NBP 2023, Vol. 28, Issue 1, pp. 16–26
https://doi.org/10.5937/nabepo28-43759
Original scientific paper

The Use of Policeware to Hack Electronic Evidence in Germany and the Netherlands

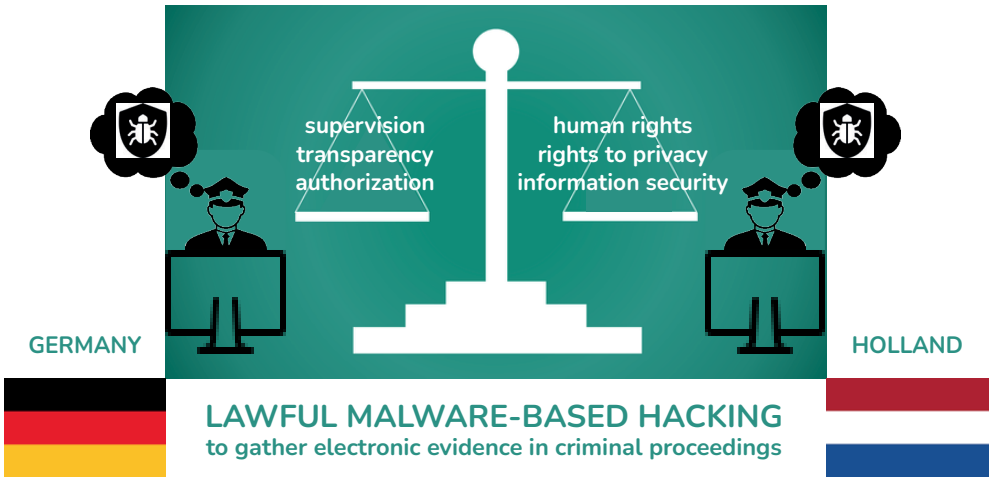
Milana Pisarić[1]
University of Novi Sad, Faculty of Law, Novi Sad, Serbia

Submitted: 2023-03-31 • Accepted: 2023-06-01 • Published: 2023-06-15

Abstract: Hacking as manipulation of software, data, computer system or network without the knowledge and permission of the user constitutes an act of criminal offence. However, given that certain technological tendencies make it difficult/impossible to collect electronic evidence, the question arises as to whether the authorities responsible for detecting and proving criminal offenses should be authorized to hack, i.e. to conduct investigations in the digital environment in such a way that they would be authorized to exploit technical, systemic and human vulnerabilities within the IT system, without knowledge and permission of the user, in order to gain a remote access to protected system and conduct further actions. Although a state authorities' hacking with the aim of collecting electronic evidence carries immense risks for information security and human rights and freedoms with it, one cannot dispute that the deployment of such techniques might be useful in criminal investigations. However, the application of hacking technique would not per se violate the right to privacy and other guaranteed rights and freedoms, only as far as such interference is properly regulated. Hence, the legal framework should explicitly regulate the lawful hacking as a special investigative measure, especially the conditions that should be met and mechanisms that should be applied. As hacking for the purposes of criminal investigation may be performed through various techniques, this paper focuses on a hacking technique based on a malware, and its regulations in two countries with explicit provisions – Germany and the Netherlands.

Keywords: electronic evidence, remote access, police hacking, policeware.

Graphical abstract



1 Corresponding author: mpisaric@pf.uns.ac.rs • https://orcid.org/0000-0001-8344-3349

Citation: Pisarić, M. (2023). The use of policeware to hack electronic evidence in Germany and the Netherlands. *NBP. Nauka, bezbednost, policija*, *28*(1), pp. 16–26. https://doi.org/10.5937/nabepo28-43759
eISSN 2620-0406

