REMOTE SEARCH OF COMPUTERS UNDER THE NEW SPANISH LAW OF 2015. HAS IT GOT THE RIGHT BALANCE?

Lorena Bachmaier Winter[1]

1. Introduction

The new forms of crime linked to the use of new technologies soon revealed the inadequacy of regulatory frameworks that had been conceived for traditional or old forms of criminality. Most procedural codes have started introducing the necessary legal amendments to take into account the new technologies and to regulate its use for prosecuting effectively the new forms of crimes, in particular cybercrime. However, inexplicably the Spanish Criminal Procedure Code (*Ley de Enjuiciamiento Criminal*, henceforth LECRIM) for many years stayed away from those needed reforms.

Until 2015, the Spanish system relied on the work done by the courts in defining the scope, requisites and formal guarantees for the search of computers, the interception of electronic communications, and other intrusive measures such as the use of location and tracking devices or the use of IMSI catchers. Spanish courts – in particular the Supreme Court and the Constitutional Court – made a huge effort to interpret the sparse rules on telephone tapping in order to make them applicable also to electronic interceptions and searches. For years, scholars, as well as all actors in the criminal justice system, have voiced repeatedly their concern about the legislator's delay in getting down to the urgent update that the LECRIM needed to cope with the existence of information flows generated by electronic and digital communication systems and to provide public authorities with powerful tools in the criminal investigation. In 2014, the Constitutional Court urged the Spanish legislator to duly regulate the use of new technologies in the criminal investigations, apropos of a case relating to the recording of conversations through a hidden device installed in the inmates' prison cells, which the Court considered unconstitutional because of the lack of sufficient legal provision.

The long-awaited reform was finally carried out by the Organic Law 13/2015 of 5 October, in which the Spanish legislator modified the LECRIM and provided a comprehensive regulation of digital investigative measures[2]. The legal amendments

[1] Professor of Law, Faculty of Law, Complutense University, Madrid.

[2] *Ley Orgánica* 13/2015, of 5 October, amending the Criminal Code of Procedure (*Ley de Enjuiciamiento Criminal*, LECRIM) on the strengthening of procedural safeguards and regulating technological investigative measures. Generally on the content of this law, however without analysing specifically the remote search of computers, see F. Bueno de Mata, „Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica", *La Ley*, No 8627, 19 October 2015; C. Jiménez Segado and M. Puchol Aiguabella, "Las medidas de investigación tecnológica limitativas de los derechos a la intimidad, la imagen, el secreto de las comunicaciones y la protección datos", La Ley, No 8676, 7 January 2016, pp. 1-10; J. García San Martín, „Consideraciones en torno al Anteproyecto de Ley Orgánica de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal, el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas", *La Ley,* No 8468, 28 January 2015.
J. Delgado Martín, Investigación del entorno virtual: el registro de dispositivos digitales tras la reforma por LO 13/2015, *La Ley*, No 8693, 2 February 2016, pp. 1-14; M. Richard González, "Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización", *La Ley*, No 8808, 21 July 2016, pp.1-15;

encompass many different investigative measures: interception of communications (telephone, digital, direct); access to stored data (content, traffic and related data); extended searches of network computers; on line undercover operations; the use of electronic tracking devices; the clandestine recording of images in public and private spaces; and the remote search of computers. In addition to these measures, the new rules provide a legal framework for data protection, the service providers' obligation to cooperate with public authorities, the obligation to disclose information, and the protection of third parties that might be affected by these investigative measures.

The scope of this reform is therefore quite far-reaching. For this reason, I will not undertake in this paper a comprehensive analysis of all the investigative measures regulated in the new law. I will focus on a particularly challenging type of problems posed by the remote search of computers. But first it is probably helpful to clarify some basic concepts.

The remote access to computers is a measure that can be performed mainly in two different manners: 1) by accessing network computer data when such data are accessible from a computer that has been found during a physical search or by other means; and 2) by clandestine access to data stored in computers which are not physically accessible or located, through the use of a specific software or spyware. The first measure is usually called *extended network search*, and the second *remote search of computers*. In addition, the remote search of a computer with the help of forensic tools can be extended also to other computers that are accessible from the hacked computer. In all cases the access is remote, and can be clandestine, but as the scope, requirements and methods are different, it is necessary to distinguish the two ways of accessing to data stored in computers.

In this paper I will deal only with the access to computers by way of installing spyware. The extended search either derives from a physical search or from a remote search, and hence it is linked to those measures.

I shall first address the provisions of the search of computers and will then comment on the regulation of the remote search of computers with the help of specific software. The main question I will address is if this legislative reform has succeeded in providing an adequate legal framework for the use of this very intrusive investigative measure, and if it has struck the right balance between, on the one hand, the public interest in prosecuting crimes committed through the use of information and communications technologies (henceforth ICTs), and on the other hand, the respect for the citizens' right to privacy. It will be argued that the criteria applied until now for assessing the proportionality and need of searches regarding tangible things, might have to be revisited in the case of searches of computers.

2. Search of computers

Until the Organic Law 13/2005 was enacted there was no specific regulation in Spain for the search and seizure of data stored in computers, although this measure was widely used in practice under the general rules on search and seizure of documents and objects (arts. 573-578 LECRIM) and on telephone interceptions (art. 579 LCRIM). That could be done because, certainly, traditional search and search of intangible data share some common characteristics: the seizure is done during the search and the requirements for obtaining access are almost the same, as for example, the presence of a certain degree of suspicion[3]. However, the seizure of intangible data requires specific provisions, for it presents particular features: it involves the seizure of the hardware where the data are stored or copying those data. As a consequence a strict protocol has to be followed to ensure the

[3] See Explanatory Report of the Cybercrime Convention, para. 186.

authenticity of the data, that they will not be subject to manipulation, and that they will later be accessible during the investigation and trial.

The lengthy new articles 588 sexies (a), 588 sexies (b), and 588 sexies (c) LECRIM provide a complete regulation of this measure, specifying all the requisites for its legitimate use. It has to be noted that these articles on „electronic investigative measures" do not establish generally different conditions, duration or formal requirements for real-time communications and for access to stored communications. Thus, the rules applicable to the interception of content data of communications are applicable *mutatis mutandis* to the access to stored electronic data. The new law seems to consider the stored communication data as communications and not as documents. However, the regulation is unclear, because, when regulating the access to stored electronic data in computers or other electronic devices, it does not distinguish between ordinary files and stored communications. Consequently, as legal provisions on the search of computers refer to the access to data, a term that is understood as encompassing documents as well as stored communications, both are ultimately subject to the same requirements.

The access to data stored in computers that are located physically in a closed space (home, office, or any other closed space which complies with the extended notion of home), will need a judicial authorization for entry into those places.

