case of searches involving mass data storage devices (Article 588.sexies.a). Therefore, the regulation is biased and inadequate with respect to this issue which is, moreover, worsened by the provisions for emergency cases.

V. Data Retention Order

Organic Law 13/2015 introduces the ‘expedited data preservation order’ (Article 588.octies). This is a proportionate provision, in line with the corresponding provisions of the Convention on Cybercrime, which is a generic preservation measure. It is designed for use with any data or types of information and is afflicated with the limitation mentioned earlier, as it is restricted to the computer systems environment: ‘specific data or information included in a computer storage system’. As provided for by the very precept that refers to it, this measure is designed to be a safeguard that precedes the obtaining of the judicial authorisation necessary for access or transfer. It so happens, however, that the omission of a comprehensive regulation on data transfer prevents the establishment of a clear, direct relationship between the expedited preservation of these data and their subsequent transfer. As already stated, this is only provided for in respect to data linked with electronic communications or as access linked to confiscation. The preservation measure is linked to the CPL only through provisions regulating the transfer of data related to the IP address or the identification of the owner or connectivity terminal or device. That is because it makes no sense for a preservation order (which, because of its compulsory nature, presupposes the risk of failure to cooperate) to be served prior to confiscation, apart from the fact that it is incompatible with the clandestine nature of remote access. In all other cases, the adoption of this measure would have to be integrated into the general regulations regarding protection of personal data, with the inevitable shortcomings in criminal matters that have become apparent.16

The scope of application of the order of retention having been determined, it must be noted that, as a safeguarding measure prior to judicial authorisation, preservation is subject to the broad powers the judicial police are acknowledged to hold for accessing information in cases of emergency. Such powers are not provided for in the regulation of communications interception (including access to traffic or subscriber data) probably because of an inappropriate influence of the right to the secrecy of communications which does not allow exceptions to judicial authorisation. Neither are they found in the regulation governing the obtaining and recording of direct oral communications (because of the serious nature attributed to this interference). However, they are present in the regulation of the use of technical monitoring devices or resources, all of which is perfectly logical and legitimate. In addition, and this is more reprehensible, there is a proviso on searching of mass data storage devices (Article 588.sexies.c.4 of the CPL) that is in line with Constitutional Court Judgment 173/2011 which allows it. Regrettfully, the proviso lacks any justification given the possibility of retaining the data with full guarantees of integrity until the pertinent judicial authorisation is obtained.17

---

16 Regarding the need for a general regulation, see J Pérez Gil and J J González López, ‘Cesión de datos personales para la investigación penal: Una propuesta para su inmediata inclusión en la Ley de Enjuiciamiento Criminal’ (13 May 2010) 7401 Diario La Ley 1-14.