INTRODUCTION

The effectiveness and practicality of applying the 'traditional' powers for collecting electronic evidence has been called into question, primarily due to certain trends in technological development – the widespread use of mobile computing, cloud computing, wireless networking, encryption (especially end-to-end encryption in electronic communication and cloud services, as well as full-disk encryption in devices), and other protective measures and mechanisms (Going Dark phenomenon). Designing an approach to overcome such a serious problem has been the subject of debate in the scientific, professional and political public for the last several years (Bellovin et al., 2014). Contrary to 'backdoor option', i.e. legally obliging technology companies and communication service providers to build in security flaws that could enable the law enforcement agencies (further: LEA) to enter a target device/systems, a more plausible is 'front door option', i.e. authorizing the LEA to access a target device/system through the existing vulnerabilities in end-user software and platforms. The essence of the second option is the use of hacking techniques, primarily malware-based, that enable a remote access to computer devices and networks, in order to collect electronic evidence (Pisarić, 2022).

The regulation of the use of such a hacking technique is relatively recent – only a few countries have in recent years introduced explicit provisions into their laws. Until then, these techniques were used without a specific legal framework. For example, in Italy, Article 266 of the Code of Criminal Procedure, which regulates the interception of communications, was used as the legal basis for the use of malware by the police. Although this practice has been criticized by the scientific and professional public, the Court of Cassation has also ruled on the permissibility of using Trojans based on general provisions (Vaciago & Ramalho, 2016). However, if these intrusive techniques would be used on the basis of the existing, general legal regime, without sufficiently clear and precise provisions, information security and human rights and freedoms would be unjustifiably exposed to a high degree of risk, disproportionate to the needs of criminal proceedings. Therefore, only a specific legal framework is an adequate one. The aim of this paper is to conduct comparative analysis and to examine such norms existing in Germany and the Netherlands (Dheri & Cobey, 2019), in order to determine whether the lawmakers have, following the recognized standards for special investigative measures, created additional requirements for this digital investigative measure and provided sufficiently clear and precise provisions.

METHODS

An authorized access to a protected computer, computer network and electronic data processing via policeware with different functionalities is prescribed as a special evidentiary action in a few countries. The author applied the comparative legal method, analysing legal framework in Germany and the Netherlands.

The relevant reform of the German Code of Criminal Procedure (Strafprozessordnung, 1987–2022) was carried out in 2017 with the adoption of the Law on More Efficient and

Practical Implementation of Criminal Procedure (Gesetz zur Effektiveren und Praxistauglicheren Ausgestaltung des Strafverfahrens, 2017). The 2017 amendments to the Code introduced explicit provisions on remote access to a computer device. Thus, by Article 3 paragraph 8 of this Law, sentences 2 and 3 have been added to paragraph 1 of Article 100a of the CPC, which governs the surveillance of telecommunications (Telekommunikationsüberwachung), which enables the secret interception and recording of telecommunications at the source, i.e. end device with the help of technical means (Quellen-Telekommunikationsüberwachung, Quellen-TKÜ). In addition, by Article 3 paragraph 9 of the Law, a new Article 100b was introduced into the Code, which regulates the secret search of information technology systems from a distance for the purpose of collecting and confiscating data with the help of technical means (Online-Durchsuchung) (Pisarić, 2021).

In the Netherlands, with the entry into force of the Law on Amendments to the Criminal Code and the Code of Criminal Procedure in order to promote and improve the investigation of computer crime and the prosecution of perpetrators (Computer Crime Act III) from 2018 (Wet, 2018), explicit provisions on authorized secret access to computers and computer network from a distance, with the help of technical means, as a special investigative action, for the purpose of subsequent exercise of certain investigative powers, were introduced into the Code of Criminal Procedure (Wetboek van Strafvordering, 2022). Namely, by Article 2 Paragraph G of this Law, Chapter IVA of the First Book of the Code has included an eighth chapter, which contains Article 126nba, which regulates the action of investigation in automatic data processing (Onderzoek in een geautomatiseerd werk). That one provision gives the police a broad and far-reaching authority to covertly, remotely access the computer, in order to undertake some of the investigative actions listed in paragraph 1. In that sense, the authority from Article 126nba represents an 'umbrella' authority (Oerlemans, 2017, 355). In addition, remote access can be determined based on Art. 126uba, contained in Section V of the First Book of the Code (investigating organized crime and terrorism).