Entry and search of premises are extensively regulated in the LECRIM[4]. Although entry is an action conceptually different from search, both are regulated and studied together as an entry usually is authorized in order to accomplish a search and collect objects that may help the investigation or serve as evidence. The LECRIM mentions which spaces must be considered „home" or private spaces and which others are to be qualified as „public" premises for the performance of the entry and search. Nevertheless, those definitions date back to 1882 and have to be reinterpreted in the light of the case law of the Spanish Constitutional Court and the Court of Strasbourg. For the purpose of entry and search the notion of „home" has to be understood in a broad sense in order to protect its inviolability. Any closed space used as dwelling, be it on a temporary or a permanent basis, as well as spaces utilized as professional rooms fall under the meaning of „home" in the context of privacy protection.

The new rules of 2015 introduce an additional safeguard in this regard: the judicial warrant authorizing the entry, search and seizure does not cover the searching of computers. Without a specific authorization, the law enforcement officers carrying out the entry and search will be allowed to seize the computer but not to access the data stored in it. The new regulation makes clear that the search of a computer requires a specific motivation and is not covered by the general search and seizure warrant. Article 588 sexies (a) LECRIM reads:

Need for specific motivation

1. When it is foreseeable that during a domicile search the apprehension of computers, telephone or electronic communications instruments, mass storage digital information devices, or the access to electronic data repositories will take place, the judicial warrant authorizing the search of dwellings shall extend its reasoning to express the reasons, if any, that authorize the agents to access the information contained in such devices.

2. The simple seizure of any of the devices mentioned in the preceding paragraph, carried out during the home search, does not authorize to access to its content, notwithstanding the possibility that such access could be authorized later by the judge[5].

[4] The rules on entry and search (arts. 545 to 572 LECRIM) have not been modified by the last amendment of the LECRIM.

[5] Author's translation. Unless otherwise indicated, all translations are the author's responsibility.

Only in case of urgent need and provided that there is a legitimate constitutional interest at stake, the police would be allowed to access the stored data, even if the search warrant does not cover specifically the search of computers (art. 588 sexies (c) (4) LECRIM).

Judicial warrants must specify the grounds that justify the search of a computer also when the computer or electronic device has been seized separately from a home seizure; again, an authorization to seize a computer does not allow searching the data stored in it[6].

In practice law enforcement agents, if they foresee that the access to data stored in computers will be necessary, they will request both measures –the authorization for entry and search and the authorization to access to the computers– from the very beginning, explaining why the search of a computer (if found in the place) is considered necessary. Otherwise, the computer hardware will be seized and brought to the scientific police premises to be examined by the IT specialists once the specific judicial warrant arrives. It must be noted that the 2015 law contains a specific rule on the seizure of computer equipment: the seizure of hardware should be avoided if it causes grave prejudices to the owner or user. In such cases the officers should seize the data stored in the computer by making a copy of them "under such conditions that the integrity of the data is safeguarded" (art. 588 sexies (c) (2) LECRIM).

3. Remote search of computers

In addition to regulating the search of computers physically located, the Organic Law 13/2015 introduces rules on the remote search of computers. The Council of the European Union had for long time encouraged the member states to regulate this measure[7], but it has not been until October 2015 that Spain finally has attended such claims. In fact, the regulation of the remote search of computers represents a great novelty within the Spanish criminal investigation as such measure was not authorized until now neither through an extensive interpretation of the rules of interception of communications nor on the basis of the rules of search and seizure of documents.

The new art. 588 septies (a) LECRIM reads as follows:

1. The judge may authorize the use of identification data and codes, as well as the installation of a software that allow the electronic remote search, without knowledge of the owner or user, of the contents of a computer, and electronic device, a computer system, or instruments for mass storage of computer data, or databases, for the aim of investigating one of the following offenses:

a) Crimes committed within criminal organizations.

b) Terrorist offenses.

---

[6] Article 588*sexies* (b). *Access to information of electronic devices seized outside the home of the suspect/defendant*.

"The requirement set out in paragraph 1 of the preceding Article shall also apply to cases in which computers, communication instruments or devices of mass data storage, and access to electronic data repositories, are seized independently from a house search. In such cases, officials shall inform the judge of the seizure of such devices. If the judge considers that the access to the information hosted in such devices, he may grant the corresponding authorization."

[7] See Council of the European Union, „Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime", 2987th Justice and Home Affairs Council meeting, 27-28 November 2008, available at http://www.ue2008.fr/webdav/site/PFUE/shared/import/ 1127 JAI/Conclusions/JHA Council conclusionsCybercrime EN.pdf

c) Crimes committed against minors or persons with legal incapacity judicially declared.
d) Crimes against the Constitution, treason and related to national defence.
e) Crimes committed through computer tools or other information technology or telecommunications or communication service.

2. The court order authorizing the remote search shall specify:
a) the computers, the electronic devices, the computer systems or part of them, the data storage media or databases to be searched, and the data or other digital content targeted by the measure.
b) The scope of it, the way in which the access and the seizure of data or computer files relevant to the case will be done, and the software by which the access and control of the information will be done.
c) The officers authorized to execute the measure.
d) The authorization, if any, for making and retaining copies of the computer data.
e) The precise measures to preserve the integrity of the stored data as well as the measures for ensuring the inaccessibility or deletion of such data from the computer system that has been accessed.

3. When the officers who conduct the remote search have reasons to believe that the data sought are stored in another computer system or part of it, they will inform the judge about this matter, who may authorize an extension of the conditions of the search."

The use of spyware to access remotely to computers is a measure that is still highly controversial, due to its intrusiveness in the privacy of the individuals[8]. Differently from the search of premises and the direct search of a computer, in the remote search of computers the suspect remains unaware of the access to his/her data[9]. The clandestine access obviously offers the law enforcement agents a very powerful tool to investigate the data stored in the computer, but at the same time, increases the encroachment upon the privacy.

Together with France, Spain is one of the few countries in the European Union explicitly permits and regulates the remote search of computers by way of using spyware as a criminal investigative measure. Following the data provided in the research study of the Max Planck Institute on interception of communications in the European Union[10] in Germany[11], Czech Republic, the use of remote forensic software is not clearly addressed in the criminal procedural law, which poses a question whether in the absence of explicit provisions the use of special tools for remote data capture is permissible. In Belgium, Netherlands and Sweden the use of remote surveillance is possible, but requires physical installation and can't be planted into a computer system remotely. In The United Kingdom

[8] An interesting analysis on the rights affected through on-line searches, was carried out by the German Constitutional Court in its judgment of 27 February 2008, available under http://www.bundesverfassungsgericht.de,1 BvR 370/07,1 BvR 595/07. On this judgment see, among others T. Böckenförde, „Auf dem Weg zur elektronischen Privatsphäre", *Juristenzeitung,* 19/2008, pp. 925-939.

[9] See, for example, W. Abel, „Agents, Trojans and tags: The next generation of investigators", 23 *Intenational Rev. of Law Computers & Technology,* vol.23 (March) 2009, pp. 99-108, p. 103.

