MARTINUS NIJHOFF PUBLISHERS

European Journal of Crime, Criminal Law and Criminal Justice 19 (2011) 363–395

brill.nl/eccl

Fighting against Cybercrime in Europe: The Admissibility of Remote Searches in Spain

Juan Carlos Ortiz Pradillo*

Associate Professor of Criminal Procedural Law, University of Castilla-La Mancha, Spain

1. The Global Threat of Cybercrime and the World's Concern about its Criminal Investigation

The use of information and communications technology (ICT), and especially the new opportunities which Internet offers, has caused a radical change not only regarding the *modus operandi* of traditional crimes and the process of shaping new types of crimes, but also in respect of new available technological advances destined to their investigation and providing evidence. Therefore, as the substantive criminal law has reacted by adjusting itself to these new forms of delinquency related to high technology, criminalising these new types of crimes, the procedural law equally requires an important adaptation to the contemporary *digital age*, not in respect of the application of the information technology in the proceeding and carrying-out of procedural acts (the most outstanding examples of which, among others, would be the definitive introduction of electronic case files, the telematics' presentation of texts, documents, as well as notifications, the digital recording of hearings in a digital format suitable for their registration and reproduction, judicial sale of goods by public auction carried out in the internet, the seizure and freezing of

* E-mail: JuanCarlos.Ortiz@uclm.es. This paper was prepared with financial support from the Spanish Ministry of Science and Technology (DER2008-03378: "Problemas procesales de la ciberdelincuencia y de la ciberresponsabilidad"). The author thanks the many people who made this paper possible. Special thanks go to Montserrat Cuesta, Professor Dr. Nicolás González-Cuéllar and Professor Dr. Ulrich Sieber (thanks for his encouragement during my research staff at the Max Planck Institute for Foreign and International Criminal Law in Freiburg i. Br., February–May 2008), without whose support the entire project would have been impossible.

 DOI: 10.1163/157181711X587800

banking assets using the ICT, or the common application of videoconference), but in particular in the aspects concerning diverse IT techniques and instruments in the service of the investigation against crime.

The current technological advances are used by the security forces and police, both in the tasks of investigation and follow-up actions (through what has come to be called *technosurveillance* or *electronic surveillance*[1]), and as well in the sphere related to the forensic analysis of varied electronic storage devices (computers, mobile phones, palmtop computers – PDAs, USB memory, and also GPS navigators[2]) through the science called "computer forensics", despite the lack of sufficient and modern legislation.[3]

Furthermore, the mentioned technology is used to obtain the evidence of any kind of crime, constituting (or not) the so-called 'computer (cyber) crimes'. It can and should be applied in the investigation of those actions in which the computer equipment, programmes or data, establish the instruments, objects or effects of the crime, or traces of its perpetration, and it is an efficient tool in the investigation of all those 'traditional' crimes in which such actions form a valuable source of evidence, due to its present capacities of storage of information and its use for all types of communication. As Professor González-Cuéllar Serrano rightly points out,

> a violent young person who videotapes a brutal beating of a homeless man with his mobile phone, or a drug dealer who records the transaction details in an electronic document in his notebook, are not *cybercriminals* but create digital data that gives information about a punishable action.[4]

---

1) See P. Bellia, 'The future of internet surveillance', 72 *The George Washington Law Review,* (2004) 1375; S. Freiwald, 'Online Surveillance: Remembering the Lessons of the Wiretap Act', 56 *Alabama Law Review* (2004) 9.

2) See O. Van Eijk and M. Röloffs, 'Forensic acquisition and analysis of the Random Access Memory of TomTom GPS navigation systems', 6 *Digital Investigation* (2010) 179–188, available at: <www.sciencedirect.com>.

3) See the document *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, (Computer Crime and Intellectual Property Section Criminal Division, 2009), availabe at: <www.cybercrime.gov>. Also see M. Mack, 'Electronic Discovery vs. Computer Forensics', 20 *New Jersey Law Journal* (2003) 1; E. Casey, *Digital Evidence and Computer Crime* (London: Elsevier, 2nd Edition, 2004); O. Kerr, 'Digital Evidence and the new Criminal Procedure', 105 *Columbia Law Review* (2005) 279 and 'Search and Seizure in a Digital World', 119 *Harvard Law Review* (2006).

4) N. González-Cuéllar Serrano, 'Garantías constitucionales en la persecución penal en el entorno digital', in *Derecho y Justicia penal en el Siglo XXI. Liber amicorum en homenaje al Profesor Antonio González-Cuéllar García* (Madrid: Colex, 2006) p. 889.

Nevertheless, in the scope of the delinquency related to IT, the investigation and prosecution of the named 'cybercrimes' presents special characteristics because of the means by which such crimes are committed (internet) and this makes the application of special technological instruments of investigation essential for multiple reasons. Among them, two stand out above the rest. First, we deal with crimes committed at a distance, with significant difficulties concerning the determination of the place of perpetration of such an offence, carried out by electronic means, in a digital sphere, the proof of which is in a digital format as well and seems to be prone to alternation or destruction as soon as it has been created.[5] From there comes the importance that the attainment of electronic evidence has acquired, including its admissibility before the courts. Second, its international dimension or cross-border, has obliged the principle international bodies to urge for different means of international cooperation (not only international treaties and conventions, but also recommendations, good practices, action plans, etc.) in the fight against cybercrime, with the awareness of the essential collaboration between the states with the aim of pursuing the mentioned crimes.

Next to a decision of the well-known *G8 group* a subcommittee in charge of the study of the cybercrimes (high-tech crimes) was created in 1997, thanks to which many reports and sets of rules referring to this matter have been presented, the UN has also shown its concern about the increase of cybercrime, and in its different resolutions, has started to promote diverse means with reference to cooperation in the aspect of cyber delinquency.[6] However, the main driving forces in respect of the international mechanisms of cooperation against cybercrimes have been the Council of Europe and the European Union, which have always been in favour of changing national legislations and adapting them to the challenges that raises the digital environment.

At first, their efforts concentrated on the evolution of the rules governing the interception of communications, and the proof is that the reunion of the ministers of the *group TREVI* in 1991 had already observed the necessity to study the effects of the legal, technical and commercial evolution in the section of telecommunications, in order to know more about the different possibilities of their interception. Afterwards, in the Appendix of the Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology (adopted by the Committee of Ministers

---

5) Cybercrimes have been rightly classified as crimes committed 'at the speed of light' (S. Brenner, 'At light speed: attribution and response to cybercrime / terrorism / Warfare', 97 *Journal of Criminal Law & Criminology* (2007) 379.

6) For a more detailed study, see M. Gercke, *Understanding Cybercrime* (2009), available at: <www.ITU.INT/itu-D/cyb/cybersecurity/legislation.html>.

on 11 September 1995), it was noticed that criminal procedural laws of member states often do not provide for the appropriate powers to search for and collect evidence in these systems in the course of criminal investigations; it was recalled that the lack of appropriate special powers may impair investigating authorities in the proper fulfilment of their tasks in the ongoing development of information technology; and it was recognised that there was the need to adapt the legitimate tools which investigating authorities are afforded under criminal procedural laws to the specific nature of investigations in electronic information systems. For example, to regulate in a clear and distinguished manner the searching of computer systems, as well as the seizure of the data stored therein or the interception of data in the course of transmission, and all of this under the conditions similar to those traditional authorizations of entry and search.

Moreover, in its Recommendation Rec (2005) 10 of the Committee of Ministers to member states on 'special investigation techniques' in relation to serious crimes including acts of terrorism (Adopted by the Committee of Ministers on 20 April 2005 at the 924th meeting of the Ministers' Deputies), the Council of Europe discussed the use of the special means of investigation related to New Technologies, for example, through the collaboration with the private sector, the existing international agreements for the judicial or police cooperation with reference to the use of special techniques of investigation, particularly those necessary in an international context, or through the signature, ratification and application of the conventions and instruments existing in the scope of the international cooperation in criminal matters, in aspects concerning the exchange of information, handing-over under surveillance, covert investigations, joint investigation teams, cross-border operations and training, with special mention to the Convention on the Cybercrime from 23 of November 2001, already in force in Spain, which now represents the main instrument of international cooperation in matter of the struggle with cybercrime.