The relevant legal provisions were analysed in order to reach answer to the following questions:

- regarding authorization: 1) What authority approves the use of policeware? 2) What is stated in the request for approval? 3) In what form is the decision made, and what does it contain?

- regarding restrictions of: 1) Purpose and goal: For what purpose is the use of malware allowed: only for the purpose of discovering and proving a committed criminal offense, or for the purpose of preventing the crime? Is a malware used in order to search the device remotely accessed, to enable secret surveillance of communication at the source, or to achieve some other goal? 2) Criminal acts: Is it a general or special evidentiary action? If it cannot be applied to all criminal offenses, how did the legislator determine such a limitation? 3) Persons and devices: Can the hacking technique be applied to an unknown suspect, or must his identity be established beforehand, and only in relation to the suspect, or in relation to third parties? Can the hacking technique be applied only to the suspect's devices or also to the devices of third parties? 4) Duration: Is it prescribed that the implementation of the technique can last indefinitely, or is there a time limit? Is there a possibility of an extension - under what conditions, based on whose approval, for how long? 5) Implementation of the action: Who implements the approved action, and in what way? Is there a prescribed

obligation for certain natural and legal persons to provide technical assistance to the state body entrusted with the execution of the action, and if so, is there a prescribed sanction for not providing assistance? 6) Gaining access to the device: Is the way in which the technical device is introduced into the system prescribed – does the legislator allow the introduction of the technical device only by physically installing it on the device, or can it be installed remotely, and under which conditions? 7) Technical means: Are conditions and restrictions for the use of technical means prescribed? 8) Uses of the collected material: How is the collected material that is not needed for specific criminal proceedings, handled? Is it permissible to use a random find? How is the collected material treated, when the need for its use ceases? Is the protection of privileged communications prescribed?

– regarding transparency: 1) Are competent authorities obliged to inform the persons in relation to whom the measure was applied? 2) Which persons are informed, when and in what way? 3) Is there a possibility to delay notification, and for how long? 4) What rights do informed persons have, and how do they exercise them? 6) Do they have the right to an effective legal remedy? 7) What happens if the person is not notified?

– regarding supervision and control of implementation of measures: 1) Are rules, standards, or limitation in the application of technical means established? 2) Is there a prescribed mechanism for reporting, control and supervision at the macro and micro level (in the specific case): who submits the report to whom, in what form, at what moment, and what does the report contain?

RESULTS

The analysed explicit provisions on lawful malware-used hacking in Germany and the Netherlands have more or less met requirements within the recognized standards for special investigative measures. The codes explicitly regulate ex ante requirements, that should be fulfilled before the authorization and application of hacking techniques, in which way it is determined that such an investigative technique is really necessary for the achievement of a certain goal and proportionate to it. Based on the principles of necessity and proportionality, certain conditions must be met that represent the basis for making a decision approving the use of malware-based hacking techniques. The standardization of these conditions is reduced to the prescription of certain restrictions, i.e. why and for what purpose the application of the investigative technique can be approved, with regard to which criminal acts, in relation to which persons and devices, and how long it can last. The legal frameworks also address the steps that follow the use of policeware, primarily notifying the person in relation to whom the measure has been applied.

DISCUSSION

Germany

In terms of Art. 100a, para. 1, sent. 1, interception and recording of telecommunications can be undertaken if: 1) certain facts indicate the suspicion that a person, either as a per-

petrator or an accomplice, has committed one of the serious crimes listed in Art. 100a, para. 2, or attempted to commit such a criminal offense in cases where the attempt is punishable, or took preparatory actions for the commission of such a criminal offense, by committing another criminal offense; 2) in the specific case, it is a particularly serious criminal offense, and 3) establishing the facts, or discovering the whereabouts of the suspect in another way would be much more difficult, or impossible. Based on Art. 100b, para. 1, a secret access to the information technology system can be achieved from a distance, with the help of a technical means, in order to search the device and collect and extract data from it, without the knowledge of the affected person, if: 1) certain facts indicate a suspicion that the person was the perpetrator or accomplice, committed one of the serious crimes listed in Art. 100b, para. 2[2] , or attempted to commit such a criminal offense in cases where the attempt is punishable[3]; 2) in the specific case, it is a particularly serious criminal offense, and 3) establishing the facts, or whereabouts of the suspect would otherwise be significantly more difficult or impossible. This authorization includes one-time access to stored data (file search and data copying), as well as continuous monitoring, surveillance and recording of data, which will be stored in the device for the duration of the operation. The provisions of Art. 100d are also relevant, while they contain the requirement that, in order to protect the core of private life, in each individual case the gravity of the specific criminal offense, the degree of suspicion and the expected success are compared with the intensity of the intervention.

Secret surveillance of telecommunications on an end device can be undertaken not only in relation to the suspect's device, but also the device of a person who, based on certain facts, can be assumed to be receiving or transmitting messages intended for, or originating from the suspect, or that the suspect is using his telephone connection or information technology system (Art. 100a, para. 3). A secret search from a distance is determined in relation to the IT system of the suspect, and in relation to the devices of a third party only on the condition that there are certain facts on the basis of which it can be assumed that: a) the suspect is using his device, and b) if the action applied only in relation to the IT system of the suspect would not be enough to determine the facts, or determine the whereabouts of the co-suspect. In doing so, it is expressly stipulated that the action can be applied even if third parties are unavoidably affected (Art. 100b, para. 3).

Intervention by technical means in IT systems refers to the necessary technical measures, that is, to infiltration with the help of appropriate software, which is undertaken in order to collect data from the IT system and transmit it electronically to the criminal prosecution authorities (Soiné, 2018). The Code does not specify how the software is installed in the IT system, however para. 5 and 6 of Art. 100a prescribe certain protective measures (the corresponding application of which is referred to in Art. 100b, with the exception of paragraph 5, sent. 1, it. 1). Namely, the technical means is installed so that: 1) it intercepts and records ongoing telecommunications, or the content and data on communication that could otherwise be intercepted and recorded, from the day the order is issued and during the transmission process in the public telecommunications network; 2) it creates in the IT system only those changes that are necessary for data collection, and 3) changes created in the IT system are automatically cancelled after the implementation of the action is completed, if it is technically feasible (Art. 100a, para. 5, sent. 1). In addition, the technical me-

2 The list contains fewer criminal offenses compared to Art. 100a, para. 2.
3 Not in terms of preparatory actions, as in Art. 100a, para. 1.

ans is used in a way to ensure protection against unauthorized access in accordance with the rules of the profession, and that the recorded data is protected from modification and unauthorized deletion, and in such a way as to enable authorized supervision over them, in accordance with the rules of the profession (Art. 100a, para. 5, sent. 2). When a technical means is used, there must be a record of it, which contains data on the specification of the technical means, the time period of use and the device to which access was achieved and the permanent changes created by the use of the technical means, identifying data on the collected data and on the unit that used a technical means (Art. 100a, para. 6). The software products used for telecommunication surveillance at the source and online searches are tested before they are put into use and comprehensively checked to see if they comply with the requirements, which, based on the provisions of the Code, were set in 2018 in the Standardized Service Description for the system for performing measurements of source telecommunications, monitoring at the source and online search (Pisarić, 2023).

The procedure for approving special evidentiary actions is regulated in Art. 100e. The interception of telecommunications at the source referred to in Art. 100a is authorized by the court at the request of the public prosecutor, and for reasons of urgency the public prosecutor can also do so, but such a decision must be approved by the court within three working days, under threat of nullity. The order is issued for a maximum period of three months, and the implementation of the action can be extended for the same time period, if the conditions for determining the action still exist, i.e. the extension is justified considering the data collected until then (Art. 100e, para. 1). The remote search referred to in Art. 100b is determined by the criminal panel of the District Court at the request of the public prosecutor, and for reasons of urgency it can also be done by the president of the panel, but such a decision must be approved by the panel within three working days, under the threat of nullity. The action can be carried out for a maximum of one month, with the possibility of extension for up to another month, if it is justified, taking into account the data collected until then (Art. 100e, para. 2).

The order for the implementation of these special evidentiary actions is issued in written form, and contains: 1. the name, surname and address of the person in relation to which it is determined, if these data are known; 2. the name of the criminal offense charged to the suspect; 3. type, scope, duration and end date for the implementation of the action; 4. type of data expected to be collected by the implementation of the action and their connection to a specific subject; 5. in the case of the action from Art. 100a, a telephone number or other identifying data for the connection that will be intercepted or for the end device, if there are no facts that lead to the assumption that these data were assigned to another end device, and 6. in the case of the action of Art. 100b, the most precise determination of the information technology system to which access will be achieved (Art. 100e, para. 3). It is necessary that the order on the determination or extension of these actions contains an explanation, especially with regard to certain facts on which the suspicion is based, and assessments of necessity and proportionality (Art. 100e, para. 4). The implementation of the action shall be terminated as soon as the circumstances justifying its determination cease to exist, and the court that issued the order shall be notified of this, without delay. With regard to the action from Art. 100b, the court is also informed during the execution of the order (Art. 100e, para. 5).

The limitation is also reflected in the request for the protection of the core of private life, in order to respect human dignity, during the collection and analysis of data collected by

these special evidentiary actions. Thereby, in accordance with Art. 100d, implementation of actions from Art. 100a and 100b is not tolerated if the factual circumstances indicate that only data from private life would be collected in that way. In addition, if such data is collected by the implementation of actions from Art. 100a and 100b, it cannot be used, and recordings and records with relevant data will be destroyed, without delay, and a record about that will be made. In carrying out the action from Art. 100b, such a technical tool is used, and in such a way that data from the area of private life are not collected, and if such data are collected, they are destroyed without delay or delivered to the court that approved the implementation of the action in order to make a decision on their deletion or the possibility of using them.

Art. 101 stipulates the obligation of the public prosecutor to inform certain persons about the implementation of special evidentiary actions and the possibility of legal protection in the sense of Art. 101, paragraph 7. On the implementation of the action from Art. 100a, participants in telecommunications are informed (Art. 101, para. 4, it. 3), and about the implementation of the action from Art. 100b, the person in relation to whose device the action was carried out (Art. 101, para. 4, it. 4). The obligation to notify does not exist in relation to persons who are accidentally affected by the measure and who can be assumed to have no interest in being notified. The aforementioned persons are informed as soon as possible, without jeopardizing the interests of the investigation, life, physical integrity and freedom of another person. A note is drawn up on the delay and the reason for the delay in notifying the aforementioned persons (Art. 101, para. 5), and if the person is not notified within 12 months from the date of completion of the action, and with regard to the action from Art. 100 b within six months, further postponement can be approved only by the court. The court may even approve that the person is never notified, if there is a probability bordering on certainty that the conditions for notification will not be met, even in the future (Art. 101, para. 6). Notified persons have the right to submit a request to the court within two weeks from the moment of notification to review the legality of the grounds, methods and means used in the implementation of these actions (Art. 101, para. 7).

The Netherlands

Based on Art. 126nba, the remote access to the device used by the suspect can be achieved, if the urgency of the investigation dictates it and there is a suspicion that the suspect has committed:

I. One of the criminal acts listed in Art. 67, para. 1 (criminal offenses for which detention can be ordered and for which a prison sentence of at least four years is generally prescribed), and which, due to its nature or connection with other criminal acts, represents a serious violation of the rule of law, for the purpose of:

a) Collection of data on certain characteristics of the computer, especially the identity of the user and the location of the device; or

b) Surveillance and recording of confidential oral communication (Art. 126m) and telecommunications (Art. 126l); or

c) Systematic supervision and monitoring of the suspect (Art. 126g);

II. A criminal offense for which a prison sentence of at least eight years or more is prescribed, for the purpose of:

d) Recording data in order to secure them, both those already stored in the computer and those that are stored from the moment of remote access and for the period approved by the order on the implementation of this action, to the extent that is reasonably necessary to establish the truth; or

e) Making certain data unavailable in the sense of Art. 126cc, and after copying those data for the purpose of evidence in criminal proceedings – for example, by deleting illegal content from the computer.

Remote access can be determined based on Art. 126uba, if there is suspicion that an organized criminal group is planning to commit criminal acts listed under I and II, or that these acts have been committed. Namely, this article stipulates that this special evidentiary action can be determined against a person who is reasonably suspected of participating in planning or execution of a criminal offense within an organized criminal group, for the purpose of: a) determining and recording identifying data about the device/network or to the user, or b) execution of the order for the implementation of the action referred to in Art. 126s (surveillance of telecommunications with entry into the premises for installation of devices) and Art. 126t (secret surveillance of communications carried out within a publicly accessible network), or c) execution of the order for the implementation of the action referred to in Art. 126o (secret surveillance and monitoring of persons), or d) recording data in order to secure them, and e) making certain data unavailable in the sense of Art. 126cc.This article foresees the corresponding application of the rules established in Art. 126nba, para. 4–9.

The order on the implementation of the action is issued by the public prosecutor in written form, and with the prior approval of the investigating judge in written form, which is issued at the request of the public prosecutor (Art. 126nba, para. 4). The order contains: the name of the criminal offense and the name and surname of the suspect, if known, that is other known identifying information, if the suspect is unknown; the number or other identifying data of the device to which remote access will be made; the circumstances from which it follows that the conditions from paragraph 1 for determining the action have been met; identifying data and description of the functionality of the technical means for remote access; the tasks that the technical device will perform, that is, which further investigative actions will be taken using the technical means for remote access, and in the case of actions from points a, d and e of paragraph 1, a clear description of the actions is also provided; marking in relation to which parts of the device, i.e. data, the order will be executed; time period in which the order will be executed; in the case of the action from point c paragraph 1, the intention to place a technical means on the person (Art. 126nba, para. 2).

The order is issued for a maximum period of four weeks, and the implementation of the action can be extended for a maximum of four weeks (Art. 126nba, para. 3), upon the re-approval of the investigating judge. Namely, the order can be amended, extended, or invalidated by the written order of the public prosecutor, only after the prior written approval of the investigating judge. Exceptionally, in urgent cases, the court approval and the public prosecutor's decision can be issued orally, but the investigating judge and the public prosecutor are obliged to make the approval and the order in writing within three days (Art. 126nba, para. 5). An important protective measure is the functional separation of

the technical and tactical part of the implementation of the action, because the order is executed by a specially trained member of the criminal police and the collected material is analysed by the inspector in charge of the specific case, which makes it impossible for the other to have unlimited technical access to the data in the device. Paragraph 6 stipulates that the technical device will be removed upon completion of the investigation. However, if this is not possible, or the technical device cannot be completely removed and this poses a risk to the functioning of the device in relation to which the action was carried out, the public prosecutor will inform the administrator of the device and provide him with the necessary data for complete removal.

Art. 126bb is applied to this special evidentiary action, which regulates the obligation of the public prosecutor to inform the person in relation to whom the action was applied, at the moment when the interests of the investigation allow it, unless it is justifiably not possible to do so. Art. 126nba, para. 6 provides for the corresponding application of Art. 126cc, para. 1, which stipulates that until the criminal proceedings are completed, the public prosecutor keeps the official reports and the entire material collected by the implementation of this action, including the part that is not attached to the court case files. After the expiration of two months from the date of completion of the procedure and the notification of the person, in accordance with Art. 126bb, the reports and the entire material are destroyed. In addition, Art. 126nba, para. 7 provides for a mechanism of ex-post supervision over the implementation of this action by the Inspectorate for Public Order and Security.

