Justyna Kurek-Sobieraj*

Hidden Spyware in the Service of State Security. Legal, Organisational and Systemic Aspects

Abstract

To meet the challenges in cybersecurity, the state and its bodies must develop classified instruments that will enable the acquisition of data without the active involvement of private sector entities. These programs are installed on a user's device without their consent to collect and send information about the operating system and any information contained therein. It is not the purpose of this article to analyse the admissibility of using tools typical for criminal activities in the digital world for ensuring state and citizen security. My interest here is to consider what substantive, procedural and institutional guarantees must be met to ensure a balance between the protection of human rights and basic procedural guarantees (such as the presumption of innocence) and the effectiveness of activities in cyberspace.

Key words: Spyware, state security, operational activity, hacking tools

* Assoc. Prof. Justyna Kurek-Sobieraj, PhD, War Studies University, Head of the Constitutional Security Department, e-mail: j.kurek@pracownik.akademia.mil.pl, ORCID: 0000-00-02-8754-5243.

General remarks

In order for operational activities, including investigative operations in the digital realm, to be effective, it is necessary to employ unconventional tools, such as hidden spyware. These programs are installed on a user's device without their consent and collect and send information about the operating system and any information contained therein[1]. It is not the purpose of this article to analyse the admissibility of using tools typical for criminal activities in the digital world for ensuring state and citizen security. Rather, it operates on the assumption that such measures are inevitable. In light of the ongoing changes in how society works, the redefinition of the model of operation of law enforcement agencies in fighting and preventing serious forms of crime seems unavoidable. Conventional tools cannot effectively counteract cyberspace threats in a digital environment. The aim of this article is to consider what substantive, procedural and institutional guarantees must be met to ensure a balance between the protection of human rights and basic procedural guarantees (such as the presumption of innocence) and the effectiveness of activities in cyberspace.

Spy tools in the service of state security

The most common criminal tool used in operational activities is software which operates like trojan horses, sniffers and loggers. A Trojan is a type of software that imitates user-friendly software but contains malicious code. Integrated into the program code, it installs in the background and remains invisible. Its detection is problematic because it is asymptomatic[2]. This tool does not replicate or spread itself. A computer is infected when a user – a carrier – intentionally installs a program. Keyloggers, on the other hand, are software which records keyboard movement and are used to comprehensively track user activities (enabling, for example, taking screenshots and searching for remembered passwords) and sending a record of these activities to a selected server. Sniffer is a computer program whose task is to capture and possibly

1 J. Kurek, *Ochrona przed niezamówioną korespondencją w komunikacji elektronicznej*, Warszawa 2023, p. 66.

2 A. Sucharzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010, p. 94.

analyse data flowing in the network. Sniffers can also be run on a router or a computer that is one of the communication parties. The sniffer can also be used to monitor third-party network activity[3].

The effectiveness of using such hacking tools in operational activity is confirmed by media experiences dating back to the 2000s. None of the traditional investigative methods seem to be as effective, even analysing transmission data from internet operators. An example is the software used by the FBI in the early 2000s – Computer and Internet Protocol Address Verifier (CIPAV)[4]. Numerous examples of using such tools are cited in European Parliament Working Document no. 1, prepared by the Committee on Civil Liberties, Justice and Home Affairs on U.S. and EU surveillance programs and their impact on the fundamental rights of EU citizens. It reveals several interesting examples of online activities undertaken by American services to analyse data and information used to counteract the most serious crimes. One example may be the PRISM program[5] – a covert data collection and mining program that was intended to provide the NSA with direct access to the central servers of nine leading U.S. Internet companies, enabling the collection of consumer material, including search history, email content, file transfers and live chat content[6]. Another example described is the Xkeyscore program, which allows NSA analysts to search, without prior authorisation, vast databases of e-mail messages, online chat content and the search history of millions of users, as well as metadata about them[7]. The report also points to the Boundless Informant program. It is a data mining tool to record and analyse global electronic information. It organises the details, including vast amounts of information, mainly metadata, collected from computer and telephone networks among countries. It is noted that this tool allows users to

3 J. Kurek, *How to achieve a balance between effective preventing crime and protecting privacy of citizens. Online search as a new challenge for e-Justice*, „Masaryk University Journal of Law and Technology" 2009, vol. 3, no. 3, p. 379 and following.

4 Ibidem, p. 381 and following.

5 *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, http://online.wsj.com/public/resources/documents/prismfactsheet0608.pdf [access: 28.02.2024].

6 *NSA Prism program taps in to user data of Apple, Google and others*, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:networkfront%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1 [access: 15.01.2024].

7 *XKeyscore: NSA tool collects „nearly everything a user does on the internet"*, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [access: 20.02.2024].

select a country on the map and obtain a preview of the number of metadata, and select details about collections within a given country[8].

In Europe, special tools for online operational activities are being created for the Secret Service. For example, in Germany, work on creating appropriate software was carried out simultaneously with a very intense public debate[9] on the conditions for using such software and the rules of exercising control over services and other entities conducting covert operational and reconnaissance activities. German case law played a special role here.

The German way to regulate secret operation activities

Two judgments were crucial for German public debate and legislative refinement of the compromise between effective legal measures that, on the one hand, allow for the effective conduct of operational and reconnaissance activities in the digital environment and – on the other hand – protect the privacy of citizens. These are the decisions of the BGH of 31 January 2007 – in Case StB 18/06[10] – and the Judgment of the BVerfG of 27 February 2008 in Case 1 BvR 370/07[11]. The case law clearly showed the need to create a legal framework and define specific, dedicated guarantees for privacy when using invasive investigative methods.

The BGH and BVerfG case law led to the creation of the first comprehensive regulation in the German legal system. The Act on Counteracting the Danger of International Terrorism by the Federal Criminal Office was adopted on 25 December 2008[12] and entered into force on 1 January 2009. It introduced

8 *Boundless Informant NSA data-mining tool – four key slides*, http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining [access: 20.02.2024].

9 For detailed information about the development of German views in the area of online searches, see i.a. C. Arzt, *Verbunddateien des Bundeskriminalamts – Zeitgerechte Flurbereinigung*, „Neue Juristische Wochenschrift" 2011, no. 6, p. 352 and following; M. Soiné, *Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder*, „Neue Zeitschrift für Verwaltungsrecht" 2012, no. 24, p. 1588.

10 BGH Decision of 31 January 2007 in Case StB 18/06, http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&nr=38779&linked=bes&Blank=1&file=dokument.pdf [access: 12.12.2023].

11 BVerfG Judgment of 27 February 2008 in Cases 1 BvR 370/07 and 1 BvR 595/07, http://134.96.83.81/entscheidungen/rs200802271bvr037007.html [access: 12.12.2023].

12 Gesetz zum Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt vom 25. Dezember 2008 (BGBl. I S. 3083) (Act of 25 December 2008 on Counteracting the Danger of International Terrorism by the Federal Criminal Office).

numerous changes to the BKA-Gesetz. More than seven years after entering into force, the aforementioned provisions were again subjected to constitutional control by the German Federal Constitutional Court. In its judgment of 20 April 2016, in Cases 1 BvR 966/09 and 1 BvR 1140/09[13], the Court found that granting special powers to counteract international terrorism to a special agency (BKA) is a necessity in a democratic state of law and confirmed the compliance of such an institutional solution with the German Fundamental Law (das Grundgesetz – GG)[14]. However, the Court pointed out that some of the provisions adopted in 2008 did not comply with the principle of proportionality and therefore found them inconsistent with the provisions of the Fundamental Law (Grundgesetz), postponing their removal from the legal system until 30 June 2018.

In its existing form, the Act on the Federal Criminal Office and Cooperation of the Federation and the States in Police-Criminal Matters of 7 July 1997 (BKA-Gesetz)[15] authorises using emergency measures, including methods of hidden infiltration. This includes using spyware to ward off the threat caused by international terrorism[16]. Legal commentators emphasise that these powers must be used in a restrictive manner and limited to cases where there is a high probability of harm to public safety occurring within a foreseeable period[17]. What is also important concerning the German experience is that the public debate led to the transfer of all development and implementation tasks to the public sector[18]. This is the first case of software developed within the justice system. The IT companies were only external consultants. They did

13 BVerfG Judgment of 20 April 2016 in Cases 1 BvR 966/09 and 1 BvR, 1140/09, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs201604201bvr096609.html [access: 12.12.2023].