[10] Study on „International Legal Cooperation in the Interception of Telecommunications", called INTLI report. I want to express my gratitude to the drafters of this report, Prof. Sieber, Mr Von zur Mühlen and Dr Tropina for sharing some of the results on remote search of computers.

[11] See, among others, T. Böckenförde (2009), pp. 933 ff.; F. Braun, „Ozapftis–(Un)Zulässigkeit von Staatstrojanern" *Kommunikation und Recht,* 11/2011, pp.. 681-686.

remote searching is not an entirely new investigation method, although it is not regulated in the criminal procedure rules, but under the police laws[12].

In the next paragraph I will analyse this article and the general requirements for granting the remote access to data stored in computers. Compliance with all the requirements has to be assessed by the competent judicial authority and have to be set out clearly in the warrant.

3.1. Specificity and degree of suspicion

In the Spanish system, law enforcement agents cannot resort to measures that restrict fundamental rights for preventive or intelligence purposes[13]. The use of electronic investigative measures in a proactive setting is prohibited expressly by art. 588 bis (a) (2) LECRIM[14]. The new measure of remote search of computers may be carried out only within the criminal procedure and with prior judicial authorization. This implies recognizing that every investigative measure that may encroach fundamental rights should be adopted in accordance with the principle of specificity, which means that the requested measure is needed for the investigation of a particular offense. Such was the dictum of the Constitutional Court in its judgment 253/2006 of 11 September: investigative measures that restrict the right to privacy (in that case interception of communications) are valid only if authorized on the basis of precise objective indications of a crime and not mere subjective hypothesis or general suspicions. This seeks to prevent a general investigation or *inquistio generalis* on the citizens. Naturally, determining which is the required level of specificity is linked to the degree of suspicion that justifies granting a concrete measure, which will be analysed next.

Mere suspicion, conjectures or guesses are not enough to grant the search of a computer, and even less the remote search of it. Neither Spanish scholars nor case law clearly differentiate between "reasonable suspicion" and "probable cause" in order to qualify the degree of suspicion[15]. Both the courts and the new legislation use the term "sufficient objective indications of the existence of the criminal offence", but it is not easy

[12] See W. Abel (2009), p. 101, who states that „the method was quietly adopted in the UK when the relevant technology to remotely access computers became available and, according to the Association of Chief Police Officers, British police have been carrying out remote searches in the past and stated that 194 remote hacking operations were undertaken in 2007-2008." Even if it was used before, a complete regulation as a police investigative measure is introduced by RIPA in 2000 (Regulation of Investigatory Powers Act). See also S.W. Brenner, „Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force", 81-5 *Mississippi Law Journal* (2011-2012), pp. 1229-1261, p.1236.

[13] On the contrary, Germany has regulated the remote search of computers in the preventive sphere, both for intelligence (*Verfassungsschutz*) as well as for law enforcement preventive purposes (*Polizeirecht*), but up to now not as an investigative measure within the criminal code of procedure. See T. Böckenförde (2009), p. 932-933.

[14] Art. 588 bis (a) (2) LECRIM: „The principle of specificity requires that the electronic investigative measure is related to the investigation of a specific criminal offence. No electronic investigative measures shall be authorized which are aimed at preventing or discovering crimes or to confirm suspicions that do not have an objective basis."

[15] The requirement of probable cause in the US Fourth Amendment is related to the likelihood of finding evidence. When applying for a search warrant officers have to demonstrate probable cause that they will find evidence of a crime, and they must describe that evidence with particularity. Of course particularity links the probable cause to a specific crime, but the probable cause is directly referred to the evidence, not to the probability that a crime has been committed, as in the Spanish system.

to establish what this will mean in practice[16]. Often it has been interpreted as referring to „facts that rationally – in an objective assessment – indicate the probability that some person is involved in a criminal act"[17]. The Supreme Court has repeatedly held that „the mere affirmation of the police about the existence of certain suspicions is not enough to order the interception of the communications"[18]. And the Constitutional Court has stated that „the relationship between the person under investigation and the crime committed has to be supported by objective data: these data shall be susceptible to be assessed by third persons, and thus cannot be only based on subjective conclusions or a hunch; secondly, they have to be based on facts that allow to infer that a crime has been committed or will be committed, but they may not involve judgments about the person. These suspicions must be based on factual evidence or indications that suggest that someone attempts to commit, is committing or has committed a serious crime"[19].

This means, that the request for a remote search of computers needs to refer to precise facts and explain the origins of the information that underpins the objective suspicions. Such elements showing probable cause have to be substantiated in the judicial warrant that authorizes the remote search of a computer. Anonymous information or information coming from a confidential source has usually been considered not enough to justify intrusive investigative measures.

Some recent judgment of the Supreme Court has raised the issue of whether information obtained from cooperation with foreign law enforcement or intelligence services may be sufficient to conclude the existence of the degree of suspicion necessary to authorize investigative measures restricting the fundamental right to privacy. The case involved the telecommunications interception and confiscation of a significant amount of drugs based on information provided by the US Drugs Enforcement Agency (DEA). The defence lawyer contended that the telecommunications interceptions were illegal, as the initial suspicion was not established by lawful means. The Supreme Court held that it cannot be presumed that the sources of information of the police are unlawful, and that in those concrete circumstances there were no indications that the information came from an illegal interception of communications (STS 884/2012, of 8 November, RJ 2012/11360).

In practice for obtaining a judicial order authorizing the remote search of computer, the police will need to undertake other previous surveillance activities in order to gather enough information to meet the standards of „probable cause". As the measure of remote search of computers is new, there is still no case law showing how the courts have evaluated the requirement of probable cause with regard to it. However, it is to be expected that the courts will use standards similar to those applied to the interception of telephone conversations.

[16] Although in theory „probable cause" entails a higher probability than mere „reasonable suspicion" and the latter is lower than „justified grounds", in practice tracing a difference between these different degrees on the probability of finding evidence is difficult.

[17] SSTC 171/1999, of 27 September, FJ 8; 299/2000, of 11 December, FJ 4; 14/2001, of 29 January, FJ 5; 138/2001, of 18 June, FJ 3; y 202/2001, of 15 October, FJ 4, all of them regarding interception of communications.

[18] Supreme Court Decision of 18 June 1992, which is one of the landmark decisions defining the requirements for the interception of communications.

[19] STC 253/2006 of 11 September, quoting also judgments of the European Court of Human Rights, precisely *Klass and others v Germany*, of 6 September 1978, Appl. Nº 5029/71 and *Lüdi v Switzerland* of 15 June 1992, Appl. Nº 12433/86.

3.2. **Whose computer can be remotely accessed and searched?**

Under the general rules applicable to all electronic investigative measures, the law provides that the measures affecting third persons can be adopted "in the cases and under the conditions provided in the specific rules regulating each of those measures" (art. 588 bis (h) LECRIM). This provision does not shed light on the question of whose computer can be accessed because under the article regulating the remote search of computers nothing is said about it. The main issue is whether it is possible to authorize access only to the computer owned by the suspect or the measure can be granted for searching any computer that is possibly being used by the suspect. And there is a further question: may the remote search of a third party's computer be granted, when that computer is not used by the suspect but there are indications that it might contain relevant information for the investigation of the crime?

In this respect, art. 588 bis (h). LECRIM foresees the possibility to grant investigative measures intercepting communications that affect third persons, in the cases and under the conditions set out in the regulation of each of the interceptions. With regard to the interception of telecommunications, art. 588 ter (c) LECRIM states:

„The interception of communications originating from terminals or electronic communication means belonging to a third person may be authorized, provided that:

1. there is evidence that the suspect or defendant under investigation that uses them to transmit or receive information, or

2. the subscriber collaborate with the investigated person in their illicit acts or benefits from its activities.

Such interceptions of communication may also be authorized when the device which is the object of the surveillance is being used maliciously and electronically (*por vía telemática*) by others without the knowledge of its owner."

Would this provision also apply to the remote search of computers? As far as the remote search implicitly affects the interception of communications, the rule mentioned above would be applicable *mutatis mutandis*. However, the 2105 law should have clarified it, because the requisites set out for the interception of communications of third persons (evidence that the suspect uses the terminal for receiving or sending communications) may not be applicable to the remote search of a computer: in case of accessing the computer it might not necessarily be relevant if the suspect uses the computer for sending or receiving communications, but what is relevant is that the suspect stores relevant data in that computer.

3.3. **Predicate offences**

As indicated above, the offences for which the remote search of computers might be authorized are listed under art. 588 septies (a) (1) LECRIM: organized crime, terrorism, offences against minors o incapable persons, against the Constitution and „those committed by means of a computer technology or any other communication of information technology".

This list of predicate offences listed in the Spanish law aims to comply with the obligations assumed when ratifying the Council of Europe Cybercrime Convention[20]. According to art. 14 of the Budapest Convention, the states shall adopt legislative measures

[20] Council of Europe Convention on Cybercrime, Budapest 23 November 2001, ETS-185, known also as the „Budapest Convention". Spain ratified the Convention on 3d of June 2010 entering into force the 1st October same year.

„as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings" (art. 14 (1) of the Convention), and this obligation encompasses the criminal offences established under articles 2 through 11 of the Convention and "other criminal offences committed by means of computer systems" (art. 14 (2) (a) and (b) of the Convention). In compliance with such obligations, Spain has regulated the investigative measures that are considered needed to prosecute serious offences and also those crimes committed by means of computer technology. Some of these measures are access to traffic data, interception of communications (traffic and content), and access to stored computer data.

However, the Budapest Convention allows states to make a reservation to their obligations under the Convention, precisely regarding Articles 20 and 21: real time access to traffic and content data. According to the Convention collection of real time traffic data applies in principle to any criminal offence, but art. 21 of the Convention specifically provides that Parties are only required to establish the measure of real time access to content data in relation to "a range of serious offences to be determined by domestic law". However, the Explanatory Report of the Convention underlines that states should consider regulating both measures – real time interception of traffic and content data – in order to provide effective means for the investigation of the computer offences and computer-related offences specified in the Convention. In short, the Convention leaves the scope of the collection of real time content data to be determined by domestic law and allows states to limit this measure only for grave crimes, but at the same time it encourages the states to make it available for any computer-related offences that otherwise could not be discovered without such measures[21].

The question that now arises is if the measure provided under art. 588 septies (a) on remote search of computers encompasses only the search of stored data. The problem is that the access to stored data can also imply accessing to communications, precisely stored communications. Does the remote access to computers entail the possibility through certain software to intercept real time communications? The Spanish law mentions the „examination of the content of a computer remotely and without knowledge of the owner or user". This appears to mean that real time interception of communications is not covered. But for e-mail communications such distinction does not make much sense, because, once they are sent or received, they are stored and –if not completely deleted – they will be accessed in the computer. Following literally the Spanish law, stored e-mails are part of the „content" of the computer.

What I am trying to explain is that, as long as the Spanish law does not make any distinction between data regarding stored communications and other data, the question that arises is whether the rules on interception of communications should also apply here or not.

In theory it could be affirmed that stored communications are like other documents found during a search, and we could make here an analogy with paper letters received. However, as long as the remote access to a computer can last for a month, communications may continue entering and being intercepted. In real terms, the duration of the measure brings it closer to an interception of telephone conversations and thus it would not be unreasonable to apply those rules to the remote search of computers. However, even if there is a dataflow for introducing the spyware, the dataflow is not the target of the measure, and thus the remote access to a computer with remote forensic tools cannot be defined in analogy with a telephone interception.

[21] See Explanatory Report paras. 211-214.

This discussion does not have a merely conceptual interest, for it may affect to the scope of the predicate offences for which the remote access of computers can be granted.

The issue is the following. Telecommunications interceptions can only be ordered in cases of criminal offences punished with a custodial penalty higher than three years, organized crime, terrorism, or offences committed through computer systems. Instead, remote search of computers is only permitted for the crimes specifically listed under art. 588 septies (a), whatever the penalty is. Thus, for example, in an investigation related to a crime against a minor, telephone tapping could only be ordered if the crime is sanctioned with a penalty higher than three years, but the remote access to computer could be granted – if all other conditions are met – even if the penalty is lower.

In my opinion, the intention of Spanish legislator when regulating the remote access to computers with the help of forensic software was not to allow the real time interception of communications. Therefore, even if stored communications are accessible by way of computer searches, and this access is not so different in many cases from real time interceptions (at least I cannot see much difference in the case of written e-mails), the list of predicate offences applicable to the remote search of computers is only the one under art. 588 septies (a), and the threshold of a three-year custodial penalty should in general not apply.

In any event, when it comes to offences committed through computer technology, the Spanish law has not introduced any minimum penalty threshold, either for telecommunications interceptions or for remote access to computers with forensic software. This, as will be discussed below, may raise questions regarding the compliance with the principle of proportionality.

3.4. Principles of adequacy, necessity and proportionality

As for any IT investigative measure, the remote access to computers with the help of forensic software requires to comply with the principles of adequacy, necessity and proportionality. These requirements are not new and there is abundant case law both of domestic courts as well as of the ECtHR related to them. The only novelty here is that the law now mentions specifically these requirements and that it has tried also to give some definition and guidelines for their interpretation. Necessity requires that the same data are not reasonably accessible by less intrusive means and that without those data the criminal investigation would be seriously hampered (art. 588 bis (a) (4) (a) and (b) LECRIM). Adequacy refers to the relationship between the evidence sought and the investigative means employed, if through such means the expected or needed evidence might be obtained.