Based on the Art. 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); 2) rules on the recording of data for the execution of an order (Chapter 4), 3) rules on standard tool requirements and its inspection (Chapters 5 and 6) (Pisarić, 2023)

CONCLUSIONS

Due to the complexity of the information environment, the invasiveness into the right to privacy and the security risks inherent in hacking, it is of crucial importance that the law expressly and clearly establishes the rules governing the use of malware-based hacking techniques for the purposes of criminal proceedings. Since this digital investigative method is highly privacy intrusive, the law regulating criminal procedure should contain a detailed basis, with strong procedural safeguards. The legal framework should: a) set high standards for authorizing the use of malware for remote access, while allowing the deployment of this authority as an ultima ratio, when other, less intrusive measures do not yield results; b) precisely prescribe malware tasks, and insist on minimizing data collection and creating risks, and c) set a request for public reporting on the use of this technique.

Hence, the use of policeware should also be regulated in detail, whereby an adequate legal framework should, as a minimum, contain certain requirements that must be met before (ex-ante) and after (ex-post) the use of malware-based hacking techniques to gather

electronic evidence. Ex-ante conditions would have to be met before the authorisation of hacking techniques, in order to determine that such an investigative technique is really necessary for the achievement of a certain goal and proportionate to it. Primarily, prior court authorization should be required, and restriction on the duration and functionalities of the use must be foreseen. The law should also prescribe appropriate ex-post mechanisms to ensure transparency and accountability for the application of malware-based hacking techniques. Transparency in the application of hacking techniques is achieved through a mechanism that consists of two elements: informing the affected person, that is, the person in relation to whom the action was carried out, and challenging the legality of the decision that determined the implementation of the action and the results of the action, through the provision of an effective legal remedy. Accountability for the application of policeware is achieved through a reporting, monitoring and control mechanism. In other words, the regulation governing criminal procedure should provide for authorized access to a protected computer system/network via malware, as a special evidentiary action.

REFERENCES

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. https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1

Dheri, P., & Cobey, D. (2019). Lawful access & encryption in Canada: A policy framework proposal. *Forthcoming in Criminal Law Quarterly*, 1-38. https://dx.doi.org/10.2139/ssrn.3470957

Strafprozessordnung in der Fassung der Bekanntmachung von 7. April 1987 (BGBI. I S. 1074, s. 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

Gesetz zur Effektiveren und Praxistauglicheren Ausgestaltung des Strafverfahrens. (2017, Avgust 23). *Bundesgesetzblatt*, I, 58. 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__1680267814537

Oerlemans, J. J. (2017). De Wet computercriminaliteit III: meer handhaving op internet. *Strafblad*, *15*(4), 350-359. https://hdl.handle.net/1887/54783

Pisarić, M. (2021). Enkripcija mobilnog telefona kao prepreka otkrivanju i dokazivanju krivičnih dela – osvrt na uporedna rešenja. *Anali Pravnog fakulteta u Beogradu*, *69*(2), 415-442. https://doi.org/10.51204/Anali_PFBU_21205A

Pisarić, M. (2022). Communications encryption as an investigative obstacle. *Journal of criminology and criminal law*, *60* (1), 61-74. http://www.iksi.ac.rs/rkk_arhiva/rkk_1_2022/rkk_1_2022_milana_pisaric_communications_encryption_as_an_investigative_obstacle.pdf

Pisarić, M. (2023). Lawful hacking – technical issues in law. In T. Kesić (Ed.), *XII International scientific conference "Archibald Reiss Days": Conference proceedings of international significance* (pp. 175–195). University of Criminal Investigation and Police Studies.

Soiné, M. (2018). Die strafprozessuale Online-Durchsuchung. *Neue Zeitschrift für Strafrecht*, *38*(9), 497–504.

Vaciago, G., & Ramalho, D. S. (2016). Online searches and online surveillance: The use of Trojans and other types of malware as means of obtaining evidence in criminal proceedings. *Digital Evidence and Electronic Signature Law Review*, *13*, 88–96. https://doi.org/10.14296/deeslr.v13i0.2299

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). (2018). *Staatsblad*, 322. https://zoek.officielebekendmakingen.nl/stb-2018-322.html

Wetboek van Strafvordering. (2022). Geldend van 01-01-2022 t/m 30-06-2022. https://wetten.overheid.nl/BWBR0001903/2022-01-01#Aanhef