14 Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949 (BGBl. I p. 2438) (Fundamental Law for the Federal Republic of Germany of 23 May 1949) as last amended by the Act of 23 December 2014 (BGBl. I S. 2438).

15 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten vom 7. Juli 1997 (BGB1, I S. 1650) (Act of 7 July 1997 on the Federal Criminal Office and Cooperation of the Federation and the States in Police and Criminal Matters), last amended by the Order of 31 August 2015 (BGBl. I S. 1474).

16 The development of German regulations has been discussed in detail [in:] J. Kurek, *Wykorzystanie szpiegowskiego oprogramowania w działalności operacyjnej organów ścigania. Gwarancje konstytucyjne i procesowe z perspektywy doświadczeń niemieckich*, „Przegląd Policyjny" 2016, no. 1, p. 159–171.

17 R. Stettner [in:] H. Dreier, *Grundgesetz-Kommentar*, Tübingen 2015, p. 54.

18 F. Roggan, *Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur*, „Neue Juristische Wochenschrift" 2009, no. 5, p. 262.

not own the source codes for the developed software. Consequently, it is not allowed to use any commercial software (i.e., RCS or PEGASUS in Poland) for public security purposes.

Most likely also in Poland[19], such spy software was or is being used by secret services. In 2011, the CBA (Polish Central Anticorruption Bureau) reportedly purchased RCS (Remote Control System) software from the Italian company Hacking Team. The tool was used to attack and monitor computers and smartphones. It also allows for infiltration of coded communication channels, such as Skype, the so-called secure e-mail boxes and a correspondence encryption tool. RCS enables real-time tracking of websites viewed by the infiltrated entity, programs deleted, closed and opened, and keyboard movements. Social media reports show that the secret services of other countries have purchased similar licenses. This could be justified by the need to analyse and research such software and market trends. Another example of special software used by Polish secret services is the Israeli PEGASUS program. It is also spying software, but intended for installation on NSO Group's IOS and Android systems.

The German „path" towards comprehensive legal regulation[20]

Redefining the model of law enforcement agencies in fighting and preventing serious crime seems unavoidable. Ensuring adequate levels of protection is no longer possible without interfering with fundamental human rights. However, using measures that drastically interfere with the sphere of privacy may only be permissible if this method is the only one that can effectively eliminate the threat to essential legally protected rights[21]. The challenge, therefore, is to define the legal framework for conducting operational activities in the digital world in such a way as to ensure a balance between effective crime prevention and the protection of private resources, including citizens' privacy

19 E. Siedlecka, *Polskie służby kupiły hakerskie oprogramowanie, które pozwala włamywać się do komputerów i telefonów?*, 16 May 2014, http://wyborcza.pl/1,76842,15975910,Polskiesluzbykupilyhakerskieoprogramowaniektore.html [access: 10.02.2024].

20 J. Kurek, *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy Big Data. Aspekty prawne, organizacyjne i systemowe*, Warszawa 2021, p. 190.

21 BVerfG Judgment of 27 February 2008 in Cases 1 BvR 370/07 and 1 BvR 595/07, http://134.96.83.81/entscheidungen/rs200802271bvr037007.html [access: 10.02.2024].

and business secrets. Therefore, the legal framework for using particular operational and investigative methods by special services must be based on institutional substantive and procedural legal guarantees[22].

In its judgment of the BVerfG of 20 April 2016, in Cases 1 BvR 966/09 and 1 BvR 1140/09[23], the German Constitutional Court indicated that the powers of services whose scope of influence interferes with private life should be limited to the protection and strengthening of essential legal rights, i.e., be used only in the case of serious crimes and to protect the security of life, health, freedom and the state. The criterion that meets the condition of uniqueness is the protection of values that are fundamental to the common interest[24]. The BVerfG, therefore, upheld the earlier line of case law. Among other things, in the judgment of 27 February 2008, in Case 1 BvR 370/07, when analysing the admissibility of using online searches, it referred to the principles of proportionality and adequacy, finding that the use of investigative measures that drastically interfere with the sphere of privacy may be used only if this method seems to be the only one that can effectively eliminate the threat to particularly important legally protected rights[25]. Online searches must, therefore, constitute an exceptional measure that will be justified on grounds of the highest importance. The German Supreme Court also referred to the principle of proportionality. In its judgment of 31 January 2007, in Case StB 18/06[26], the BGH clearly indicated that this measure may be ordered only in the event of suspicion of committing serious crimes and, therefore, its application must be subject to very strict formal requirements.