The European Union, is interested in the use of diverse technological advances in the criminal investigation of transnational delinquency, and especially, computer crime. Next to the widely-recognized study by Sieber, *Legal Aspects of Computer-Related Crime in the Information Society* – COMCRIME, is the Communication *e-Europe 2002,*[7] in which important recommendations were included, referring to both substantive Criminal Law and Procedural Law. In fact, advice specified in the aforesaid Communication in respect to the retention of the traffic related data as a valuable instrument of investigation of computer crimes had their reflection in the approval of the Directive 2006/24/EC of the European Parliament and of

7) COM (2000) 890 final.

the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and the amending Directive 2002/58/EC[8]. Later, in the Communication *Towards a general policy on the fight against cyber crime,*[9] the European Union set its specific target to promote global international cooperation in the matter of fighting against cyber delinquency, and more specifically, "Take concrete action to encourage all Member States and relevant third countries to ratify the Council of Europe's Cyber Crime Convention and its additional protocol and consider the possibility for the Community to become a party to the Convention", what should be added are the special operational measures and research proposals in the *Council's strategy to reinforce the fight against cyber crime*[10], such as cyber patrols, joint investigation teams and remote searches to become part of the fight against cybercrime in the next five years. The strategy also introduces concrete steps for closer cooperation and information exchange between law enforcement authorities and the private sector. In the Communication *An area of freedom, security and justice serving the citizen,*[11] it is advised that the rules are clarified on jurisdiction and the legal framework applicable to cyberspace in order to promote cross-border investigations; establish a legal framework that would allow cooperation agreements between law enforcement authorities and operators, which would allow quicker reactions in the event of cyber attacks; and create a specialised network comprising the national representatives in charge of the fight against cybercrime that coordinates the actions taken by the Member States (e.g., Europol). Subsequently, the European Commission published the *Green Paper on obtaining evidence in criminal matters from one Member State to another and securing its admissibility,*[12] with the aim of replacing the existing rules and unifying the instruments on obtaining evidence in criminal matters in the EU with a new rule which would cover all types of evidences and in which norms regulating electronic evidence could be included. In the Annex to the *Stockholm*

---

8) OJ L 105, 13 April 2006 pp. 54–63. for a comparative study of the Directive, see J. C. Ortiz Pradillo, 'Tecnología versus Proporcionalidad en la Investigación Penal: La nulidad de la ley alemana de conservación de los datos de tráfico de las comunicaciones electrónicas, 75 *La Ley Penal* (2010) 80–94.

9) COM (2007) 267 final.

10) See Europa Press Releases, Reference: IP/08/1827, Date: 27/11/2008, available at: <europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827&format=HTML&aged=1&language=EN&guiLanguage=es>.

11) COM (2009) 262 final.

12) COM (2009) 624 final.

Plan,[13] the EU has also taken over the task to promote important measures to be adopted against cybercrime, such as measures aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as the one on modernised Network and Information Security Agency (ENISA) plus other measures allowing faster reactions in the event of cyber attacks; a legislative proposal on attacks against information systems; the creation of a cybercrime alert platform at European level; developing a European model agreement on public private partnerships in the fight against cybercrime and for cyber security; or the ratification of the Council of Europe Convention on Cybercrime from 2001 by all the member states. And, finally, in its meeting on 23 February 2010, the Justice and Home Affairs Council of the EU released its *Draft Internal Security Strategy for the European Union: 'Towards a European Security Model',*[14] in which the Council recognizes cybercrime as one of the main criminal risks Europe faces nowadays, because it represents "a global, technical, cross-border, anonymous threat to our information systems and because of that, it poses many additional challenges for law-enforcement agencies".

2. New Instruments of Legal Hacking: Real-Time Electronic Surveillance

The forensic examination of hard drives and peripheral elements of computer equipment seized after a house search, and any other electronic communication or storage device, has become a habitual and the most effective practice for obtaining evidence from all types of crime, whether or not are they catalogued as a computer crime. The use of specialised hardware and software in the search and analysis of the information employed constitutes a major technological step forward, applicable in the criminal investigation despite the outdated legal regulation. It is sufficient to notice how the legal authorisation in Spain proceeds with the search and seizure of the information stored on such equipments. There is a *refreshing* interpretation of the existing regulation concerning the inspection of 'books and papers' from the collection of "effects, instruments or evidence of the crime of which their disappearance would be a danger' and from the regulation about 'ocular inspection and *corpus delicti*'.[15]

---

[13] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – *Delivering an area of freedom, security and justice for Europe's citizens – Action Plan Implementing the Stockholm Programme*. COM (2010) 171 final.

[14] Available at: <register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf>.

[15] See the Spanish Supreme Court sentences (STS) on 18 May 2001 and 14 February 2006. Available at: <www.poderjudicial.es/eversuite/GetRecords?Template=cgpj/ts/principal.htm>.

Furthermore, this forensic science is appealing because it has at its disposal a massive use of electronic means and because of the gradual abandonment of paper in favour of the virtual environment. Therefore, the obtainment, analysis and valuation of the evidence in the electronic media are gradually forming a regular part of all types of legal actions, both civil and penal. And thus, generically defined as *all information of probative value that is stored or transmitted in binary form.*[16] Electronic evidence plays an essential role in several phases of the cybercrime investigation, since this is (digital environment) the medium in which such crimes are committed and therefore, the format in which to look for, locate and apprehend the tracks left on the occasion of the commission of crimes mentioned. Also, we are facing particular problems such as the knowledge required from officers and experts who are responsible for the collection and analysis of the information, the standardisation of norms, practices or protocols which guarantee the integrity of attained digital data or constant evolution of technology and thus, new instruments, programmes, formats, capacities, etc., all of which increase the challenges faced by computer experts when they have to analyse hardware and software in order to proceed with the recovery of the archives, decipher them, identify the user of the equipment or persons involved in a communication through telematic systems, etc.

However, forensic computing, originated in the 1980s as a response to early computer virus attacks on Internet, became more common during the early 1990s, and law enforcement agencies began to gather evidence in relation to pornographic and fraud investigations by conducting investigations that primarily involved computers as storage devices, but nowadays forensic computing has evolved over recent years to include "pro-active involvement" in the collection of intelligence relating to criminal, illegal and inappropriate computer behaviour, particularly in relation to terrorist activities, organised crime syndicates and recidivist behaviour.[17] Now it includes 'active means' of search and collection of information of any type, whether it is stored in computer equipments or 'circulating' in the internet and can be used by intelligence services and authorities responsible for criminal investigation, for the prevention and detection of all types of crimes in which IT plays an important role in its preparation, execution or concealment.

---

16) See *SWGDE and SWGIT Glossary of Terms*, The Scientific Working Group on Digital Evidence (SWGDE), available at: <www.swgde.org/documents/archived-documents/>.

17) See M. Hannan, 'To Revisit: What is Forensic Computing' (2004) available at: <scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf>); P. Bellia, 'Spyware and the Limits of Surveillance Law', 20 *Berkeley Technology Law Journal* (2005) 1283; E. Nissan, 'Legal Evidence, Police Intelligence, Crime Analysis or Detection, Forensic Testing, and Argumentation: an overview of Computer Tools or Techniques', 17 *International Journal of Law and Information Technology* (2009) 1–82.

Those are the new and sophisticated electronic instruments and computer applications which are capable of interception and recording in real-time all the data transmitted and received by different media of communication (and with regard to the actual content of the communication, such as traffic data or location data), or including those which are found saved in the memory devices of the aforementioned equipment. This might be considered by some as hacking or computer intrusiveness. In spite of being incorporated into other regulations as a legal means of electronic investigation, in Spain they remain orphans without any regulation, which has motivated some convictions for misuse of the software called 'spyware'. This is able to record all activities conducted through a mobile phone or PC and send that information to another computer via e-mail.[18]

Therefore, the use of the new technological means must be analysed by the authorities responsible for criminal investigation and determine if it is possible to use those means in Spain, in accordance with the current legislation and case-law regarding data protection and related rights in this matter (privacy, inviolability of home, ambulatory freedom, *habeas data*, etc.). In particular, there are two new electronic surveillance techniques that have become important in representing the present and the future of the application of IT to criminal investigations: the first one (acquiring certain data from mobile phones), has been legitimized by the Spanish Supreme Court case-law, and the second one (remote search of computer equipment), recommended by Europe as a special investigation technique to be used by countries.[19]

2.1. *Electronic Surveillance over Mobile Phones*

Thanks to technological improvement, it is possible 'to clone' a mobile phone through the implantation of a chip that makes this phone the same replica. By means of its installation it is possible to monitor the entire management of the original phone from the replica, serving as the listening station of the original telephone traffic, helping to know its location from the data obtained from the Base Transceiver Station (also called 'Cell Site') closest to the original, or activate the microphone of the phone without having to turn the original one on. Today, that cloning can be done remotely, through the installation of software that has to be downloaded to the phone.[20]

---

18) About the use of spyware programms in Spain, see the judgements of the Audiencia Provincial (Appeals court) of Madrid, Section 17ª, from 25 May 2005, and Section 27ª, 30 June 2009.

19) Recommendation Rec(2005) 10, *loc. cit.*

20) See B. Mellars, 'Forensic examination of mobile phones', 1 *Digital Investigation* (2004) 266–272 (available at: <www.sciencedirect.com>), and W.Clark, 'Cell Phones as Tracking Devices', 41 *Valparaiso University Law Review* (2007) 1413. In Spain, see M. Llamas Fernández and M. Gordillo Luque,

We do not know if these instruments of electronic surveillance on mobile phone terminals have already been implemented and used in Spain, but what has entered the legal arena has been the use of electronic devices. Apart from the physical location of the terminals, The IMSI number and the mobile phone number are identical.

Other countries have regulated the use of these devices, and the most notable example is the U.S., where real-time electronic surveillance in federal criminal investigations is governed primarily by two statutes: the federal Wiretap Act (18 U.S.C. §§ 2510–2522), first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (and generally known as "Title III"), and the Pen Registers and Trap and Trace Devices chapter of Title 18 –'the Pen/Trap statute'-, (18 U.S.C. §§ 3121–3127), first passed as part of the Electronic Communications Privacy Act of 1986. The Title III and the Pen/Trap statute regulate access to different types of information. Title III permits the government to obtain the contents of wire and electronic communications in transmission. In contrast, the Pen/Trap statute concerns the real-time collection of addressing and other non-content information relating to those communications. About these real-time electronic surveillance instruments used for the acquisition of information concerning electronic communications that do not include the contents thereof, special attention must be paid to the mentioned cell site stimulators, (also known as *digital analyser* or *triggerfish*).

