ARTICLE:

The use of malware as a means of obtaining evidence in Portuguese criminal proceedings

By **David Silva Ramalho**

The use of malware as a means of obtaining evidence has increased in the course of the past years due to its effectiveness to counter the anti-forensic measures adopted by cyber criminals. In Portugal, it appears that this investigative tool was inserted in the Cybercrime Law as a technological device to be used in undercover operations. However, the terms in which this provision was foreseen lack clarity, precision and most of all respect for the defendant's rights, thus raising doubts as to its constitutionality. This paper discusses the implications of this legislation. The topic is extensive, and certain important areas are not covered, such as: the issue of national reach beyond its borders, and the reliability of the evidence. These are topics for another paper.

Introduction: The problem

On 15 September 2009, Lei n.º 109/2009 de 15 de setembro (Law no. 109 of 15 September 2009), also known as the Cybercrime Law, was published in the Portuguese Official gazette.[1] In addition to the transposition into the national legal order of Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems,[2] and adapting the national law to the Convention on Cybercrime,[3] the Cybercrime Law also created a procedural mechanism that was never explained and whose meaning remains unclear.

The Commission for Constitutional Affairs, Rights, Freedoms and Guarantees of the Portuguese Parliament did not refer to the provision in question in its motion upon the Draft Bill 289/X (4th), which would later become the Cybercrime Law. The Portuguese Parliament approved it without any dissenting vote, the decisions of the higher courts – as far as we know – have never referred to it, and those that write on these subjects rarely mention it, limiting themselves, if ever, to transcribing it or questioning its reach.

This procedural mechanism is included in the last number of the last article of the chapter dedicated to the procedural provisions of the Cybercrime Law, article 19, under the title 'Acções encobertas' (undercover operations). Paragraph 2 states the following:

> Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.
>
> Rules on interception of communications shall apply, as appropriate, where the resort to computer means and devices is required.[4]

The analysis of this provision immediately elicits the need to know what the 'computer means and devices' refer to. Is it possible that, as Paulo Dá Mesquita suggests, 'through this path, one is opening, without enough weighing (or clear brakes) the door to intercepting communications for prevention purposes'.[5] Or is it that the reference included in this provision to the application of the 'rules on interception of communications' aims precisely to remove these 'computer means and devices' from the concept of interception of communications provided in article 18 of the Cybercrime Law? This would qualify them as a means of obtaining evidence that is merely analogous to the interception but not an interception. The 'means' in question would require the use of other technologies, perhaps of a more invasive nature. Such an understanding would place upon the interpreter – meaning the jurist that does not have a significant knowledge of technology – a difficulty in understanding the legal meaning of 'computer means and devices'. A difficulty that tends to be dismissed as belonging to the knowledge of technical concepts

[1] D.R. n.º 179 (Serial I), of 15 September 2009.

[2] OJ L 69, 16.3.2005, 67–71.

[3] Council of Europe, Budapest, 23.XI.2001.

[4] Translation of the Cybercrime Law is taken from http://www.anacom.pt/ .

[5] Paulo Dá Mesquita, *Processo Penal, Prova e Sistema Judiciário* (Coimbra: Wolters Kluwer, 2010), 127. Translation by the author.

commonly understood as exterior to law and considered exempt from legal interpretation.[6]

The question this provision elicits is far from being uncontroversial, and it will set the theme for the present study: whether the use of malware as a means of obtaining evidence in criminal proceedings is admissible in light of the current Portuguese legal and constitutional framework.[7]

As can be inferred from this question, the problem is twofold: on the one hand, it is necessary to search for the possible existence of legal grounds in the current legal framework to support the use of these means of obtaining evidence, particularly in respect of the provision of article 19 (2) of the Cybercrime Law. On the other hand, it is necessary to analyse the constitutional framing of the use of malware, thus seeking to assess the requirements and assumptions of its application in criminal procedures, as well as its conformity with the Constitution of the Portuguese Republic.

This article provides a brief understanding of the problem, while presenting our first – and thus preliminary – thoughts on this subject.

[6] On this subject, see Denise H. Wong, 'Educating for the future: teaching evidence in the technological age', *Digital Evidence and Electronic Signature Law Review*, 10 (2013), 16 – 24; Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice', *Digital Evidence and Electronic Signature Law Review*, 10 (2013), 23 – 28. Also, for an introduction for legal practitioners on the relevant concepts of digital evidence, see Stephen Mason, gen ed., *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), Chapter 1.

[7] If we replace the generic term malware with the term Trojan horse, we will inevitably conclude that this question could have been answered in the parliamentary debate on the general principles pertaining to the Draft Bill 289/X (4th). In fact, immediately after the beginning of the parliamentary debate on the Draft Bill, Fernando Negrão, from the Social-Democratic Party, asked the following question: 'why is it not contemplated in this bill the possibility for the criminal investigation authorities to introduce in a given computer system under investigation what we might call "technical Trojan horse" in order to gather continuous and live information, thus facilitating criminal investigations, namely by means of computer systems?'. Having failed to receive any answer, at the closing of the debate on the general principles pertaining to this Bill, the same Member asked the following question: 'Mr. President, just to reiterate the questions that I posed to which Mr. Secretary of State did not answer […] Secondly, I asked the following: why not the creation of a new type of legal crime that would facilitate the criminal investigation in order to introduce technical "Trojan horses" in computer systems so as to facilitate the criminal investigation? I would just like to record that Mr. Secretary of State did not answer any of these questions'. The President of the Assembly of the Republic answered in the following terms: 'Mr. Secretary of State no longer has time to answer. Maybe he can do it some other time, perhaps during the course of the debate on the details, if so'. During the debate on the details, as far as we know, this question was never raised and this provision was approved by the majority, including the Social-Democratic Party: Parliament Gazette, 27 July 2009, 2nd ser., section A, No. 167/X/4.

The use of malware as a means of obtaining digital evidence

For an appropriate framing of the problem, we have chosen a two-step analysis of the subject: the first phase will include a brief historical and comparative analysis on the use of malware as a means of obtaining digital evidence in three selected legal systems in order to provide an empirical overview and a factual framing of the problem; the second phase will be limited to a legal study on a national level.

As for the first phase, we shall begin with a brief analysis of the use of malware as a means of obtaining evidence in the United States of America, where, as far as we know, it first emerged as a supporting tool for criminal investigations. We will conduct a brief analysis of the German experience with particular focus on the decision of the Federal Constitutional Court (Bundesverfassungsgericht) addressing the use of malware and on the functioning of what is commonly called the Bundestrojaner. Thirdly, we will proceed to summarise the Spanish legal framework, where a Draft Code of Criminal Procedure expressly including the admissibility of this technology is currently under discussion. This phase will end by considering the tendency to permit the use of malware as a criminal investigation tool through the influence of supranational initiatives, particularly in the countries of the Caribbean, as well as in the European Union.

The second phase of this article offers a summary study of the legal provisions at the Portuguese criminal procedural level for the use of malware – namely of article 19 (2) of the Cybercrime Law –, including the analysis of the sufficiency of the provisions already established by law and some of their main constitutional problems.

Concepts

For a proper understanding of the reality of cybercrime and digital evidence, it is acknowledged that, with the advent of the internet and the technological evolution, new realities have emerged that no longer fall into existing legal concepts. When this happens, a methodological option needs to be made; either pre-existing concepts are adapted in order to cover the new realities – with the possible distortion of its initial meaning through the fading of its features – or new concepts are imported from other areas of knowledge and given a legal definition.

The legislator and the Portuguese doctrine are usually prone to the first of these options. Though the Cybercrime Law is in general an exception to this tendency, it is not totally immune to it. This is partially shown by the option made by the Portuguese legislator to uncritically submit the undercover operations in a digital environment to the general legal framework of undercover operations established in Law 101/2001, of 25 August.[8] As to the doctrine, the same tendency is made manifest, namely by the use of the term 'online search'[9] in order to qualify what is, strictly speaking, the use of malware as a secret method of criminal investigation.[10]

For the purpose of this article, given that we understand that we are before a new concept that deserves detachment from other concepts with different features and objectives, we have chosen to use the term malware or one of its categories,[11] and not the terms online search or remote search[12] – except where the use of these terms may be necessary. We have done so essentially for two reasons: because it is not a search (*busca*) in the sense given to it by Portuguese Criminal Procedure Code, for it does not occur in a physical environment; and secondly because its installation and use is not limited to an online context.

Regarding the first objection, the generic reference to the concept of search without any reference to the term 'house' or 'domicile', might lead to the conclusion that the public prosecutor can authorize such a search in accordance with article 174 of the Código de Processo Penal (Portuguese Criminal Procedure Code). If this is accepted, it may be used to exempt the use of malware from judicial authorization. On the other hand, if the online search is compared with a house search[13] – which we find to be destitute of technical acuity –, the result will inevitably be a mischaracterization of the concept of 'house' or 'domicile'. This failure extends to the elements that underlie and legally justify the increased protection given to the suspect's (or others) rights affected by this measure[14] – especially if we take into consideration that malware can be set up in mobile telephones, laptops or tablets, wherever these are found, both inside the suspect's house or somewhere else. Furthermore, in an online search, the investigator can monitor all of the suspect's activity in real time, while also having the ability of activating, if necessary, the computer system's webcam or microphone, thus being able to witness the practice of unlawful acts while they are being perpetrated without the suspect being aware of it – contrary to what is the case with a search in a physical environment.

In regard to the second of the objections for qualifying the use of malware as an online search, some cyber-espionage malware such as Flame and Stuxnet[15] demonstrate that the installation of this type of software can occur offline by means of infected removable drives – namely USB flash drives – programmed to seize the intended data in order to

[8] Lei n.º 101/2001, de 25 de Agosto.

[9] Manuel da Costa Andrade, in one of his many notable works on secret methods of criminal investigation, defines online searches as 'a comprehensive and broad concept, perhaps not entirely accurate, that amounts to a set of encroachments in computer systems, performed through the internet, that are updated in the observation, search, copy, vigilance, etc., of the data stored in those computer systems': "Bruscamente no Verão passado" a Reforma do Código de Processo Penal – Observações Críticas sobre uma Lei que Podia e Devia ter sido Diferente (Coimbra: Coimbra Editora, 2009), 166. Translation by the author.

[10] In Portugal, the term 'search' may be translated into the terms 'busca', 'revista' and 'pesquisa'. The first term refers to a search in a closed environment or in a space that is not freely accessible to the public, according to article 174 (2) of the Portuguese Criminal Procedure Code. The second term refers to a body search, to be performed whenever there is reason to believe that someone is hiding on his/her person any objects related to a crime which may be used as evidence, in accordance with article 174 (1) of the Portuguese Criminal Procedure Code. The third term is used for the search of computer data in article 15 of the Cybercrime Law. When the term 'online search' is used in Portuguese language it is said to be a 'busca online', which is, in our opinion, technically inaccurate.

[11] Such as Trojans, logic bombs, rootkits, spyware, virus, worms or blended threats.

[12] The concept of a remote search is not established in Portuguese law or doctrine.

[13] On this subject, after comparing the computer to a person's digital soul, Benjamim Silva Rodrigues refers to the idea of digital domicile for the purpose of online searches – Da Prova Penal – Bruscamente… A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, 6 vols. (2010-2011, Lisboa: Rei dos Livros), vol. 2 (2010), 472 – 473.

[14] On this subject, Costa Andrade, comments that 'In any case it is without controversy that it [the online search] is not covered by any of the criminal procedure provisions that allow for the violation of the domicile, within the context of the classic figure of the search [busca]', 168.

[15] Given that these are cyber-espionage tools that are outside of the scope of this study (as are Duqu or Gauss), they will not be considered. For an interesting analysis of Stuxnet, see the compilation of information performed by the Federal Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS CERT), available at https://ics-cert.us-cert.gov/advisories/ICSA-10-272-01 . For a brief analysis of Flame and Stuxnet, see K. F. Morton and David Grace, *A Case Study on Stuxnet and Flame Malware* (2012), http://vixra.org/pdf/1209.0040v1.pdf. Finally, for an explanation and comparison between Flame, Stuxnet, Gauss and Duqu, see Will Gradigo, Daniel Molina, John Pirc and Nick Selby, *Blackhatonomics – An Inside Look at the Economics of Cybercrime* (Syngress, 2013), 47 – 52.

carry them to another removable drive until it finally reaches a computer system connected to the internet, from which it will be sent to its controller.

Finally, attention should be paid to the fact that, as far as we know, the term 'online search' has its origin in the debate that took place in American courts on the application of the concept of search provided for in the Fourth Amendment to the use of malware for criminal investigation purposes, namely for the purpose of requiring a prior judicial order authorizing its use.[16] Even though this debate has been repeated in a similar manner in different legal systems, such as Germany, the term loses relevance once we step into the Portuguese constitutional lexicon and, as such, should be subject to an independent analysis, removed from the value and configuration that is given to it by other legal systems, as well as from the concept of 'house' or domicile'.[17] For all of these reasons we will henceforth refer to the use of malware as a means of obtaining evidence, instead of the concept of online search.

Origin and evolution of the use of malware as a means of obtaining evidence in criminal proceedings

The North-American experience: from Magic Lantern to CIPAV

The American experience has been of interest with regard to the use of malware as a means of obtaining digital evidence in criminal proceedings. The secret use of different types of malware by the police has been the topic of interpretation of the U.S. Constitution. However, this article does not provide an analysis of this topic.

The first case to be subjected to widespread media attention on the use of keyloggers by the police dates from January 1999 (though, in this case, it was both malware and malicious hardware), when, as part of a criminal investigation conducted by the FBI on Nicodemo S. Scarfo, an alleged member of a mafia organization suspected of criminal offences related to the management of an illegal gambling business. The FBI discovered that a substantial part of the files with potential evidential value were encrypted.[18]

Given the need to obtain such data, and since the data encrypted by the software used by the suspect could only be decrypted with the password (perhaps known only by the suspect himself), the FBI sought a new warrant, this time to introduce a keylogger directly on the suspect's computer, in order to capture the password[19] and send it via radio waves to the FBI. The warrant was obtained and the keylogger, in this case in the form of hardware and software, was physically installed between the suspect's keyboard and his computer. After two months[20] the password[21] was finally obtained,[22] thus allowing the FBI to arrest the suspect and decrypt the contents of the files.[23]

The understandable practical difficulties raised by the physical installation of keyloggers in computers suspected of being used for the purpose of engaging

[16] This question was initially raised on the subject of the interception of telephone calls, whose subjection to the Fourth Amendment was established by the United States Supreme Court in *Katz v. United States* 389 U.S. 347, for which see Susan Landau, *Surveillance or Security – The risks Posed by new Wiretapping Technologies* (MIT Press, 2011), 70, and Iñaki Saiz Garitaonandia 'La intervención de las comunicaciones en el derecho comparado: los casos de Francia e los Estados Unidos de America', in *Derecho Penal Informático* (Pamplona: Thomson Reuters, 2010), 321 – 345, 337 – 339. The problem would be reawakened with the advent of the interception of communications and the use of malware in the context of criminal investigations, and would be settled in a similar manner than phone tapping – Susan Brenner, 'Law, Dissonance and Remote Computer Searches', 14 N.C. J.L. & Tech. 43 (2012), 43 – 92, 81.

[17] Unless, like Buermeyer we could conclude that by entering someone's computer system the state is setting its virtual foot through the door of someone's house for which see Costa Andrade, 167. Due attention should be paid to the fact that on 31 January 2007, the BGH rejected the position adopted by some German authors that the online searches could be subject to the rules applicable to traditional searches and entries: Juan Carlos Ortiz Pradillo, 'Remote Forensic Software as a Tool for Investigating Cases of Terrorism', *ENAC – E-newsletter on the fight against cybercrime*, 4 (2009), 1 – 8, 3 http://polis.osce.org/library/f/3643/2779/NGO-ESP-RPT-3643-EN-2779 .

[18] The facts are set out in *United States v Scarfo*, 180 F.Supp.2d 572 (D.N.J. 2001).

[19] Statement from the FBI agent who requested the issuance of the warrant, describing the operation of the keylogger and other relevant information, available at: http://epic.org/crypto/scarfo/murch_aff.pdf .

[20] Angela Murphy, 'Cracking the Code to Privacy: How Far Can the FBI Go?', 1 *Duke Law & Technology Review*, 1 – 6 (2002).

[21] The password turned out to be NDS09813-050, Scarfo's father's prison identification number, for which see George Mohay, Alison Anderson, Byron Collie, Olivier De Vel and Rodney McKemmish, *Computer and Intrusion Forensics* (Massachusetts: Artech House, 2003), 120.

[22] To avoid violations of the Wiretap Act (18 U.S. Code § 2511 – Interception and disclosure of wire, oral, or electronic communications prohibited), this keylogger only worked when the computer was disconnected from the internet, for which see Michael Sheetz, *Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers* (Wiley, 2007), 142.

[23] It should be noted, however, that a plea bargaining agreement prevented a thorough appellate consideration. The documents relating to this case are available here: http://epic.org/crypto/scarfo.html .

in criminal activity, along with the increasing severity and international scope of crime, had heightened the sense of need to install such mechanisms remotely and without hardware.

Thus, in 2001, Magic Lantern arose. It was a keylogger that could be installed surreptitiously and remotely via the internet at a specific computer system – even if it was not physically located in the U.S. – when it belonged to individuals suspected of being related to criminal activities, in particular of a terrorist nature. Magic Lantern could be installed either by opening attachments in e-mail messages sent to the suspect's computer system, or through the exploitation of vulnerabilities in the operating systems.[24] However, since certain anti-virus programs could detect Magic Lantern, it is reported that the U.S. government requested some companies devoted to marketing these products to avoid interfering with Magic Lantern.[25]

Magic Lantern would be replaced by the Computer and Internet Protocol Address Verifier (CIPAV),[26] a type of malware that added to the list of collected information, among others, the IP address and MAC address or both of the suspect's computer system, as well as his or her location, the list of programs running at any given time, the operating system used (type, version and serial number), the user account logged in the target computer, and the last web site visited.[27] Although there are reports of its use dating back to 2001, the CIPAV would only come to light in 2007, when the media published an application for a warrant submitted by FBI Special Agent Norman Sanders, requesting the use of this software to detect the author of several bomb threats.[28]

However, it was not until April 2011, following a request by the Electronic Frontier Foundation submitted under the Freedom of Information Act,[29] that the FBI disclosed various documents with detailed information on the use and operation of the legal framework and functioning of CIPAV.[30] The analysis of such documents allows us to draw two preliminary conclusions: first, that this program was used abundantly, even by government agencies other than the FBI; and, secondly, that initially there were various understandings as to the legal requirements for its admissibility, which met, on one side, the proponents of the absence of any legal requirements for its use, and, on the other side, the advocates of the necessity for judicial authorization prior to its use.[31]

Despite the effect that the disclosure of this information had, the resort to malware in the context of criminal investigations continued. A demonstration of this may be found in the publication, on April 2013, of a court order[32] signed by Judge Stephen Smith, of the Houston Division of the Southern District Court of Texas, denying judicial authorization for the use of an unidentified type of malware in a criminal investigation on the grounds that its installation was not properly specified and, consequently, that there would be uncertainty as to whether the malware in question could be installed on computer systems other than that of the intended recipient.[33]

Even though the decision does not mention the name of the malware in question, if it was a newer version of CIPAV, it had to be a more advanced version than the one referred to in the documents provided by the FBI, since it includes the following to the functions described above: records of internet activity, including firewall logs, caches, browser history, cookies, 'bookmarked' or 'favourite' web pages, search terms that the user entered into any internet search engine,

[24] Kevin Curran, Peter Breslin, Kevin McLaughlin and Gary Tracey, 'Hacking and Eavesdropping', in Lech J. Janczewski and Andrew M. Colarik, eds, *Cyber Warfare and Cyber Terrorism* (New York: Information Science Reference, 2008), 309.

[25] Christopher Woo and Miranda So, 'The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance', *Harvard Journal of Law & Technology*, Volume 15, Number 2, Spring 2002, 521 – 538, 524.

[26] Christopher Soghoian, 'Caught In The Cloud: Privacy, Encryption, And Government Back Doors In The Web 2.0 Era', 8 J. On Telecomm. & High Tech. L. (2009) 359 – 424, 400 – 401.

[27] Susan Landau, *Surveillance or Security – The risks Posed by new Wiretapping Technologies*, 133.

[28] A scanned copy of the affidavit is available at http://www.wired.com/images_blogs/threatlevel/files/timberline_affidavit.pdf .

[29] 5 U.S.C. § 552, as amended by Public Law No. 110-175, 121 Stat. 2524, and Public Law No. 111-83, § 564, 123 Stat. 2142, 2184.

[30] Available at https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government .

[31] According to the documentation, the solution adopted would be the a two-step procedure: the first one would be to require a judicial warrant prior to the intrusion in the target computer system; the second step would be to request a Pen/Trap order to authorize the surveillance, for which see 169 of the documentation provided by the FBI, available at https://www.eff.org/files/FBI_CIPAV-08-p169.pdf .

[32] *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F.Supp.2d 753, the memorandum and order is available at https://www.eff.org/files/smithorderdenyingwebcamwarrant.pdf .

[33] Though the court makes a reference to CIPAV in footnote 10 of the decision, it is not clear whether the malware in question was a newer version of CIPAV or not.

records of user-typed web addresses, user names and passwords recorded, e-mail contacts, e-mail contents, chat and other messaging program logs, photographs on the target computer system, among others. Furthermore, the malware in question also allows for the remote control of the target computer system, including the capability of using the subject's webcam to take pictures in order to allow for the identification of the user and his or her location.

The German experience: The Bundestrojaner

In 2006, as part of a criminal investigation concerning facts allegedly related to terrorism, a public prosecutor requested that a judicial warrant be granted, authorizing a remote search on a suspect's computer through the installation of a Trojan. The request was rejected on 25 November 2006, and the prosecutor appealed to the German Federal Court of Justice (Bundesgerichtshof), arguing that the legal provisions included in the German Strafprozeßordnung (Code of Criminal Procedure), pertaining to (physical) search and entries allowed for the use of such means of obtaining evidence.[34] The Federal Court concluded that no such analogy could be made and that the use of this measure lacked a legal basis, thus rendering it inadmissible in criminal procedure.[35]

Less than a month after this decision, on 20 December 2006, the Gesetz über den Verfassungsschutz in Nordrhein-Westfalen (North Rhine-Westphalia Constitution Protection Act) was altered, and a provision was introduced in article § 5.2 (11), which provides:

> 2. Die Verfassungsschutzbehörde darf, soweit nicht der Schutz des Kernbereichs privater Lebensgestaltung entgegensteht, zur Informationsbeschaffung als nachrichtendienstliche Mittel die folgenden Maßnahmen anwenden:
>
> …
>
> 11. Zugriff auf zugangsgesicherte Telekommunikationsinhalte und sonstige Informations- und Kommunikationsinhalte im Internet auf dem technisch hierfür für jede Nutzerin und jeden Nutzer vorgesehenen Weg, ohne selbst Kommunikationsadressatin oder -adressat und ohne von den an der Kommunikation teilnehmenden Personen oder vergleichbaren Berechtigten hierzu autorisiert zu sein, unter den Voraussetzungen des § 7a; eine Online-Durchsuchung ist ausgeschlossen;
>
> 2. The Constitution Protection Authority may, to the extent that it is not contrary to the protection of the core area of private life, apply for the following measures for the gathering of information and intelligence:
>
> …
>
> 11. Access to the content of secure telecommunications and other information and the content of communications on the Internet using technical means provided for each and every user, without the addressee of the communication or the individuals participating in the communication being aware, under the requirements of § 7; an online search is excluded;

This clause grants the Constitution Protection Authority (Bundesamt für Verfassungsschutz) the powers to use measures to acquire information through secret monitoring and other reconnaissance of the internet, including covert participation in chats and even – though this solution is less clear – access to web mail or to web sites with restricted access by using the credentials collected from various sources, such as informants.[36] Finally, the law in question also allowed for secret access to computer systems through the use of techniques that made the discovery and exploitation of technical vulnerabilities for the installation of malware possible.[37] The

[34] Giuseppe Vaciago, *Digital Forensics, Italian Criminal Procedure and Due Process Rights in the Cyber Age* (Torino: G. Giappichelli Editore, 2012), 125.

[35] Judgment of the Third Criminal Chamber of the Federal Supreme Court of 31 January 2007, BGH StB 18/06, available at http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&Datum=2007-1&nr=38779&pos=11&anz=268 .

36 Wiebke Abel and Burkhard Schafer, 'The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems – a case report on BVerfG, NJW 2008, 822', *SCRIPTed – A Journal of Law, Technology & Society*, 1, Vol. 6 (2009), 106 – 123, 107 – 110.

[37] The court stated that '[s]uch measures were already executed in isolated cases by federal authorities without a specific statutory empowerment. Little is known of the nature of the practical execution of previous "online searches" or of their successes', Judgment of the First Senate of 27 February 2008 on the basis of the oral hearing of 10 October 2007, 1 BvR 370, 595/07. The official English translation is available at https://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html

malware in question would then allow that authority to spy, monitor and analyse content, as well as to control the computer systems affected – although the applicability of this measure was limited to the functions of the Constitution Protection Authority, as provided for in § 3 of the North Rhine-Westphalia Constitution Protection Act:

> (1) Aufgabe der Verfassungsschutzbehörde ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen über
>
> 1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziel haben,
>
> 2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht,
>
> 3. Bestrebungen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden,
>
> 4. Bestrebungen und Tätigkeiten, die gegen den Gedanken der Völkerverständigung (Artikel 9 Abs. 2 des Grundgesetzes) oder das friedliche Zusammenleben der Völker (Artikel 26 des Grundgesetzes) gerichtet sind, im Geltungsbereich des Grundgesetzes, soweit tatsächliche Anhaltspunkte für den Verdacht solcher Bestrebungen und Tätigkeiten vorliegen.
>
> […]
>
> (1) Collection and evaluation of information, in particular of factual and personal information, messages and documents on
>
> 1. activities targeting the free democratic fundamental order, the continued existence or the security of the Federation or of a Land or an unlawful impairment of the exercise of office by the constitutional bodies of the Federation or of a Land or of their members.
>
> 2. activities for a foreign power which endanger security, or for a foreign security service,
>
> 3. activities which endanger foreign interests of the Federal Republic of Germany by means of the use of force or preparatory acts aimed thereto,
>
> 4. efforts and activities targeting the ideal of international understanding (Article 9.2 of the Constitutional Law) or peaceful relations between nations (Article 26 of the Constitutional Law), within the area of application of the Constitutional Law, insofar as there exist factual indications of the suspicion of such efforts and activities.[38]
>
> …[39]

An appeal was submitted before the German Federal Constitutional Court. On 27 February 2008, the court reached a decision.[40] It first considered the issue in light of three fundamental rights: (i) the right to secrecy of correspondence, post and telecommunication, (ii) the right to the inviolability of the home, and (iii) the right to informational self-determination. However, the method by which the evidence was obtained was at issue. It was argued that the constitutional protection was not limited to the object of each of these fundamental rights. Thus, in view of the need to offer, in a more comprehensive way, constitutional protection in relation to the integrity of computer systems, as well as to the data

. A manifestation of the German interest in the use of this type of malware can also be found in the documents provided by the FBI about CIPAV, in which there is an e-mail sent from an Assistant Legal Attaché stationed in Frankfurt, Germany, with the following content: 'I am embarrassed to be approaching you again with a request from the Germans (after your previous help and offers of assistance have not yet been followed up on by our German colleagues), but they now have asked us about CIPAV (Computer and Internet Protocol Address Verifier) software, allegedly used by the Bu [bureau]?', available at https://www.eff.org/files/FBI_CIPAV-08-p9.pdf .

[38] English translation available at https://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html

[39] Though the purpose of the law was to allow for the use of malware as a tool to deal with terrorism, it was not sufficiently clear in stating it and the German Constitutional Court, found that 'the area of application of the revision is not restricted to the fight against terrorism, either explicitly or as a consequence of the systematic context. The provision requires a justification for its entire area of application'.

[40] Judgment of the First Senate of 27 February 2008 on the basis of the oral hearing of 10 October 2007, 1 BvR 370, 595/07, available at: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

stored and transmitted through it, the court established the fundamental right to the guarantee of the confidentiality and integrity of information technology systems[41] (Grundrecht aug Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme). The fundamental right is based on human dignity and especially on the general right of personality, and is formulated, at [204]:

> … Grundrecht aug Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben.
>
> … the basic right to the confidentiality and integrity of information technology systems is first the interest of the user in ensuring that the data which are created, processed and stored by the information technology system that is covered by its scope of protection remain confidential.

The court balanced its conclusion with the following statement, at [206]:

> Der grundrechtliche Schutz der Vertraulichkeits- und Integritätserwartung besteht unabhängig davon, ob der Zugriff auf das informationstechnische System leicht oder nur mit erheblichem Aufwand möglich ist. Eine grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung besteht allerdings nur, soweit der Betroffene das informationstechnische System als eigenes nutzt und deshalb den Umständen nach davon ausgehen darf, dass er allein oder zusammen mit anderen zur Nutzung berechtigten Personen über das informationstechnische System selbstbestimmt verfügt. Soweit die Nutzung des eigenen informationstechnischen Systems über informationstechnische Systeme stattfindet, die sich in der Verfügungsgewalt anderer befinden, erstreckt sich der Schutz des Nutzers auch hierauf.
>
> An expectation of confidentiality and integrity to be recognized from the fundamental rights perspective however only exists insofar as the person concerned uses the information technology system as his or her own, and hence may presume according to the circumstances that he or she alone or together with others entitled to use it disposes of the information technology system in a self-determined manner. Insofar as the use of the personal information technology system takes place via information technology systems which are at the disposal of others, the protection of the user also covers this.

After subjecting the provision under analysis to constitutional scrutiny, particularly to the newly named fundamental right, the court concluded that it violated the principles of clarity, legal certainty and proportionality, and that it was therefore unconstitutional. However, the court suggested a future legal formulation of the use of such means of obtaining evidence in accordance with constitutional requirements.[42]

The admissibility of the use of malware in cases of international terrorism was introduced into German law via the Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (Law on the Defence against the Dangers of International Terrorism through the Federal Criminal Police) of 25 December 2008.[43] This took into consideration the comments provided by the Federal Constitutional Court, although not for the purpose of criminal prosecution, but merely for the purposes of prevention.[44]

[41] It should, however, be noted that in 2006 González-Cuellar Serrano had already introduced, in similar terms, the idea of the existence of a right not to have intrusions in one's digital environment (derecho a la no intromisión en el entorno digital), deriving from the right to information technology freedom (derecho a la libertad informática) –'Garantías constitucionales de la persecución penal en el entorno digital', in AA.VV. Derecho Y Justicia Penal en el Siglo XXI – Liber Amicorum en Homenaje al Profesor Antonio González-Cuellar Garcia (Madrid: Editorial Colex, 2006), 887 – 916, 916.

[42] For a detailed analysis of the court's decision, see Juan Carlos Ortiz Pradillo, *Problemas Procesales de la Ciberdelincuencia* (Madrid: Editorial Colex, 2013), 181 – 185.

[43] Pradillo, 'Remote Forensic Software as a Tool for Investigating Cases of Terrorism',5.

[44] Klaus Rogall, 'A nova regulamentação da vigilância das telecomunicações na Alemanha', in Maria Fernanda Palma and others, AA.VV., 2.º Congresso de Investigação Criminal, Coord., (Coimbra: Almedina, 2009) 177 – 220, 120 – 121.

On 8 October 2011, a hacker group named Chaos Computer Club released information reporting on the use of a type of malware by the German police – commonly classified as a Trojan but apparently a blended threat[45] – which was to become known as the Bundestrojaner or Staatstrojaner.

This type of malware is sent to the suspect's computer system in the form of an apparently harmless software update. After the user installs it, the authority behind it is able to record VoIP calls (including Skype), monitor all of the suspect's activity online, record passwords, enter data into the target computer system and even activate the hardware, thus allowing the remote use of the microphone and the webcam to take pictures and record sounds that are subsequently sent to the investigating authorities.[46]

Therefore, despite the observations established by the Federal Constitutional Court for the use of malware, and regardless the exceptional nature in which it is legally based, there were in reports 2011 of the Bundestrojaner being used over fifty times, not limited to the cases to which it is legally destined.[47]

The Spanish legal framework and the Gallardón Draft Bill

No specific legislation exists in Spain at present on the use of malware as a means of obtaining evidence in criminal proceedings. This does not warrant the conclusion that it is currently inadmissible,[48] nor that it will not be created by means of a judicial extension of existing procedural provisions. Illustrating this point with an example, Ortiz Pradillo demonstrates the establishment, through three judgments of the Spanish Supreme Court,[49] of the use of electronic devices called IMSI catchers or Cell Site Simulators. These are designed to determine, from the physical location of certain mobile telephones and their proximity to the antennas that provide them with a connection to the telephone network, their approximate physical location, their IMSI number (International Mobile Subscriber Identity), and the mobile telephone number associated with it.

The Spanish Supreme Court considered that the evidence obtained from such devices was admissible in relation to the legal framework governing the collection and processing of personal data by security forces and corps for the purposes of law enforcement.[50] However, as noted by Ortiz Pradillo, the law does not provide for a warrant for the collection and processing of this data. Taking into account the provisions of article 22 of the Organic Law 15/1999, judicially applied to the collection of these data – qualified by the court as personal data –, and the legal framework governing the transfer of the same data to telephone operators,[51] which provides for the necessity of the precedence of warrant, one can draw the rather illogical conclusion that judicial authorization will not be required when the police may, on its own impulse, obtain them, but it will be legally mandatory when the same entity requires cooperation from telephone operators.[52]

Highlighting the unjustified disparity of the criteria in this matter, Ortiz Pradillo warns that the

[45] A blended threat is the name given to a type of malware that combines certain characteristics of different types of malware. An example of a blended threat can be found in spy-phishing, a tool used to perform phishing attacks that combines different types of malware, such as Trojans or spyware, that allow for the collection of confidential information: Gregor Urbas and Kim-Kwang Raymond Choo, *Resource Materials on Technology-Enabled Crime*, Technical and Background Paper 28 (Canberra: Australian Institute of Criminology, 2008), 5.

[46] For a detailed analysis on the origin and functioning of the Bundestrojaner and of the use of this type of malware by the Swiss and Austrian authorities, see Rolph H. Weber and Ulrike I. Heinrich, *Anonymization* (London: Springer, 2012), 60 – 65.

[47] Marcel Rosenbach, Holger Stark and Steffen Winter, 'Trojan Trouble: The shady past of Germany's Spyware', *Spiegel Online International*, 17 October 2011, http://www.spiegel.de/international/germany/trojan-trouble-the-shady-past-of-germany-s-spyware-a-792276.html .

[48] Velasco Nuñez, for example, though recognizing the difficulties raised by the lack of legal provision on this subject, is of the opinion that these means may be legally admissible through the application, by analogy, of the electronic and magnetic communication interception provisions, in accordance with the conditions imposed by the jurisprudence of the Spanish Supreme and Constitutional Courts on interferences on the right of privacy on telecommunications, for which see Eloy Velasco Núñez, *Delitos cometidos a través de Internet. Cuestiones procesales* (Madrid: La Ley, 2010), 136 – 137; and 'ADSL y Troyanos: Intervención de sus datos y telecomunicaciones en la investigación penal', La Ley Penal, 82 (2011), 18 – 25, 24.

[49] The first dated 20 May 2008 (RJ 2008/4387), the second dated 18 November 2008 (RJ 2009/2089) and the third dated 28 January 2009 (RJ 2009/3299).

[50] Article 22 of the Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Organic Law 15/1999, of 13 December, on protection of personal data).

[51] Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (Law 25/2007 of 18 October, on the retention of data relating to electronic communications and public communication networks).

[52] Juan Carlos Ortiz Pradillo '"Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delinquencia informática', in Redacción Editorial Aranzadi, *Delincuencia Informática. Tiempos de Cautela y Amparo* (Navarra: Thomson Reuters Aranzadi, 2012) 187 – 191; Pradillo, *Problemas Procesales de la Ciberdelincuencia*, 188 – 191.

jurisprudential understanding, according to which the collection of data 'in the context of a criminal investigation – never of an exclusive exploratory nature – for the discovery of a particularly serious crime may be considered proportionate, necessary and, as such, free of any violation of fundamental rights and freedoms', may likewise pave the way for attempts to obtain personal data from open Wi-Fi networks, resorting to 'spyware'.

Objecting to this tendency of case law to place itself in the legislator's stead, and expressing his opposition to an interpretation that seeks to legitimize the use of malware as a means of obtaining evidence without any express provision to that effect, Ortiz Pradillo acknowledges that it is possible that Spanish jurisprudence could interpret certain rules so as to substantiate the admissibility of the use of malware in violation 'of the minimum requirements of legality and clarity established by the ECHR'.[53]

If this were to happen in the absence of the reform of the Spanish Code of Criminal Procedure, certain requirements for the use of malware should be judicially set out which include (i) the requirement of precedence of judicial authorization; (ii) the imposition of the secret nature of the use of the measure; (iii) the establishment of the compulsory cooperation of third parties, including telecom operators when necessary; (iv) the duty of stating the legal basis for the court ruling; (v) the exceptional nature of the measure and its respective application only to particularly serious crimes; and (vi) the collection in a fashion such that the authenticity and integrity of the information obtained are ensured.

The path followed in the Spanish legal system seems to have been different. There is presently a discussion towards a reform at the Spanish procedural level, which will predictably lead to the adoption of a new Spanish Code of Criminal Procedure, effected through what is called by some as the Gallardón[54] Draft Bill.

The legal arrangement provided for in new Title XI, set out under the heading 'remote recordings of computer systems' ('registros remotos sobre equipos informáticos') seems to comply, in general, with the requirements proposed by Ortiz Pradillo, providing for a – in our view essential – duty to state the legal basis for the suitability, necessity and proportionality of the measure. Article 350 of the Draft Bill provides as follows:

> 1.- El Tribunal de Garantías podrá autorizar, a petición razonada del Ministerio Fiscal, la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que la medida resulte proporcionada para la investigación de un delito de especial gravedad y sea además idónea y necesaria para el esclarecimiento del hecho investigado, la averiguación de su autor o la localización de su paradero.
>
> 2.- La resolución judicial que autorice el registro, además de motivar la idoneidad, necesidad y proporcionalidad, deberá especificar:
>
> a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios de almacenamiento de datos informáticos o bases de datos y datos informáticos almacenados objeto de la medida.
>
> b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.
>
> d) Los agentes autorizados para la ejecución de la medida.
>
> e) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.
>
> f) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.
>
> …

[53] Pradillo, '"Hacking" legal al servicio de la investigación criminal: nuevos instrumentos para la investigación y prueba de la delinquencia informática', 198.

[54] The name Gallardón was informally attributed after Spain's Minister of Justice Alberto Ruiz Gallardón.

> 1. The Court of Guarantees may authorize, upon a reasoned request by the public prosecutor, the use of identification data and codes, as well as the installation of a software, which allow, in a remote and telematic manner, the examination at a distance and unbeknownst to its owner or to the user, the contents of a computer, electronic device, computer system, mass storage instrument or database, whenever the measure is proportionate to the investigation of an offence of a particularly serious nature, and is moreover suitable and necessary for clarifying the fact under investigation, the investigation of its perpetrator or the location of his whereabouts.
>
> 2. The legal decision that authorizes the recording, besides having to justify the suitability, necessity and proportionality, shall specify:
>
> a) The computers, electronic devices, computer systems or part thereof, means of storing computer data or databases and data which are subject to the measure.
>
> b) the scope of the measure, the way in which the access to and seizure of the data or computer files that are relevant for the cause will be performed, and the software by means of which the information control will be executed.
>
> d) The agents authorized for the execution of the measure.
>
> e) The authorization, if applicable, for conducting and retaining copies of the computer data.
>
> f) The measures necessary to preserve the integrity of the stored data, as well as for the inaccessibility or deletion thereof from the computer system which it accessed.

Article 351 further provides for the duty to cooperate, including internet service providers and those responsible for the computer system or database subject to the measure.

Notwithstanding the fact that the legislative technique could lead to an excessive margin of latitude for the investigating judge, and that the concept of 'offence of a particularly serious nature' is not duly specified,[55] in the event that the proposal in question is approved, the Spanish legal system will gain in terms of clarity and certainty when applying such measures.

The propensity for the establishment of malware as a means of obtaining evidence in a digital environment

The HIPCAR Project[56] and the Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA[57] are discussed in this section.

With the refinement of the techniques used for the practice of cybercrime on a global scale, interest has been increasing in establishing uniform instruments at the international level to deal this new form of criminality. Indeed, considering that the state in which the target subject operates cannot be the state in which the typical result is produced, and since the application of these instruments is still (or at least should be) limited by the principle of territoriality of the application of criminal procedural law, it is of the utmost interest that the instruments which are deemed more effective are established in the largest possible number of states.

Thus, particularly since the Convention on Cybercrime, a number of supranational initiatives have developed, aiming to promote the adoption of the use of malware as a means of obtaining evidence in a digital environment. Hence, in December 2008, the European Commission and the International Telecommunication Union initiated the Harmonization of ICT Policies Legislation and Regulatory Procedures in the Caribbean (HIPCAR) for the purpose of promoting uniformity of legislation in the countries of the Caribbean Community (CARICOM[58]) in nine areas[59] in relation to information

[55] For a review of this Draft Bill, see Pradillo, *Problemas Procesales de la Ciberdelincuencia*, 193 – 196.

[56] http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx .

[57] OJ L 335, 17.12.2011, p. 1–14.

[58] The members of CARICOM are Antigua and Barbuda, the Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Montserrat, Saint Lucia, Saint Kitts and Nevis, Saint Vincent and the Grenadines, Suriname and Trinidad and Tobago.

[59] Namely, electronic commerce (transactions), electronic commerce (evidence), privacy and data protection, interception of

technology. The result was possibly the most detailed legislative model of cybercrime and digital evidence in existence, which may serve as a guide for the various states that wish to implement it.[60]

Thus, in article 27 of *Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts*,[61] a rule was created which provides for the use of malware for the purposes of criminal investigation (remote forensic software), which reads:

> Sec. 27 – Forensic Software
>
> (1) If a judge is satisfied on the basis of [information on oath/affidavit] that in an investigation concerning an offence listed in paragraph 5 herein below there are reasonable grounds to believe that essential evidence can not be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge/magistrate] [may/shall] on application authorize a police officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:
>
> (a) suspect of the offence, if possible with name and address, and
>
> (b) description of the targeted computer system, and
>
> (c) description of the intended measure, extent and duration of the utilization, and
>
> (d) reasons for the necessity of the utilization.
>
> (2) Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation it is necessary to log
>
> (a) the technical mean used and time and date of the application; and
>
> (b) the identification of the computer system and details of the modifications undertaken within the investigation;
>
> (c) any information obtained.
>
> Information obtained by the use of such software need to be protected against any modification, unauthorized deletion and unauthorized access.
>
> (3) The duration of authorization in section 27 (1) is limited to [3 month]. If the conditions of the authorization are no longer met, the action taken is to stop immediately.
>
> (4) The authorization to install the software includes remotely accessing the suspects computer system.
>
> (5) If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled.
>
> (6) If necessary a police officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process.
>
> (7) [List of offences]
>
> (8) A country may decide not to implement section 27.

Fully aware of the highly intrusive nature of this medium, the proposal introduces certain restrictions for its application, such as the requirement that the evidence cannot be obtained otherwise, the need for the authorization by a judge or magistrate, the obligation to state reasons leading to the authorization, and the limitation of its scope of application.

This provision is a good example of legislative technique that could be used by states wishing to integrate this means of obtaining evidence in their procedure.

On the other hand, the EU has also – albeit with little emphasis – sought to foster the establishment of this means of obtaining evidence. As early as 2008, on the occasion of the adoption of the strategy to strengthen the provisions dealing with cybercrime, the Council of Ministers of the European Union announced that its strategy for the next five years would include, among others, cyber-patrols for the purpose of tracking of

communications, cybercrime, access to public information (freedom of information), universal service and access, interconnection and access and, finally, licensing.

[60] Marco Gercke, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (Geneva: ITU, 2012), 143.

[61] (ITU, 2012), available at http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx .

criminals online and remote searches.[62] However, with greater expressiveness, it was noted in recital 27 of Directive 2011/92/EU of the European Parliament and of the Council, on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, that:

> Effective investigatory tools should be made available to those responsible for the investigation and prosecutions of the offences referred to in this Directive. Those tools could include interception of communications, covert surveillance including electronic surveillance, monitoring of bank accounts or other financial investigations, taking into account, inter alia, the principle of proportionality and the nature and seriousness of the offences under investigation. Where appropriate, and in accordance with national law, such tools should also include the possibility for law enforcement authorities to use a concealed identity on the Internet.

In view of the popularity that this means of obtaining evidence has been increasingly garnering, and given its obvious advantages, it is possible that in the future, Member States might establish it by law, not only in regard to dealing sexual abuse and sexual exploitation of children and child pornography, but also regarding other kinds of serious crime, such as terrorism.

The use of malware and the Cybercrime Law

Direct (in)applicability of the legal framework for the interception of communications and search and seizure of digital data

It is argued, mainly by members of the police – always surrounded by secrecy and never put into writing –, that the admissibility of online searches is based on a direct application of the legal framework for the interception of communications, provided for in article 18 of the Cybercrime Law:

> Artigo 18.º Intercepção de comunicações
>
> 1 - É admissível o recurso à intercepção de comunicações em processos relativos a crimes:
>
> a) Previstos na presente lei; ou
>
> b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.
>
> 2 - A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.
>
> 3 - A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.
>
> 4 - Em tudo o que não for contrariado pelo presente artigo, à intercepção e registo de transmissões de dados informáticos é aplicável o regime da intercepção e gravação de conversações ou comunicações telefónicas constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal.
>
> Article 18 Interception of communications
>
> 1 – The interception of communications shall be permitted in proceedings on criminal offences:
>
> a) Provided for herein; or
>
> b) Committed by means of a computer system or which require the collection of electronic evidence, where such criminal offences are provided for in article 187 of the Criminal Procedure Code.
>
> 2 - Interception and record of transmission of computer data shall only be authorized during

[62] Press Release IP/08/1827 (Brussels, 27 November 2008) available at http://europa.eu/rapid/press-release_IP-08-1827_en.htm?locale=es .

> 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.
>
> 3 - The interception may concern the record of data on the content of communications or aim only at the collection and record of traffic data, and the order referred to in the preceding paragraph shall specify the respective scope, according to the specific needs of the investigation.
>
> 4 - With regard to all matters which are not contrary to this article, the regime of interception and recording of telephone conversations or communications laid down in articles 187, 188 and 190 of the Criminal Procedure Code shall apply to the interception and record of transmissions of computer data.[63]

In addition, the argument is sometimes mixed with the legal framework provided for in article 15 of the Cybercrime Law, which provides:

> Artigo 15.º Pesquisa de dados informáticos
>
> 1 - Quando no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente autoriza ou ordena por despacho que se proceda a uma pesquisa nesse sistema informático, devendo, sempre que possível, presidir à diligência.
>
> 2 - O despacho previsto no número anterior tem um prazo de validade máximo de 30 dias, sob pena de nulidade.
>
> 3 - O órgão de polícia criminal pode proceder à pesquisa, sem prévia autorização da autoridade judiciária, quando:
>
> > a) A mesma for voluntariamente consentida por quem tiver a disponibilidade ou controlo desses dados, desde que o consentimento prestado fique, por qualquer forma, documentado;
> >
> > b) Nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco a vida ou a integridade de qualquer pessoa.
>
> 4 - Quando o órgão de polícia criminal proceder à pesquisa nos termos do número anterior:
>
> > a) No caso previsto na alínea b), a realização da diligência é, sob pena de nulidade, imediatamente comunicada à autoridade judiciária competente e por esta apreciada em ordem à sua validação;
> >
> > b) Em qualquer caso, é elaborado e remetido à autoridade judiciária competente o relatório previsto no artigo 253.º do Código de Processo Penal.
>
> 5 - Quando, no decurso de pesquisa, surgirem razões para crer que os dados procurados se encontram noutro sistema informático, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, a pesquisa pode ser estendida mediante autorização ou ordem da autoridade competente, nos termos dos n.os 1 e 2.
>
> 6 - À pesquisa a que se refere este artigo são aplicáveis, com as necessárias adaptações, as regras de execução das buscas previstas no Código de Processo Penal e no Estatuto do Jornalista.
>
> Article 15
>
> Search of computer data
>
> 1 - Where, in the course of proceedings, the collection of evidence, necessary to uncover the truth, requires that specified computer data, stored in a specific computer system, are obtained, the competent judicial authority shall authorize or order the search to that computer system, overseeing such investigations whenever possible.

[63] Translation from http://www.anacom.pt/ .

2 - The order provided for in the preceding paragraph shall be valid for a maximum period of 30 days, on pain of being deemed null and void.

3 - Criminal police bodies shall undertake the search, without a prior authorization from the judicial authority:

> a) Where whoever holds or controls data under consideration voluntarily consents to the search, insofar as the consent is documented in any way;
>
> b) In cases of terrorism, violent or highly-organized crimes, or where there is evidence to substantiate the imminent commission of a criminal offence threatening the life or integrity of any person.

4 - Where criminal police bodies undertake the search pursuant to the preceding paragraph:

> a) In the situation provided for in point b), the investigation shall be promptly communicated to the competent judicial authority, and assessed by the latter as far as the validation of the measure is concerned, on pain of being deemed null and void;
>
> b) In any other situation, the report provided for in article 253 of the Criminal Procedure Code shall be drawn up and submitted to the competent judicial authority.

5 - Where, in the course of the search, there are grounds to believe that the data sought is stored in another computer system or part of it, and such data is lawfully accessible from the initial system, the search may be extended to the other system, by means of an authorization or order from the competent authority, pursuant to paragraphs 1 and 2.

6 – To the search referred to herein shall apply, duly adapted, the rules on execution of searches provided for in the Criminal Procedure Code and in the Journalists Statute.[64]

[64] Translation from http://www.anacom.pt/ .

However, none of the precepts noted above is sufficient to provide a legal basis for the installation and use of malware in computer systems used by those suspected of committing criminal offences, nor is it possible to combine these provisions in order to construct a legal basis for it.

First, with regard to the interception of communications, neither the provisions of article 18 of the Cybercrime Law, nor the legal framework for interception under paragraph 4, provide any legal basis to support the remote installation of malware with a view to obtaining information. On the contrary, the rules concerned permit the interception of communications, that is, obtaining the communications between the time that they are sent by the sender and the moment they arrive with the recipient, but never the monitoring of a device that may even not be used to send any communication (e.g., if the suspect is typing a password to decrypt files stored in his computer).[65]

Some could argue, however, that article 189 of the Portuguese Criminal Procedure Code, providing for the extension of the rules governing the interception of telephone conversations and communications to environmental intercepts, could provide the legal basis for the installation and use of malware in specific computer systems. Given that paragraph 4 of article 18 of the Cybercrime Law allows for the application of the rules governing the interception of telephone conversations and communications that are included in the Portuguese Criminal Procedure Code, and given that article 189, governing environmental intercepts, provides for an extension of those rules, it could be argued that the similarity between environmental intercepts and the use of malware could provide the legal basis for the use of the latter. However, notwithstanding the existence of

[65] In this regard, the German Constitutional Court stated in its judgment of 27 February 2008, that 'If a complex information technology system is technically infiltrated in order to perform telecommunication surveillance ("source telecommunication surveillance"), the infiltration overcomes the critical hurdle to spying on the system as a whole. The endangerment thereby brought about goes far beyond what is entailed by the mere surveillance of ongoing telecommunication. In particular, the data stored on personal computers which does not relate to the use of the system for telecommunication can also be obtained. For instance, the conduct in using a personal computer for personal purposes, the frequency of accessing certain services, in particular also the contents of files created or – insofar as the infiltrated information technology system also controls appliances in households – the conduct in the personal dwelling can be discovered', official English translation available at https://www.bundesverfassungsgericht.de/en/decisions/rs20080227_1bvr037007en.html

more substantive arguments regarding this matter, to be presented in a future paper, the fact is that, not only are we not necessarily before an interception (the suspect may be monitored even if no communication is being sent by him or her), but also the reference made by the legislator in paragraph 4 of article 18 of the Cybercrime Law to the legal framework for telephone interception is restricted to the 'legal framework for the interception and recording of conversations or telephone calls referred to in articles 187, 188 and 190 of the Criminal Procedure Code', and not to the legal extension of the rules governing the interception of telephone conversations and communications to environmental intercepts provided for in article 189 of the Criminal Procedure Code, which was excluded by the legislator.

Given that the collection of evidence by this means is made in two stages – that of the installation of malware and that of its use –, the highly invasive method used to obtain the information directly from its source cannot be ignored. Neither can it be argued that the use of malware only allows (or intends) the obtaining of information that is available through interception. Moreover, no legal basis can be found in the provisions for the installation of keyloggers that are aimed to obtain, for example, passwords to encrypted documents in the target computer and not to intercept communications.

In fact, the use of malware is not only – not even mainly – to intercept communications. The observation of Manuel da Costa Andrade regarding what he considered to be an online search is relevant:

> '… being in itself an act of telecommunication and assuming that the target computer is connected to the internet, it does not focus or fall on an act of telecommunication. It is, in short, an act of telecommunication whose object is not telecommunication. An attack through telecommunication is not necessarily an attack on freedom of telecommunication … because the online search does not constitute an invasion or perversion of an act of telecommunication, it is not covered or legitimized by the rules of procedural law concerning interference with telecommunications.'[66]

If there are no legal grounds for the methods by which evidence is obtained, it is not possible to create a new rule in which to fit an unusual method of obtaining proof – especially a secret method of obtaining evidence –, ignoring the legal and constitutional limits to its use. In this respect, Paulo de Sousa Mendes observes that 'the catalogue of the typical methods of obtaining evidence includes the respective legal frameworks and does not allow their rules to be flouted, in order that related but atypical methods of obtaining evidence are created. [...] So, the only existing freedom with respect to the choice of the method of obtaining proof of a fact is the possibility of selecting from the catalogue of typical methods of proof those that are regarded as suitable for the process that is taking place'.[67]

Furthermore, as previously noted, some commentators have addressed this matter, and suggested that, with the establishment of article 15 of the Cybercrime Law, particularly paragraph 5, the legislator intended to introduce online searches in the Portuguese legal system. For instance, Paulo Pinto de Albuquerque argues that:

> '[the] online search has now been established in the new Article 15 of Law 109/2009, of 15.9, which provides for the "search in computer system" by order of the judicial authority or even a decision by the criminal police. The law does not place any restrictions relative to the contents of the data that can be searched, contrary to what is the case with the seizure of computer data. The new law also does not require that a computer search that is ordered by the Public Prosecutor or the criminal police has to be validated by the judge. This intrusion into the privacy of the person concerned is manifestly disproportionate, in view of article 26, paragraph 1 and 2, and 32, paragraph 4, of the Portuguese Constitution, which reserves to the judge the investigative measures that represent an intrusion on privacy.'[68]

Notwithstanding the inevitable conclusion of unconstitutionality reached by Paulo Pinto de Albuquerque in view of the assumptions presented, these assumptions do not appear to be verified in this

[66] Costa Andrade, 168.

[67] Paulo de Sousa Mendes, *Lições de Direito Processual Penal* (2013, Coimbra: Almedina), 174.

[68] V. Paulo Pinto de Albuquerque, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem* (2011, 4th edn., Lisboa: Universidade Católica Editora), 502.

case, and there is no need to consider the unconstitutionality of such an interpretation of article 15. This is because, first, paragraph 1 of article 15 of the Cybercrime Law refers to the collection 'of specific and determined computer data, stored in a specific computer system', which, from the outset, excludes the collection of generic data in real time (e.g. passwords to be typed or online activity such as participation in chatrooms or visiting webpages). Secondly, the provisions of paragraph 5 of article 15 of the Cybercrime Law imply that obtaining access to the second computer system should be via the first system that is searched, and not from any other system used by the criminal investigator. Finally, article 15 is silent on the remote installation of any software in the subject's computer. The article refers to the carrying out of the search 'in that system', and the rules governing searches provided for in the Criminal Procedure Code (particularly to paragraph 1 of article 176 of this act), clearly indicate that the search is always carried out physically in the system itself, except as provided for in paragraph 5 of article 15 of the Cybercrime Law, in which case the search is carried out remotely to another computer system, but typically from the system that was initially the subject of the search.

This being so, the necessary conclusion is that these rules do not provide legal basis for the use of malware in the context of criminal investigations in a digital environment.

The use of malware in the context of undercover operations in the digital environment

A different problem, as mentioned briefly above, is the use of malware in the context of undercover operations in a digital environment. In an initiative that is notable for its usefulness[69] but objectionable for lack of specific regulation, as well as to its excessively wide objective scope of application, the legislator introduced, in article 19 (1) of the Cybercrime Law, the undercover agent in the digital environment:

> Artigo 19.º Acções encobertas
>
> 1 - É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:
>
> a) Os previstos na presente lei;
>
> b) Os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico-financeiras, bem como os crimes consagrados no título iv do Código do Direito de Autor e dos Direitos Conexos.
>
> 2 - Sendo necessário o recurso a meios e dispositivos informáticos observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações.
>
> Article 19
>
> 1 – Undercover operations governed by Law no. 101/2001, of 25 August, shall be permitted in the manner specified therein, in the course of the investigation of criminal offences:
>
> a) Provided for herein; or
>
> b) Committed by means of a computer system, to which correspond, in abstract, a term of imprisonment with a maximum band of over 5 years or, even where lower penalty has been provided for, and as regards intentional offences, those against freedom and sexual self-determination, in case victims are minors or incapacitated adults, qualified swindling, computer-related and communication forgery, racial, religious or sexual discrimination, economic and financial infringements, as well as criminal offences laid down in title IV of the Code of Copyright and Related Rights.

[69] The legislator included it, it should be noted, without it being stated in the Convention on Cybercrime nor the Framework Decision 2005/222/JHA, of the Council, of February 24th, on attacks against information systems.

> 2 - Rules on interception of communications shall apply, as appropriate, where the resort to computer means and devices is required.[70]

The provisions of paragraph 2 are formulated in extremely vague terms. The provision has not received particular attention from legal commentary, because it is commonly overlooked or seen as a provision that aims solely to provide the criminal police with certain technical means to intercept communications in the context of covert action in the digital environment. However, the practical application on an operational level of these 'computer means and devices' leads to the conclusion that this is (i) a new (secret) means of obtaining evidence, and (ii) a particularly invasive (secret) method of obtaining evidence.

The novelty of this method of obtaining evidence is clear from the fact that the 'computer means and devices' mentioned here do not fall within any of the means of obtaining evidence provided in the Portuguese criminal procedure law. This conclusion can be drawn from the fact that the Portuguese legislator felt the need to introduce a new rule to legitimize the use of 'computer means and devices', which means that this provision arose because of the failure of other provisions to legitimize the use of such 'computer means and devices'.

A different view would imply that the Portuguese legislator had introduced a redundant and superfluous provision in this article, allowing for the use of an existing means of obtaining evidence in the context of undercover operations. This is a view that would not survive confrontation with the wording of the provision in question, given that it refers to the application of the rules on the interception of communications 'as appropriate', and not in its entirety (which means that some differences exist as to the applicability of these rules, and that no other rules exist that govern the use of 'computer means and devices').

Regarding the particularly invasive character of the use of the 'computer means and devices', it suffices to say that its use is limited to the exceptional context in which covert actions are allowed and, even in this context, they can only be applied 'if necessary' (article 19, paragraph 2, of the Cybercrime Law), or 'if there are reasons to believe that the search is essential for the discovery of the truth or that proof would be otherwise impossible or very difficult to obtain' (article 18, paragraph 2 of the Cybercrime Law). They are also serious enough to require a reasoned order by the investigative judge, upon request of the public prosecutor, in accordance with the provisions of the relevant articles.

Taking into account that the resort to undercover operations is one of the most serious secret methods of criminal investigation, and the use of the most invasive means is only admissible when the use of a less invasive means is not possible, the very existence of a provision authorizing the use of a given secret method, subjecting its use to conditions of necessity and subsidiarity, indicates that it has to be a method that is even more invasive than undercover operations.

This leads to question what these 'computer means and devices' are. The answer implies that they comprise means and devices that are not expressly provided for in the Portuguese criminal procedure law. Their exceptional, invasive and insidious nature can be compared to resorting to the undercover agent and further limited and regulated by the legal framework of interception of communications (though they do not fall within the concept of interception of communication). The only means that could fall within this category and still be qualified as 'computer means and devices' is, in our view, the use of malware as a secret method of criminal investigation in the digital environment.

Taking the legal framework of the undercover agent and the legal framework of interception of communications into account, the following requirements for the use of malware can be derived:

> 1. A fitness for the purposes of the criminal prevention[71] and repression, that is specifically identified and proportionate, both to those purposes and to the severity of the crime under investigation (article 3, paragraph 1 of Law 101/2001 of 25 August).
>
> 2. Well-founded suspicions that (i) one of the crimes defined in the Cybercrime Law has

[70] Translation from http://www.anacom.pt/ .

[71] The fitness for the purposes of prevention does not justify, in terms of the established law, the use of malware on covert operations of preventive nature (by contrast with those of a repressive nature), not least because these actions could seem to be permissible under the provisions of article 3, paragraph 4 of Law 101/2001 of 25 August, and article 18, paragraph 2, of the Cybercrime Law refers explicitly to 'the interception and registration of computer data transmissions can only be authorized during the investigation'.

been committed, or (ii) of crimes committed by means of a computer system, to which correspond, in the abstract, a term of imprisonment with a maximum of over 5 years or, even where lower penalty has been provided for; and regarding intentional offences, such as those against freedom and sexual self-determination, where victims are minors or incapacitated adults, qualified swindling, computer-related and communication forgery, racial, religious or sexual discrimination, economic and financial infringements, as well as criminal offences laid down in title IV of the Code of Copyright and Related Rights (article 19, paragraph 1, of the Cybercrime Law).

3. Its use can only occur when there is reason to believe that the search is essential for the discovery of truth or evidence that is otherwise impossible or very difficult to obtain[72] (article 18, paragraph 2, of the Cybercrime Law).

4. The precedence of reasoned order by the investigative judge, upon request of the Public Prosecutor (article 18, paragraph 2 of the Cybercrime Law).

5. The specification of the data sought, according to the specific needs of the investigation (article 18, paragraph 3 of the Cybercrime Law).

Observing the requirements listed above, nothing appears to preclude, in terms of the established law, the use of malware as a means of obtaining evidence in the digital environment.

The use of malware as a restriction on fundamental rights

The use of malware as a means of obtaining evidence in criminal proceedings is, in some cases, essential. However, the framing of the topic as established in the Portuguese legislation is questionable. The installation of malware is, perhaps even more than the undercover agent, possibly the gravest means of obtaining evidence that is susceptible to being subject to legal control in a democratic state. The high level of social detriment that the remote monitoring of an individual's private conduct when using his computer system represents – perhaps even accompanied by the recording of image and sounds – is a potentially unacceptable intrusion into the intangible core of personal intimacy. When combined with the encroachment on such fundamental rights as the preservation of the intimacy of private life, the inviolability of the domicile, confidentiality, image, word and moreover, the confidentiality and integrity of information systems, it is imperative that the legal establishment of such a provision is appropriately controlled, and that the features of the technical means to be used are limited in a clear and precise way, in compliance with the principle of proportionality.[73]

It is not enough that a rule exists which generically – even if by referral to another legal framework – provides for the use of malware. The supremacy of law is legal precision,[74] which is not compatible with the creation of a method of obtaining evidence of this nature when the legislation fails to provide for the functioning and purpose of the intrusion.

Ultimately, the use of malware is not compatible – as is the case in article 19 (2) of the Cybercrime Law – with merely a reference to a given criminal procedure, followed by a generic referral 'where it is applicable' to a legal framework which, in turn, refers to another legal framework 'with regard to all matters which are not contrary to' that framework. On the contrary, to comply with the provisions of article 18 (2) of the Portuguese Constitution, it is necessary for the legislator to put in place an appropriate protective legal regime, providing the rule in question with special clarity and precision, explicitly pointing out the purposes and limits of the intrusiveness.[75] By not doing so, the rule in question is unconstitutional – at least – by breach of the combined provisions of

[72] Arguably, the use of 'computer means and devices' in the context of covert operations of a preventive nature is unambiguously illegal. This is because these actions appear to be permissible under the provisions of article 3, paragraph 4 of Law 101/2001 of August 25th, but article 18, paragraph 2, of the Cybercrime Law states that 'the interception and registration of computer data transmissions can only be authorized during the investigation'.

[73] Rodrigues, 474 – 475.

[74] Maria de Fátima Mata-Mouros, *Juiz das Liberdades – Desconstrução de um Mito do Processo Penal* (2011, Coimbra: Almedina), 38, 123 – 126 and 242 – 252.

[75] The European Court of Human Rights has already pointed out that a specific 'quality of the law' is required in order for citizens to understand the circumstances and conditions under which the public authorities can obtain redress, for which see by way of example: *Malone v United Kingdom* (ECHR, application no. 8691/79, of 2 August 1984) and *Vetter v France* (ECHR, application no. 59842/00 of 31 May 2005); see also Pradillo, *Problemas Procesales de la Ciberdelincuencia*, 174 – 175.

articles 18 (2),[76] 26 (2),[77] and 1[78] of the Constitution of the Portuguese Republic.

Inquiry of evidence obtained through the use of malware

The analysis of the provisions of article 19 (2) of the Cybercrime Law poses a particularly serious problem, because it is intrinsically linked to the safeguarding of the guarantees of the defendant: that of the disclosure of the methods used to obtain the evidence.

The use of 'computer means and devices' is, by virtue of its insertion in the article on undercover operations, subject to prior resort to the undercover agent. On the other hand, it is also conditional on the rules relating to the interception of communications. However, the Portuguese legal framework in force allows for the non-disclosure of the existence of an undercover operation at any time during the criminal procedure – including during trial – so that the defendant might never know that it ever occurred (this happens mainly for the safety of those involved in the undercover operation). In comparison, however, the legal framework for interception provided for in article 188 (8), which applies by means of article 18 (4) of the Cybercrime Law, provides as follows:

> 8. A partir do encerramento do inquérito, o assistente e o arguido podem examinar os suportes técnicos das conversações ou comunicações e obter, à sua custa, cópia das partes que pretendam transcrever para juntar ao processo, bem como dos relatórios previstos no n.º 1, até ao termo dos prazos previstos para requerer a abertura da instrução ou apresentar a contestação, respectivamente.
>
> 8. From the termination of the investigation onwards, the assistant and the defendant may examine the technical medium for storing the conversations or communications and obtain, at their expense, a copy of the segments they wish to transcribe and add to the process, as well as of the reports provided for in paragraph 1, until the end of the deadlines for requesting the opening of the investigation or submitting a defence, respectively[79].

Thus, taking the provisions of article 19 (2) and article 18 of the Cybercrime Law as including a reference to the legal framework of interception under article 188 of the Criminal Procedure Code, the absurdity is that the existence of an undercover operation is not necessarily disclosed to the defendant, but the rules on interception will require that the defendant be provided with the technical medium used for storing the evidence that is collected using malware. This raises a question: if malware may only be used in the context of undercover operations, how can the existence of these operations not be disclosed and, at the same time, the technical medium used for storing the evidence that is collected using malware be provided to the defendant?

This perplexity cannot justify the non-disclosure of the use of malware as a means of obtaining evidence in a given criminal proceeding. It cannot, because – when no particular issues of safety to those involved in undercover operations arise – any measures constituting an intrusive preliminary enquiry have to be noted in the case file under penalty of a violation of the constitutional guarantees of the defendant.

Moreover, in the case of digital evidence, the authentication of the evidence is important if it is to be admitted into evidence. Its volatility and fragility imposes verification requirements of trustworthiness and assurance of the chain of custody that might not exist with proof commonly collected by undercover

[76] 'A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos.' 'The law may only restrict rights, freedoms and guarantees in cases expressly provided for in this Constitution, and such restrictions shall be limited to those needed to safeguard other rights and interests protected by this Constitution.' Translation taken from http://app.parlamento.pt/site_antigo/ingles/cons_leg/Constitution_VII_revisao_definitive.pdf .

[77] 'A lei estabelecerá garantias efectivas contra a utilização abusiva, ou contrária à dignidade humana, de informações relativas às pessoas e famílias.' 'The law shall lay down effective guarantees against the procurement and misuse of information concerning persons and families and its use contrary to human dignity.' Translation taken from http://app.parlamento.pt/site_antigo/ingles/cons_leg/Constitution_VII_revisao_definitive.pdf .

[78] 'Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária.' 'Portugal shall be a sovereign Republic, based on the dignity of the human person and the will of the people and committed to building a free, just and solidary society.' Translation taken from http://app.parlamento.pt/site_antigo/ingles/cons_leg/Constitution_VII_revisao_definitive.pdf .

[79] Translation by the author.

agents.[80] It is possible that the evidence might be contaminated, for example, by attacks against forensic examinations.[81] Malware that is corrupted or affected by errors is liable to, or even able to diminish the trustworthiness of the evidence. Further, if the computer system itself in which the malware is installed is infected with other types of malware that allow a third party to control that computer system, this might lead to the defendant using the Trojan horse defence.[82]

Since access to information through which digital evidence was collected is essential to its inquiry and subsequent verification of its trustworthiness, it remains possible to conclude that the probable concealment of the use of malware, as well as the omission of reference to the use of malware, might lead to the defendant not being able to examine the evidence so gathered. In such circumstances, this would breach his guarantee of defence and his right to be heard, as provided for in article 32 paragraphs 1 and 5 of the Constitution of the Portuguese Republic:

> 1. O processo criminal assegura todas as garantias de defesa, incluindo o recurso.
>
> …
>
> 5. O processo criminal tem estrutura acusatória, estando a audiência de julgamento e os actos instrutórios que a lei determinar subordinados ao princípio do contraditório.
>
> 1. Criminal proceedings shall ensure all necessary safeguards for the defence, including the right to appeal.
>
> …
>
> 5. Criminal proceedings shall possess an accusatorial structure, and trial hearings and such preliminary investigative acts as the law may require shall be subject to the principle of pleading and counter-pleading.

Conclusions

The use of malware as a means of obtaining criminal evidence is of unparalleled usefulness and effectiveness in the context of criminal investigations in a digital environment. Indeed, the advent of anti-forensic techniques, allied to their ease of use, act to hamper how the police deal with cybercrime. In cases of more serious criminality, it is urgent to impose measures of a graver nature for their prosecution. The usefulness of these methods of obtaining evidence is made manifest not only by their use by several states worldwide, but by the development of supranational initiatives aimed at standardizing their requirements.

In this respect, it appears that it was in order to establish the use of malware that the Portuguese legislator established the use of 'computer means and devices' in the context of undercover operations in a digital environment in article 19 (2) of the Cybercrime law. It did so, however, in a dubious fashion and with a severe shortage of legal clarity, foreseeability and precision, in violation of the provisions of articles 18 (2), 26 (2) and 1 of the Constitution of the Portuguese Republic. This in turn allows for different interpretations of the legislation, which necessarily affects the level of constitutional guarantees provided to the defence in an area where the evidence is of particular weakness.

The legislator should reconsider this legislation in the interests of setting out a fair and transparent means by which the use of malware can be used as a means of obtaining evidence in criminal proceedings, while allowing for the defendant to have access to information concerning the use of the relevant means, in compliance with article 32 paragraphs 1 and 5 of the Constitution of the Portuguese Republic.

David Silva Ramalho is a lawyer at Sérvulo & Associados. He graduated from the Faculty of Law, University of Lisbon, where he also concluded post-graduation courses in IP Law and in Law and Cybersecurity. He is currently a researcher at the Lisbon Research Center for Criminal Law and Criminal Sciences and a Fellow at the Milan Tech and Law Center.

dsr@servulo.com

[80] On the authentication of digital data, see Stephen Mason, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 109 – 147.

[81] Which have an undeserved presumption of trustworthiness: Gary C. Kessler, 'Anti-Forensics and the Digital Investigator', in Craig Valli and Andrew Woodward, eds, *Proceedings of the 5th Australian Digital Forensics Conference* (Perth: Edith Cowan University, 2007); on the undeserved presumption that a computer is reliable, see Stephen Mason, *Electronic Evidence*, chapter 5 and Stephen Mason, 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay', *Computer Law and Security Review*, Volume 30 Issue 1 (February 2014), 80 – 84.

[82] Susan Brenner, Brian Carrier and Jef Henninger, 'The Trojan horse defense in cybercrime cases', *Santa Clara Computer and High Technology Journal*, Vol. 24 (2004), 1 – 53; and Jonathan Clough, *Principles of Cybercrime* (Cambridge: Cambridge University Press, 2010), 34.