Pursuant to § 102 StPO, it is permitted to search the apartment, other rooms and items belonging to a person suspected of being, among others, perpetrator, accomplice, beneficiary of a crime, participant, or person in charge

22 For more, see: J. Kurek, *Przeszukanie online. Postulaty de lege ferenda* [in:] *System bezpieczeństwa w cyberprzestrzeni RP*, eds. W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, Warszawa 2018, p. 215–235.

23 BVerfG Judgment of 20 April 2016 in Cases 1 BvR 966/09 and 1 BvR 1140/09, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs201604201bvr096609.html [access: 29.01.2024]..

24 M. Rössel, *Teilweise Verfassungswidrigkeit des BKAG*, „IT-Rechtsberater" 2016, no. 1, p. 149.

25 T. Stadler, *Zulässigkeit der heimlichen Installation von Überwachungssoftware – Trennung von Onlinedurchsuchungen und Quellen – Telekommunikationsüberwachung möglich?*, Multimedienrecht 2012, no. 18, p. 21.

26 BGH Decision of 31 January 2007 in Case StB 18/06, http://juris.bundesgerichtshof.de/cgibin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&nr=38779&linked=bes&Blank=1&file=dokument.pdf [access: 30.07.2016].

if there is a suspicion that the search may lead to obtaining evidence. However, under § 110 section 3 StPO, it is permissible to search electronic data carriers and secure them if there is a suspicion that the data will otherwise be lost. According to the BGH's interpretation in the judgment of 31 January 2007, in Case StB 18/06[27], these standards do not apply to hidden online searches. As indicated by the BGH, the provisions of the Code of Criminal Procedure relating to searches are based on fundamental pre-trial guarantees, the fulfilment of which is impossible in the case of remote searches, primarily the guarantee of transparency of activities performed by officers. During a search, the owner has the right to remain on the premises. In their absence, a representative or adult family member and bystanders may be present (§ 105 and § 106 StPO). At the request of the interested party, once the search is over, a written certificate should be prepared based on which it will be possible to examine the legality of the activities performed by the investigative authorities – in particular, their authorisation. Moreover, as stated by the BGH, under the provisions of the StPO, the investigating judge cannot order a hidden search, which would preclude the protective guarantees of § 105 and § 106 of the StPO.

The Federal Court of Justice also found that hidden online searches are not permissible under § 100a StPO (telecommunications monitoring). It follows that this measure may be ordered only in the event of suspicion of committing serious crimes, and, therefore, its application is subject to very restrictive and strict formal requirements. Moreover, the very nature of this provision is inconsistent with the purpose of a hidden online search. The disposition of the norm in § 100a StPO refers to the control of communication between a suspect and a third party, while the purpose of a remote computer search is to achieve different results. The BGH judgment led directly to the conclusion that general procedural provisions cannot create a legal framework for investigative instruments based on Trojan horse spy programs.

A noteworthy contribution to the public debate on the legal framework of remote hearings was also the judgment of the BVerfG of 27 February 2008 in Cases 1 BvR 370/07 and 1 BvR 595/07[28]. The BVG's examined the compliance of online search provisions in force in the state of Nordhein-Westfalen with the constitutional models contained in the German Fundamental Law. The BVerfG's

27 Ibidem.

28 BVG Judgment of 27 February 2008 in Cases 1 BvR 370/07 and 1 BvR 595/07, http://134.96.83.81/entscheidungen/rs200802271bvr037007.html [access: 12.12.2023].

considerations referred to the provisions of Art. 2 Sec. 1 GG (protection of personality development), Art. 1 Sec. 1 GG (protection of human rights), Art. 10 GG (secrecy of correspondence) and Art. 13 GG (inviolability of the home). Pursuant to Art. 2 Sec. 1 GG, everyone has the right to the free development of personality if it does not violate the rights of third parties and as long as it does not contradict the constitutional order and moral rights. Pursuant to Art. 1 Sec. 1 GG, human dignity is inviolable, and state authorities must respect and protect it. Article 10 GG refers to the secrecy of correspondence. According to its instructions, the secrecy of correspondence, as well as the secrecy of postal items and communications, is inviolable. Restrictions in this respect must arise from statutory provisions. If the restrictions protect the free, democratic legal order or the existence of a republic or a federal state, the law may provide that these restrictions will be applied without the knowledge of the person concerned. Furthermore, legal recourse will be replaced by subsequent control by democratically established bodies and subsidiary bodies.