A cell site simulator (digital analyzer or triggerfish) can electronically force a cellular telephone to register its mobile identification number ('MIN', i.e., telephone number) and electronic serial number ('ESN', i.e., the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identify the cell location and geographical sub-sector (from which the telephone is transmitting) is transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signalling data (ESN/MIN, channel/cell site codes) are not dialled or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode. If the cellular telephone is used to make or receive a call, the screen of the digital cell site simulator would

---

"Medios técnicos de vigilancia', in *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia* (Madrid: Cuadernos de Derecho Judicial, 2007) 237.

include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialled, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected). *Cell site simulators and similar devices may be capable of intercepting the contents of communication and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized.*[21]

Germany amended its procedural law (StPO) in August 2002, through the reform of Article 100i, in order to legitimise the police to obtain data which identifies the device number of a mobile terminal, the card number used and the location of a mobile terminal in case of an emergency.

In Spain, however, the obtainment by the police of such information emitted by mobile phones has been supported by case law. This was expressed by the Supreme Court of Spain in its sentences (STS) of 20 May and 18 November 2008, and 28 January 2009. Without prior judicial authorization, it considers such information not as traffic data but 'personal data' related to Art. 18.4 of Spanish Constitution (CE), so that the legal regime that governs the obtaining of such information, would be the one referred to the in the collection and processing for law enforcement purposes of Personal Data by the Security Forces (Art. 22 of the Organic Law 15/1999 of December 13, of Personal Data Protection, LOPDP) and not the one who requested its assignment by the operators (Law 25/2007, from 18 October, related to electronic communications' Data conservation and public communications networks). This continues to be questionable, because of equally having to obtain the IMSI with a conventional surveillance work, which is determined by the person who is being investigated, with whom he speaks, where is he localised or what objects he touched, or the brand and model of the mobile phone, by using special wireless 'binoculars'.[22]

This judicial interpretation debunks the whole conditions and guarantees laid down in the aforementioned Law 25/2007, because it would be necessary for the police to have the technology needed to collect the data regulated in this Act without the need to apply for cession from network operators through a court

---

21) See the document *Electronic Surveillance Manual. Procedures and Case Law Forms*, prepared by the Electronic Surveillance Unit, Office of Enforcement Operations, Criminal Division, 2006. Available at: <www.usdoj.gov/criminal/foia/docs/elec-sur-manual.pdf>.

22) As a detailed study of the case law concerning this point, see F. Gudín Rodríguez-Magariños, 'Legalidad de los mecanismos de barrido policial que permiten obtener los números IMEI/IMSI de las tarjetas de telefonía móvil', 18 *Revista General de Derecho Procesal* (2009); J. L. Rodríguez Láinz, 'Dirección IP, IMSI e intervención judicial de comunicaciones electrónicas', 7086 *Diario La Ley* (2009) pp. 1–12; and J. M. Sánchez Siscart, 'A vueltas con el secreto de las comunicaciones: Algunos supuestos críticos en la jurisprudencia de la Sala 2ª del Tribunal Supremo', 7338 *Diario La Ley* (2010) 1.

order, provided they do not relate to the subject of the statement. That law also requires a court order to obtain the necessary data for the geographic location of a mobile terminal (in particular for the geographic location of the cell used at the beginning of the communication and those used during the period for which communication data are stored) and yet, if the police who, through certain electronic devices, obtain that location, the Supreme Court of Spain also ruled that *it could be considered a breach of privacy of the person investigated if this location indicates the exact place where the investigated person was; but when that location (…) can only be calculated with an approximation of several hundred meters, which is the area covered by the BTS that captures the signal, the right to privacy under the practice of care can be regarded as affected, at least in a relevant form.*[23] This doctrine legitimizes 'de facto' attainment of the geographic location of persons always if the latter may be inaccurate in any way, and therefore it does not affect the right to privacy or this affection is minor. In our opinion, this depends on the requirement of the judicial authorisation (because it affects the 'relevantly' aforesaid Fundamental Rights) and on the degree of precision with which the geographical location of a person can be determined through any electronic means. This only adds more confusion and legal uncertainty in this matter, and technology will soon be developed to such an extent that it will be able to locate accurately and with almost with no margin of error, the geographical position of a person, and for such the doctrine of the Supreme Court should be reviewed. We must not forget, that the Spanish law (in particular Art. 33.7 of the General Law of Telecommunications – LGT, Law no. 32/2003 from 3 November) requires that "information on the geographical location of the terminal or network termination point of origin of the call and the destination of the call be provided. In the case of mobile services the *most accurate position as possible* to the communication point and, in any case, the identification, location and type of the BTS affected will be provided".[24]

And finally, because the recognition that *the capacity to collect the data that the Law 15/1999 grants to the police cannot, of course, be treated as an excuse for creating an uncontrolled regime of exception in its favour. But there is no denying that the collection of this data in the context of a criminal investigation – never with a purely exploratory character – for the discovery of a particularly serious crime, can be deemed proportionate, necessary and, therefore, free from any violation of constitutional rights and freedoms*, opens the door to further confiscation of various electronic data by

---

23) See STS from 19 December 2008 (sentence no. 906/2008).

24) In the U.S., academic opinion is divided as to whether the geographical location from the mobile phone affects the Right to Privacy. See K. McLaughlin, 'The Fourth Amendment and Cell Phone Location Tracking: Where Are We?' 29 *Hastings Communications and Entertainment Law Journal* (2007) 421.

the police without a judicial order, as a part of a criminal investigation of a serious crime, such as the case of personal data 'obtained' from within the open Wi-Fi networks by some spyware, which is rejected when it is an individual who proceeds with the collection and the storage of such data.[25]

2.2. *Remote Searches of Computers*

Computer equipment from which different criminal activities are carried out has turned into the Rosseta Stone for the authorities in charge of investigations of cybercrimes, and its expert analysis is essential to achieve criminal convictions for the authors of the mentioned crimes. Hence, for example, the investigation of a crime concerning child pornography in the Internet normally begins with a citizen's complaint or with the police inquiry referring to the existence of the determined paedophile's material. This material circulates in the web and is exchanged by the P2P systems, followed by certain tasks of 'cyber patrols'[26] who investigate the IP addresses which obtained and spread the aforesaid material and the investigation is terminated with a home search and confiscation of the used computer equipment.

However, what would happen if we did not have physical access to the mentioned computer equipment? The transnational character of cybercrime makes it possible that the author of the crime and, his/her instruments and victims might be in different countries. To solve this problem we must join the mobility of the different electronic devices, the allocation of the information stored, which despite being accessible from home, can be physically stored on an Internet server located in any foreign country, as well as advanced protection measures used by criminals (for example, deleting and self-destructing programmes when the suspect feels he is being watched, or in the case of the police trying to entry his home). It also may be interesting to manage a *live access* to the computer equipment, to capture the same codes used to decrypt the possible use of cryptography in the information stored, or passwords for web portals that offer e-mail (Hotmail, Yahoo, Gmail, etc.), so that such data which are only stored in RAM on a computer, are recovered before it is turned off.

These questions constitute serious obstacles for the investigation of cybercrime, so obtaining 'remote' information stored or communicated through a computer, without the need for search and seizure *in situ* is a very important step towards the

---

25) About the "Google Street View case" in Spain, see the Spanish Nacional Data Protection Agency (AEPD) information available at: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/octubre/101018_np_google.pdf.

26) About child pornography investigations, see S. Kreston, 'Computer Search and Seizure Issues in Internet Crimes against Children Cases', 30 *Rutgers Computer and Technology Law Journal* (2004) 327.

investigation of this type of delinquency. Just remember how the Recommendation R (95) 13 Council of Europe, after noting the inadequacy of the laws of most Member States regarding the existence of appropriate measures for the search and seizure of the evidence contained in computer equipment, proposed the adaptation of national legislation to regulate not only the search of computer equipment, but also *the power to extend a search to other computer systems,* that *should also be applicable when the system is located in a foreign jurisdiction, provided that immediate action is required. In order to avoid possible violations of state sovereignty or international law, an unambiguous legal basis for such extended search and seizure should be established. Therefore, there is an urgent need for negotiating international agreements as to how, when and to what extent such search and seizure should be permitted.*

The proposal contained in the cited Recommendation was collected, but with limitations, in the Convention on Cybercrime. Art. 19.2 allows the search of a computer to be extended to other computer systems on which it has reason to believe that the data which are being investigated are stored, but only if those other systems are located *in its territory.*[27] Article 3.2 authorizes trans-border access to the data stored, but only in the case of the stored computer data *publicly available* or *with the lawful or voluntary consent of the person who has the lawful authority to disclose the data to the other Party through that computer system.*

Nevertheless, in the absence of a detailed explanation of what is meant by an 'authorized person', the question remains about the admissibility or trans-border records ordered by a judicial authority when it comes to access to information stored on computers that are not an 'open source'.[28] But even if we recall that the

---

[27] See the Explanatory Report, at para. 195. Available at: <conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

[28] See M. Gercke (*loc. cit.,* p. 207: The second situation in which law enforcement agencies are allowed to access stored computer data outside their territory is when the investigators have obtained the lawful and voluntary consent of the person who has lawful authority to disclose the data. This authorisation is heavily criticised. There are good arguments against such regulations. The most important one is the fact that by establishing the second exemption, the drafters of the Convention are violating the dogmatic structure of the mutual legal assistance regime. With Art. 18 the drafters of the Convention enabled the investigators to order the submission of data. This instrument cannot be applied in international investigations because the corresponding provision in Chapter 3 of the Convention is missing. Instead of giving up the dogmatic structure by allowing the foreign investigators to directly contact the person who has control over the data and ask for the submission of this data, the drafters could have simply implemented a corresponding provision in Chapter 3 of the Convention). See also the Explanatory Report, at para. 293: *they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data, as provided in the Article*. In favour of cross-border searches, see J.Goldschmith, 'The Internet and the Legitimacy of Remote Cross-Border Searches, *The University of Chicago Legal Forum*, available at: <papers.ssrn.com/abstract=285732>.

Council of the European Union, in its Common Position 1999/364/JHA, of 27 May 1999, adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the Draft Convention on Cyber Crime held in the Council of Europe, was in favour of admitting the *transborder computer search for the purpose of the investigation of a serious criminal offence, (…). It may be considered in exceptional cases, and in particular where there is an emergency, for example, when necessary to prevent the destruction or alteration of evidence of the serious offence, or to prevent the commission of an offence that is likely to result in the death of or serious physical injury to a person.*[29] Those types of 'serious criminal offences' should have, but have not yet been further defined in greater detail in the Convention.

However, the inexistence of an international Convention or a Treaty which would legitimate the application of the mentioned technological advance, did not prevent some countries from introducing it as a measure of investigation. Again, the United States were the country who first approved the use of electronic monitoring software based on the idea of 'Trojan programs,' able of being remotely installed on the computer to investigate, record everything typed on a hard drive, and transmit that information to another computer (the one of the investigating authority), which would apply to the rules of *the pen register* to monitor the Internet use being done on the computer investigated, and record the IP addresses which the computer equipment contacts, always, if the content of such communications is not accessed or recorded.[30]

In Europe, Germany was the first country to legislate on the use of this new technology as an exceptional measure of investigation of the crimes related to international terrorism by the Law of 25 December 2008, on the Defence against

---

29) OJ 5 june 1999 L 142. See the arguments of Seitz, 'Transborder Search: A New Perspective in Law Enforcement', *Yale Law School* (2004) 48, available at: <www.yjolt.org/files/seitz-7-YJOLT-23.pdf>.

30) Called 'Magic Lantern' and CIPAV (Computer and Internet Protocol Address Verifier). See R. S. Martin, 'Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome', 40 *American Criminal Law Review* (2003), C. Woo, 'The case for Magic Lantern: September 11 Highlights. The need for increased surveillance', 15 *Harvard Journal of Law & Technology* (2002). A comparative study about the spanish regulation at J. C. Ortiz Pradillo, 'El registro 'online' de equipos informáticos como medida de investigación contra el terrorismo (Online Durchsuchung)', in *Terrorismo y Estado de Derecho* (Madrid: Iustel, 2010. pp. 457–478) and 'Cooperación penal europea e internacional en la obtención de prueba electrónica', in *Presente y Futuro de la E-Justicia en España y la Unión Europea* (Navarra: Aranzadi, 2010, pp. 559–574).

International Terrorism.[31] After that, the German Constitutional Court (BVerG)[32] declared it unconstitutional and quashed the law of the Land of North Rhine-Westphalia, which sought to regulate remote computer searches and records as a measure of the police prevention. The German Constitutional Court also set out the guidelines and guarantees required to support the records online, recognizing a new content called the right to informational self-determination: 'the fundamental right to guarantee confidentiality and integrity of computers' (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).

The regulation of these measures in a unilateral form by some countries does not solve the problem, due to the characteristics that are derived from the international scale of cybercrime to which we have referred. Carrying out a remote search of a computer would constitute a performance with extraterritorial effects if the computer is located outside the jurisdiction of the ordering state. In other words, the unilateral adoption of national measures is useless when dealing with a threat that knows no boundaries, and may be counter-productive to the legitimate purposes of criminal investigation, because a remote search legally regulated in one state may constitute an unauthorized access to a computer system in another. For example, the online search authorized in Germany under the Law of 25 December 2008, to investigate the connections between various terrorist cells in Europe, the Middle East and North Africa, would be considered in Spain as an 'unauthorized access to computer data or programmes contained in a computer system' punishable according to the Art. 197.3 of the Spanish Criminal Code (CP).

3. The Legislative Apathy in Spain opposite the New Challenges of Cybercrime

It is true that the current European and international guidelines call for a reinterpretation of existing rules under the new challenges posed by the specific nature of the digital environment, but the fact remains that the interpretation efforts should be, in any case, additional and should not replace a detailed regulation of the typology of the legal measures of investigation related to Information Technology, their scope, requirements and guarantees. However, Spain has not yet undertaken the necessary and urgent update of the Spanish Code of Criminal Procedure (LECrim) that collects, with an appropriate degree of discretion, known as a margin of appreciation, depending on the circumstances of each case, the modern techniques of investigation that provides computer science, as the doctrine has

---

31) *Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt* (BGBl. I, Nr. 66, S. 3083), that amends the Law of 7 July 1997 (*Bundeskriminalamtgesetz, –BKA-Gesetz–*. BGBl. I, S. 1650).

32) Resolution from 27 February 2008 (BverfG, 1 BvR 370/07).

repeatedly claimed.[33] As Galán Muñoz declared, *neither the enormous technological advances, the wide range of innovative communication techniques available on the Internet, nor the development of an important and complex legislation intended to establish a system enabling the investigation of crimes committed within this network, have led to any change in the Code of Criminal Procedure.*[34]

The more paradigmatic example is the judicial interpretation carried out with respect to Art. 579 LECrim. In 1992, *the need to carry out a kind of jurisprudential construction via the right way to pursue this measure, using in the analogous way the Code of Criminal Procedure regarding the detention of private correspondence and other similar assumptions*[35] was defended. As we have already mentioned, the insufficient procedural regulation of the interception of communications, was repeatedly denounced by both the doctrine, the Spanish Supreme Court (*Tribunal Supremo*, TS) and the Spanish Constitutional Court (*Tribunal Constitucional*, TC). This was the reason why the ECHR sentenced against Spain twice and has forced the courts to be the institutions responsible for establishing and specifying the requirements for the legitimate interception of telecommunications and their validity as evidence. In particular, the Constitutional Court has declared, having expressly recognized that Art. 579 LECrim does not meet the requirements necessary to protect the secrecy of correspondence,[36] that the *problem would not be resolved properly with a matter of unconstitutionality because Art. 55.2 LOTC (Spanish Organic Law of the Constitutional Court) is expected to estimate recourses of protection regarding legal provisions that contradict the Constitution, but not in respect of those which dovetail with the former and whose unconstitutionality derives not from its content but from what is passed over in silence*. That is why the Court has defended (or justified) its duty to fill gaps in the legal order *until the time that the necessary legislative action is performed.*[37]

This doctrine in favour of the work of jurisprudence integrating the legal spheres regarding the interception of communications was supported by the ECHR in its

---

33) See N. González-Cuéllar Serrano, *loc. cit.*; J. Pérez Gil, 'Criminalidad informática y reforma procesal penal: un decálogo de propuestas', 26 *E-newsletter CYBEX sobre Prueba electrónica* (2007), available at: <www.cybex.es>; E. Rovira del Canto, 'Adaptación y reforma de la normativa procesal en la persecución del ciberdelito', 46 *E-newsletter CYBEX sobre Prueba electrónica* (2009), and J. C. Ortiz Pradillo, 'El registro online…, *loc. cit.*'.

34) A. Galán Muñoz, 'La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales', 24 *Revista Penal* (2009) 100 (Author's translation).

35) The Spanish Supreme Court Decision (ATS) on 18 June 1992.

36) STC 184/2003 from 23 October 2003.

37) For all, see the case law contained in the STC 49/1999, from 5 April 1999.

Inadmissibility Decision of 25 September 2006 (case *Abdulkadir Coban* v. *Spain*), where it admitted the Spanish government's argument that the legal regime for the wire-tapping is based not only on the arts. 18.3 of the Spanish Constitution and 579 LECrim, but also in the details and conditions established by the jurisprudence. For the ECHR, the shortcomings of the Spanish law of 1988 have been allayed by the jurisprudence, particularly the Supreme Court and the Constitutional Court from the ATS of June 18, 1992, from which the 'foreseeability' of the law in its broad sense cannot be questioned. And, while acknowledging *the desirability of a legislative amendment to incorporate these jurisprudential principles or guarantees*, it finishes by estimating that Art. 579 LECrim, *as amended by the L.O. 4/1988 and completed by the jurisprudence of the Supreme and Constitutional Court, contains clear and detailed rules and specifies, a priori, with sufficient clarity and extension the procedures for exercising the discretion by the authorities in the considered field.*

3.1. *Solution a): The Future (but Inadvisable) 'Complementary' Doctrine of the Courts*

As there was, at the time, a broad interpretation of the concept of 'document' which was included within the same notion as magnetic tape, diskette, CD-ROM, etc., or the concept of 'currency' which included the counterfeit of credit cards, it is forecasted that our Supreme Court will hold, in the near future, a consistent interpretation of the LECrim that would legitimize the remote search of computer equipments to gather stored information that the police considers to be necessary for the inquiry of the crime under investigation; from analogous implementation of budgets, conditions and guarantees required for home searches, the occupation of documents, the detention of the postal and telegraph correspondence and wire-tapping, and several judges have already ruled in favour of this technique.[38] This consistent interpretation is already being implemented, for example, in the investigation and interventions concerning emails and other types of communications made through the Internet[39], and on the basis of this analogous application, sometimes forced, it has legitimized certain police practices under the general coverage of their own assumed proportionality, in a way that does not fulfil, in our opinion, the minimum requirements of legality, clarity and quality provided

---

[38] See E. Urbano de Castrillo, 'La investigación tecnológica del delito", in *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia* (Madrid: Cuadernos de Derecho Judicial, 2007) pp. 19–76 and E. Velasco Núñez, *Delitos cometidos a través de Internet. Cuestiones Procesales* (Madrid: La Ley, 2010) 131.

[39] See F. Hernández Guerrero, 'Medios informáticos y proceso penal, *Estudios Jurídicos. Ministerio Fiscal* (1999-IV) 497; J. M. García Ruiz, 'Correo electrónico y proceso penal, *La Ley* (2003) 1; M. Marchena Gómez, 'Dimensión jurídico penal del correo electrónico', *La Ley* (2006) 4–17.

by the ECHR,[40] such as in the case of the police authority who proceeds with the inquiry into the memory of mobile phones without previous judicial authorization, within the legitimate powers to a superficial search of the person detained and confiscation of the property the said person is carrying.[41] It should be noted that this line of jurisprudence has fortunately since been abandoned, after the STC no. 230/2007, of 5 November 2007, as currently seen from the Sentences of SSTS from 8 April and 14 May 2008, and 18 December 2009.

3.2. *Solution b): The Reform of the Spanish Code of Criminal Procedure (LECrim)*

In our opinion, it is not acceptable, from the jurisprudential point of view, to legitimize the use of the remote searches of computer equipments, in the subsidiary and exceptional manner, on the legal basis of that mentioned legislation regulating the home entries and searches, etc. It is true that, in the absence of express rules governing the possibility of using this technology in the field of law enforcement, our Courts have been forced to make an authentic jurisprudential reinterpretation of existing legislation to allow the use of new methods of investigation, under the reprehensible excuse that criminals make use of innovative equipment and software every day, which has transformed the criminal activity into a real science[42].

However, as we do not want to raise doubts about the legality of such actions, we consider a thorough reform of the LECrim necessary, which would include as a mean of investigation, the explicit and detailed search of computer equipments (the remote search would be nothing more than a form to proceed with the search of equipments) and, in general, would regulate specifically the possibility of using new technological advances in police and judicial fields, taking into account the legitimate purposes of criminal investigation, in a manner that would constitute a real development of a fundamental right to *Habeas Data* from Art. 18.4 CE.

Remote and secret access to the information stored in an electronic device, even though legally authorized and with the aim of obtaining valuable information for the detection of a crime, cannot be justified on the jurisprudential distinction that says that the right to privacy protected by Art. 18.1 of the Spanish Constitution does not require, in all cases, the necessary judicial authorization required under

---

40) See ECHR *Kruslin* and *Huvig v. Francia* from 24 april 1990, at para. 33: '*Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.*'

41) See the SSTS from 27 June 2002, 25 July and 25 September 2003.

42) See E. Velasco Núñez, 'Eliminación de contenidos ilícitos y clausura de páginas web en Internet (medidas de restricción de servicios informáticos)', in *Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia* (Madrid: Cuadernos de Derecho Judicial, 2007) 107.

Art. 18.3. Since Art. 18.4 also does not refer to a judicial restraint, and yet, to obtain traffic data from operators a judicial mandate is needed;[43] neither in the absence of a 'virtual home'[44] protected by the guarantees derived from the Art. 18.2, since in Spain, the audio-monitoring of the home from outside is not allowed; nor in the extrapolation in the digital sphere of the classic arguments used for the intervention in the *already read* letters, personal organizers or papers which the detained subject carries with him/herself. These could be confiscated by the police to proceed with the superficial search of the said person's belongings, because the comparison of traditional letters, diaries or backpacks with current electronic devices would create an action infringing the principle of proportionality, due to the extraordinary number and diversity of information stored in them.

4. Requirements and Guarantees for the Admissibility of Remote Searches in Spain

The regulation of remote searches, especially when it comes to the search and seizure of data stored on computers located in the territory of the Member States, could be incorporated into the national systems in a homogeneous way with the approval of the relevant European legal instruments, for example, a new regulation of the *European Evidence Warrant.*[45] Or, the initiative of several European countries (including Spain) for a Directive of the European Parliament and of the Council regarding the European Investigation Order in criminal matters (EIO),[46] to regulate a general and single instrument that would replace all existing instruments in the field of acquiring evidence, meaning any measure of investigation (with some exceptions), and that would include the obtaining of evidence that is already in the possession of the executing authority.

However, while not producing the desired reform of the Spanish Criminal Procedure Law (LECrim) in this area, the potential admissibility of using the remote searches as a measure of criminal investigation in Spain should be taken into account, at least, the following requirements we propose below.

---

43) See the Agreement of the TS from 23 February 2010, ratified by the STS from 18 March 2010.

44) See O. Morales García, 'Delincuencia informática: problemas de responsabilidad', 9 *Cuadernos de Derecho Judicial* (2002) 28.

45) Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters (OJ L 350, 30.12.2008, p. 72).

46) OJ C 165/22, 24 June 2010.

4.1. *A Prior Judicial Authorization*

The access to the content of the various types of electronic equipment, with the purpose of monitoring and collecting information stored in them, should be conditioned to a prior judicial authorization, which would reasonably justify the opportunity and proportionality of the interference in the sacrificed fundamental right. And this, irrespective of the information stored on such equipment, which is trying to be acquired, has nothing to do with the content of communications, the circumstances in which they took place or the external traffic data generated from them, not even in the case of intimate data of the passive subject of the performed action (Articles 18.1 and 18.3 CE) or if the computer to which access is sought is or is not located at the suspect's house (Art. 18.2 CE).

In Spain, the need for a judicial decision has been made dependent on the Fundamental Right affected, distinguishing observable warrantees, hinging on affected right is the fundamental right to privacy enshrined in Art. 18.1 CE or the secrecy of correspondence in Art. 18.3 CE. In accordance with the sentences of the Constitutional Court of Spain (STC) no. 70/2002, from 3 April, and no. 123/2002, of 20 May, *Art. 18.3 CE contains a special protection of communications, whatever system is used to perform these communications, which is declared unharmed against any judicially unauthorized interference*, to which the Court adds a specification that *the protection of the right to secrecy of correspondence goes with the trial constructed for communication itself, but ending the process in which the problem of communication is judged, the constitutional protection of the data acquired is made in such case through the rules that protect the privacy or other rights and freedoms*. Therefore, *according to Art. 18.3 CE, the intervention in communications requires always a judicial decision, but in the Constitution there does not exist an absolute provision of a prior judicial decision regarding the right to privacy (Art. 18.1 CE). But, also in regard to the right to privacy we have said that the constitutional requirement of judicial monopoly governs, as a general rule when concerning the limitation of fundamental rights, although we have admitted that exceptionally in certain cases and with sufficient and accurate legal empowerment and development, it should be possible for the police to perform determined practices which could constitute a slight interference in the privacy of individuals*.

There are several authors who have highlighted the lack of a prior judicial decision in the fundamental right enshrined in Art. 18.4 CE,[47] which could be understood permissible, exceptionally, in cases of police action without prior

---

[47] See F. Hernández Guerrero, 'La intervención de las comunicaciones electrónicas', 3 *Estudios Jurídicos. Ministerio Fiscal* (2001) 350 et 391; M. Marchena Gómez, *loc. cit*., 105; F. Bañuls Gómez, 'Las intervenciones telefónicas a la luz de la jurisprudencia más reciente' 2007, available at: <noticias.juridicas.com>.

judicial authorization, when it is deemed necessary for the prevention and crime investigation, the detection of criminals and attainment of the incriminating evidence. However, we reject the applicability of remote searches to this doctrine on police intervention as a prevention and it should be based on exceptional cases of urgency, for several reasons.

First, because to allow such police behaviour there are certain requirements demanded which are absent in the case of remote searches. The access to information contained in any electronic device cannot be considered as minor in the field of personal privacy (there exists a sufficient and precise legal empowerment; that such police practices should constitute only a slight interference in the privacy of individuals; and that such behaviour should be carried out with the respect of the principle of proportionality). If, moreover, we refer to the course of action of such infiltration, which is secret and remote, in a suspect's computer, by using its various connections to the communication networks, we would be capable of affecting, restricting, and cancelling, completely, the privacy of a person, entering to the depths of their ideas, thoughts, tastes, phobias, etc., which, in any case, should be under the control of the judicial powers. These powers must be activated in an adequate manner if there is the need to reach for this grievous measure, or, the intervention in communications of the suspect itself.

Second, we must take into consideration the necessary information that needs to be at the police disposal from the outset before the police can 'connect' with the computer equipment in order to search remotely. Due to the mobility and allocation of such electronic devices that do not need a 'Postal address' from which they may be operating, the police might not know the domicile or residence of the suspect, and it may even be irrelevant for the police to know the place from where the bills are being sent, for that individual (suspect). The decisive thing is to know the connection details of the computer in relation to the Internet (e.g., the IP address used), or geographical location in the case of a mobile phone or a computer that accesses the network through the mobile broadcast terrestrial repeaters. And, for the acquirement of such data a judicial order is required – as it is established in the Law 25/2007 and has been confirmed by the Supreme Court.[48]

Finally, we cannot omit the argument used by the German Constitutional Court in its judgement of 2 March 2010,[49] which abolished the German Law that had transposed into the German legislation the Directive 2006/24/EC relating to preservation of the traffic data of electronic communications. This had explicitly

---

48) STS from 28 March 2010.

49) BVerfG, 1 BvR 256/08. For a more detailed discussion comparing German cases with the Spanish Law, see J. C. Ortiz Pradillo, 'Tecnología versus Proporcionalidad…' *loc. cit.*

stated that the storage of telecommunication traffic data, however must not detain the content of the communication, from analysis and comparison with other data, it must show the intimate sphere, entail detailed conclusions about the personality and even the movement outlines of a person, and 'since an analysis of this data permits penetration into a person's private life, it can no longer be assumed that the use of this general information has lesser interference than the interception of the content of the communication (F. J. no. 227)'. In other words, the doctrine according to which the attainment and use of the traffic data is supposed to be an *interference of lower intensity* in the right to secrecy of correspondence expressed in Art. 18.3 CE should be revised, concerning the acquirement of their content.

4.2. *Secret Character*

Similar to the interception of communications, the implementation of a remote searching must be secretly adopted, because it would become ineffective if the passive subject were to be previously informed on the action to be executed. For that reason, the provisions of the arts. 566 and 569 LECrim should not be applicable (notification of the order authorising the entry and search to the person concerned, and the carrying out of the registration in the presence of the person concerned). Therefore, the adoption of this measure should be accompanied by the subsequent declaration of secrecy *sub iudice*, either in the same authorising court order, or in other coetaneous acts, although the Supreme Court – regarding wire-tapping – has accepted the validity of evidence obtained when there had been no expressly stated declaration of '*sub iudice*' with a prior character, considering that *the secret, even if not expressly adopted, is inherent in the nature of the wire-tapping and that the mentioned secret of the sub iudice should be understood as extended for the time of the duration of the intervention in communications.*[50] However, the Circular 1/1999, of 29 December, of the Public Prosecutor's Office (Fiscal General del Estado) gives more guarantees in this matter, indicating that *if the use of those instruments had been agreed upon without having declared at the same time the secrecy of the proceedings, such declaration should be urged by the Prosecutor, as otherwise unconstrained access to the proceedings could not be prevented and all this with an infringement of the right to defence of the passive subject. For the same reason, if it is the Prosecutor who seeks the measure for intervention in telephone communications, he needs to press for this at the same moment when the secrecy of* sub iudice *is declared*.

---

50) See the SSTS from 4 November 1994, 8 June 2000 and 30 January 2003.

4.3. *Duties of Cooperation of Third Parties*

The ability to remotely access a computer to record and extract portions of the stored digital information is a particularly complex task that requires the collaboration of others, and particularly, of the private sector and of the operators who explore public networks of electronic communications or render electronic communications services available to the public in accordance with the provisions of existing regulations of the telecommunications in Spain. For example, to access a computer it may be necessary to know how it functions, or if it possesses measures to protect such access (antivirus, firewalls, etc., which could detect spyware sent by the authorities). The law provides with certain obligations, for the various persons involved in the provision of telecommunications, telephonic and electronic services that could be extrapolated at the time when carrying out a remote search of computer equipments, as essential duties for the success of the measure.

4.3.1. *Duty of Conservation and Transfer of Data*

From the catalogue of data listed in Art. 3 of the mentioned Law 25/2007, the data being claimed by the police will depend on the device being inspected, but will refer mainly to the 'necessary data used to identify the type of communication' (Art. 3.1.c), for example, if the person investigated uses an ADSL line or a Wi-Fi, i.e., 'Data needed to identify the communication equipment of the users or what is considered to be communication equipment' (Art. 3.1.e), and 'Data necessary to identify the location of mobile communication equipment' (Art. 3.1.f). Moreover, within this duty of data conservation must also be included a duty, on the part of operators of mobile telephony services who commercialize the services by a stimulation system through the form of prepaid cards, by keeping a logbook in which are reflected the full name and nationality of the purchaser and the number of the identity document used and the kind and description of the document in the case of natural persons, and the number of tax identification card and the names, if concerning legal persons.

4.3.2. *Duty of Prior Information*

Before proceeding to the interception of a particular electronic communication, arts. 89 and 90 of Royal Decree 424/2005 establish a list of data with which the obligors shall provide the authorized agent prior to the interception, and referrals to services and features of the telecommunications system used by the subjects who under the measure of interception. These rules referring to prior information should also be considered applicable to cases in which it is intended to carry out a computer's remote search of the passive subject of the measure performed.

4.3.3. *Duty of Material Carrying Out the Interception*

The practical performing of interception of communication, telephone or electronic, is not carried out directly by the judicial police, but the operating companies themselves, who have the duty to conduct court authorized interceptions and send them through an interface of transfer to the reception centres of those, according to Art. 33 LGT (General Law of Telecommunications) and the Arts. 17.h) and 95 of Royal Decree 424/2005. Nevertheless, if it is used to try to send a spy program to equipment meant to be inspected, in order to gain control and submission of certain information to another computer (the computer from the police), the operators would not have to bear the obligation to materially carry out this measure, but only to enable and maintain the connection between the investigated equipment and the equipment receiving the information, while the connection depends on them, for as long as deemed necessary.

4.3.4. *Duty of Confidentiality*

Operators must maintain the secrecy in respect of the intercepted communications, the affected individuals, or the timing and duration of such interventions. And besides, *the interception must be done so that neither the subject of the interception, nor any unauthorized person may have knowledge of it. In particular, the performance of the service must be the same as in the absence of interception, and no alteration of it should raise suspicions that an interception is being carried out* (Article 93.2 of R.D. 424/2005). Extrapolating this obligation to the assumption of remote searches of computer equipments is one of the most difficult issues to resolve in practice. This must be resolved without raising any suspicions on the part of the passive subject of the action that the equipment has been an object of an access without the subject's consent and that certain information is being sent or has already provided certain information through the network (a slowdown of the operating system, installed software detection, detection of the information received, the time and destination of the communication, etc.).

In the absence of a specified period during which such secrecy should be kept by others, we understand that they must remain silent as long as they are not authorized otherwise by the authority conducting the criminal investigation, and in any case, for the duration of the *sub iudice* secret, since once it is revealed, the passive subject of the measure will be entitled to know the interferences suffered in the field of its computer privacy.

4.3.5. *Duties of Cooperation and Technical Assistance*

Finally, the duty of cooperation and technical assistance by the operators is also important, for example, to prevent a situation in which the Trojan fixed in the equipment inspected could be discovered by the defence of such equipment, as

well as in decoding the communications of the suspect or the data stored on his computer. Art. 36.2 LGT requires the operating companies to provide the authorities with algorithms or any other encryption procedures used, and the obligation to provide, at no cost, decoding devices for the purposes of control under the current regulations. Article 96 of Royal Decree 424/2005 establishes for the case in which operators are to apply for communications subject to a lawful interception a procedure of compression, encryption, digitalization or any other encoding, the duty to deliver such communications, devoid of the effects of such procedures and then shall forward the intercepted communications to the centre receiving them, with a quality not inferior to that obtained by the recipient of the communication.

Similar duties of provision to the authorities of the encryption and decryption devices should be enforceable in the case of remote searches, while it would be worth discussing whether such duties should also include the delivery of software which facilitates obtaining and decryption of the keys, codes or passwords of the subject investigated. For example, Art. 90.d) of R.D. 424/2005 includes, within the data as background information, to facilitate the lawful interception of communication, 'the identification code if the user is to activate the terminal for communication'. Despite this, it is unclear whether there is an obligation for operators or service providers, to provide authorities with those computer programmes meant to locate and decipher codes or passwords. In the digital environment, would this duty be redirected to the obligation imposed by Art. 575 LECrim that *Everyone is obliged to display the objects and papers that are suspected to be related to the cause*? Art. 19.4 of the Cybercrime Convention allows the competent authorities to order any person who has knowledge about the functioning of the computer system or knows the applied measures to protect the computer data therein, to provide the necessary information to enable searching of the equipment, so it could be defended that the operators might be forced by threat of taking a legal action in order to make them facilitate those keys of which they have knowledge.[51]

---

[51] See the Explanatory Report of the Cybercrime Convention, at para. 200: … *It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted. This provision, therefore, allows law enforcement to compel a system administrator to assist, as is reasonable, the undertaking of the search and seizure*). Against, see S. Marler, 'The Convention on Cyber-Crime: Should the United States Ratify?', 37 *New England Law Review* (2000) 201): *the Convention will allow authorities to require individual persons to disclose their passwords, which allow them to access various encrypted material and databases. The Convention achieves this forced disclosure by requiring each signatory State to pass laws that guarantee "any person who has knowledge about … measures applied to secure computer data can be ordered to "provide all necessary information' to allow law enforcement to access that data*".

