http://dx.doi.org/10.12775/CLR.2018.010

Duarte Rodrigues Nunes*

THE MEANS OF OBTAINING EVIDENCE PROVIDED BY THE PORTUGUESE CYBERCRIME LAW (LAW NO. 109/2009 OF 15 SEPTEMBER 2009)

Abstract

The Portuguese legislator has provided, for the first time, in the Portuguese legal system, means of obtaining evidence specific for Cybercrime in Law no. 109/2009, of September 15, in which Framework Decision no. 2005/222/JHA, of the Council of February 24, concerning attacks against information systems and the Convention on Cybercrime of the Council of Europe were transposed to the Portuguese legal system. While the legislator's options are considered to be mostly correct, there are some critical issues. In the present Article, the legal regime of these means of obtaining of evidence is critically analyzed.

Keywords

Cybercrime – Criminal investigation – Computer data – Interception of communications – Seizure – Computer search.

Introduction

The Portuguese legislator has provided, for the first time, in the Portuguese legal system, means of obtaining evidence specific for Cybercrime in Law no. 109/2009, of September 15[1]. Through this law, Council Framework

* Judge. PhD in Criminal Law and Criminal Procedure. Investigator (Centre for Research in Criminal Law and Criminal Sciences and Centre for Legal Research of Cyberspace, Faculty of Law of Lisbon). Author. E-mail: duarterodriguesnunes@hotmail.com.

Decision 2005/222/JHA of February 24 on attacks against information systems and the Convention on Cybercrime of Budapest, of November 23, 2001, were transposed to the Portuguese legal system.

Although the 2007 reform[1] of the Code of Criminal Procedure (*Código de Processo Penal*)2 and the means of obtaining evidence provided by the Code of Criminal Procedure (clearly designed to obtain "tangible" evidence) were inadequate to effectively investigate computer-related crimes, only in 2009 the legislator provided means of obtaining evidence specific to investigate Cybercrimes.

Thus, until then, means of obtaining evidence provided by the Code of Criminal Procedure – such as searches and seizure, although they were designed to focus on tangible realities and not on intangible realities such as computer data[3], or interceptions of telecommunications – , were the only means of obtaining evidence used to investigate this kind of criminal offences.

Unlike the majority of states that signed the Convention on Cybercrime, the Portuguese legislator chose to draft a new law which provided the means of obtaining evidence instead of providing them in the Code of Criminal Procedure[4].

I. Scope of the rules on the means of obtaining evidence

In accordance with Article 11 of Law no. 109/2009, except in the case of the interception of communications and undercover operations (which

---

Hereinafter referred to as Law no. 109/2009. The text of Law no. 109/2009 available at: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=*leis* (in Portuguese only).

[1] Through Law no. 48/2007, of August 29.

[2] The text of Portuguese Code of Criminal Procedure is available at: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis (in Portuguese only).

[3] Defined in Article 2, b) of Law no. 109/2009 as "any representation of facts, information or concepts in a form susceptible of processing in a computer system, including programs capable of making a computer system perform a function".

[4] However, there is nothing to prevent the use of means of obtaining evidence provided by the Criminal Procedure Code in the investigation of Cybercrimes.

may only be used in the investigation of criminal offences referred to in Article 18, paragraph 1, and Article 19, paragraph 1, of Law no. 109/2009, respectively), the other means of obtaining evidence may be used to investigate criminal offences punishable under Law no. 109/2009[5] and any criminal offences committed by means of a computer system[6] or criminal offences which investigation requires the collection of evidence in electronic form.

And in paragraph 2 of this Article 11, the legislator determines that the provisions of Articles 12 to 19 of Law no. 109/2009 do not affect the regime of Law no. 32/2008 of July 17 (on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks)[7]. This is a rule that raises enormous interpretative difficulties, since it does not clarify whether Article 9 of Law no. 32/2008 (which regulates the use in the criminal proceedings of data previously retained[8]) was or was not revoked by Articles 12 to 19 of Law no. 109/2009[9], and Article 9 of Law 32/2008, which only applies to serious crimes, provides a regime of use of retained data much more restrictive than the regime of Articles 12 to 19 of Law no. 109/2009, which apply to a much broader range of criminal offences.

---

[5] Crimes of computer-related forgery, damage to programs or other computer data, computer sabotage, illegal access, illegal interception and illegitimate reproduction of protected program.

[6] Defined in Article 2, a) of Law no. 109/2009 as "any device or set of interconnected or associated devices in which one or more of them develops automated processing of computer data in connection with a program network that supports the communication between them and the set of computer data stored, processed, retrieved or transmitted by that or those devices with a view to their operation, use, protection and maintenance".

[7] Hereinafter referred to as Law no. 32/2008. The text of Law no. 32/2008 available at: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=1264A0004&nid=1264&tabela=leis&pagina=1&ficha=1&so_miolo=&nversao=#artigo (in Portuguese only).

[8] The categories of data that is object of retention are referred in Article 4 of Law no. 32/2008.

[9] In this respect, it is understood mainly that Article 9 of Law no. 32/2008 was not revoked by Articles 12 to 19 of Law no. 109/2009. A minority opinion (which we endorse) has the opposite view. On this issue, see Duarte Rodrigues Nunes, *Os meios de obtenção de prova previstos na Lei do Cibercrime* [*The means of obtaining evidence provided by the Law of Cybercrime*], Gestlegal, Coimbra, 2018, at p. 24–32 (with bibliographic references).

II. Expedited preservation of stored computer data (Article 12 of Law no. 109/2009[10])

The expeditious preservation of stored computer data consists in giving an order to who has the availability or control over any specific computer data, which already exists in a stored form, to take the necessary measures for protecting them from anything that might alter or deteriorate its quality or condition, keeping the data safe from any modification, damage or elimination, in order to enable the competent authorities to seek its disclosure.

The person who receives the preservation order must immediately preserve the data in question, protecting and preserving its integrity for the time set, in order to enable the competent judicial authority to obtain the data and is obliged to keep confidential the undertaking of such procedural measure[11].

The order must be given by the judicial authority[12] or by the criminal police with the authorization of the competent judicial authority or in exigent circumstances, in which case the criminal police should inform

---

[10] The expedited preservation of computer data is also provided by Article 16 of the Convention on Cybercrime.

[11] See Article 12, para. 4, of Law no. 109/2009.

[12] Combining Article 12, para. 2, of Law no. 109/2009 with Article 1, b) of the Code of Criminal Procedure (which contains the legal concept of "judicial authority"), the order must be issued by the Public Prosecutor in the inquiry phase, by the Examining Judge in the preliminary judicial phase and by the Judge in the trial phase. The Portuguese criminal procedure consists of four phases, two obligatory and two optional. The first phase is the inquiry (*Inquérito*), after which, a decision will be made to submit (indictment), or not (discharge), the defendant to trial. This decision may be challenged by means of a request for the initiation of an preliminary judicial phase, thus initiating an optional phase, the preliminary judicial phase (*Instrução*), at the end of which a new decision will be issued, in order to submit (pronunciation), or not (no pronunciation), the defendant on trial; the request for the opening of the preliminary judicial phase shall be filed by the defendant in cases where there has been an indictment or by the assistant (who, as a rule, will be the victim of the crime) when the case has been closed. If the defendant has been charged and, if there has been a preliminary judicial phase, has been pronounced, a new mandatory phase, the trial phase (*Julgamento*), will be opened. And, at the end of the trial phase, another optional phase may occur, which is the appeal phase (*Recurso*).

the judicial authority immediately and forward a report where he briefly mentions the investigations carried out, the results of the investigations, the description of the facts found and the evidence gathered[13].

The expeditious preservation of computer data is determined whenever it is of relevance to the discovery of the truth and/or for use as evidence[14], in respect of any type of crime[15].

The preservation order must discriminate (under sanction of nullity) the nature of the data to be preserved, its origin and destination (if known) and the period of time by which they must be preserved, up to a maximum of three months (extendable up to a maximum of one year)[16].

In accordance with Articles 2, b), and 12, both of Law no. 109/2009, the preservation order may include any type of computer data[17].

As the preservation order does not imply any access to preserved data, it does not restrict any fundamental right[18]. So, Article 12 of Law no. 109/2009 does not violate any provision of the European Convention on Human Rights. In addition, the Portuguese legislator complied fully with the provisions of Article 16 of the Convention on Cybercrime.

---

[13] See Article 12, para. 2, of Law no. 109/2009 in conjunction with Article 253 of the Code of Criminal Procedure.

[14] See Article 12, para. 1, of Law no. 109/2009

[15] See PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário* [*Criminal Procedure, Evidence and Judicial System*], Coimbra Editora, Coimbra, 2010, at p. 98, and Judgments of the Court of Appeal of Évora of 06/01/2015 (Case 6793/11.6TDLSB-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579 bf005f080b/847dae6b85353cb880257de10056ff4c?OpenDocument [last accessed 22/06/2018] and 20/01/2015 (Case 648/14.6GCFAR-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf280 2579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument [last accessed 22/06/2018].

[16] See Article 12, paras. 3 and 5, of Law no. 109/2009.

[17] See Pedro Verdelho, "*A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei portuguesa", in Direito da Sociedade da Informação,* VI [*The Convention on Cybercrime of the Council of Europe – Repercussions in Portuguese Law, "Information Society Law", VI*], Coimbra Editora, Coimbra, 2006, at p. 270, and Benjamin Silva Rodrigues, *Da Prova Penal*, *II* [*On Criminal Evidence, II*], Rei dos Livros, Lisbon, 2010, at p. 439.