When it comes to the strict proportionality requirement – importance of prosecuting a crime vis-à-vis the importance of respecting a fundamental right – the Spanish law, when defining the general principles for granting the newly regulated electronic investigative measures, expressly indicates the elements that the judge shall take into account to assess the proportionality of any measure. Art. 588 bis (a) (5) states that the investigative measure shall only be considered as proportionate if all of the following circumstances have been considered: the seriousness of the offence to be investigated, its social significance, or the fact that it has been committed through computer systems („within the digital environment", in the literal terms of the law), the degree of suspicion and the relevance of the results to be obtained in comparison with the gravity of the encroachment of the fundamental rights. The fact that the crime has been committed through the use of computer technology does not justify automatically the adoption of the remote search of computers but opens the possibility to authorize it, even if the crime is not considered grave from the

point of view of the punishment. If the measure is needed, because other means will not allow investigating the offence –due to its digital nature, the measure could be granted. As we will mention below, this approach complies with the principles set out in the Budapest Convention but also leaves a door open to abusive use of these measures.

3.5. **Duration**

The general rule is that any measure restrictive of fundamental rights shall not last longer than it is indispensable for the discovery of the facts (Art. 588 bis (e) (1) LECRIM). The remote search of computers can only be authorized for one month, with a maximum extension up to three months (Art. 588 septies (c) LECRIM). It has to be noted that the duration of this measure is much shorter than it is provided for other IT investigative measures, which can be authorized usually for three months, extendable for equal terms up to a maximum of eighteen months (Art. 588 ter (g) LECRIM).

The investigating judge can authorize the extension of the investigative measure if the reasons that justified its adoption remain. To that end the investigating judge has to check what has been the information obtained and if the need, adequacy and proportionality of the measure still exist. The extension can be authorized either *ex officio* or upon application of the public prosecutor or the judicial police.

The request for prolongation shall be filed with enough time before the term for which it was authorized expires. The application for extension shall be accompanied by: a detailed report on the execution of the measure and its results and the reasons that may justify the need for extension. The judge shall decide on this application within two days (Art. 588 bis (f) LECRIM).

If the time for which the authorization expires and the time extension has not been granted, the measure will cease (Art. 588 bis (e) (3) LECRIM). Any evidence obtained after expiry of the date is unlawful and will not have any evidentiary value, even if there was no abuse on the part of the authorities.

The whole process of execution of the measure is subject to judicial control. The judicial police shall inform about the progress of the investigation within the time periods established in the judicial warrant authorizing the remote search of the computer (Art. 588 bis (g) LECRIM). To that end, it is assumed that the judge may request the integral data seized. As a consequence of this periodical control, the investigating judge may revoke the initial authorization, even if the maximum time period has not lapsed.

The investigative measure will cease once the conditions that led to its adoption disappear or it is made clear that no results are to be obtained through it; and in any event once the timeframe has expired (Art. 588 bis (j) LECRIM).

Al the rules on the duration of the remote search of computers resemble very much those already in place for telephone tapping, with the only difference of reducing the ordinary time frame from three months to one, and also the possible extension. However, is this reasonable? If this measure is aimed to access and collect (copy) data that are stored in a computer, once the spyware is successfully installed in the computer to be searched the data can be copied in a very short time. Once this occurs the measure should ceased, because it has accomplished its aim. This should require the law enforcement agents to disable the spyware[22].

On the other hand, it may take some time until the forensic tool is operative and the data can be accessed, and this can last longer than one month or even three months if the

[22] In this sense also S.W. Brenner, „Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force", 81-5 *Mississippi Law Journal* (2011-2012), p. 1245.

suspect never opens the file that allows the spyware to enter into that computer system. Once the three months since the warrant was issued have lapsed, does it become ineffective, even if the authorized measure could never be executed? These issues need to be clarified.

3.6. **Requirements for the application**

The competent authorities that can apply for a remote search of computers are the he public prosecutor and the judicial police, but the investigative measure can also be granted *ex officio* by the investigating judge (art. 558 bis (b) (1) LECRIM). According to art. 588 bis (b) (2) LECRIM, any request for an IT investigative measure shall contain:

1. The description of the facts under investigation and the identity of the subject or otherwise affected person by the measure, provided that such data are known.
2. The detailed statement of the reasons justifying the necessity of the measure according to the guiding principles set out in Article 588 bis, as well as indications of the offence that have been found during the investigation prior to the application for authorization for the restrictive measure.
3. Identification data of the suspect or defendant under investigation and, if appropriate, of the means of communication used by him that will allow the execution of the measure.
4. The extension of the measure specifying its content.
5. The investigative unit of the judicial police who will take over the interception.
6. The form of execution of the measure.
7. The duration of the measure sought.
8. The precise person obliged to execute the measure, if known.

3.7. *The judicial warrant*

As mentioned above, the remote search of computers, as any other investigative measure that entails encroachment of a fundamental right, requires in Spain judicial authorization[23]. The competence to issue the judicial warrant lies with the investigating judge (arts. 588*bis* (b) and 588*bis* (c) LECRIM). The fact that these measures can be granted *ex officio* by the same investigating judge does not seem to be completely adequate from a theoretical point of view, for the same judge who is seeking for the truth in the criminal case will end up being also the one who shall ensure that the conditions for restricting human rights within such investigation are met. However, as weird as it may sound, in practice this has not caused major problems due to the strictly independent position of the investigating judge and the continuous supervision exercised by the public prosecutor upon all the pre-trial stage.

It is unclear if in cases of urgency the Ministry of Interior can provisionally authorize the remote search of computers with the help of forensic software. Under the rules regulating the interception of communications, the Minister of Interior (or, in his/her absence, the Secretary of State for Security, who is the next in the hierarchical line) can exceptionally order the interception in urgent cases, in the context of the investigation of

[23] Differently in the UK, where the remote search of computers can be authorized by a senior law enforcement officer according to RIPA for preventing or investigating serious crimes (criminal offences sanctioned with a custodial penalty higher than 3 years). See W. Abel (2009), p. 104.

offences related to organised groups or terrorism and provided that there are reasonable facts that indicate that the measure is indispensable[24].

However, this exception is not mentioned by the 2015 law when dealing with the general requirements for all technological investigative measures (arts. 588 bis (a) to 588 bis (k) LECRIM). Neither is it foreseen under the specific rule on remote access to computers (art. 588 septies (a) LECRIM), although it is provided for the extended search of computers. In fact, according to art. 588 sexies (c) (3) and (4), additional judicial authorization shall be sought to perform an extended search of computer networks that are accessible from the equipment for which the warrant was originally issued. However, in urgent cases the police or the public prosecutor doing the initial search of computers can also carry out the extended search, but they must notify the judge within the next twenty-four hours. After examining the reasons given for such extended search, the judge shall confirm or reject its validity.