4.4. *Reasoned Order*

The judicial resolution which allows the limitation of any fundamental right must be sufficiently motivated to show 'the set of reflections that led the judge to make the decision he took, including assumptions of undetermined legal concepts'.[52] Such reasoning is a prerequisite for the constitutionality of the interference, to assess whether or not it is proportional, because *the breach of duty of motivation suggests that the court has not made the necessary counterweight to the competing interests in the particular case. Lack of motivation is a symptom of excess, which reflects the lack of respect of the body acting for fundamental rights for the individual, and that forces us to consider the disproportional restriction.*[53] It should also be noted that where judicial decisions limit a fundamental right, the motivation required exceeds the general duty of inherent motivation for effective judicial protection, because "it needs to find a specific cause, and the fact or reason justifying it has to be explicit, to make known the reasons why the right was sacrificed. For that reason, the reasoning for the act of limitation, in the double sense of expressing the legal grounds on which the decision and reasoning taken to reach it are based, is an indispensable requirement for the act of limitation of a certain right act".[54]

In the judicial authorization needed to proceed with the remote search of a computer equipment, would be demanded the same requirements of reasoning, content, duration, persons affected, etc., as those declared by the jurisprudence required for wire tapping, but according to the particular characteristics of the means in which the action is performed and the objective to achieve with such search.[55] Thus, for example, for the remote search of a computer, the legal requirements can be extrapolated for the occasion of searching the accounting books and papers of the accused or other person[56] (to avoid 'unnecessary inspections' and 'not to harm or intrude the subject more than necessary and not to compromise the subject's reputation' – Art. 572 LECrim, the existence of a suspicion of the commission of a crime based on objective data, reasonable grounds for suspicion, subsidiarity and proportionality of the measure, the probability of founding effects or instruments of crime or verification of any facts or circumstances of the case – Art. 573 LECrim, or that the collection of data is 'necessary to the outcome of the investigation' – Art. 574 LECrim).

---

52) See STC 62/1982, from 15 October, and ATS from 18 June 1992.

53) N. González-Cuéllar Serrano, *Proporcionalidad y derechos fundamentales en el proceso penal* (Madrid: Colex, 1990), p. 146.

54) Among all, see SSTC 29/2001, from 29 January, and 138/2002, from 3 June.

55) For all, see the STS from 30 January 2002, No. 1844/2002.

56) See N. González-Cuéllar Serrano, *loc. cit.* (2006), p. 895.

We must also bear in mind the necessary relationship that must exist between motivation and proportionality, in the terms expressed in the well-known ATS from 18 June 1992: *greater importance of the decision, greater demand, if possible, in respect of foundation and motivation*. Assuming that the essential motivation to permit intervention in telephone conversations must be sufficiently precise and clear, is a measure that is one of the most serious interferences in the privacy of an individual, the motivation required to arrange entry and remote search of the computer and electronic devices must contain a measurable advantage, because that search is a much greater interference than that committed to obtaining the knowledge of the postal and telegraph correspondence, or eavesdropping of a person, and this should adhere to the secrecy of its performance. The measure of investigation consisting of online access to electronic and computer equipment in order to obtain the information stored in them would unite into a single measure capable of different actions carried out with the interception of communications, obtaining traffic data generated during these communications, with the entry and search of a house or private dwelling, and the seizure of computer equipment. For that reason, given its capacity to attain knowledge including the last glimmer of human thought and allowing the formation of an x-ray of the personality of the investigated subject, from the heterogeneity of the information that may be stored in the computer and electronic equipment by citizens, the motivation required to agree on an online search needs to be superior to those required for the measures implemented so far.

4.5. *Exceptionality: Particular Seriousness of the Crimes*

The massive interference that a remote search concerning fundamental rights to privacy, and particularly the protection of the individual *Habeas Data*, together with its secret character, provides as a consequence the need to render clear the exceptional nature of the application of this measure.

By exceptionality it should be understood, on the one hand, the natural need within the principle of proportionality of any measure restricting fundamental rights, according to which a remote search could be carried out only when there does not exist any other means of investigation adequate for the detection of the crime and its author, which is of a minor impact or hardship when it comes to the rights and freedoms of the individual (e.g., in cases where the police cannot physically access the computer to investigate), because the physical obtaining of the source of evidence turns out to be preferable to having remote access to its contents, especially as the online access will require prior preparation – preparation and sending necessary software, removing any potential barriers or firewalls to make the connection to such equipment, etc. – that in cases of urgency, can thwart the success of the operation. On the other hand, the exceptionality of the use of remote

searches needs to be explained by the argument that this measure is limited to the investigation of 'serious crimes'.

However, what should we regard as a 'serious crime'? The development of a legal catalogue of crimes in which this exceptional measure of investigation would be admissible presents itself as a possibility, especially after checking that the sentences on Spain by the ECHR regarding our legal regulations concerning the interception of telephone communications were based, inter alia, on the absence of a statutory list of crimes which supports the use of this measure.

Unlike other European legal systems where the possibility of agreeing on the interception of communications is usually made dependent, with a reference to a list of crimes, or on the case of the punishment,[57] in Spain there is not the slightest intention to defining legally what is considered to be a 'serious crime' for the purpose of sheltering certain investigative measures restricting fundamental rights, and Courts take into account, not only the punishment, but also certain criteria, such as weighing up the protected legal goods, or the social relevance of the facts, or "the incidence of the use of information technology, both for the commission of the offence and for obstruction to its persecution".[58]

We consider that it is appropriate to give some margin of appreciation to the judge to assess the proportionality of its application, regardless of the existence of a list of offences or function of punishment, in the way that agrees with the specific circumstances of the case, but always through the prism of a restrictive interpretation of the conditions under which the remote search of the contents of the computer equipments could be ordered, according to the constitutional mandates and principles, as the commission of any crime, not just strictly computer crimes, can be reflected digitally.

4.6. *Inevitable Discoveries, Plain View Doctrine and the Digital Evidence*

The importance of specifying the assumptions and the scope in which a remote search of the data stored in computer equipments (either by a legal list of crimes, or in the authorizing court's order) is essential, because as in wiretapping, the *principle of specialty* of the investigation should be governed. This requires that in the resolution that determines the adoption of the measure, an identification of the crime it makes it necessary to investigate shall be included, in order to evaluate the concurrence of the required proportionality of the decision, and avoidance of

---

57) See, Arts. 100a y ss. German Code of Procedure (StPO); Art. 100 French Procedural Code, or Art. 266 Italian Code of Criminal Procedure.

58) About the use of Information Technology in order to facilitate the commission of the crime and impede its prosecution, see, STC 104/2006 from 3 April.

indiscriminate 'searches' of a solely preventive or random character, without factual background of the commission of a certain crime.[59] But, above all, because of its significance, in the case of detection of other crimes with the aim of carrying out the implementation of the measure; if remote and secret access to the contents of a computer equipment is authorized under the reasonable belief that its owner (or anyone using it) is spreading child pornography through the Internet, and because of that searching, information that reveals a pattern of fraud against the Public Treasury is revealed, should the case law relating to inevitable discoveries be applied?

In the United States, several federal district courts and state courts have applied the *plain view doctrine* to the admitting of digital evidence found outside the technical scope of a warrant. The plain view doctrine is an exception to the Fourth Amendment that allows the police to use evidence found during the execution of a warrant that is technically outside the scope of the warrant. "To satisfy the plain view doctrine: (1) the officer must be lawfully in the place where the seized item was in plain view; (2) the item's incriminating nature was immediately apparent; and (3) the officer had a lawful right of access to the object itself."[60] This has been criticized and questioned by some authors on the grounds that *Police cannot see digital property directly. When police look at a hard drive, they cannot interpret the magnetic charges on the surface of the disks with their bare eyes. Police cannot see whether digital property is evidence of a crime without electro-mechanical assistance. One bit 'looks' much like another bit until a machine reads a digital property storage device and a program, which is also a set of bits, translates the digital property into a perceivable form that may or may not represent the true nature of the digital property. Plain view considerations make digital property's special characteristics even more apparent. Is it really plain view if police must "open" every "file" on a digital storage device in order to see what data is really contained within that file? Is it really plain view if one has to reconstruct the bit structure of a file? Are "hidden files" really in plain view? What if file tables contain incorrect information? When forensic specialists reconstruct files and recover data that a person might assume is permanently deleted, is that plain view? What about file size? After all, the size of a file does not accurately predict its contents; a one kilobyte (1K) file containing child pornography is just as illegal as a one hundred megabyte (100MB) file containing child pornography.*[61]

In Spain, it is possible to distinguish two different types of case law: the one relating to searches of houses or private dwellings, and the one concerning the

---

59) Vid. SSTS de 3 de junio de 2002; 19 de septiembre de 2004 y 29 de enero de 2008.

60) See *United States* v. *Beatty*, 170 F.3d 811, 838 (8th Cir. 1999) (citing *Horton* v. *California*, 496 U.S. 128, 136–137 (1990)).

61) See C. RayMing, 'Why the Plain View Doctrine should not apply to digital evidence', XII *Journal of Trial & Appellate Advocacy* (2007) 32–67. Electronic copy available at: <ssrn.com/abstract=949575>.

wiretaps. In the first case (concerning house searches) the STS of 30 March 1998, recalls that "it has been imposed on the doctrine of this court a favourable position on the legality of the investigation of those other criminal conducts arising from the findings occurred in legally authorized searches (Sentences of 4 October 1996, 25 April 1996 and 3 October 1996). It cannot be continued, as pointed out the Sentence of this court of 8 March 1994, the same approach as in the case of a wiretap. With reference to this one, by its very nature, the prolongation of time that allows eavesdropping in cases concerning other criminal actions, an extension of enabling judicial authorization, is presupposed. The same does not occur with the entries and searches, which are characterized by their realization in a single act, that's why in their practice appear objects constituting a possible crime other than that for which, the authorization was extended, such detection places itself it the notice of flagrance. Nothing prevents, then, that in the procedure of searching evidence of a crime other than that for which investigation was initially granted may be obtained, especially when such evidence could have been obtained through a judicial authorization of entry and search which is what has happened in these cases".[62]

Regarding the wiretaps, the well-known ATS of 18 June 1992 (*Naseiro* case) reasoned that 'regarding the problem of divergence between the crime under investigation – child pornography – and the one that is actually discovered by tapping – fraud –. (…) it would be sufficient that the police reported immediately to the judge in order that the magistrate, knowing the concurring circumstances, can resolve it appropriately. As the Intervention of communications in real/current time does not take place in a single act, the police should request for a second judicial order extending the scope of the investigation to the fact discovered, if it is a crime of such gravity that it would legitimize the adoption of a limitation of fundamental rights, so as not to proceed, because the mentioned communication to the investigating judge for the expansion of the investigation, the evidence data obtained would lack effectiveness.[63]

When it comes to remote computer searches, the criteria to be applied would be that applied to house searches, since access to the investigated equipment takes place in a single act (the act when the police 'send' the spy programme to the suspects' computer), irrespective of the duration of the collection of information, unless the spyware allows the possibility of sending several shipments of data at different times. And when analyzing the information obtained, *it cannot be expected from*

---

62) In the same direction, see SSTS from 1 December 1995, 25 April 1996, 1 February and 18 June 1999, 3 December 2002, 3 and 24 July 2003. About the Spanish Constitutional Court case-law, see the STC 41/1998, from 24 February.

63) See SSTS from 8 October 1992, 8 July 1993 and 21 January 1994.

the police officers to close their eyes to the evidence of a crime which may be presented to their sight, although incidentally found to be different from the facts contained in its official investigation, provided that it is not fraudulently used to flout the guarantees of fundamental rights.[64]

For that reason, a possible solution to avoid indiscriminate searches would be the prior establishment of rules or patterns of investigation to carry out actions concerning different data storage devices, depending on the facts investigated by the police and which have been exposed, in its request for the adoption of judicial authorisation; the intervention of a different and separate group of officials to those who conducted the investigation, to examine the files and separate the information subject to secrecy and the one that can be revealed, or the attribution of the work of filtering the stored information to a third party ('special master') in order to exclude confidential data. This is the procedure followed in the USA when agents seize a computer that contains legally privileged files. A trustworthy third party must examine the computer to determine which files contain privileged material. After reviewing the files, the third party will offer those files that are not privileged to the prosecution team. However, there are three options:[65] First, the court itself may review the files *in camera*. Second, the presiding judge may appoint a neutral third party known as a 'special master' to the task of reviewing the files. Third, a team of prosecutors or agents who are not working on the case may form a 'filter team' or 'taint team' to help execute the search and review the files afterwards. The filter team sets up a so-called 'ethical wall' between the evidence and the prosecution team, permitting only unprivileged files to pass over the wall.

However, the civil courts in Spain have already admitted the use of 'blind searches' in the reports of experts tracking down certain files to be appropriate, proportionate and not contrary to the privacy of the suspect.[66]

4.7. *Authentication of Computer Stored Records and Availability of the Evidence*

One of the most difficult issues to solve in practice is, along with the method of proceeding to access the computer to investigate, is to ensure the authenticity and integrity of the information attained, in the manner that there are no doubts about its possible alteration during the process of searching and collection, or its

---

64) STC 41/1998, from 24 February.

65) See the Manual *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Computer Crime and Intellectual Property Section Criminal Division*, published by Office of Legal Education Executive Office for United States Attorneys (1009) 110. Available at: <www.cybercrime.gov/ssmanual/ssmanual2009.pdf>.

66) See the Decision (Auto) of the Audiencia Provincial (AP) of Barcelona, sec. 15, from 2 February 2006 (No. appellation 711/2005) and Sentence from 9 May 2008 (No. appellation 189/2007).

subsequent modification by computer experts who would analyse that information. Obtaining digital data from a distance will take place through a *live acquisition*, so the result will the same as when it comes to a device that cannot be disconnected in order to proceed with making a clone copy or 'forensic image' of its hard drive (e.g., a bank's online web server or a computer controlling the operation of a nuclear plant). Due to this, the image produced by means of a live acquisition will be blurry: since the computer is turned on and running, it is constantly creating, modifying and deleting files as the forensic image is being created. The result will be a blurry picture, where each area of the picture (forensic image) will reflect the state of a particular area from the original hard drive, at the precise moment when it was being copied. Taking into account that a forensic copy can take hours, that could be a very blurry picture indeed, and apart from that 'blurriness', live acquisitions present another, and even more serious problem: the installation of a software tool in charge of generating the image would mean that the crime scene is contaminated by the introduction of an external agent.[67]

These questions must be taken into account when considering the admissibility of such evidence and its legal implications. Therefore, as well as having the developed technology to carry out such investigative measures, it is essential to have performance protocols and working standard methods[68] to ensure the integrity and authenticity of the information obtained and dispel any doubts about its possible 'taint', including the possible introduction of such evidence in the investigated device through the software used by the authorities, because we must not forget that in the case of a remote search the original source of the evidence is not possessed (the computer remotely inspected). Thus, as in the field of wire-tapping a previous judicial order, stating exactly, the precautions to record completely and uninterruptedly, with the aim of possible control both by the judge and the defence, as well as the circumstances in which it can or should be carried out, the erasure or destruction of the conversations, is required. In case of a remote access to electronic devices and the subsequent obtainment of the information stored on them, the judge shall indicate in detail the requirements to be met by those who

---

67) See M. Bevilacqua, 'Seizing and Analysing Electronic Evidence in Practice', in *Syllabus. Cybercrime and Electronic Evidence* (Barcelona, published by Cybex experience S.L. and the European Commission, 2009), p. 86.

68) See M. Meyers and M. Rogers, 'Computer Forensics: The Need for Standardization and Certification', 3 *International Journal of Digital Evidence* (2004). Specifically referred to live acquisitions, see the document *Capture of Live Systems*, group SWGDE (available at: <www.swgde.org/documents/swgde2008/SWGDELiveCapture.pdf>); E. Casey and A. Stanley, 'Tool review – Remote forensic preservation and examination tools', 4 *Digital Investigation* (2006), pp. 284–297; R. Koen and M Olivier, 'An evidence acquisition tool for live systems', in *Advances in Digital Forensics IV* (Boston: Publisher Springer, 2008), pp. 325–334.

are to make the access, collection of the data and subsequent analysis, so that the attained data would constitute a true and unaltered copy of the ones existing in the memory of the device at the time of the search. And for this, the applicant for the measure (e.g., the public prosecutor or police) should explain earlier to the judge the functioning of this technology, the information which he can obtain through it, as well as the safeguards which guarantee the authenticity of data obtained. That will enable, if the need arises, an independent third party to validate that the included software does what it is supposed to do, and nothing else.

On the other hand, such an investigatory measure would require two consecutive expertises: first, consisting of obtaining remotely the data stored in the equipment investigated, and the second, an expertise relating to analysis of content, which would include the recovery of hidden, encrypted, or deleted archives. Therefore, it would be advisable that such expertises were carried out by different experts, and both experts would deliver their report in an oral cross examination and subsequently submit those reports to the necessary contradiction between the parties. The experts responsible for carrying out the secret infiltration in the investigated device and the collection of data stored in it should explain in their report, as provided in Art. 292 LECrim *et seq*., the manner in which they obtained the exact copy of the seized data, along with the applications used and steps taken to obtain such information.

Acquiring data from live systems requires additional planning and management of resources, and of course, advanced training and tools to accomplish the desired results while minimizing the possible destruction of data or hardware, but it also provides important benefits: Additional data is captured that will not be available when conducting a static acquisition. The ability to capture data from a running system allows the system to continue serving its data. While the static acquisition of a system may be desired, the pros and cons of each method must be weighed to conform to the limitations encountered while conducting the search.[69]

---

69) See the document *Capture of Live Systems*, *loc. cit*.