[18] See Pedro Verdelho, "*A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei portuguesa", in Direito da Sociedade da Informação*, VI [*The Convention on Cybercrime of the Council of Europe – Repercussions in Portuguese Law, "Information Society Law", VI*], Coimbra Editora, Coimbra, 2006, at p. 270.

III. Expedited disclosure of traffic data[19] (Article 13 of Law no. 109/2009[20])

In accordance with Article 13 of Law no. 109/2009, a person who has received an expedited preservation order of computer data must indicate to the entity that has given the preservation order, as soon as it knows, other service providers who were involved in the transmission of that communication, in order to ensure that they are also subject to a preservation order. In fact, often more than one service provider may be involved in the transmission of a communication and each service provider may possess only some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication or each one of them possesses only one part of the puzzle.

The expedited disclosure of traffic data is ancillary to the expeditious preservation of data, since its purpose is only to ensure the efficacy of the expeditious preservation of data[21].

As the expedited disclosure of traffic data does not imply any access to preserved data, it does not restrict any fundamental right[22]. Thus, Article 13 of Law no. 109/2009 does not violate any provision of the European Convention on Human Rights. In addition, the Portuguese legislator

---

[19] Defined in Article 2, c) of Law no. 109/2009 as "computer data related to a communication made through a computer system generated by this system as part of a communication chain, indicating the origin of the communication, the destination, the path, time, date, size, duration or type of the underlying service".

[20] The expedited disclosure of traffic data is also provided by Article 17 of the Convention on Cybercrime.

[21] See Benjamin Silva Rodrigues, *Da Prova Penal*, II [On Criminal Evidence, II], Rei dos Livros, Lisbon, 2010, at p. 444.

[22] See Pedro Verdelho, "*A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei portuguesa*", [in:] *Direito da Sociedade da Informação*, VI [*The Convention on Cybercrime of the Council of Europe – Repercussions in Portuguese Law, "Information Society Law", VI*], Coimbra Editora, Coimbra, 2006, at p. 270.

complied fully with the provisions of Article 17 of the Convention on Cybercrime.

IV. The order for submitting or granting access to data (Article 14 of Law no. 109/2009[23])

The order for submitting or granting access to data consists in a judicial authority[24] orders a person to submit or allow the access to specified computer data in that person's possession or control, whenever it is of relevance to the discovery of the truth and/or for use as evidence[25].

Likewise, service providers may receive an order to submit or allow access to data relating to their customers or subscribers (other than traffic data or content) held by them and to determine the type of communication service used, the technical measures taken thereto and the period of service, as well as the subscriber's identity, postal or geographical address and telephone number and any other access number, data relating to billing and payment available on the basis of a service agreement or any other information on the location of the communication equipment available on the basis of a service agreement[26].

The order for submitting or granting of access to data relates to computer data (other than traffic data or content of communications) and the key to access the encryption of the data concerned[27]. The order must specify which data the submission or access is intended for[28], so

---

[23] The order for submitting or granting access to data is also provided by Article 18 of the Convention on Cybercrime, under the designation of "Production order".

[24] Combining Article 14, para. 1, of Law no. 109/2009 with Article 1, b) of the Code of Criminal Procedure (which contains the legal concept of "judicial authority"), the order must be issued by the Public Prosecutor in the inquiry phase, by the Examining Judge in the preliminary judicial phase and by the Judge in the trial phase.

[25] See Article 14, para. 1, of Law no. 109/2009.

[26] See Article 14, at para. 4, of Law no. 109/2009.

[27] See David Ramalho, *Métodos Ocultos de Investigação Criminal em Ambiente Digital* [*Covert Methods of Criminal Investigation in Digital Environment*], Almedina, Coimbra, 2017, at p. 170.

[28] See Article 14, at para. 2, of Law no. 109/2009.

that access only affects the data relevant to the investigation and there is no indiscriminate access to all data[29].

However, pursuant to Article 14, paragraph 5, of Law no. 109/2009, the order for submitting or granting access to data may not be addressed to the defendant or to the suspect who has not yet been constituted as defendant[30], in order to safeguard the privilege against self-incrimination[31].

The order for submitting or granting access to data relates only to computer data that has already been collected and stored by its holders, not including obtaining real-time computer data or the retention of future traffic data or real-time access to the content of the communications[32], which will have to be obtained by means of interception of communications provided by Article 18 of Law no. 109/2009[33].

Failure to comply with the order for submitting or granting access to data will be treated as the crime of simple disobedience[34].

---

[29] See Pedro Verdelho, *Cibercrime*" [in:] *Direito da Sociedade da Informação*, *IV* [*Cybercrime, "Information Society Law", IV*], Coimbra Editora, Coimbra, 2003, at p. 377.

[30] See Pedro Verdelho, "*A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei portuguesa*", [in:] *Direito da Sociedade da Informação*, *VI* [*The Convention on Cybercrime of the Council of Europe – Repercussions in Portuguese Law, "Information Society Law", VI*], Coimbra Editora, Coimbra, 2006, at p. 271.

[31] See Rita Castanheira Neves, *As Ingerências nas Comunicações Electrónicas em Processo Penal* [*The Interferences in Electronic Communications in Criminal Procedure*], Coimbra Editora, Coimbra, 2011, at p. 235.

[32] See BENJAMIM SILVA RODRIGUES, *Das Escutas Telefónicas*, II [*On Wiretapping, II*], Rei dos Livros, Lisbon, 2008, at p. 336, and Judgments of the Court of Appeal of Évora of 06/01/2015 (Case 6793/11.6TDLSB-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005 f080b/847dae6b85353cb880257de10056ff4c?OpenDocument [last accessed 22/06/2018] and 20/01/2015 (Case 648/14.6GCFAR-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf28025 79bf005f080b/2fbdd21285478f5f-80257de10056ff7a? OpenDocument [last accessed 22/06/2018].

[33] See Carlos Pinho, "*Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho", in Revista do Ministério Público, n.º 129* [*The interpretative problems resulting from Law no. 32/2008, of July 17, "Public Ministry Review", no. 129*], at p. 78, and Judgments of the Court of Appeal of Évora of 06/01/2015 (Case 6793/11.6TDLSB-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf280 2579bf005f080b/847dae6b85353cb880257de10056ff-4c?OpenDocument [last accessed 22/06/2018] and 20/01/2015 (Case 648/14.6GCFAR-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579 bf005f080b/2fb-dd21285478f5f80257de10056ff7a?OpenDocument [last accessed 22/06/2018].

[34] See Article 14, at para. 1 and 3, of Law no. 109/2009 and Article 348, par. 1, a), of the Portuguese Penal Code. Pursuant to Article 348, para. 1, a), of the Portuguese Penal Code,

The order for submitting or granting access to computer data may be used to investigate any type of crime[35].

Regarding professional confidentiality, pursuant to Article 14, paragraph 6, of Law no. 109/2009, the order for submitting or granting access to data may not be directed to computer systems used for lawyer, medical and banking activities and for the profession of journalist. Although only some cases of professional confidentiality are specified, we consider that Article 14, paragraph 6, of Law no. 109/2009, applies to any activity subject to professional confidentiality.

At first sight, it seems that the use of the order for submitting or granting access to data is not admissible in such cases. However, Article 14, paragraph 7, provides for the possibility of lifting of professional confidentiality. Therefore, it is possible to direct the order for submitting or granting access to data stored on computer systems used for activities subject to professional confidentiality, provided that professional confidentiality has been lifted, by permission of the Judge or, in the cases provided by law, by the Public Prosecutor[36].

It is not understandable that Article 14 of Law no. 109/2009 does not provide any special procedure in exigent circumstances as are provided

---

anyone who fails to comply with a lawful order or mandate, regularly communicated or emanating from the relevant authorities or official, shall be punished by imprisonment for up to one year or a fine of up to 120 days if a legal provision sanctions in this case the simple disobedience.

The text of Portuguese Penal Code is available at: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=109&tabela=leis (in Portuguese only). There is an English version (outdated) of the General Part of the Code available at: http://www.legislationline.org/documents/section/criminal-codes/country/9.

[35] See Paulo Da Mesquita, *Processo Penal, Prova e Sistema Judiciário* [*Criminal Procedure, Evidence and Judicial System*], *Coimbra Editora, Coimbra*, 2010, at p. 98, and Judgments of the Court of Appeal of Évora of 06/01/2015 (Case 6793/11.6TDLSB-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf28025 79bf005f080b/847dae6b85353cb-880257de10056ff4c?OpenDocument ([last accessed 22/06/2018] and 20/01/2015 (Case 648/14.6GCFAR-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f 39bf-2802579bf005f080b/2fbdd21285478f5f80257de10056ff7a?OpenDocument [last accessed 22/06/2018].

[36] On this issue, with more developments, Duarte Rodrigues Nunes, *Os meios de obtenção de prova previstos na Lei do Cibercrime* [*The means of obtaining evidence provided by the Law of Cybercrime*], Gestlegal, Coimbra, 2018, at p. 73–83 (with bibliographic references).

in Articles 12, paragraph 2, 15, paragraph 4, and 16, paragraph 2. Firstly, exigent circumstances may also arise in connection with the order for submitting or granting of access to data. Secondly, such a possibility is provided by the case of searches of computer data and seizure of computer data. Such a difference is not understandable, since the order for submitting or granting access to data is not more damaging to fundamental rights than the search of computer data or the seizure of computer data (and may even be less damaging than the search of computer data).

With respect to the restriction of fundamental rights, the order for submitting or granting access to data restricts the fundamental rights to privacy and informational self-determination protected by Article 8 of the European Convention on Human Rights[37]. Pursuant to Article 8 (2), there shall be no interference by a public authority with the exercise of these rights, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The explanatory report notes that, in the course of a criminal investigation, subscriber information may be needed mainly in two situations. Firstly, to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used, the type of other associated services used (for example, call forwarding, voicemail), or the telephone number or other technical address (for example, the e-mail address). Secondly, where a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned.

As the ECtHR emphasizes[38], "[…] *the Convention on Cybercrime obliges the States to make measures such as the real-time collection of traffic data and the issuing of production orders available to the authorities* […]. *However, such measures are, pursuant to Article 15 of that Convention, "subject to conditions*

---

[37] See *ECtHR, Benedik v. Slovenia*, Application no. 62357/14, Judgment of 24.04.2018, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%22production%20order\%22%22],%22documentcollectionid 2%22:[%22GRANDCHAMBER%22,%-22CHAMBER%22], %22itemid%22:[%22001-182455%22]} [last accessed 07/11/2018].

[38] Ibid.

and safeguards provided for under [State parties'] domestic law" and must "as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure"".

An order for submitting or granting access to data provides a less intrusive and less onerous measure which law enforcement authorities can apply instead of measures such as interception of content data and real-time collection of traffic data, which must be used only to investigate serious offences (Articles 20 and 21 of the Convention on Cybercrime)[39]. And because Article 14 of Law no. 109/2009 does not include access neither to traffic data nor to the content of communications, the order for submitting or granting access to data does not constitute an intense restriction of fundamental rights. Thus, we consider that neither Articles 15 and 18 of the Convention on Cybercrime nor Article 8 of the European Convention on Human Rights require that the order for submitting or granting access to data depend on judicial authorization.

Thus, Article 14 of Law no. 109/2009 empowers the investigating authorities to order (1) a person in Portugal to submit specified computer data in that person's possession or control, which is stored on a computer system or computer-data storage medium or (2) a service provider offering its services in the territory of Portugal to submit subscriber information relating to such services in that service provider's possession or control. And respects the safeguards imposed by Articles 14 and 15 of the Convention on Cybercrime and Article 8 of the European Convention on Human Rights.

V. Search of stored computer data (Article 15 of Law no. 109/2009[40])

The search of stored computer data consists in the authorities access a computer system or part of it and computer data stored therein,

---

[39] See ECtHR, *K.U. v. Finland*, Application no. 2872/02, Judgment of 02.12.2008, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22\%2 2production%20order\%22%22],%22document collectionid2%22:[%22GRANDCHAMBER%22, %22CHAMBER%22],%22itemid%22:[%22001-89964%22]} [last accessed 07/11/2018].

[40] The search of computer data is also provided by Article 19 of the Convention on Cybercrime.

whenever it is of relevance to the discovery of the truth and/or for use as evidence[41]. Thus, the search may focus on all or part of the computer system or an independent data storage device.

The search of stored computer data may be used to investigate any type of crime[42].

The search of stored computer data is authorized by the judicial authority (who, whenever possible, shall be present during the search)[43], and the authorization has a maximum period of validity of 30 days, under sanction of nullity[44].

Pursuant to Article 15, paragraph 3, of Law no. 109/2009, the search may also be conducted by the criminal police without prior authorization from the judicial authority in two situations:

a) Upon consent of any person who has the availability or control of the computer data in question (the consent must be documented); or
b) In cases of terrorism and violent or highly organized crime, when there is evidence of the imminent commitment of a criminal offence which seriously endangers the life or integrity of any person.

In both cases, a report containing a summary of the investigations carried out, the results of the investigations, a description of the facts found and the evidence gathered must be submitted to the judicial authority and, in situation b), the execution of the search must be communicated to the competent judicial authority in the shortest possible time for validation[45].

---

[41] See Article 15, para. 1, of Law no. 109/2009.

[42] See Paulo Da Mesquita, *Processo Penal, Prova e Sistema Judiciário* [*Criminal Procedure, Evidence and Judicial System*], Coimbra Editora, Coimbra, 2010, p. 98, and Judgments of the Court of Appeal of Évora of 06/01/2015 (Case 6793/11.6TDLSB-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf280 2579bf005f080b/847dae6b85353cb-880257de10056ff4c? OpenDocument [last accessed 22/06/2018] and 20/01/2015 (Case 648/14.6GCFAR-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf280 2579bf005f080b/2fbdd21285478f5f80257 de10056ff7a?OpenDocument [last accessed 22/06/2018].

[43] Combining Article 15, para. 1, of Law no. 109/2009 with Article 1, b), of the Code of Criminal Procedure (which contains the legal concept of "judicial authority"), the authorization must be issued by the Public Prosecutor in the inquiry phase, by the Examining Judge in the preliminary judicial phase and by the Judge in the trial phase.

[44] See Article 15, para. 2, of Law no. 109/2009.

[45] See Article 15, para. 4, of Law no. 109/2009.

The paragraph 5 of Article 15 of Law no. 109/2009 provides that if there are reasons to believe that the data sought is found in another computer system or in a different part of the system searched, but is legitimately accessible from or available to the initial system, the search can be extended upon authorization of the competent judicial authority.

With regard to professional confidentiality, pursuant to Article 15, paragraph 6, of Law no. 109/2009, computer searches in computer systems used for activities subject to professional confidentiality[46] must be authorized by the Judge (who must also be present during the search). The Judge must notify the President of the local council of the Bar Association or of the Order of Physicians, the president of the regional council of the Order of Solicitors and Execution Agents, the president of the most representative trade union organization of journalists or, in the other cases, a similar entity, so that the same, or a delegate, may be present; in the case of a search in an official health establishment, the notification shall be made to the chairman of the board of directors or management of the establishment or to his/her legal substitute. And the professional wanted by the search may also be present.

With respect to the restriction of fundamental rights, the search of stored computer data restricts the fundamental rights to privacy and to informational self-determination, protected by Article 8 of the European Convention on Human Rights[47]. Pursuant to Article 8 (2), there shall be no interference by a public authority with the exercise of these rights, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

[46] We consider that, although Article 15, para. 6, of Law no. 109/2009 only mentions the professional confidentiality of physician, lawyer or journalist, it shall apply to all cases in which computer research is carried out in a computer system used for an activity subject to professional confidentiality.

[47] See ECtHR, *Prezhdarovi v. Bulgaria*, Application no. 8429/05, Judgment of 30.09.2014, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22 CASE%20OF%20 PREZHDAROVI%20v.%20BULGARIA%22], %22documentcollectionid2%22:[%22JUDG-MENTS%22], %22itemid%22:[%22001-146565%22]} [last accessed 07/11/2018].

The explanatory report notes that Article 19 of the Convention on Cybercrime "aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings. Any domestic criminal procedural law includes powers for search and seizure of tangible objects. However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data".

The ECtHR analyzed the compliance of Portuguese Law in matter of search of stored computer data with Article 8 of the European Convention on Human Rights in the Judgement of the Case Sérvulo & Associados – Sociedade de Advogados, RL and Others *v.* Portugal[48] and considered that Portuguese Law did not violate the European Convention on Human Rights[49]. Furthermore, pursuant to Article 19 (5) of the Convention on Cybercrime, the search of stored computer data is subject to Articles 14 and 15 of that Convention.

Like an order for submitting or granting access to data, the search of stored computer data provides a less intrusive measure which law enforcement authorities can apply instead of measures such as interception of content data and real-time collection of traffic data, which must be used only to investigate serious offences. Although Article 15 of Law no. 109/2009 may include access to traffic data and even to the content of communications stored on a computer system, the search of stored computer data does not constitute an intense restriction of fundamental rights like, for example, an interception of communications. Thus, we consider that neither Articles 15 and 19 of the Convention on Cybercrime

---

[48] ECtHR, *Sérvulo & Associados – Sociedade de Advogados, RL and Others v. Portugal*, Application no. 27013/10, Judgment of 03.12.2015, available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-156519%22]} [accessed 07/11/2018].

[49] Although the Court did not analyse Articles 15 and 16 of Law no. 109/2009, but, among others, Articles 174, 176 and 178 of the Code of Criminal Procedure, whose regime was similar to Articles 15 and 16 of Law no. 109/2009.

nor Article 8 of the European Convention on Human Rights require that the order for submitting or granting access to data depend on judicial authorization.

Article 15 of Law no. 109/2009 empowers the investigating authorities to search or similarly access a computer system or part of it and computer data stored therein and a computer-data storage medium in which computer data may be stored and respects the safeguards imposed by Articles 14 and 15 of the Convention on Cybercrime and Article 8 of the European Convention on Human Rights. However, there are some differences between Article 15 of Law no. 109/2009 and Article 19 of the Convention on Cybercrime.

Thus, pursuant to Article 19 of the Convention on Cybercrime, only computer data stored on computer systems or computer-data storage mediums located in the territory of each Party may be searched. However, in Article 15 of Law no. 109/2009, the Portuguese legislator only refers to the search of stored computer data without mentioning whether the computer system is located in the Portuguese territory or abroad.

Therefore, we consider that Article 15 of Law no. 109/2009 allows the search of computer data in computer systems that are not located in the Portuguese territory without to resort to international judicial cooperation mechanisms. Firstly, if the Portuguese legislator wanted to restrict the search of computer data to the systems that are located in the Portuguese territory, he would have done it, but he did not. Secondly, computer crime knows no frontiers and, therefore, the application of criminal procedural law must be adapted to that reality. And finally, when the authorities know where data is stored but don't know in which country the computer system is located, the rejection of the possibility of Article 15 of Law no. 109/2009 allow remote cross-border access to computer systems located in foreign countries without resort to international judicial cooperation mechanisms, would make impossible to carry out such a measure[50].

And we find another difference between Article 15 of Law no. 109/2009 and Article 19 of the Convention on Cybercrime. In fact, the

---

[50] For further arguments, see Duarte Rodrigues Nunes, *Os meios de obtenção de prova previstos na Lei do Cibercrime* [*The means of obtaining evidence provided by the Law of Cybercrime*], Gestlegal, Coimbra, 2018, p. 91–94.

Portuguese legislator did not empower the authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of a search of computer stored data. Thus, we consider that, in this aspect, the Portuguese legislator has not fully complied with Article 19 of the Convention on Cybercrime[51].

VI. Seizure of stored computer data (Article 16 of Law no. 109/2009[52])

The seizure of computer data consists in seize or similarly secure computer data that has been searched or similarly accessed[53], as well as the programs necessary to access such data[54].

---

[51] The explanatory report notes that "This power is not only of benefit to the investigating authorities. Without such cooperation, investigative authorities could remain on the searched premises and prevent access to the computer system for long periods of time while undertaking the search. This could be an economic burden on legitimate businesses or customers and subscribers that are denied access to data during this time. A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data".

[52] The seizure of computer data is also provided by Article 19 of the Convention on Cybercrime.

[53] Where we may include the collection of computer data by a specialist in the place where the computer system is located, a search in the place where the computer system is located or the access to the computer system or to the autonomous device by means of an order for submitting or granting access to data (see David Ramahlo, *Métodos Ocultos de Investigação Criminal em Ambiente Digital* [*Covert Methods of Criminal Investigation in the Digital Environment*], Almedina, Coimbra, 2017, p. 133–134).

[54] The printing by the authorities of what appears on a web page or on a social network profile constitutes a seizure of computer data [see Judgments of the Court of Appeal of Oporto of 13/04/2016 (Case 471/15.0T9AGD-A.P1) *in http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/ef54d51d3972157d80257fa4002e2d75?OpenDocument* [last accessed 22/06/2018] and 04/04/2017 (Case 671/14.0GAMCN.P1), available at: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257 cda00381fdf/16ebc99e65fc-19038025810c0051991a?OpenDocument [last accessed 22/06/2018].

The seizure of computer data is authorized by the judicial authority[55], whenever it is of relevance to the discovery of the truth and/or for use as evidence[56], and can be used to investigate any type of crime[57].

Pursuant to Article 16, paragraphs 2 and 4, of Law no. 109/2009, the seizure may be carried out by the criminal police in the course of a computer search legitimately ordered and executed in accordance with Article 15 of Law no. 109/2009 or in exigent circumstances; and the police must inform the competent judicial authority, for validation, within 72 hours.

Pursuant to Article 16, paragraphs 5 and 6, of Law no. 109/2009, the seizure of stored data in computer systems used for lawyer, medical and banking activities must be authorized by the Judge (who must also be present during the seizure)[58], without prejudice to the power of the judicial authority provided by special laws. The Judge or the judicial authority must notify the President of the local council of the Bar Association or of the Order of Physicians, the president of the regional council of the Order of Solicitors and Execution Agents, the president of the most representative trade union organization of journalists or, in the other cases, a similar entity, so that the same, or a delegate, may be present; in the case of a search in an official health establishment, the notification shall be made to the chairman of the board of directors or management of the establishment or to his/her legal substitute. And the professional wanted by the seizure may also be present.

---

[55] Combining Article 16, paragraph 1, of Law no. 109/2009 with Article 1, b), of the Code of Criminal Procedure (which contains the legal concept of "judicial authority"), the authorization must be issued by the Public Prosecutor in the inquiry phase, by the Examining Judge in the preliminary judicial phase and by the Judge in the trial phase.

[56] See Article 16, paragraph 1, of Law no. 109/2009.

[57] See Paulo Da Mesquita, *Processo Penal, Prova e Sistema Judiciário* [*Criminal Procedure, Evidence and Judicial System*], Coimbra Editora, Coimbra, 2010, p. 98, and Judgments of the Court of Appeal of Évora of 06/01/2015 (Case 6793/11.6TDLSB-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b /847dae6b-85353cb880257de10056ff4c?OpenDocument (accessed 22/06/2018) and 20/01/2015 (Case 648/14.6GCFAR-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db-04f39bf280 2579bf005f080b/2fbdd21285478f5f80257de100 56ff7a?OpenDocument (accessed 22/06/2018).

[58] See also Articles 180, paragraph 1, 181 and 268, paragraph 1, c), of the Code of Criminal Procedure.

Pursuant to Article 16, paragraph 7, of Law no. 109/2009, the seizure of computer data may be carried out by means of:

a) Seizure of the device where the system is installed or seizure of the device where the computer data is stored, as well as the other devices that are necessary for its reading;
b) Realization of a copy of the data to an autonomous device, that will be added to the process;
c) Preservation by technological means of the integrity of the data, without copying or removal thereof; or
d) Non-reversible elimination or blocking of data access.

And, in accordance with paragraph 8 of the same Article, if the seizure consists in making a copy of the data, the copy must be made in duplicate and one of the copies must be sealed and entrusted to the judicial clerk of the Court where the process is taking place and, if technically possible, the seized data will be certified by digital signature.

The choice of one of the ways of carrying out the seizure is not arbitrary and the authorities shall choose the one that, being appropriate to pursue the purposes of the investigation, is less damaging to the fundamental rights of the people affected by the measure[59].

With respect to the restriction of fundamental rights, the seizure of stored computer data restricts the fundamental rights to privacy and to informational self-determination, protected by Article 8 of the European Convention on Human Rights[60]. Pursuant to Article 8 (2), there shall be no interference by a public authority with the exercise of these rights, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

[59] Rita Castanheira Neves, As *Ingerências nas Comunicações Electrónicas em Processo Penal* [*The Interference in Electronic Communications in Criminal Procedure*], Coimbra Editora, Coimbra, 2011, p. 273, and BENJAMIM SILVA RODRIGUES, *Da Prova Penal, II* [*On Criminal Evidence, II*], Rei dos Livros, Lisbon, 2010, p. 452.

[60] See ECtHR, *Prezhdarovi v. Bulgaria*, Application no. 8429/05, Judgment of 30.09.2014, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22CASE%20OF%20 PREZHDAROVI%20v.%20BULGARIA%22], %22documentcollectionid2%22:[%22JUDGMENTS%22], %22itemid%22:[%22001-146565%22]} [last accessed 07/11/2018].

The explanatory report notes that Article 19 of the Convention on Cybercrime "aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings".

The ECtHR[61] analyzed the compliance of Portuguese Law in matter of seizure of stored computer data with Article 8 of the European Convention on Human Rights and considered that the Portuguese Law did not violate the European Convention on Human Rights[62]. Furthermore, pursuant to Article 19 (5) of the Convention on Cybercrime, the seizure of stored computer data is subject to Articles 14 and 15 of that Convention.

The seizure of stored computer data provides a less intrusive measure which law enforcement authorities can apply instead of measures such as interception of content data and real-time collection of traffic data, which must be used only to investigate serious offences. Although Article 15 of Law no. 109/2009 may include access to traffic data and even to the content of communications stored on a computer system, the search of stored computer data does not constitute an intense restriction of fundamental rights like (except when the content of computer data is likely to reveal personal or intimate data), for example, an interception (in real-time) of communications. Thus, we consider that neither Articles 15 and 19 of the Convention on Cybercrime nor Article 8 of the European Convention on Human Rights require that the order for submitting or granting access to data depend on judicial authorization.

However, pursuant to Article 16, paragraph 3, of Law no. 109/2009, when the content of computer data is likely to reveal personal or intimate data, which may jeopardize the privacy of the respective holder or of a third party, such data or documents shall be submitted to the judge, who shall decide about their relevance to the case, taking into account the interests of the particular situation, under sanction of nullity[63].

---

[61] ECtHR, *Sérvulo & Associados – Sociedade de Advogados, RL and Others v. Portugal*, Application no. 27013/10, Judgment of 03.12.2015, available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-156519%22]} [last accessed 07/11/2018].

[62] Although the Court did not analyse Articles 15 and 16 of Law no. 109/2009, but, among others, Articles 174, 176 and 178 of the Code of Criminal Procedure, whose regime was similar to Articles 15 and 16 of Law no. 109/2009.

[63] On this issue, with more developments, Duarte Rodrigues Nunes, Os *meios de*

Article 16 of Law no. 109/2009 empowers the investigating authorities to seize or similarly secure a computer system or part of it or a computer-data storage medium, make and retain a copy of those computer data, maintain the integrity of the relevant stored computer data or render inaccessible or remove those computer data in the accessed computer system and respects the safeguards imposed by Articles 14 and 15 of the Convention on Cybercrime and Article 8 of the European Convention on Human Rights.

However, there are some differences between Article 16 of Law no. 109/2009 and Article 19 of the Convention on Cybercrime.

Thus, pursuant to Article 19 of the Convention on Cybercrime, the seize of stored computer data can only occur on computer data stored on computer systems or computer-data storage mediums located in the territory of each Party. However, in Articles 15 and 16 of Law no. 109/2009, the Portuguese legislator only refers to the search and seize of stored computer data without mentioning whether the computer system is located in the Portuguese territory or abroad.

Therefore, for the same reasons as we referred with regard to the search of stored computer data, we consider that Article 16 of Law no. 109/2009 allows the seizure of computer data in computer systems that are not located in the Portuguese territory without to resort to international judicial cooperation mechanisms.

And we find another difference between Article 16 of Law no. 109/2009 and Article 19 of the Convention on Cybercrime. In fact, the Portuguese legislator did not empower the authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of a seizure of computer stored data. Thus, we consider that, in this aspect, the Portuguese legislator has not fully complied with Article 19 of the Convention on Cybercrime.

---

obtenção de prova previstos na Lei do Cibercrime [*The means of obtaining evidence provided by the Law of Cybercrime*], Gestlegal, Coimbra, 2018, p. 120–127 (with bibliographic references).

VII. Seizure of electronic mail and records of communications of asimilar nature (Article 17 of Law no. 109/2009[64])

Article 17 of Law no. 109/2009 regulates the cases in which, during a computer search or other legitimate access to a computer system, the authorities find electronic messages or records of communications of a similar nature[65], subjecting their seizure to the legal regime of seizure of postal items provided by the Code of Criminal Procedure (Articles 179 and 252)[66].

The seizure of e-mails or records of communications of a similar nature must be authorized by the Judge, whenever such seizure is of great relevance to the discovery of the truth and/or for use as the evidence[67], and may be used in the investigation of any type of crime[68]. Due to the specificity of electronic mail, authorization can only be granted *a posteriori* and it will not be possible to return the seized electronic mail that is irrelevant to the investigation, and therefore, paragraphs 1 and 3 of Article 179 of the Code of Criminal Procedure will have to be applied

---

[64] The Convention on Cybercrime does not contain any provision specifically providing the seizure of electronic mail and communication records of a similar nature.

[65] E.g. SMS MMS, conversations in Messenger, voice messages related to communications via Whatsapp, Viber, Skype, Facebook, etc.

[66] This legislative option is subject to strong criticism, being understood that the seizure should be regulated by Article 16 of Law no. 109/2009 and not by the legal regime of seizure of postal items. On this issue, with more developments; Duarte Rodrigues Nunes, *Os meios de obtenção de prova previstos na Lei do Cibercrime* [*The means of obtaining evidence provided by the Law of Cybercrime*], Gestlegal, Coimbra, 2018, p. 141–146 (with bibliographic references).

[67] See Article 17 of Law no. 109/2009.

[68] See Paulo Da Mesquita, *Processo Penal, Prova e Sistema Judiciário* [*Criminal Procedure, Evidence and Judicial System*], Coimbra Editora, Coimbra, 2010, p. 98, and Judgments of the Court of Appeal of Évora of 06/01/2015 (Case 6793/11.6TDLSB-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf280 2579bf005f080b/847dae6b85353cb-880257de10056ff4c? OpenDocument [last accessed 22/06/2018] and 20/01/2015 (Case 648/14.6GCFAR-A.E1), available at: http://www.dgsi.pt/jtre.nsf/134973db04f39bf280 2579bf005f080b/2fbdd21285478f5f80257de 10056ff7a?OpenDocument [last accessed 22/06/2018].

with the necessary adaptations to the seizure of electronic mail or records of communications of a similar nature.

In exigent circumstances, authorities may use the police measures provided by Article 252 of the Code of Criminal Procedure[69], but only the measure provided by paragraph 3[70].

Due to the reference of Article 17 of Law no. 109/2009 to the legal regime of seizure of postal items pursuant to Article 179, paragraph 1, a), of the Code of Criminal Procedure, only e-mails or other similar realities that have been sent by the suspect or addressed to him or her, even if under a different name or through a different person, may be seized.

With regard to professional confidentiality, in accordance with Article 179, paragraph 2, of the Code of Criminal Procedure, no seizure or other control of electronic mail and records of communications of a similar nature between the defendant or suspect and between the defendant and his defence counsel is allowed unless the judge has reasonable grounds to believe that the said communication is the object or the constitutive element of a criminal offence.

Although we disagree with the legislative option to submit the seizure of e-mails or records of communications of a similar nature to the legal regime of seizure of correspondence provided by the Code of Criminal Procedure[71], Article 17 of Law no. 109/2009 complies with the provisions of Article 8 of the European Convention on Human Rights. In

---

[69] See Pinto De Albuquerque, *Comentário ao Código de Processo Penal, 4.ª Edição* [*Commentary on the Code of Criminal Procedure, 4th Edition*], Universidade Católica Editora, Lisbon, 2011, p. 510.

[70] Due to the specificity of the electronic mail and communications of a similar nature, which does not include package-equivalent realities, the measure provided by Article 252, para. 2, of the Code of Criminal Procedure cannot be applied to the seizure of electronic mail and communications of a similar nature).

[71] Because the seizure of electronic mail and communication records of a similar nature, provided by Article 17 of Law No. 109/2009 applies to obtaining electronic mail, SMS, etc. that has already been received by the recipient and is stored on a computer system that has been legitimately accessed by the authorities and not to obtaining, in real-time, electronic mail, SMS, etc. Therefore, unlike the seizure of correspondence provided by the Code of Criminal Procedure, there is no restriction on the right to confidentiality of correspondence. In fact, the seizure of electronic mail and communication records of a similar nature restricts exactly the same fundamental rights as the seizure of computer stored data provided by Article 16 of Law no. 109/2009.

fact, pursuant to Article 8 (2), there shall be no interference by a public authority with the exercise of these rights, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Thus, the ECtHR considers that the seizure of correspondence can only be justified if the conditions set out in the second paragraph of Article 8 are satisfied: the seizure of correspondence must be "in accordance with the law", pursue one or more "legitimate aims" and be "necessary in a democratic society" in order to achieve them[72].

VIII. Interception of communications (Article 18 of Law no. 109/2009[73])

Article 18 of Law no. 109/2009 provides for the interception[74] of computer communications, which includes obtaining real-time communication content data[75] (e-mail, SMS, Messenger conversations, news, chats,

---

[72] See ECtHR, *Silver and Others v. The United Kingdom* Application no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, Judgment of 25.03.1983, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22: [%22silver%22],%22documentcollectionid2%22: [%22GRANDCHAMBER%22,%22CHAMBER%22], %22itemid%22:[%22001-57577%22]} [last accessed 07/11/2018].

[73] This mean of obtaining evidence is also provided by Articles 20 and 21 of the Convention on Cybercrime.

[74] Defined in Article 2, e), of Law no. 109/2009 as "the act intended to capture information contained in a computer system by means of electromagnetic, acoustic, mechanical or other devices".

[75] Paulo Da Mesquita, *Processo Penal, Prova e Sistema Judiciário* [*Criminal Procedure, Evidence and Judicial System*], Coimbra Editora, Coimbra, 2010, p. 122, Pedro Dias Venacio, *Lei do Cibercrime* [*Law of Cybercrime*], Coimbra Editora, Coimbra, 2011, p. 119, and Judgments of the Court of Appeal of Lisbon of 03/05/2016 (Case 73/16.4PFCSC-A.L1-5), available at: http://www.dgsi.pt/jtrl.nsf/33182fc73231603980 2565fa00497eec/7eafd3bff46e1a-1b80257fd400314510? OpenDocument [last accessed 22/06/2018] and 07/03/2017 (Case 1585/16.5PBCSC-A.L1-5), available at: http://www.dgsi.pt/jtrl.nsf/33182fc73231603980 2565fa00497eec/ec0f3a35d90f697d802580ea0056629e?OpenDocument [last accessed 22/06/2018].

videoconferences and web conferences, etc.[76] and communications carried out by VoIP[77]) and traffic data (whether real time or data retained under the terms of Law 32/2008)[78].

The interception of computer data shall only be authorized during the investigation stage, where there are reasons to believe that this measure is essential to the uncovering of the truth or that, otherwise, it would be impossible or very difficult to obtain evidence, on the basis of a substantiated order from the examining judge, further to a request from the Public Prosecution[79]. The authorization shall be limited to a maximum time-limit of three months, renewable for equal periods, provided that the respective requirements for admissibility have been met[80].

In exigent circumstances, the authorization may be granted by the Judge with jurisdiction over the locations from where the telephone conversation or communication is likely to occur, or over the central office of the entity competent to conduct the criminal investigation, but only when dealing with one of criminal offences provided by Article 187, paragraph 2, of the Code of Criminal Procedure[81]. Likewise, the criminal police authority may directly request an interception of communications to the Judge without any intermediation by the Public Prosecutor[82].

However, under Article 11, paragraph 2, b), of the Code of Criminal Procedure, the interception, recording and transcription of conversations or communications involving the President of the Republic, the President

---

[76] Pinto De Albuquerque, *Comentário ao Código de Processo Penal, 4.ª Edição* [*Commentary on the Code of Criminal Procedure, 4th Edition*], Universidade Católica Editora, Lisbon, 2011, p. 542, and Pedro Dias Venancio, *Lei do Cibercrime* [*Law of Cybercrime*], Coimbra Editora, Coimbra, 2011, p. 119.

[77] See Pedro Dias Venancio, *Lei do Cibercrime* [*Law of Cybercrime],* Coimbra Editora, Coimbra, 2011, p. 119; different opinion, David Ramalho, *Métodos Ocultos de Investigação Criminal em Ambiente Digital* [*Covert Methods of Criminal Investigation in Digital Environment*], Almedina, Coimbra, 2017, p. 339 et seq.

[78] See Article 18, para. 3, of Law no. 109/2009.

[79] See Article 18, para. 1, of Law no. 109/2009.

[80] See Article 187, para. 6, of the Code of Criminal Procedure, applicable *ex vi* Article 18, para. 4, of Law no. 109/2009.

[81] See Article 187, para. 2, of the Code of Criminal Procedure, applicable *ex vi* Article 18, para. 4, of Law no. 109/2009.

[82] See Article 269, paras. 1, e), and 2, in conjunction with Article 268, para. 2, both of the Code of Criminal Procedure.

of the Parliament or the Prime Minister must be authorized by the President of the Supreme Court of Justice, which includes the interception of communications provided by Article 18 of Law no. 109/2009.

Pursuant to Article 18, paragraph 1, of Law no. 109/2009, the interception of communications may only be authorized to investigate criminal offences punishable under Law no. 109/2009 (Articles 3 to 8) and criminal offences committed by means of a computer or criminal offences which investigation requires collection of evidence in electronic form, when criminal offences are referred to in Article 187, paragraphs 1 and 2, of the Code of Criminal Procedure[83]. And pursuant to Article 187, paragraph 4, of the Code of Criminal Procedure (applicable *ex vi* Article 18,

---

[83] "Article 187: 1 – Interception and tape recording of telephone conversations or communications may only be authorized during the inquiry where there are grounds for believing that this step is indispensable for the discovery of the truth or that the evidence would, by any other means, be impossible or very hard to collect. Such authorization shall be granted by means of a reasoned order issued by the Examining Judge and upon the request of the Public Prosecution Service, as regards the following criminal offences:

a) Criminal offences to which a custodial sentence with a maximum limit over three years applies;

b) Drug-related offences;

c) Possession of a prohibited weapon and illicit trafficking in weapons;

d) Smuggling offences;

e) Insult, threat, coercion, disclosure of private life and disturbance of the peace and quiet, whenever committed by means of a telephone device;

f) Threat with the commission of a criminal offence or abuse and simulation of danger signals; or

g) Escape from justice, whenever the defendant has been sentenced for a criminal offence referred to in the preceding sub-paragraphs.

2 – The authorization provided for in paragraph 1 above may be requested to the judge with jurisdiction over the locations from where the telephone conversation or communication is likely to occur, or over the central office of the entity competent to conduct the criminal investigation, when dealing with the following criminal offences:

a) Criminal offences to which a custodial sentence with a maximum limit over three years applies;

b) Illegal restraint, kidnapping and taking of hostages;

c) Offences against cultural identity and personal integrity, as provided for in Book II, Title III, of the Criminal Code and in the Criminal Law on Violations of International Humanitarian Law;

d) Offences against State security foreseen in Book II, Title V, Chapter I, of the Criminal Code;

paragraph 4, of Law 109/2009), regardless of the entity who owns the means of communication used, the interception can only be authorised against (1) the suspect or the defendant, (2) any person acting as an intermediary, against whom there are grounds to believe that he/she receives or transmits messages aimed at, or coming from, the suspect or the defendant or (3) the victim of a crime (upon his/her effective or alleged consent). Evidence obtained in a process by means of the interception of communications cannot be used in other proceedings (either ongoing or to be initiated) unless it has resulted from the interception of a means of communication used by the suspect, defendant, intermediary or victim and insofar as it proves to be indispensable for obtaining evidence of a criminal offence set out in Article 18, paragraph 1, of Law no. 109/2009. However, the information obtained can always be used as *notitia criminis*[84].

Pursuant to Article 187, paragraph 5, of the Code of Criminal Procedure (applicable *ex vi* Article 18, paragraph 4, of Law no. 109/2009), no interception of computer data transmissions between the defendant and his defence counsel is allowed unless the judge has reasonable grounds to believe that the said communication is the object or the constitutive element of a criminal offence, and the evidence may be used against the accused and the defender[85].

---

e) Counterfeiting of currency or securities equivalent to currency foreseen in articles 262, 264 – to the extent that it refers to article 262 – and article 267 – to the extent that it refers to articles 262 and 264 – of the Criminal Code;

f) Offences covered by a convention on the safety of air or maritime navigation".

[84] See Article 187, para. 7, of the Code of Criminal Procedure, applicable *ex vi* Article 18, para. 4, of Law no. 109/2009.

[85] See Lamas Leite, *As escutas telefónicas – algumas reflexões em redor do seu regime e das consequências processuais derivadas da respectiva violação*, [in:] S*eparata da Revista da Faculdade de Direito da Universidade do Porto, 2004* [*The wiretapping – some reflections around its regime and the procedural consequences derived from the respective violation, "Offprint of the Journal of the Faculty of Law of the University of Oporto", 2004*], p. 46, Helena Susano, *Escutas Telefónicas* [*Wiretapping*], Coimbra Editora, Coimbra, 2009, p. 39, and Pinto De Albuquerque, *Comentário ao Código de Processo Penal, 4.ª Edição* [*Commentary on the Code of Criminal Procedure, 4th Edition*], Universidade Católica Editora, Lisbon, 2011, p. 527. Differently Marcolino de Jesus, *Os Meios de Obtenção de Prova em Processo Penal* [*The Means of Obtaining Evidence in Criminal Procedure*], Almedina, Coimbra, 2011, p. 246, Ana Conceicao, *Escutas Telefónicas* [*Wiretapping*], Quid Juris, Lisbon, 2009, p. 112, and Costa Andre, *Das*

Although the law only refers to the communications between the defendant and his defence counsel, it is discussed whether the rule also includes other cases of communications involving persons subject to the duty of professional confidentiality[86].

The criminal police that carries out the interception of communications draws up the respective records and produces a report pointing out the parts which bear relevance for use as evidence, describing in brief the respective contents and explaining the respective importance for the discovery of the truth[87].

Pursuant to Article 188, paragraphs 3 to 6, of the Code of Criminal Procedure, the criminal police that carries out the interception of communications provides the Public Prosecutor, every fortnight counted

---

Escutas Telefónicas, [in:] *I Congresso de Processo Penal* [*On Wiretapping, "I Congress of Criminal Procedure"*], Almedina, Coimbra, 2005, p. 221, consider that the evidence can only be used against the defence counsel, in order not to prejudice the defence.

[86] Duarte Rodrigues Nunes, *Os meios de obtenção de prova previstos na Lei do Cibercrime* [*The means of obtaining evidence provided by the Law of Cybercrime*], Gestlegal, Coimbra, 2018, p. 184–186, and Lamas Leite, *As escutas telefónicas – algumas reflexões em redor do seu regime e das consequências processuais derivadas da respectiva violação*, [in:*] Separata da Revista da Faculdade de Direito da Universidade do Porto*, 2004 [*The wiretapping – some reflections around its legal regime and the procedural consequences derived from the respective violation, "Offprint of the Journal of the Faculty of Law of the University of Oporto"*, 2004], p. 48, consider that Article 187, para. 5, of the Code of Criminal Procedure does not apply to such cases. On the other hand, the Majority Doctrine considers that Article 187, para. 5, of the Code of Criminal Procedure also applies in these cases (see Costa Andrade, *Das Escutas Telefónicas*, [in:] *I Congresso de Processo Penal* [*On Wiretapping, "I Congress of Criminal Procedure"*], Almedina, Coimbra, 2005, p. 220, Pinto De Albuquerque, *Comentário ao Código de Processo Penal, 4.ª Edição* [*Commentary on the Code of Criminal Procedure, 4th Edition*], Universidade Católica Editora, Lisbon, 2011, p. 527, Germano Marques Da Silva, *Curso de Processo Penal, II, 4.ª Edição* [*Course on Criminal Procedure, II, 4th Edition*], Editorial Verbo, Lisbon, 2008, p. 252, Rita Castanheira Neves, *As Ingerências nas Comunicações Electrónicas em Processo Penal* [*The Interference in Electronic Communications in Criminal Procedure*], Coimbra Editora, Coimbra, 2011, p. 295 et seq., Helena Susano, *Escutas Telefónicas* [*Wiretapping*], Coimbra Editora, Coimbra, 2009, p. 41, Benjamin Silva Rodrigues, *Das Escutas Telefónicas, I* [*On Wiretapping, I*], Rei dos Livros, Lisbon, 2008, p. 291 et seq., Ana Conceicao, *Escutas Telefónicas* [*Wiretapping*], Quid Juris, Lisbon, 2009, p. 111, and Guedes Valente, *Escutas Telefónicas, 2.ª Edição* [*Wiretapping, 2nd Edition*], Almedina, Coimbra, 2008, p. 92).

[87] See Article 188, para. 1, of the Code of Criminal Procedure, applicable *ex vi* Article 18, para. 4, of Law no. 109/2009.

from the first interception made, with the respective technical material, as well as with the respective records and reports[88]. Then, the Public Prosecutor submits those elements to the judge within a maximum time limit of forty-eight hours[89]. The Judge, in order to become acquainted with the content of the communications, is assisted, whenever appropriate, by a criminal police body and shall appoint, if necessary, an interpreter[90] and orders the immediate destruction of the technical materials and reports clearly bearing no interest to the case and concerning communications between persons who could not be subject to an interception of communications, covering matters under professional confidentiality, under confidentiality binding officials or under State confidentiality or which disclosure may seriously affect rights, liberties and guarantees[91].

With respect to the restriction of fundamental rights, the interception of communications restricts the fundamental rights to privacy, to informational self-determination, to confidentiality of communications and, in the case of the interception of communications by means of VoIP, the right to confidentiality and to integrity of information technology systems, protected by Article 8 of the European Convention on Human Rights[92]. Pursuant to Article 8 (2), there shall be no interference by a public authority with the exercise of these rights, except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

---

[88] See Article 188, para. 3, of the Code of Criminal Procedure, applicable *ex vi* Article 18, para. 4, of Law no. 109/2009.

[89] See Article 188, para. 4, of the Code of Criminal Procedure, applicable *ex vi* Article 18, para. 4, of Law no. 109/2009.

[90] See Article 188, para. 5, of the Code of Criminal Procedure, applicable *ex vi* Article 18, para. 4, of Law no. 109/2009.

[91] See Article 188, para. 6, of the Code of Criminal Procedure, applicable *ex vi* Article 18, para. 4, of Law no. 109/2009.

[92] See ECtHR, *Valenzuela Contreras v. Spain*, Application no. 58/1997/842/1048, Judgment of 30.07.1998, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22valenzuela%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58208%22]}[last accessed 07/11/2018].

According to ECtHR's case-law, the interception of communications constitutes an interference by a public authority in the right to respect for private life and correspondence and such an interference will be in breach of Article 8 (2) of the European Convention on Human Rights unless it is in accordance with the law, pursues one or more legitimate aims under paragraph 2 and is necessary in a democratic society to achieve those aims. "In accordance with the law" require firstly that the impugned measure should have some basis in domestic law. However, that expression does not merely refer back to domestic law but also relates to the quality of the law, requiring it to be compatible with the rule of law. The expression thus implies that there must be a measure of protection in domestic law against arbitrary interference by public authorities with the rights safeguarded by paragraph. From that requirement stems the need for the law to be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him. Especially where a power of the executive is exercised in secret the risks of arbitrariness are evident. In the context of interception of communications by public authorities, the requirement of foreseeability implies that the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to take any such secret measures. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is constantly becoming more sophisticated. ECtHR's case-law mentions the following minimum safeguards that should be set out in the statute in order to avoid abuses of power: a definition of the categories of people liable to have their telephones tapped by judicial order, the nature of the offences which may give rise to such an order, a limit on the duration of telephone tapping, the procedure for drawing up the summary reports containing intercepted conversations, the precautions to be taken in order to communicate the recordings intact and in their entirety for possible inspection by the judge and by the defence and the circumstances in which recordings may or must be erased or the tapes destroyed, in particular where an accused has been discharged by an investigating judge or acquitted by a court[93].

---

[93] About the analysis of ECtHR's case-law, see ECtHR, Valenzuela Contreras *v.* Spain, Application no. 58/1997/842/1048, Judgment of 30.07.1998, available at: https://hudoc.

Thus, as we can see, Article 18 of Law no. 109/2009 complies with the provisions of Article 8 of the European Convention on Human Rights.

With regard to the Convention on Cybercrime, Articles 20 and 21 empower the investigating authorities to collect or record through the application of technical means on the territory of that Party and compel a service provider, within its existing technical capability to collect or record through the application of technical means on the territory of that Party or to co-operate and assist the competent authorities in the collection or recording of content data and traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. However, pursuant to Articles 20 (4) and 21 (4) the collection or recording of content data and traffic data in real-time is, pursuant to Article 15 of that Convention, "subject to conditions and safeguards provided for under domestic law" and must "in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure". And the explanatory report notes that "the conditions and safeguards applicable to real-time interception of content data may be more stringent than those applicable to the real-time collection of traffic data, or to the search and seizure or similar accessing or securing of stored data".

Thus, as we can see, Article 18 of Law no. 109/2009 also complies with the conditions and safeguards of Articles 14 and 15 of the Convention on Cybercrime.

IX. Undercover operations (Article 18 of Law no. 109/2009[94])

The Portuguese legislator defines undercover operations as "any operations conducted by criminal investigation officers, or third persons

---

echr.coe.int/eng#{%22fulltext%22:[%22valenzuela%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58208%22]} [last accessed 07/11/2018].

[94] The Convention on Cybercrime does not contain any provision specifically providing for the use of undercover agents in digital environment.

subject to the scrutiny of the Judiciary Police (*Polícia Judiciária)*, acting under undisclosed capacity and identity for the purpose of preventing or punishing the offences specified in this Act"[95], regulating in Article 19 of Law no. 109/2009 the undercover operations in digital environment.

Pursuant to Article 3, paragraphs 3 to 5, of Law 101/2001, undercover operations within the framework of the inquiry are subjected to prior authorisation of the competent member of the Public Prosecution, to mandatory communication to the investigating judge, and will be deemed to be ratified if no order refusing permission is issued within seventy-two hours and if the operation is carried out in the framework of crime prevention, it falls within the competence of the investigation judge of the Criminal Instruction Central Court to give the required authorisation upon proposal by the Public Prosecution.

Pursuant to Article 19, paragraph 1, of Law no. 109/2009, undercover operations in a digital environment may only be used to investigate:

a) Criminal offences punishable under Articles 3 to 8 of Law no. 109/2009;
b) Criminal offences committed by means of a computer system, to which correspond, in abstract, a term of imprisonment with a maximum band of over 5 years; and
c) Regardless of the applicable penalty, intentional criminal offences, those against freedom and sexual self-determination, in case victims are minors or incapacitated adults (Articles 163 to 176 A of the Penal Code), qualified swindling (Article 218 of the Penal Code), computer-related fraud (Article 221 of the Penal Code), racial, religious or sexual discrimination (Articles 240 to 245 of the Penal Code), criminal offences laid down in title IV of the Code of Copyright and Related Rights (Articles 195 to 199) and economic and financial infringements when committed by means of a computer system[96].

---

[95] See Article 1, paragraph 2, of Law no. 101/2001, of August 25, hereinafter referred to as Law no. 101/2001. The text of Law no. 101/2001 available at: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=89&tabela=leis (in Portuguese only).

[96] The catalogue of criminal offences of Article 19, paragraph 1, of Law no. 109/2009 is of dubious constitutionality by allowing the use of undercover operations to investigate criminal offences of small or medium gravity such as the crimes punishable under Article 4,

Pursuant to Article 19, paragraph 2, of Law no. 109/2009, when it is necessary to use computer means and devices in the context of undercover operations, Article 18 of Law no. 109/2009 shall apply.

Pursuant to Article 4, paragraph 4, of Law no. 101/2001, when the judge, should, on grounds of evidential indispensability, order the undercover officer to attend the hearing, the public must be excluded and, as a rule, the undercover agent will give his testimony without its identity being revealed and using image concealment, voice distortion and videoconference, to protect the agent from being influenced by possible pressures and reprisals and to allow the agent to be used in future investigations[97]. In such cases, pursuant to Article 19, paragraph 2, of Law no. 93/99, of July 14[98], no conviction may be based, exclusively or decisively, on the testimony or statements produced by one or more witnesses whose identity was not revealed.

Pursuant to Article 6, paragraph 1, of Law no. 101/2001, any conduct of an undercover agent which, in the framework of an undercover operation, amounts to the commission of preparatory or instrumental acts in any form of participation other than incitement shall not be punishable whenever due proportionality is kept with regard to the aim to be achieved.

Finally, pursuant to Article 3, paragraph 6, of Law no. 101/2001, the Judiciary Police will report the undercover agent operation to the competent judicial authority within 48 hours at the latest as from the date on which the operation was completed.

---

paragraphs 1 and 3, Article 6, paragraphs 1,2 and 3, Article 7 and Article 8 of Law no. 109/2009 – related to crimes of damage caused to programmes or other computer data, illegal access, illegal interception and illegal reproduction of protected programmes – (see PAULO DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário [Criminal Procedure, Evidence and Judicial System], Coimbra Editora, Coimbra, 2010, p. 126, and Pinto De Albuquerque, *Comentário do Código de Processo Penal, 4.ª Edição* [*Commentary on the Code of Criminal Procedure, 4th Edition*], Universidade Católica Editora, Lisbon, 2011, p. 681–682).

[97] See David Ramalho, *Métodos Ocultos de Investigação Criminal em Ambiente Digital* [*Covert Methods of Criminal Investigation in Digital Environment*], Almedina, Coimbra, 2017, p. 304–305.

[98] The text of Law no. 93/99 is available at: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=234&tabela=leis (in Portuguese only).

With respect to the restriction of fundamental rights, undercover operations in a digital environment restrict the fundamental rights to privacy, to informational self-determination and to confidentiality and to the integrity of information technology systems. However, the ECtHR usually analyses the admissibility of undercover operations in the context of the right to a fair trial [Article 6(1) of the Convention on Human Rights.

In Ramanauskas *v.* Lithuania[99], the ECtHR set out the general principles concerning the issue of undercover operations and entrapment:

"49. The Court observes at the outset that it is aware of the difficulties inherent in the police's task of searching for and gathering evidence for the purpose of detecting and investigating offences. To perform this task, they are increasingly required to make use of undercover agents, informers and covert practices, particularly in tackling organised crime and corruption.

50. Furthermore, corruption – including in the judicial sphere – has become a major problem in many countries, as is attested by the Council of Europe's Criminal Law Convention on the subject […]. This instrument authorises the use of special investigative techniques, such as undercover agents, that may be necessary for gathering evidence in this area, provided that the rights and undertakings deriving from international multilateral conventions concerning "special matters", for example human rights, are not affected.

51. That being so, the use of special investigative methods – in particular, undercover techniques – cannot in itself infringe the right to a fair trial. However, on account of the risk of police incitement entailed by such techniques, their use must be kept within clear limits […].

53. More particularly, the Convention does not preclude reliance, at the preliminary investigation stage and where the nature of the offence may warrant it, on sources such as anonymous informants. However, the subsequent use of such sources by the trial court to found a conviction is a different matter and is acceptable only if adequate and sufficient safeguards against abuse are in place, in particular a clear and

---

[99] ECtHR, *Ramanauskas v. Lithuania*, Application no. 74420/01, Judgment of 05.02. 2008, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22Ramanauskas%20v.%20Lithuania%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-84935%22]} [last accessed 07/11/2018].

foreseeable procedure for authorising, implementing and supervising the investigative measures in question (…). While the rise in organised crime requires that appropriate measures be taken, the right to a fair trial, from which the requirement of the proper administration of justice is to be inferred, nevertheless applies to all types of criminal offence, from the most straightforward to the most complex. The right to the fair administration of justice holds so prominent a place in a democratic society that it cannot be sacrificed for the sake of expedience […].

54. Furthermore, while the use of undercover agents may be tolerated provided that it is subject to clear restrictions and safeguards, the public interest cannot justify the use of evidence obtained as a result of police incitement, as to do so would expose the accused to the risk of being definitively deprived of a fair trial from the outset […].

55. Police incitement occurs where the officers involved – whether members of the security forces or persons acting on their instructions – do not confine themselves to investigating criminal activity in an essentially passive manner, but exert such an influence on the subject as to incite the commission of an offence that would otherwise not have been committed, in order to make it possible to establish the offence, that is, to provide evidence and institute a prosecution […].

56. In Teixeira de Castro […] the Court found that the two police officers concerned had not confined themselves "to investigating Mr Teixeira de Castro's criminal activity in an essentially passive manner, but [had] exercised an influence such as to incite the commission of the offence". It held that their actions had gone beyond those of undercover agents because they had instigated the offence and there was nothing to suggest that without their intervention it would have been committed […].

In reaching that conclusion the Court laid stress on a number of factors, in particular the fact that the intervention of the two officers had not taken place as part of an anti-drug trafficking operation ordered and supervised by a judge and that the national authorities did not appear to have had any good reason to suspect the applicant of being a drug dealer: he had no criminal record and there was nothing to suggest that he had a predisposition to become involved in drug trafficking until he was approached by the police […].

More specifically, the Court found that there were no objective suspicions that the applicant had been involved in any criminal activity.

Nor was there any evidence to support the Government's argument that the applicant was predisposed to commit offences. On the contrary, he was unknown to the police and had not been in possession of any drugs when the police officers had sought them from him; accordingly, he had only been able to supply them through an acquaintance who had obtained them from a dealer whose identity remained unknown. Although Mr Teixeira de Castro had potentially been predisposed to commit an offence, there was no objective evidence to suggest that he had initiated a criminal act before the police officers' intervention. The Court therefore rejected the distinction made by the Portuguese Government between the creation of a criminal intent that had previously been absent and the exposure of a latent pre-existing criminal intent […]

60. The Court has also held that where an accused asserts that he was incited to commit an offence, the criminal courts must carry out a careful examination of the material in the file, since for the trial to be fair within the meaning of Article 6 § 1 of the Convention, all evidence obtained as a result of police incitement must be excluded. This is especially true where the police operation took place without a sufficient legal framework or adequate safeguards […]

61. Lastly, where the information disclosed by the prosecution authorities does not enable the Court to conclude whether the applicant was subjected to police incitement, it is essential that the Court examine the procedure whereby the plea of incitement was determined in each case in order to ensure that the rights of the defense were adequately protected, in particular the right to adversarial proceedings and to equality of arms […]".

Thus, in its case-law in matter of entrapment, the Court has developed criteria to distinguish entrapment breaching Article 6 (1) of the Convention from permissible conduct in the use of legitimate undercover techniques in criminal investigations, developing the examination of complaints of entrapment on the basis of two tests: the substantive and the procedural test of incitement[100].

---

[100] See ECtHR, Bannikova *v.* Russia, Application no. 18757/06, Judgment of 04.02.2011, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22bannikova%22], %22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22], %22itemid%22:[%22001-101589%22]} [last accessed 07/11/2018].

However, since undercover operations in a digital environment is a mean of obtaining evidence that restricts fundamental rights protected by Article 8 of the European Convention on Human Rights, its admissibility must be analyzed also in the light of these fundamental rights. Therefore, we consider that the requirements referred to in Judgment Valenzuela Contreras *v.* Spain[101] (and quoted above) apply *mutatis mutandis* to undercover operations in a digital environment.

Thus, as we can see, Article 19 of Law no. 109/2009 and Law no. 101/2001 comply with the provisions of Articles 6 and 8 of the European Convention on Human Rights, except when the use of undercover operations is allowed to investigate criminal offences of small or medium gravity[102].

X. Online search of stored computer data (Articles 15 and 18 of Law no. 109/2009)

The online search consists in a "clandestine infiltration into a computer system to observe its use and access stored data"[103], which is carried out online using technical means and by means of the surreptitious installation of a computer program of the type Trojan horse in the computer system[104], which may consist of a single access or occur continuously and over time.

---

[101] ECtHR, *Valenzuela Contreras v. Spain*, Application no. 58/1997/842/1048, Judgment of 30.07.1998, available at: https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22valenzuela%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58208%22]} [last accessed 07/11/2018].

[102] Such as criminal offences punishable under Article 4, paras. 1 and 3, Article 6, paras. 1, 2 and 3, Article 7 and Article 8 of Law no. 109/2009, that are punishable with imprisonment up to 3 years (Article 4, paras. 1 and 3, 6, para. 3, and Article 8) and 1 year (Article 6, paras. 1 and 2, and Article 7). In fact, this possibility violates the principle of proportionality, that regulates the restriction of fundamental rights.

[103] See Costa Andrade, *Bruscamente no Verão Passado* [*Suddenly Last Summer*], Coimbra Editora, Coimbra, 2009, p. 166, and Pinto De Albuquerque, *Comentário ao Código de Processo Penal, 4.ª Edição* [*Commentary on the Code of Criminal Procedure, 4th Edition*], Universidade Católica Editora, Lisbon, 2011, p. 502 and 541.

[104] See Costa Andrade, *Bruscamente no Verão* Passado [*Suddenly Last Summer*], Coimbra Editora, Coimbra, 2009, p. 166, and Pinto De Albuquerque, *Comentário ao Código de Processo*

In the absence of express legal provisions in our legal system[105], the admissibility of this means of obtaining evidence in Portuguese law is discussed[106]. However, we consider that Article 15 of Law no. 109/2009 is the legal basis of the online search in Portuguese Law. However, when the online search is carried out in a continuous and prolonged way in time, it will be prejudicial to fundamental rights similar to the interception of communications. Therefore, operating an interpretation according to the Constitution, even if this form of execution of the online search is admissible in the light of Article 15 of Law no. 109/2009, the legal regime (much more restrictive) of the interception of communications provided by Article 18 of Law no. 109/2009[107] shall apply to such cases.

Penal, 4.ª Edição [*Commentary on the Code of Criminal Procedure, 4th Edition*], Universidade Católica Editora, Lisbon, 2011, p. 502 and 541.

[105] We can find cases of express legal provisions of online searches in German Law (*online Durchsuchung*) [§100b of the *Strafprozessordnung* (Criminal Procedure Code)], in Spanish Law (*registros remotos sobre equipos informáticos*) [Article 588c*septies* a of the Ley de enjuiciamiento criminal (Criminal Procedure Code)] and in Italian Law (*captatore informatico*) [Article 266 (2) of the *Codice di Procedura Penale* (Criminal Procedure Code)].

[106] See Pinto De Albuquerque, *Comentário ao Código de Processo Penal, 4.ª Edição* [*Commentary on the Code of Criminal Procedure, 4th Edition*], Universidade Católica Editora, Lisbon, 2011, p. 502 and 545, and Conde Correia, *Prova digital: as leis que temos e a lei que devíamos ter*, [in:] *Revista do Ministério Público, n.º 139* [*Digital Evidence: The Laws We Have and the Law We Should Have, "Public Ministry Review", no. 139*], p. 42 et seq., consider that it is admissible. Differently, Rita Castanheira Neves, *As Ingerências nas Comunicações Electrónicas em Processo Penal* [*The Interference in Electronic Communications in Criminal Procedure*], Coimbra Editora, Coimbra, 2011, p. 196 et seq., 248 and 273, David Ramalho, *Métodos Ocultos de Investigação Criminal em Ambiente Digital* [*Covert Methods of Criminal Investigation in Digital Environment*], Almedina, Coimbra, 2017, p. 346 et seq., Benjamin Silva Rodrigues, *Da Prova Penal, II* [*On Criminal Evidence, II*], Rei dos Livros, Lisbon, 2010, p. 474–475, Marcolino De Jesus, *Os Meios de Obtenção de Prova em Processo Penal* [*The Means of Obtaining Evidence in Criminal Procedure*], Almedina, Coimbra, 2011, p. 196, and Armando Ramos, *A prova digital em processo penal: O correio eletrónico* [*The digital evidence in criminal proceedings: Electronic mail*], Chiado Editora, Lisbon, 2014, p. 91, consider that it is inadmissible.

[107] About our opinion, with more developments, see Duarte Rodrigues Nunes, *Os meios de obtenção de prova previstos na Lei do Cibercrime* [*The means of obtaining evidence provided in the Law of Cybercrime*], Gestlegal, Coimbra, 2018, p. 226–234.

XI. Final remarks

The Portuguese legislature has regulated, for the first time in the Portuguese legal system, the means of obtaining evidence specific for Cybercrime in Law no. 109/2009, with which we cannot fail to agree.

However, not all legislative options deserve this approval as, for example the option of subjecting the seizure of electronic mail or records of communications of a similar nature to the legal regime of seizure of postal items provided by the Code of Criminal Procedure. And the same applies to the catalogue of criminal offences that allow the use of undercover actions in the digital environment (because it includes criminal offences of small and medium gravity) and the lack of provision for a special procedure in exigent circumstances in matter of an order for submitting or granting access to data.