On the contrary, art. 588 septies (a) LECRIM contains no similar provision on the remote search of computers. Should this be interpreted as a lacuna of the law, in order to accept that a subsidiary application of the provisions on extended searches is possible? Or should we understand that when the legislator did not purposely include an ad hoc provision for the remote search of computers it was with the aim of eliminating the possibility of doing it without a *previous* judicial authorization?

The law is unclear at this point. I am personally in favour of a restrictive interpretation. Thus, even if the remote search of a computer could be considered as a form of accessing the content of (stored) communications, so that the rules for interception of communications could be applied, my opinion is that it should be only allowed if there is a prior judicial warrant due to the intrusiveness of such measure, which implies – it must be underlined – accessing someone's computer by installing spyware in it. In emergency cases, it should suffice that the law enforcement officers or the public prosecutor apply for an urgent warrant.

The judicial warrant authorizing any IT investigative measure, according to new Art. 588bis (c) LECRIM, shall be rendered within twenty-four hours since the request was filed, and its content is regulated in detail to ensure that the judicial authority has checked the compliance with all substantive and formal requirements[25]. This general rule is to be

[24] In such a case, the adoption of this measure shall be immediately communicated to the competent investigating judge, within a maximum time period of 24 hours, expressing the reasons for its adoption, the acts undertaken, and the results obtained. The judge will confirm or reject the adoption of the measure in a reasoned decision within a maximum time of 72 hours since it was adopted. (art. 588*ter* c. LECRIM).

[25] Art. 588bis (c) (3) LECRIM: The judicial warrant shall at least express:

a) The punishable acts under investigation and their legal qualification, stating the reasonable suspicion to ground the measure.
b) The identity of the suspects/defendants and any other third person affected by the measure, if known.
c) The scope of the restrictive measure, specifying the extension and the compliance with the guiding principles established in Article 588 bis.
d) The judicial police investigative unit that will take over the interception.
e) The duration of the measure.
f) The manner and frequency in which the requesting authority shall inform the judge about the results of the measure.
g) The aims sought by the measure.
h) The person obliged to execute the measure, if known, expressly stating his/her duty to cooperate and to keep the acts secret, where appropriate, being liable for the offence of disobedience of a court order."

complemented with the specific provision provided for the search of computers under art. 588 sexies (c) (1) LECRIM:

The judicial warrant authorizing access to the information contained in the devices this section refers to, shall determine the conditions and scope of the search and may authorize the copying of the computer data found. It shall also determine the conditions necessary to ensure data integrity and preservation guarantees to enable, where appropriate, the examination by an expert for preparing an expert opinion.

The judicial warrant has to show that all requirements for the intrusion into the privacy of a citizen are met. If the warrant is not adequately motivated, the encroachment shall be unlawful, with direct negative consequences for the admissibility of the evidence obtained. The general rules and principles on exclusionary rules of evidence shall apply also to the evidence collected through an unlawful search or interception of communications. Spanish legislation provides for a very strict exclusionary rule. The key statutory provision regarding the exclusion of evidence is art. 11.1 of the 1985 Organic Law of the Judicial Power (*Ley Orgánica del Poder Judicial*, hereinafter LOPJ), which was enacted one year after the Constitutional Court's landmark decision STC 114/184 and clearly influenced by it. Art. 11.1 LOPJ reads: „Evidence obtained, directly or indirectly, in violation of fundamental rights or liberties, shall have no effect."

The doctrine of the indirect or „reflex effects" – fruit of the poisonous tree – determines the exclusion not only of the main evidentiary elements but also of those other elements of evidence that constitute a derivation of the originally illegal act. Spanish courts have followed the doctrine of the „reflex effects" in those cases where not applying it, would result in leaving fundamental rights unprotected. For instance, recordings obtained through illegal phone tapping are not accepted, neither is accepted the testimony of the officer in charge of the recording, for otherwise the meaning and purpose of the exclusionary rules would be dodged and it would encourage the adoption of measures that are contrary to the constitutional right to the confidentiality of communications.

4. Assessing the proportionality of the measure

Not meeting the proportionality test or not justifying the grounds for considering the measure restrictive of a fundamental right in compliance with the proportionality test, will render the investigative measure unconstitutional – and therefore void – for breach of the right to privacy, data protection and the right of the confidentiality of the communications. The proportionality of the measure is one of the essential safeguards for the respecting human rights, and IT investigative measures have to strictly comply with it[26].

In this section I will point out some of the challenges that judges face when assessing the proportionality of the remote search of a computer. There is, first, the problem of how

[26] See the Explanatory Note to the Budapest Convention, para.146: Another safeguard in the convention is that the powers and procedures shall „incorporate the principle of proportionality." Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures. Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle.

to evaluate the necessity of the measure if the law enforcement officers do not know where the data are located. And second, the problem of seizing the digital data that fall within the scope of the judicial warrant. I will mention here also the jurisdiction problems that may arise if the law enforcement officers do not know where the data are located and these are stored in a foreign jurisdiction or in numerous jurisdictions.

1) One of the main difficulties – and responsibilities – for judges when deciding on whether an investigative measure is to be authorized or not, is to determine if such measure is proportionate or not, if the sacrifice in the sphere of the fundamental rights is justified by the aim of prosecuting a crime. In case of very serious crimes, such assessment is much easier, provided that the degree of suspicion is sufficiently shown. There is agreement that for prosecuting transnational organized crime and terrorism, or even crimes against minors and incapable persons, the restriction of the suspect's privacy might be legitimate, even by way of searching his computer with the help of forensic tools. However, when it comes to criminal offences committed through computer technology, the assessment on the proportionality of the measure may represent a difficult challenge, because the damage to society by those crimes may be not so evident. In those cases in which the criminal penalty for such offences remains low, the seriousness of the offence is certainly not a ground to justify the sacrifice of the fundamental right to privacy. Then, why has the legislator opened the possibility to authorize a measure like the "hacking" of a computer by the police for prosecuting crimes that are not even considered as grave crimes?

The answer, as explained also in the Budapest Convention, is to be found in the necessity of the measure: unless these IT investigative measures are not provided, most of the crimes committed through computer technology will remain undiscovered. In order to avoid that the Internet becomes an „outlaw place", citizens will have to take into account that their privacy might be encroached, even for investigating minor crimes. The perils the global citizen is facing might render such approach reasonable, and I cannot object to it. Nevertheless, this approach is not without controversy and proof of this is the preliminary referral to the European Court of Justice filed by the Provincial Court of Tarragona (Spain), asking for guidance on how to interpret the principle of proportionality[27].

However, when the rule on remote access to computers allows this measure to be adopted within the investigation of „offences committed through computer systems", in no way this means that whenever there is suspicion that this type of crime has been committed the remote access to a computer with the help of special software shall be granted. Before taking that decision, the investigating judge shall evaluate all the other elements that would render the measure proportionate. First, the seriousness of the crime, taking into account not only the penalty threshold but also the need for the deterrence effect of enforcing the criminal law, and the damage that such behaviours are causing to society or to the relevant individual. Furthermore, the judicial authority has to carefully scrutinize if such evidence is really relevant for the investigation because there are no other means of evidence. And finally, and most important, if there are no other means less intrusive to the right to privacy that could lead to similar evidentiary elements.

At this point, I would like to return to a question that has been mentioned above: when is the remote search of a computer really necessary? The question is certainly relevant, for the „hacking" of a computer will be proportionate within a criminal

[27] Although the case that causes the preliminary reference is the search of a mobile telephone and the facts occured prior to the entering into force of the Organic Law 13/2015, of 5 October, it shows how preoccupied the judges are when it comes to assesing the proportionality of the IT investigative measures. See http://www.iustel.com/diario_del_derecho/, of 8 April 2016.

investigation only when it is strictly needed, because no other less intrusive means to access the data are available. The assessment in each case of the compliance with this requirement is to be done by the investigating judge, which in some cases will request that other means are tried first and other times will consider that those other means are likely to be unsuccessful. This is one of the points that needs a deep empirical analysis. In practice, the necessity of the remote search should be clearly and specifically explained in the judicial warrant. Judges should check if less intrusive means are really viable or not, and bad practices such as introducing in the warrant general formulary statements as „considering that the data needed for the investigation cannot be acceded through other less intrusive means, etc." should be avoided.

In principle, the remote search of computers should be granted only if the law enforcement agents cannot identify the physical location of the stored data, for only then the remote access would be necessary. When the data are located at a physical address, a traditional search and entry measure with authorization to search the computers seized at that place would suffice. But then another question arises: if the investigating judge, prior to issuing the warrant authorizing the remote search must be satisfied that finding the physical location of the computer was not possible; or if it would it suffice to justify that, although the location was known, the entry and search measure would impede the advancement of the investigation, and therefore a surreptitious search of the computer is needed.

There is still another issue that will need to be addressed in the future practice and relates to the location of the data. If the law enforcement agents present evidence that the data are not accessible through a traditional search of a computer, because the data are stored in the cloud or out of the country, what should the investigating judge decide? Can he authorize an extraterritorial remote search of the computer on the basis that the Spanish law does not expressly prohibit it? Or should the judge reject it, following the principles of the Budapest Convention that provides to ensure the access to stored data „in the territory"?[28] Accessing computers or data stored in another country is an action that raises issues on sovereignty principles and international comity, and should not be taken lightly[29]. The fact that technology allows access those data regardless of territorial borders does not mean that it should be permitted. But in this respect, once again the Spanish legislation is too ambiguous. Perhaps this ambiguity has been sought on purpose awaiting for future international agreements or a regulation at the EU level, as has been already pointed out in the Directive on the European Investigation Order[30]. In the USA, art. 41 (b) of the Federal Rules of Criminal Procedure limits the searches to the district issuing the warrant of the remote search of a computer. However, this is causing problems for in many cases the law enforcement agents applying for the measure do not know where the information to be seized is physically located. A legal amendment of this rule has been requested and is being currently discussed to authorize the remote search of computers also beyond the district where the warrant has been issued[31].

---

[28] See arts. 19, 20 and 21 of the Convention, referring to the own territory of the party. Trans-border access to stored computer data following the Convention is allowed either upon consent of the person who has authority to disclose the data, or without consent when those data are open source or publicly available data regardless where they are geographically stored (art.32 of the Budapest Convention)

[29] See J.L. Goldsmith, „The internet and the legitimacy of the remote cross-border searches", 2001*University Chicago Law Rev.,* pp. 103-118.

[30] See art.31 of the Directive 2014/41/EU of 3 April 2014 regarding the European Investigation Order, OJ 1.5.2014, L 130/1.

[31] See, for example, D.R. Benemann and D.L. Elm, „Extraterritorial Search Warrants. Rule Change.",

On the other hand, if the domestic law of the state where the data are located does not allow foreign authorities to search the computers that are in their territory, the remote search would not comply with the *lex loci*. Which means that, being the measure unlawful in the state of execution, the admissibility of evidence could be questioned. This topic, however, has generated so much debate that it cannot be adequately analysed within the scope of this article.

The above-mentioned aspects are not addressed by the 2015 law and therefore will require a fine assessment by the judges seeking to comply with human rights standards. I must reiterate, however, that the „hacking" of computers is such an intrusive measure that it should be granted only after the investigators have made reasonable efforts to identify the physical location of the computer and the stored data. This could, and probably should, have been set out specifically by the rules on remote access of computers in order to avoid that the general requirement of „absence of less intrusive measures" is not adequately understood – or is manipulated – in practice.

2) Another highly problematic issue arises with regard to the data to be seized during the search of a computer. Art. 588 septies (a) LECRIM states that the judicial authorization shall define the scope of the search and also determine if the data can be copied and how these copies are to be preserved.

In traditional searches of homes or other premises, only those elements of evidence that are related to the crime under investigation can be subject to seizure. The problem with the search of computers lies in the way the data may be stored, where irrelevant data may be kept together with those data that fall within the scope of the search warrant. The retrieval of computer data usually involves transferring all data through a cloned copy of all the files. Once all the data stored in the searched computer have been retrieved and copied, how should the IT law enforcement officers proceed to discriminate between the relevant and irrelevant files? Can they scrutinize all the data in order to select those that fall within the scope of the warrant? Should forensic tools be used also to limit the computer search only to certain types of files or data? Should the law impose the obligation to use these types of targeted search tools?

Starting with the latter question, we must accept that using certain keywords or targeting certain files to limit the scope of the search in the computer can help identify the relevant data. However, they can also cause that important information for the investigation is not be detected. The use of searching tools to limit the seizure of data does not seem adequate for it will not ensure that all the needed data have been retrieved and preserved.

If such tools are not adequate, there should be some way to maintain the privacy of the materials that are mixed with the seizable data. But how to segregate the data that are relevant for the criminal investigation from those falling out of the scope of the judicial warrant? Who should do it?

We must take into account that this type of searches affects not only the rights to privacy, data protection and confidentiality of communications of the computer's owner or user but also the right to privacy of numerous persons completely unrelated to the crime. The Spanish law insists on the compliance with the specificity and the proportionality principles in granting and executing the measure, but it does not say anything about how these principles shall be respected in the remote search of computers. The judicial warrant

29 *Criminal Justice* 2014-2015, pp. 9-12, p. 10.On the problems of remote search of computers within different states of the USA, due to the different scope of the 4th Amendment protection in them, see S. W. Brenner, „Law, Dissonance, and Remote Computer Searches",14 *North Carolina Journal of Law & Technology*, vol. 14-1, 2012-2013, pp. 43-92, pp.60 ff.

shall specify if the law enforcement authorities are authorized to copy and preserve the data and shall also set out the precise measures to be carried out to preserve the integrity of the data. These are general formulae that need to be concretized. The proportionality principle can be infringed at the stage of granting the access as well as at the stage of executing the measure, but regarding to latter nothing is stated in the law. It shall be defined in the judicial warrant, but at the present judges lack of guidelines on how to proceed in this regard.

At the same time, it is important to keep in mind that the volatility of digital data requires adopting quick measures to preserve the data and avoid its destruction. It is logical that, during the execution of the remote search of a computer, the law enforcement officers cannot undertake the task of scrutinizing all the files in order to copy only those that are relevant for the investigation. The data collection process is automated and no human officer will actively decide what data is relevant and, more importantly, is highly sensible private data, such as medical and financial information or documents equivalent to diary entries[32]. All the data will be copied, and the segregation of the data will come later. If we trace an analogy with the proportionality of documents that can be seized within a traditional home or office search, seizing all data would be clearly disproportionate. The judgment of the ECtHR in *Niemietz v Germany* is very illustrative in this regard[33]: the search of the premises of a lawyer, related to the crime investigated, was held in violation of art. 8 of the European Convention of Human Rights, precisely because a disproportionate number of files not linked to the crime and not useful for the criminal investigation were seized during the search. Should this case law be also applicable to remote searches of computers? If we answer in the affirmative, we face the dilemma that either all the computer data could not be copied or all computer searches would be infringing the proportionality principle. Which leads us to conclude that the same criteria for assessing the proportionality of the seizure of tangible data cannot be applied to the digital data.

Having said this, the question remains: how to segregate the relevant from the irrelevant data? How to discriminate data that affect the core area of privacy from those that do not? There are no rules in the 2015 law to that purpose with regard to the remote search of computers. In the case of the interception of communications, Spanish courts have been very strict in requiring law enforcement officers to hand over all the intercepted material to the investigating judge; the police cannot select conversations or communications, and all the communications are to be disclosed and make available to the defence (save those affecting the core element of the intimacy)[34]. If we apply those criteria by analogy, all the data seized during the remote search of a computer must also be transferred to the investigating judge[35]. This entails further practical problems: on the one side the huge

[32] W. Abel (2009), p. 103.

[33] ECtHR *Niemietz v Germany*, of 16 December 1992, Appl. Nº. 13710/88.

[34] Art. 588*ter* (i) LECRIM, now provides that those conversations affecting to the intimacy of the parties, those parts will not be made available to the parties to the proceedings. The parties have to be informed that such parts have been excluded from the copies of the communications they have obtained. It is unclear how this provision will be interpreted and applied. It is to be welcomed that the LECRIM has introduced this rule to better protect the core of the right to intimacy of the persons whose communications have been intercepted, however it will have to be balanced if those communications affecting the intimacy are relevant as evidence or not. There is no exclusionary rule of evidence based on the protection of the core content of the right to privacy (or intimacy).

[35] The German courts have also stated that the selection of data has to be done by a judicial authority – encompassing this concept also the public prosecutor and a judicial officer –, but not the police.

workload that this causes, for the amount of data might be enormous; and second, the possible lack of experience of the judicial authorities to carry out such duties, for they may also need the use of complex software.

One of the difficulties of this matter is that electronic storage devices contain so much information about the life of a person that retrieving and preserving those data through a comprehensive copy clearly goes beyond the scope of the investigation of a particular crime. It would amount to an *inquisitio generalis* upon the person under investigation. Giving so much power to the state is something that every democratic system should avoid. And still, how to avoid it? Without the aim of proposing conclusive solutions I can think of two ways. One would be to appoint an independent authority to segregate the data retrieved and exclude from the investigation those that fall out of the scope of the judicial warrant. The other would consist in limiting the use of such materials as evidence in other criminal investigations or, in other words, in restricting the possibility of using accidental findings of evidence related to other crimes. However, none of these approaches seems to have been followed by the Spanish law.

If we focus on the question of accidental discoveries – data collected by chance during the interception of the communications, relating to another criminal offence different from the one for which the judicial warrant was issued – until the Law 13/2015 there was no specific rule in the LECRIM. The courts, however, had developed a set of principles to be applied to accidental discoveries, mainly within the realm of the execution of home searches, but also with regard to telephone interceptions. The new rule on accidental discoveries only states that those elements can be used to trigger another criminal investigation upon judicial authorization, only once the investigating judge has checked how the evidence was collected and has assessed the circumstances of such accidental finding (art. 588 bis (i) referring to art. 579 bis LECRIM). But no further details as to their evidentiary value are provided.

In sum, in my view, by simply ignoring the above-mentioned problems the law has failed to ensure compliance with human rights standards and with the proportionality principle when regulating the remote access to computers with the aid of forensic tools.

5. Concluding remarks

The encroachment by the state on the right to privacy through the search of a computer needs to be subject to clear and principled controls. These controls must be even stricter when this measure is carried out in a clandestine way, by using forensic malware to provide remote access to data stored in a computer. Although this measure may be necessary for investigating certain types of crimes, it should not be authorized as a general law enforcement measure. On the contrary, it should be granted only in very exceptional circumstances, if there is a stringent necessity and all the elements to assess the proportionality of such intrusive measure have been adequately taken into account by the judicial authority.

The regulation of the IT investigative measures in the Spanish law of October 2015 is to be welcomed, as Spanish authorities until now were acting in most cases at the edge of legality, precisely because of lack of specific legal provisions. Providing a complete regulation of the IT investigative measures not only promotes the efficiency in fighting grave crimes but also strengthens the legal security.

With regard to the remote access and search of computers with the help of forensic tools, the Spanish law has taken a significant step in the use of technological measures in the criminal investigation. Many other countries already had introduced this measure in their laws, and Spain has tried to adapt to the new technological possibilities, which merits

a positive assessment. Courage in modernizing the criminal investigation measures, as well as efforts to comply with international obligations, should be praised. However, when highly intrusive measures as remote access to computers are newly introduced, it is important to balance very carefully the interests at stake and to provide all possible safeguards to ensure that human rights will be respected. In this sense, an adequate protocol to ensure compliance with the proportionality principle when granting and executing the remote access to data stored in computers is missing in the 2015 law. Although the law provides for a quite comprehensive regulation, there are still many pending issues that need to be addressed. And, as it happens with many other measures that imply a restriction of fundamental rights, the final assessment shall rely in the judicial authority issuing the warrant, his evaluation of the proportionality and necessity of the measure in a precise case. And only by checking the grounding of these warrants it will be possible to see what is finally the price we citizens are paying with our privacy for combatting cybercrime and other forms of crimes that use the ICTs.

It can be exceptionally accepted that trojans become the new investigators, but not that those trojans are used to give the state access to the whole life of a person that is under investigation for a crime that might not be even serious. Granting access to all data opens the doors to the prospect of a state that engages in a dangerous *inquisitio generalis,* which not only poses risks to the right to privacy but also to the basic principles of the rule of law.