Under Art. 13 GG, however, the inviolability of the apartment is guaranteed. Searches may be ordered exclusively by a judge and, in urgent cases, also by legally prescribed bodies. The search must be carried out in the form prescribed for this purpose. If firm facts warrant the assumption that a particularly serious crime, as defined by law, has been committed, it is permitted, under a judge's order, to prosecute the perpetrator using technical means for acoustic monitoring of the apartment where the suspect is supposedly staying, unless the facts are examined differently. This method would be disproportionately problematic or pointless. Such measures must be limited in time. The order must be passed by an adjudicating panel of three professional judges. In urgent cases, an order from one professional judge is sufficient. To ward off direct and imminent danger to public safety, measures for monitoring premises may be used based on a court order. In urgent cases, these measures may also be ordered by other statutory bodies; in such a case, these actions must be confirmed by a court order issued immediately. In other cases, interventions and restrictions may be applied only to ward off a general danger or threat to human life and, under the provisions of the Act, in the event of a sudden threat to public safety and order.

The above provisions of the German Fundamental Law, in particular Article 13 GG, clearly stipulate that the measure of home search may only be used exceptionally and is subject to strict procedural requirements intended to protect citizens against unwarranted interference with their legally protected

fundamental rights, such as the right to privacy, dignity and the inviolability of the secrecy of correspondence and privacy.

In its ruling, the BVerfG found, in particular, that the constitutional guarantees under Art. 2 Sec. 1 in connection with Art. 1 Sec. 1 GG relating to personal rights also include the confidentiality of correspondence and the integrity of ICT systems. Hidden infiltration of an IT system, which is used to monitor the system and allows access to the content of data carriers, is permissible under the Fundamental Law only if there is evidence of a specific threat to essential legally protected rights. The following are considered essential legally protected rights: bodily integrity, human life and freedom, or general rights whose violation affects the foundations of the existence of the state or the existence of its citizens. Remote infiltration constitutes a clear violation of the guarantee of human dignity referred to in Art. 1 GG. It is inextricably linked to interference in private life and obtaining personal information collected on media (e.g., diaries, films and other data)[29]. These measures may be considered legally warranted when there is a reasonable probability that the danger will occur in the near future and when specific facts indicate a threat to an important legally protected right from specific persons.

Covert infiltration of an IT system must generally be carried out based on a court order. An act allowing such a measure must also contain arrangements protecting the essence of private life. Therefore, legally allowing the use of remote hearings requires, in the opinion of the BVerfG, an amendment to Art. 1 and 10 GG.

The Federal Constitutional Court, therefore, indirectly referred to the principles of proportionality and adequacy, finding that the use of investigative measures that drastically interfere with the sphere of privacy, such as remote computer searches, may only be used when this method seems to be the only one that can effectively eliminate a threat to important legally protected rights. Online searches must, therefore, constitute an exceptional measure that will be justified on grounds of the highest importance.

As indicated by German legal commentators, to limit the scope of interference in privacy as much as possible, the BVerfG defined the so-called two-step protection test[30]. Firstly, using remote infiltration should be categorically prohibited if only leading to the collection of information relating

29 M. Kutscha, *Das Computer-Grundrecht – eine Erfolgsgeschichte*, „Datenschutz und Datensicherheit" 2012, no. 6, p. 391.
30 Ibidem, p. 392.

to private life. Secondly, the entity responsible for conducting operational activities should subsequently verify whether or not the information extends beyond private-life matters. If not, the collected data should be deleted immediately[31].

BKA-Gesetz – 2017 – comprehensive regulation on the rules of data processing and protection as part of secret searches[32]

Due to the questioning in the German case law of the basis for conducting operational activities, a new Act on the Federal Criminal Office and Police Cooperation Between the Federal Government and the States in Criminal Matters was adopted in 2017[33]. The provisions of the Act regulate, among others, the conduct of operational activities by BKA using special means of obtaining information. Pursuant to § 49 Sec. 1 BKA-Gesetz 2017, the Federal Criminal Office may directly apply, without the knowledge of the data subject, technical measures in the IT systems used by the data subject and obtain data directly if the facts justify the assumption that there is a risk of 1) violating the essential legally protected rights (i.e. body, life, freedom or person) or 2) a public right being jeopardised in a manner that affects the foundations or existence of the Federation or a federal state, or the foundations of human existence.

The Federal Commissioner for Data Protection and Freedom of Information supervises personal data processing activities. Following the provisions of the Act, the Federal Commissioner for Data Protection and Freedom of Information also controls the processing of data in the information system of the Federal Criminal Office. In addition, the Commissioner checks, on a liability basis, at least once every two years, whether access to personal data in the information system and information network takes place exclusively within

31 F. Roggan, op. cit., p. 262.

32 See more in J. Kurek, *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych*..., p. 195 and following.

33 Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten vom 1. Juni 2017 (Bundeskriminalamtgesetz – BKAG) (Gültig ab 25. Mai 2018) zuletzt geändert durch Art. 1 des Gesetzes vom 1. Juni 2017 (BGBl. I S. 1354).

the scope of access rights under § 15 Sec. 1 of the Federal Data Protection Act. If the Federal Commissioner for Data Protection and Freedom of Information finds a violation of § 16 Sec. 2 of the Federal Data Protection Act, they may order appropriate measures if this is essential to eliminate a significant breach of data protection provisions.

The Act also explicitly requires the Federal Criminal Office to technically ensure minimal interference. As indicated, only necessary changes to obtain data may be introduced to the IT system. Furthermore, if technically possible, the authority must ensure that these changes are automatically reversible once the operational measure has been completed. The agent must be protected against unauthorised use by the latest available technology. However, regarding copied data, the regulations require that they be protected against changes, unauthorised deletion and unauthorised access. Significantly, German regulations prohibit mass preventive surveillance. The regulations clearly stipulate that extraordinary measures may only be taken against the person responsible within the meaning of § 17 or § 18 of the Federal Police Act [§ 49(3) BKA-Gesetz 2017].

The Federal Criminal Office Act also provides a significant guarantee for protecting privacy and personal data. Pursuant to § 49 Sec. 7 of the BKA-Gesetz of 2017, if there is anything to indicate that the extraordinary measures taken will only enable insight into the main area of private life, the measure is inadmissible. As far as technically possible, it should be ensured that data relating to the basic sphere of private life is not collected by BKA. The Act also regulates the procedure for deleting personal data. Pursuant to § 79 BKAG, immediate deletion is required for personal data obtained by secret means or data which relates exclusively to private life or is no longer necessary for the purposes for which it was collected, or for possible judicial review of the application of the measure. If the personal data is no longer necessary and processed, it must be deleted immediately. The fact of deletion must be documented. The records must be retained for a period of six months beyond the period of any usefulness of the data or information on procedures relating to the data. It is, therefore, deleted six months after the date of the final court refusal to grant consent to processing or notification to the target person. This documentation may only be used to control data processing and may not have an operational function.

An interesting legislative solution the critical analysis of which can be requested *de lege ferenda* by the Polish legislator is the provisions on the rules for notifying a person under supervision about operational activities carried

out against them. These provisions are essential from the point of view of the data subject's right to information. Under § 74 BKA-Gesetz 2017, the target person and persons significantly affected by covert operational measures must, in principle, be informed that a covert search of information systems has been carried out within the meaning of § 49 BKA-Gesetz 2017. The Federal Criminal Office submits notifications. The notification may be refrained from if running counter to the overriding legitimate interests of the data subject. Besides, notification to a person against whom no action has been taken may be refrained from if the measure has a negligible impact, and it must be assumed that the person supervised would not be interested in being notified. The authority conducting preparatory proceedings may postpone the proceedings by six months. Additional postponement requires the consent of the court. The court determines the duration of the additional delay but for no longer than six months. Extensions to the deferral period are permitted. Five years after the end of the measure, the court may definitively waive the obligation to notify if the terms of notification will almost certainly not be provided in the future, the further use of the data against the person concerned is precluded and the data has been deleted.

BKA also has the option to continue using the acquired data. Pursuant to § 12 BKA-Gesetz 2017, the Federal Criminal Office may continue processing the personal data it collects in two cases. Firstly, to perform the same tasks for which they were initially collected and to safeguard the same legally protected rights, or to investigate or prevent the same crimes for which they were collected. Moreover, as indicated in the regulations, further processing of data initially collected depends on existing urgent danger. The Act also allows for a change in the purpose of personal data processing. BKA may, to fulfil its duties, process personal data for purposes other than those for which they were collected if, as a minimum, it prevents or combats comparably serious crimes [§ 12(2)(a) of the BKA-Gesetz 2017] or protects comparably important legal interests [§ 12(2)(b) BKA-Gesetz 2017].

To conclude the above discussion of the regulations in force in Germany, it should be emphasised that the Federal Criminal Office has no discretion in applying extraordinary measures in operational activities. The regulations require that the use of a measure can generally be made by court order at the request of the President of the Federal Criminal Office or his representative [§ 49(4) BKA-Gesetz 2017]. The Act also regulates the formal requirements for the application and court order. The order may not be issued for a period longer than three months. However, it may be extended for no longer than

three additional months, provided that, considering the current state of knowledge, the original conditions for the initial application of the measure are still present. If the conditions warranting the application of a measure have ceased to exist, the measures adopted under the order must be withdrawn immediately.

In emergencies, the Act allows for an exception enabling action without court consent. Pursuant to § 49 Sec. 8 BKA-Gesetz 2017, in the event of an immediate threat, the President of the Federal Criminal Office or his representative may, in consultation with the data protection officer of the Federal Criminal Office, decide on the use of the information. When reviewing the collected data, he may benefit from technical assistance from two other BKA officers, one of whom must be qualified as a judge. BKA employees must keep any knowledge secret and cannot be used. In such a case, a court order should be issued immediately.

Both in the case when the actions result from a court order and in the case when the authority acted without a prior court order, the Federal Criminal Office may not immediately start analysing the acquired data after completing the operational activities. The information must first be submitted to the competent court, which is required to immediately decide on their usefulness or order their removal. If the data concerns only private-life matters, it must be deleted immediately. All facts related to data collection and deletion must be documented for control and supervisory purposes.

In accordance with the recommendations of the BVerfG, the Act, as amended in 2008, also introduced the principle of a two-stage privacy protection test[34]. Firstly, using remote infiltration is categorically prohibited if only leading to the collection of information relating to private life. Secondly, the entity responsible for conducting operational activities should subsequently verify whether the information obtained does not refer only to private life. In such a case, the data should be deleted immediately[35].

34 M. Kutscha, op. cit., p. 392.
35 F. Roggan, op. cit., p. 262.

Suggestions for the comprehensive regulation of classified operational and reconnaissance activities – particularly in the context of personal data

The analysis of the evolution of German regulations and their comparison with Polish experiences indicate the need to create comprehensive legal regulations in this area. Good laws and a good army are the key foundations of every country[36]. Following the example of German law, this should cover the autonomous regulation of personal data based on EU law standards. This need is additionally justified by the fact that in the Polish legal system, all activities of secret services and other security actors are excluded from European personal data protection regulations.

Comprehensive legal regulations should include at least the following elements:

First. Defining the substantive grounds for the use of spyware by legal protection authorities (including police services and secret services) in operational activities. Online search tools are particularly invasive instruments. In my opinion, we should agree with the views of the legal commentators indicating the need to use such powers in a restrictive manner[37]. It should be limited to cases where there is a high probability of harm to public safety within a foreseeable period[38]. Legal and political approval for using emergency tools must be limited to exceptional cases. Measures that drastically interfere with the sphere of privacy may only be used if this method appears to be the only one that can effectively eliminate the threat to essential legally protected rights[39]. This method should, therefore, be allowed only based on „exceptionality" if there are actual indications of an existing specific threat to essential legally protected rights[40]. Other methods of obtaining information are useless or very difficult[41].

Second. Defining pre-trial and procedural guarantees of individuals as a means of securing and protecting their privacy in connection with the use of

36 M. Maciavelli, *The Prince*, Chapter XII.
37 R. Stettner op. cit., p. 54.
38 F. Roggan, op. cit., p. 262.
39 BVerfG Judgment of 27 February 2008 in Cases 1 BvR 370/07 and 1 BvR 595/07, http://134.96.83.81/entscheidungen/rs200802271bvr037007.html [access: 14.01.2024]..
40 T. Stadler, op. cit., p. 21.
41 M. Soiné, op. cit., p. 1588.

spyware in operational activities. Due to the massive impact of surveillance measures, using remote infiltration should be strictly prohibited if only leading to the collection of information on private life. The entity conducting operational activities should be obliged to subsequently verify whether or not the information obtained is limited to private-life matters. As proposed in the literature, the data should be deleted immediately if the information relates to private life only[42]. Privacy protection should also cover information that will be collected and will refer only to third parties who are not in the sphere of interest of state authorities. The provisions should also define the conditions under which the authority conducting the proceedings could continue using information obtained as part of operational, analytical and information activities. These conditions should take into account the requirements of proportionality and necessity. The additional use of data beyond the activity in which the data was obtained should be allowed only if they are used by the same authority to carry out the same task to protect the same legally protected rights. Due to the particular invasiveness of measures such as online searches of premises and IT systems, and in each case of further data use, the authority should guarantee that the initial conditions that warranted obtaining the data are met. As the German Federal Constitutional Court has noted in its case law, such use does not constitute use for a purpose other than the original purpose of obtaining the data[43]. However, the data cannot be used as circumstantial evidence in other proceedings unless the condition of an urgent and imminent danger or threat is met[44].

Third. Creating a competence map covering entities such as courts, police, prosecutor's office, secret services, personal data protection authorities, privacy and constitutional rights protection authorities, and indicating areas that should be subject to special restrictions due to privacy protection and information. In the judgment of 20 April 2016, in Cases 1 BvR 966/09 and 1 BvR 1140/09, the BVerfG also indicated the admissibility of changing the purpose of using data. The legislator may allow the use of data for purposes other than the original purpose of obtaining it. In particular, one example

42 F. Roggan, op. cit., p. 262.

43 M. Rössel, op. cit., p. 149.

44 J. Kurek, *Ocena ustawy o działaniach antyterrorystycznych. Wskazówki wynikające z orzeczenia BVerfG z 20.04.2016 w sprawie 1 BVR 966/09 i 1 BVR 1140/09* [in:] *Polska ustawa antyterrorystyczna jako odpowiedź na zagrożenia współczesnym terroryzmem*, red. K. Jałoszyński, W. Zubrzycki, A. Babiński, Szczytno 2016, p. 445.

of such use is the transfer of data to other entities under the national cooperation procedure. As indicated by the Court, meeting the requirement of proportionality for such a change in objectives requires an assessment of the hypothetical justification for obtaining the data. In its case law, the BVerfG draws attention to the fundamental principle of the German legal system – the so-called Trennungsgebot[45], which should also be implemented in the Polish legal system. This principle requires the separation of intelligence protection from police powers. This duality means, at the organisational level, a prohibition on obtaining information by constitutional protection bodies using typical police coercion and results in the institutional separation of powers of the police, prosecutor's offices and intelligence services[46].

Fourth. Creating a model procedure for cooperation and division of powers connected with conducting operational activities using spyware between police authorities, secret services and constitutional protection authorities. Based on the concept of divided powers, it would be necessary to define a cooperation model between the involved authorities used to conduct remote searches. Therefore, it is vital to establish an optimum division of powers and lay down the rules of cooperation between these bodies, including the method of transmitting and securing information. It is also necessary to define the rules for deleting or suspending the processing of data and all digital copies held by all entities when, for operational reasons, their processing is no longer warranted by operational activities. The cooperation model should also include an effective model of supervision over activities and data processing. For example, in the Judgments passed in Cases 1 BvR 966/09 and 1 BvR 1140/09, the BVerfG questioned not only the procedure for exercising „internal" control over data relating to the essence of private life by officers of the German Federal Criminal Office (BKA) but also indicated that due to the principle of proportionality, preventive control by an independent body was required. This control may, for example, take the form of a court order. The court also noted that due to the need to limit the risk of subjectivity, supervisory and investigative powers required distinct transparency, legal protection and supervisory control by the Federal Commissioner for Personal

45 For more about the concept of Trennungsgebot, see i.a. K. