LAWFUL HACKING – TECHNICAL ISSUES IN LAW

Milana Pisarić, PhD[1]
Faculty of Law, University of Novi Sad, Serbia

PURPOSE

Several recent trends in technological development have challenged law enforcement agencies' (LEA) ability to lawfully access and examine data at rest and data in transit, especially the increase in use of encryption, wireless networks, cloud services and mobile computing (Going Dark Phenomenon) (Pisarić 2020a:612). This has inevitably urged legislative intervention. In order to restore the balance between the criminal investigation and these technological developments, i.e. to strengthen the LEA position in the fight against IT-enabled crime, in several countries in recent years legislators have introduced amendments in criminal procedure rules, thus creating regulatory framework for new digital investigative measures. One of these measures, and the one of particular controversy, is lawful hacking, i.e. the power of LEA to secretly access a computer device or network in order to gather data to be used as digital evidence. Namely, the legitimacy, necessity and efficacy of empowering LEA to hack back is the subject of political, expert and scientific debate[2] (Pisarić, 2021)[3]

1mpisaric@pf.uns.ac.rs

2 Although the use of hacking techniques by LEA evolved organically to solve the challenge of Going Dark problem, it is not only the part of the encryption debate but goes beyond, since these techniques may also be applied to devices protected by security mechanisms other than encryption.

3 Justification for legal regulation of lawful hacking lacks a quantitative analysis, since there is no publically available and/or accurate and precise data on the number and proportion of cases in which LEA did not have the ability to conduct criminal investigation because they could not access communications or a device and did not have an exploit; the number and proportion of cases in which LEA relies on technology vulnerabilities to obtain evidence; in cases in which LEA used hacking, whether obtained evidence is more crucial compared to other case evidence; whether alternative ways to obtained relevant data other than to obtain this evidence exist; the financial

Lawful hacking

It is not news that, as a part of criminal investigations, LEA have been using hacking techniques for accessing IT system,[4] in order to uncover and gather information relevant to a case that otherwise might be inaccessible. The LEA have been conducting these activities sporadically, while methods and techniques have gradually evolved over the years. Firstly, they used keylogging programs to obtain encryption keys and subsequently access devices, and over time they commenced to rely on exploits of software and hardware vulnerabilities in order to bypass software/hardware protections (via specially designed malware, so called policeware, govware), and even to induce vulnerabilities in software designed to secure data and limit access to information (Quinlan & Wilson, 2016). In this article the author is only interested in the analysis of LEA's use of software tool for hacking.

The hacking tool is a software usually based on some vulnerability - a flaw in software or hardware of a target IT system, that alone, or combined with others, enables unauthorized party to covertly perform activities on the target IT system. Consequently, the essence of hacking technique, as investigative measure, is in LEA using such a tool and exploiting some of these vulnerabilities, specific for targeted IT system, in order to gain access to the system and somehow manipulate it, without knowledge and consent of the user.

The hacking tool may be installed on a target's IT system either remotely, or in situ, after gaining physical access to the system itself (in this case, a vulnerability might not be exploited to install malware or access data on the device, e.g. if the passcode is known). This article considers only hacking tool that enters the target IT system remotely.

The use of hacking tool in the context of criminal investigations may serve different purposes, namely (i) remote access to an IT system, in order to conduct online search and seizure of data stored within the system, or monitoring and interception of data transmitted within/through the system), and (ii) in situ forensic examination of a seized device, in order to conduct search and seizure of data stored within the system (e.g. after breaking into an encrypted phone). Although vulnerabilities may be also the basis for forensic analysis tools, the author refers only to the tools that use vulnerabilities for security bypassing, in order to gain remote access to the IT system, and further conduct some activities within the system, primarily, to extract data and send them to LEA IT infrastructure. The remote investigation in IT system with technical tool consists of two phases. The

cost of developing or purchasing vulnerability exploits, etc. The analysis of these data could help designate the possible effectiveness of using, or exploiting vulnerabilities. Further argumentation on this issue is not the purpose of this paper.

4 This term refers to both devices and network.

first phase concerns the remote secret intrusion into the IT system. The second phase concerns the performance of certain investigative actions in penetrated IT system, in order to access and collect data that may serve as digital evidence. The purpose of this paper is only to consider the LEA use of hacking tool for remotely accessing IT system and conducting further investigative activities, primarily electronic communications surveillance (Pisarić, 2021) and online search and seizure (Pisarić, 2022).

The controversy with state hacking lays in its risks. On the legal side, there might be a negative effect on integrity of digital evidence and potential privacy violations. In order to address these significant risks properly, the appropriate legal conditions and mechanisms governing law enforcement hacking should exist, since in the absence of clear legal and procedural framework they will intensify. Hence, starting from the principle of legality, the legal framework for the use of hacking techniques by LEA for the purpose of criminal procedure should not be too broad and general, but clear, specific and precise instead. General consideration of a legal framework governing hacking as special investigative measure is not the subject of this article (Pisarić, 2020b)

On the technical side, there is the issue of informational security weakening. The risks associated with LEA use of hacking tool, due to intrusiveness and scope of this investigative measure, includes: creating a disincentive to disclose vulnerabilities that should be disclosed because other attackers might independently discover them; cultivation of a market for surveillance tools and 0-days; risking that vulnerabilities exploited by the malware will be identified and used by other attackers, as a result of either LEA losing control of the hacking tools, or discovery by outsiders of law enforcement's hacking activity; creating an incentive to push for less-secure software and standards; and risking that the malware will affect innocent users (Pfefferkorn, 2018: 2). These risks should be taken into consideration, as well, when regulating the technical side of lawful hacking. So, the purpose of this research is to consider regulatory framework for lawful hacking, primarily the regulation of technical side of this digital investigative measure.

DESIGN/METHODS/APPROACH

In this article the author uses normative and comparative legal method.

Integrity of digital evidence acquired by lawful hacking during criminal investigation is accomplished by following standard operating procedures and principles of digital forensics. Still, the law should properly address several technical issues, mainly by prescribing requirements for hacking tools. In order to diminish the se-

curity risks to the minimum, the law should also set limitations for the use of vulnerabilities and their destiny after the use. During research, the author considers these requirements, in general, and explores the main technical issues that should be tackled in establishing a proper legal framework for lawful hacking, primarily regarding hacking tools and vulnerabilities.

Deployment of technical measures in order to covertly and remotely infiltrate an IT system, collect data from it, and electronically transmit them to LEA for the purpose of criminal investigation, is explicitly regulated only in a few countries. So, parallelly, the author analyses how technical means and techniques used by LEA for the purpose of criminal investigation are regulated in two countries, with explicit norms on LEA hacking powers - Germany and the Netherlands.

Scope of hacking power

Since 2017 the German Code of Criminal Procedure (Strafprozeßordnung BGBI, 2022)[5] empowers the LEA to use special *technical means* to gain *covert access to devices and data* as a part of criminal investigation, with regard to telecommunications surveillance (Article 100a) and covert remote search of information technology systems (100b). In other words, regarding its functionalities, a hacking tool may be used for the *purpose* of conducting surveillance of telecommunications on source or remote online search of IT system. As for *surveillance*, the Code envisages that, if certain conditions are fulfilled, telecommunications may also be intercepted and recorded in such a manner that technical means are used to interfere with the information technology systems used by the person concerned, if this is necessary to enable interception and recording in unencrypted form in particular (Article 100a, paragraph 1, sentence 2). Also, the content and the circumstances of the communication stored in the person concerned information technology systems may be intercepted and recorded if they could also have been intercepted and recorded in encrypted form during ongoing transmission processes in the public telecommunications network (Article 100a, paragraph 1, sentence 3). As for *covert remote search*, the Code envisages that, if certain conditions are fulfilled, technical means may be used even without the knowledge of the person concerned to gain covert access to an information technology system used by the person concerned and to extract data from that system (Article 100b, paragraph 1).

Since 2018 the Dutch Code of criminal procedure (Wetboek van Strafvordering)[6] stipulates that *investigation in automated work* may be conducted with the aid

5 After being amended by the Law to make criminal proceedings more effective and practical (Gesetz zur Effektiveren und Praxistauglicheren Ausgestaltung des Strafverfahrens, BGBI, 2017).
6 After being amended by so-called Computer Crime Act III (Act of 27 June 2018 amending the Criminal Code and the Code of Criminal Procedure with regard to improving and

of *technical means* (Article126nba CCP). Namely, if certain conditions are set, hacking power may be used for several *purposes*: A) in the event of a suspicion of a serious crime (as described in Article 67, paragraph 1), in order to: a) determine certain characteristics of the automated work, or the user (such as identity or location), and record them; b) execute an order as referred to in Article 126l (recording of telecommunications) or Article 126m (monitoring of telecommunications); c) execute an order as referred to in Article 126g (systematic observation); B) in the event of a suspicion of a crime, which is punishable by a prison sentence of eight years or more, or a crime that has been designated by order in council, in order to: d) record data stored in the automated work, or stored only after the time of issue of the warrant, to the extent reasonably necessary to reveal the truth; e) make data inaccessible, as referred to in Article 126cc, paragraph 5. These measures are enforceable also in investigating organized crime (Article 126uba) and terrorism (Article 126zpa), since Article 126nba applies *mutatis mutandis*.

Based on these provisions, if procedural requirements are met, the German and Dutch LEA may use hacking tools as a part of criminal investigation. The author further analyses these provisions with connection to provisions regulating technical aspects of lawful hacking.

FINDINGS

As a result of the research for the purpose of the article, the author demonstrates a proper regulation of technical issues for lawful hacking in a legal framework, primarily regarding (i) hacking tools; and (ii) vulnerabilities.

Limitations regarding vulnerabilities

Vulnerabilities exploited in lawful hacking are the ones either previously known but not yet patched by software/hardware vendors (n-days vulnerabilities), or previously unknown to the developer and general public, undisclosed and hence unpatched (0-day, or zero-day vulnerabilities). LEA may also rely upon known vulnerabilities that may be patched but users may continue to rely on outdated, unpatched versions. Regarding vulnerabilities, the legislator should consider at least two issues, as the most important and relevant: the type of vulnerabilities LEA could use, and vulnerabilities disclosure.

strengthening the investigation and prosecution of computer crime - Wet tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit, Staatsblad 2018).

Type of vulnerabilities

Giving that acquiring and retaining unknown vulnerabilities comes with an extensive set of critical challenges, especially because exploiting an unknown vulnerability always carries the risk of exposure, and therefore degradation of its operational value, it might be only legitimate that LEA hacking operations are limited to the use of known vulnerabilities. However, although it is justified to allow only the use of malware based on the existing vulnerabilities due to security risks, using zero-day exploits might be also regarded as necessary and preferable. Nonetheless, there should exist a proper policy response that would responsibly govern the use of zero-day exploits and limit potential damage, including: the implementation of technical defences to prevent rediscovery of the vulnerability; the requirement for law enforcement agencies to report the vulnerability when it is discovered and to gain a warrant to continue (barring emergency circumstances); the deletion (or ignoring) of any additional information discovered not specified in the warrant; and the regulation of exploitation tools under 'dual-use' restrictions (Bellovin, et al., 2014: 64).

The only example of a legislative response towards zero-day vulnerabilities is found in the Netherlands. Namely, Dutch Code recognizes the term 0-day vulnerability, defining it as a vulnerability in an automated work of which it is plausible that it is not known or can be assumed not to be known to the manufacturer of the device or of the program on the basis of which computer data is automatically processed, and that can be used to penetrate that automated work (Article 126ffa, paragraph 2). The Code permits the use of zero-day vulnerabilities, while dictating that law enforcement must not purchase zero-day vulnerabilities and must report any exploited vulnerabilities.

Disclosing Vulnerabilities

The process leading vulnerability from 0-day to n-day is called vulnerability disclosure. Currently one of the most difficult regulatory challenges with regard to lawful hacking is considering the question whether LEA should retain, or disclose zero-day vulnerabilities that they discover/obtain, i.e. report them to vendors, targeted individuals or the general public. The need for disclosure of vulnerabilities discovered, or received is essential because unpatched vulnerabilities needlessly perpetuate global risks to IT infrastructure and users. Although non-disclosing 0-days bears a much higher risk, n-days can be as damaging - WannaCry and NotPetya ransomware are example of lack of proper vulnerability management. On the other hand, disclosed vulnerabilities, if patched, may render them useless to

LEA, for a subsequent investigation. That is why LEA should not stock vulnerabilities, but disclose them properly, while delay in disclosure should be time-limited and extraordinary.

Handling, maintaining or disclosing vulnerabilities in LEA possession is of utmost importance. For this purpose, the *vulnerability equities policies* (VEP) are useful to be defined, as it may help LEA to access reasons for, or against retaining a particular vulnerability from disclosure. Several factors may be taken into consideration when deciding whether or not to disclose vulnerability,[7] and if the cons outweigh the pros, the policies should detail how to disclose vulnerabilities responsibly to minimize the potential harm to the public. Only a few countries have so far developed or publicly released such policies. One example is the VEP being implemented in the USA since 2008, for deciding whether or not to disclose a vulnerability, in case LEA discovers or obtains a newly discovered vulnerability.

The Dutch Code does not only permit the use of zero-day, but it envisages the *possibility of delaying the notification of unknown vulnerabilities*. It is stipulated that public prosecutor may, on the basis of an important investigative interest, and after prior written authorization by examining magistrate, order that disclosure to producer of an unknown vulnerability used for penetrating an automated work (as referred to in Aricles 126nba, 126uba and 126zpa) is postponed. An order is in writing and it should state: a. the vulnerability, and b. the weighty investigative interest (Article 126ffa, paragraph 1).

Requirements for hacking tools

Notwithstanding the type, or source of vulnerability, or the origin of the tool based on its exploit, the technical means must serve its purpose, which is to collect data, otherwise not accessible, that are to be used as digital evidence. In order for the collected data to be accepted as evidence in legal proceedings before the court of law, in addition to procedural requirements concerning this investigative measure, the hacking tool must be reliable and relevant as a standard of digital forensics. In addition, certain technical requirements should be met, so IT security and privacy risks are reduced to minimum.

7 Namely: the scope of the use of the vulnerable system in critical infrastructure systems, economy, and/or in national security systems; degree of the risk imposed by unpatched vulnerability; possibility of harm caused if the vulnerability is used by adversaries and probability of knowledge about the use; degree of need for information that is to be gained from exploiting the vulnerability; alternatives to gain this information; possibility to use the vulnerability for a short period of time before disclosure; probability of someone else discovering the vulnerability; alternatives for the vulnerability to be patched or otherwise mitigated.

The origin of hacking tools

Depending on the type and complexity of IT system to be accessed, vulnerabilities may be rare and difficult to find in some cases, only temporarily useful (since, once discovered, there is an urge for them to be patched) and expensive - especially when it comes to zero-day vulnerabilities. LEA may gain knowledge of vulnerabilities in various ways – they could use publicly available information on pre-existing vulnerabilities,[8] or purchase exploits of vulnerabilities off-the-shelf from third party in vulnerabilities marketplace, or develop exploits in-house, tailored to suit specific needs (Ohm, 2017: 314-315).

As for the option of purchasing vulnerabilities, or more often, hacking tools based on vulnerabilities, from third parties, it should be borne in mind that the state's participation in the vulnerabilities market could contribute to its growth and cultivation, by increasing incentives against disclosure of the vulnerability or by increasing the market for vulnerabilities and thus encouraging greater participation in it (Pfefferkorn, 2018). Namely, some public reporting have shown recently the grey market for zero-days and government hacking technology is developed, with several prominent private companies selling software vulnerabilities and exploits along with surveillance capabilities, such as spyware and other services to government actors (Antis, 2021:4). In order to avoid LEA reliance on individuals and companies connected to governments, or other entities that have been reported to conduct unlawful government hacking or violate human rights, like in case of the FinFisher (Deutsche Welle, 2020, October 14), or NSO group Pegasus (New York Times, 2022, January 28), LEA should purchase hacking tools, vulnerabilities, and services only from third parties which are transparently vetted, according even to the UN (Associated Press, 2021, August 12). Also, these off-the-shelf products and services may not be useful to law enforcement who need to customize them for legal use.

Instead of purchasing external hacking tools, the LEA might develop its own tools. However, in-house developing of hacking tools faces several challenges: cost, complexity, lack of technical and human resources.

Unfortunately, LEA rely too much on commercial software and vendors' capability to validate their own tools (like with other digital forensics tools) which often do not fulfil basic security requirements. That brings us to another important issue.

8 An example of the option of using publicly available information is National Vulnerability Database (NVD) in the USA, which is the repository of standards based vulnerability management data, which enables automation of vulnerability management, security measurement, and compliance.

Standardization of tools

In deploying methods and techniques of digital forensics in order to gain digital evidence, LEA should follow rigorous standardized procedures. Still, even when closely following predetermined digital investigation steps and recommendations, errors can be made. For this reason, it is essential that digital investigators develop appropriate skills, and certifications are a good way to develop them. Also, one of the main standard requirements concerns the tools. As for other tools used in digital investigation, the software tool based on vulnerability, with the functionality to remotely access IT system and acquire data, should be used in legal setting. Besides that, in order to maintain the integrity of the digital evidence, hacking tools need to be reliable and relevant, hence thoroughly developed and tested, and secured in line with state-of-the-art guidelines. This is, unfortunately, not always the case (Horsman, 2019). The Daubert standard[9] may be useful in the court of law, but it is not enough. In order to improve standards of evidence, the required level of reliability should be prescribed by the law, and connected with tool-testing. Since each tool needs to be tested before it can be used in the field, the tool-testing should be obligatory and systematically arranged at state level. The essence of this requirement is the guarantee that when an approved tool is used in conducting investigative activities, it can be assumed that the legal requirements regarding the reliability, integrity and traceability of the data have been met. The German and Dutch approach towards standardization of the tools may be regarded as examples of good practice.

In **Germany** the software products used to carry out source telecommunications surveillance on source and online searches are tested before they are released for use and comprehensively checked for compliance with legal requirements set in 2018 by *Standardized service description for system for performing measures of source telecommunications surveillance and online searching*. This Act concretizes the specifications resulting from the legal provisions of the Code, and it is meant to serve as a guideline to ensure the development, procurement and use of a software system within a uniform framework. This system consists of various components that work together as an overall system: access and monitoring software, which is applied to the target system, where data is collected and forwarded to the LEA; control and recording unit: a software unit used by LEA to control the access and monitoring software, to make the recording and evaluation of data and to log all activities; and network connection, with function to forward data from target system to control and recording unit, and back.

9 Daubert test utilizes four guiding questions to assess reliability of tools (with regard to testing: can and has the procedure been tested; error rate: is there a known error rate of the procedure; publication: has the procedure been published and subject to peer review; acceptance: is the procedure generally accepted in the relevant scientific community.

Chapter 3 sets *technical requirements* that should be met, so three essential basic values of IT security (availability, confidentiality, integrity) are addressed. In order to maintain confidentiality, all data[10] transmitted between a target system and the LEA control and recording unit are protected against unauthorized access by appropriate procedures. In addition, monitoring software must be protected against detection and disclosure. As for integrity, data collected must be protected against changes using suitable procedures, and any manipulation of data must be recognizable. Regarding availability, it is stated that appropriate security measures must be taken to avoid loss of exported data, as well as other failures and disruptions.

A software is accepted on the basis of a defined *test procedure*, the results of which are documented as a part of the overall acceptance process. Besides, before each use of the software onto specific target system, compliance with the legal requirements adapted to the specific conditions of use is carried out.

Providers of the software should be carefully selected with regard to their professional competence and trustworthiness, while the providers contractually ensure compliance with the requirements and framework conditions resulting from the legal standardizations, and also guarantee that they: comply with the state of the art in secure software development; restrict physical access, as well as logical access, and access to the development environment to the persons authorized; procure external components from verified sources and certify their security properties before they are used; inform the LEA immediately about security incidents, identified security deficiencies or other events that endanger the safe, lawful and proper implementation of investigative measures.

In the **Netherlands**, based on Article 126ee of the Code, *Decree on investigation in a computerized work* is published in 2018. The Decree contains technical rules on the exercise of the power to penetrate an automated work and to conduct an investigation: 1) *rules about the expertise and authorization of the investigating officers* who conduct investigations in a computerized system and the cooperation with other investigating officers (Chapter 3);[11] 2) rules on the recording of data for

10 E.g. control commands to the target system, update the monitoring software on the target system, the data transferred from the target system.

11 The Decree also prescribes functional separation between technical and tactical investigation officers, since the order is executed by specifically designated and expert technical investigation officers, while the collected data is analyzed by officers investigating the case (Article 126nba, paragraph 8, item b). An investigating officer may be appointed by his employer for penetrating automated work and carrying out investigative acts, only if he is a member of a technical team, and he may be designated as a member of a technical team by the chief of police, only if he has met the qualifications designated by Minister of Justice and Security (Article 3 of Decree).

the execution of an order (Chapter 4), 3) rules on standard tool requirements and its inspection (Chapters 5 and 6).

A technical tool is regarded as a software application that contains functionalities which allow data to be detected, recorded and transported. In order to guarantee the reliability and integrity of technical tools, the reliability and integrity of the data recorded with them and the traceability of the data, the Decree in Chapter 5 sets various *technical requirements*. Chapter 6 contains *rules on the prior inspection* of a technical means, which, before used to carry out an order, must be approved by an inspection service. During the inspection, it is checked whether the means complies with the technical requirements set out in Chapter 5. The part of the National Unit of the National Police, the Inspection Service of the National Operational Cooperation Service, is designated for the inspection of technical means used for carrying out investigative actions in an automated work. In order to guarantee the quality and consistency of the inspection, an inspection service draws up an inspection protocol, which requires prior approval of the Minister of Justice and Security. A report is drawn up of the inspection, stating in the case of approval that the technical means meets the technical requirements set by the Decree. The report of an approved technical tool states, at least: a) that it satisfies the requirements of Articles 8 to 13; b) a reference number; c) a description of the operation of the technical tool; d) an indication of the functionality or functionalities of the technical tool; e) relevant mandatory replacement guarantees with which one or more requirements referred to in Articles 8 to 13 can be met; f) relevant information regarding the operation of a functionality or functionalities of the technical tool; g) the period for which the inspection applies, as long as the functioning of the technical tool is unchanged.

However, the rules of Chapters 5 and 6 are *relativized*, because Article 21 of the Decree states that the public prosecutor may order that investigative acts are performed with an unapproved technical means, if the investigative interest requires so. If an unapproved technical aid is used for the execution of an order, the public prosecutor also states the outcome of the inspection or re-inspection after use in the procedural documents. However, an inspection or re-inspection may be omitted after use, if, in the opinion of the public prosecutor, the nature of the technical means precludes this. In that case, the public prosecutor states in the procedural documents that Article 21(4) has been applied and which additional safeguards have been taken to guarantee the reliability, integrity and traceability of the data recorded with the technical tool.

Logging Requirement - transparency and traceability

First of all, as vulnerability used in the hacking operation, combined with the software and hardware, could tamper with integrity of evidence, it should be allowed that an independent, outside expert audit them. In order to do so, disclosure of some relevant information is of clear interest for the defence in a criminal procedure. The core information sought by the defence, in order to consider the integrity of digital evidence acquired by the hacking, is the complete source code of the hacking tool, including the exploit and payload – the so-called Graymail tactic (Bell, 2018). However, when using a tool purchased from a third party, the complete source code is protected by a non-disclosure agreement. There are examples that defence lawyers have requested the source code for the exploit and sought judicial compulsion for these requests – e.g. in the PlayPen case, at least one magistrate judge has ordered the government to produce the source code, and the government has decided to drop the charges instead (for examples, see: ACLU Foundation, Electronic Frontier Foundation, National Association of Criminal Defense Lawyers, 2017). The prosecution should disclose not only the hacking tool, but also the attack vector and the method used for hacking, which devices were targeted, and what digital evidence was accessed (Kaleigh & Aucoin, 2018: 26).

Secondly, since lawful hacking is a covert measure, it is of particular importance that the processes for acquiring information is traceable without any doubt at a later stage of the procedure, hence hacking tools need to be equipped with a tamper-proof logging mechanism, which guarantees the integrity and authenticity of digital evidence, by enabling judiciary and others to retrace and comprehend the operation of data collection, evaluation and processing by LEA.

In **Germany**, the Code requires that each time technical means are used (both with regard to telecommunications surveillance on source and with covert remote search of information technology systems), a record needs to be made, containing information about the designation of the technical means and the time of their use, information required to identify the information technology system and changes made which are not only transient, information enabling the identification of the data captured and the unit implementing the measure (Article 100a, paragraph 6). Additionally, Standardized service description requires that the software should contain a proper logging mechanism that serves to prove that the data actually originate from the target system, that they are complete and have not been modified. In order to ensure traceability, the software should also contain archiving functionality (Chapter 5).

In the **Netherlands**, the *automated recording* of data collected in the course of execution of the order is obligatory (Article 126nba, paragraph 8, item b). More precise rules are set in Chapter 4 of the Decree, regulating recording data in log

files**.** Firstly, during the execution of an order, data is continuously and automatically recorded in log files, about: a) acts performed in the execution of an order;[12] b) access to a technical infrastructure; c) data recorded on the technical infrastructure; d) the functioning of the technical infrastructure (Article 5). The recording of data in log files should take place in such a way that it can be established, both during the period stated in the order and after its expiry. Also, a record must be made on whether an irregularity that affects reliability and integrity of data recorded has occurred on a technical infrastructure during the execution of an order. In case of such an irregularity, an investigating officer of a technical team draws up an official report, which is sent to the public prosecutor (Article 6). The contents of log files should not be changed, and they may be accessible only to the officials designated by the chief of police. When recording data in log files, measures are taken to prevent log files from being changed, or accessed by unauthorized persons, and to enable afterwards whether changes during, or after inspection occurred (Article 7).

Additionally, after target IT system is accessed, a *registration officer records*, at least: an indication of technical infrastructure to which access is granted; time of access; the indications in the order of the nature and functionality of a technical tool; period specified in the order within which the order must be executed; an indication of the investigating officer of a technical team requesting access (Article 22). After automated work is accessed, the investigating officer who places a technical tool, draws up an official report of the placement, which is sent to the public prosecutor. Any irregularity occurred during installation of a technical means, or in the course of investigative acts, is reported in the official report (Articles 23-24). Also, the official report of complete or incomplete removal of the technical tool is to be created (Articles 25-26), and sent to the public prosecutor.

Additional requirements - protective measures

Since the data obtained through lawful hacking possibly includes a large amount of sensitive and private information, the law must contain the appropriate safeguards. First of all, the *functionality* of tool needs to be limited and precisely indicated. In order to ensure privacy protection, the collected data not relevant for the case need to *be deleted* immediately, with state-of-the-art software that ensures that once deleted, the data cannot be restored. Additionally, the fact that information is deleted needs to be properly logged. Because smart devices are equipped with various *sensors* (e.g. biometric sensors), which upon accessing the device, reveal LEA private information on the user, and may be generated, stored, and/or

12 If these data cannot be recorded automatically due to their nature, an investigating officer manually records the actions.

manipulated, hacking power enabling LEA access these sensors should be limited by the legal restrictions and properly addressed in a warrant (European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, 2017).

In this sense, the **German** Code in Article 100a, paragraphs 5 and 6 prescribes *certain protective measures* that apply to telecommunications surveillance on source and covert remote search of IT systems. Namely, the technical mean is installed so that: 1. only the following can be intercepted and recorded: a) ongoing telecommunications, or b) content and circumstances of communication which could also have been intercepted and recorded from the date on which the order was made, during ongoing transmission processes in the public telecommunications network; 2. only those changes are made to information technology system which are essential in order to capture data; and 3. the changes made are automatically reversed once the measure is concluded, insofar as this is technically possible. Additionally, using methods reflecting the state of the art, technical means should provide protection against unauthorized access, while the copied data should be protected against modification, unauthorized deletion and authorized inspection (Article 100a, paragraph 5).

Further, standardized service description requires that before introducing monitoring software, it must be checked and documented that only an impairment of the target system that is limited to the unavoidable is to be expected, since the security and stability of the target system is affected by installing, operating and the deletion of the monitoring software. Additionally, the software should be set in such a manner that it causes only the necessary changes. At the latest, when the ordered measure has expired, the software must be deleted immediately. Changes to the system and other files on the target system must be reversed as far as technically possible, and as long as the target system can be reached by the control and recording unit. For this purpose, the software must have the appropriate functions (Chapter 5).

The **Dutch** Code envisages that the order allowing the use of technical means for the mentioned purposes must, among other, state an indication of the nature and functionality of the technical means that is used for the execution of an order; and part or parts, with a view to which an order is given and a clear description of the actions to be performed (Article 126nba, paragraph 2, items d and e). The Code further requires that after an investigation has ended, a technical mean should be removed. If it cannot be removed (completely), and this poses risks to the functioning of the targeted automated work, the public prosecutor informs the administrator of an automated work thereof and provides necessary information for the complete removal (Article 126nba, paragraph 6), while the investigating officer charged with removal terminates the transport of data registered by technical tool to technical infrastructure of LEA (Article 26 Decree).

Additionally, in order to guarantee the lawfulness of its deployment, the Decree requires that the tool must be set up in such a way that it is possible to enable only the functionality(s) as specified in an order, and only to detect and register data for the purpose of this functionality. A technical tool must be able to record data in such a way that the content is identical to the data detected in an automated work, and to provide the registered data with the date and time of registration, with their unique characteristics. This enables that, when data are recorded on storage location and are recognized, the origin of data can be determined at any time. Further, integrity is safeguarded by setting the requirements for security of a technical tool and the data registered and transported by a technical device. Also, a technical tool should automatically transfer the registered data to a technical infrastructure, and during that transfer it should protect the registered data against alteration and unauthorized access. In addition to technical requirements for technical tool, the Decree also lays down the requirements with regard to the quality of technical infrastructure on which the data, registered with a technical device, are recorded (Chapter 5).

ORIGINALITY/VALUE

If legislative action regarding hacking techniques for the purposes of criminal proceedings is deemed necessary, the legislator should regulate their use as a special evidentiary act, by establishing a mechanism that consists of certain, specific ex-ante and ex-post elements of the normative framework (Pisarić, 2022). Alongside, the guidelines for handling digital evidence should be designed and implemented, while digital evidence needs to be gained, transferred, analysed, stored, and presented in a tamper-proof chain of custody (Herpig, 2018: 13).

As for legal regulation of the technical side of lawful hacking, special attention should be primarily paid to defining legal rules that would govern the use of hacking tools and vulnerabilities. In this paper the author discussed how technical means (i.e. hacking tools and vulnerabilities) should be addressed in law, and analysed relevant legal provisions in Germany and the Netherlands. Based on the analysis, several elements of legal framework, regarding technical side of lawful hacking, are proposed:

Rules governing hacking tools - an adequate regulation should contain certain provisions that act to help manage the risks posed by law enforcement hacking, by addressing technical requirements for the tools:

a. Tool development and purchasing - the law should define the appropriate steps that should be taken to effectively monitor the development of hacking tools, ei-

ther in-house, or by third parties; special attention should be paid to purchasing hacking tools from third parties so as to avoid legitimizing the growth and cultivation of a "vulnerabilities market";

b. Tool requirements - reflecting the state of the art, the law should define standardized technical requirements, as safeguards ensuring reliability, integrity and traceability, at least with regard to:

- *Functionalities minimization* - the tool should be used only for the functionalities allowed;

- *Changes minimization* - the tool should be set in such a manner that it causes only necessary changes;

- *Data minimization* - the tool should be configured in a way that ensures the data collected are minimized to the greatest extent possible;

- *Handling and storage of data during an investigation* – the tool should be configured in such a way that protection against unauthorized access is provided, while the copied data are protected against modification, unauthorized deletion and authorized inspection;

- *Logging details of a hacking operation* - key information related to the tool should be logged, including, at least: the designation of the technical means and its date of use; the organizational unit implementing the action; and information related to the identification of the target system and the collected data;

c. Tool testing - the law should define procedure, so the tool may be approved after determining its compliance with legal requirements;

d. The future of used tool once the operation has ended – the law should stipulate that, after the operation, the hacking tool *needs to be removed* from the target device. Additionally, if it cannot be (completely) removed and removal poses risks to the functioning of the hacked computer, *the device owner/administrator* should be informed and provided with sufficient information to enable them to completely remove the tool;

RULES GOVERNING VULNERABILITIES

a. Establish a national vulnerability assessment and management process - Since mitigating and patching vulnerabilities is crucial for protecting IT security, a proper vulnerability assessment and management process (vulnerability equities policies - VEP) should be defined and implemented.

b. Define vulnerability disclosure – If after policy and technical considerations, it is decided in favour of vulnerabilities disclosure, there are still a few issues that the

law should address: 1. the moment of disclosure (right after its exploitation for the investigation, or right after the end of the investigation), 2. the manner of disclosure (finding the most secure way, to avoid malicious misuse before disclosed vulnerability is patched), 3. the parties informed (who the vulnerability is disclosed to – the software/hardware vendors, or others as well).

If the legislator chooses to empower LEA to exploit vulnerabilities in software and hardware products in order to gain remote access to IT system and to remotely search and monitor user activity in order to collect the data to be used as digital evidence in criminal procedure, the presented finding should be used as guidelines for creating the appropriate legal framework.

During the research the author has noticed that information on techniques and methods used are mainly classified and not publicly available, and this non-disclosure is comprehensible, in order to preserve operational effectiveness. Nevertheless, and because of that, the legislation should contain as much as possible specific and precise provisions governing the technical side of lawful hacking.

REFERENCES

ACLU Foundation, Electronic Frontier Foundation, National Association of Criminal Defense Lawyers (2017) Challenging government hacking in criminal cases, Downloaded June 16, 2022 https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf;

Bell, C. (2018). Surveillance Technology and Graymail in Domestic Criminal Prosecutions, *Georgetown Journal of Law & Public Policy*, 16(2), 537-558;

Bellovin, S.M., Blaze, M., Clark, S. & Landau, S. (2014). Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet, *Northwestern Journal of Technology and Intellectual Property*, 12(1), 1-64;

Besluit van 28 september 2018, houdende regels over de uitoefening van de bevoegdheid tot het binnendringen in een geautomatiseerd werk en het al dan niet met een technisch hulpmiddel onderzoek doen als bedoeld in de artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering (Besluit onderzoek in een geautomatiseerd werk), Staatsblad 2018, 340, https://zoek.officielebekendmakingen.nl/stb-2018-340.html;

Daniel, M. (2014) Heartbleed: Understanding When We Disclose Cyber Vulnerabilities, Downloaded June 1, 2022 https://nsarchive.gwu.edu/document/17627-white-house-heartbleed-understanding-when-we;

European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs (2017)

Gesetz zur Effektiveren und Praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. Avgust 2017, BGBI. I 2017 Nr. 58 23.8.2017, S. 3206, https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5B@attr_id=%27bgbl117s3202.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s3202.pdf%27%5D__1655289087690;

Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics, *Digital Investigation*, 28 (4), 163-175

Kaleigh E. Aucoin, K. (2018). The Spider's Parlor: Government Malware on the Dark Web, *Hastings Law Journal*, 69(5), 1433-1469;

Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices, Downloaded June 16, 2022 https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf;

Ohm P. (2017). The Investigative Dynamics of the Use of Malware by Law Enforcement, *William & Mary Bill of Rights Journal*, 26(2), 303-335;

Pfefferkorn, R. (2018) Security Risks of Government Hacking, Downloaded May 15, 2022 http://cyberlaw.stanford.edu/publications/security-risks-government-hacking;

Pisarić, M. (2020a). Encryption as a Challenge for European Law Enforcement Agencies, In: Thematic conference proceedings of international significance/ International Scientific Conference "Archibald Reiss Days", Belgrade, 18-19 November 2020, Belgrade, University of Criminal Investigation and Police Studies, 611-619;

Pisarić, M. (2020b). Enkripcija kao prepreka otkrivanju i dokazivanju krivičnih dela, *Zbornik radova Pravnog fakulteta u Novom Sadu*, 54 (3), pp. 1079-1100;

Pisarić, M. (2021). Enkripcija mobilnog telefona kao prepreka otkrivanju i dokazivanju krivičnih dela – osvrt na uporedna rešenja, *Anali Pravnog fakulteta u Beogradu*, 69 (2), 415-422;

Pisarić M. (2022). Communications encryption as an investigative obstacle*, Revija za kriminologiju i krivično pravo,* 60 (1), 61-74;

Antis, S. (2021). Government procurement law and hacking technology: The role of public contracting in regulating an invisible market, *Computer Law & Security Review*, 41, 1-16;

Quinlan S., Wilson A. (2016) A Brief History of Law Enforcement Hacking in the United States Downloaded May 10, 2022 https://www.newamerica.org/cybersecurity-initiative/policy-papers/brief-history-law-enforcement-hacking-united-states/

Standardisierende Leistungsbeschreibung für Software zur Durchführung von Maßnahmen der QuellenTelekommunikationsüberwachung und der On-

lineDurchsuchung, 2018, https://www.bka.de/SharedDocs/Downloads/DE/Sonstiges/standardisierendeLeistungsbeschreibungQuellenTKUE.html?nn=51828&cms_dlConfirm=true;

Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 des Gesetzes vom 25. März 2022 (BGBl. I S. 571) geändert worden ist, https://www.gesetze-im-internet.de/stpo/BJNR006290950.html;

Wet van 27 juni 2018 tot wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), Staatsblad 2018, 322, https://zoek.officielebekendmakingen.nl/stb-2018-322.html;

Wetboek van Strafvordering, https://wetten.overheid.nl/BWBR0001903/2022-01-01;

Bergman, R., Mazzetti, M. (2022, January 28). The Battle for the World's Most Powerful Cyberweapon. *New York Times*, Accessed on January 31, 2022 https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html;

Kaeten, J. (2021, August 12). UN experts call for more rules on countries' use of spyware. *Associated Press*. Accessed on January 15, 2022 https://apnews.com/article/technology-united-nations-spyware-e1bfa1f8242f39da856fc0a8bf2793aa;

Martyr, K. (2020, October 14). Police carry out raids linked to German spyware firm FinFisher. Deutsche Welle. Accessed on January 15, 2022 https://www.dw.com/en/police-carry-out-raids-linked-to-german-spyware-firm-finfisher/a-55270507;

Herpig, S. (2018). A Framework for Government Hacking in Criminal Investigations, Downloaded April 202 https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf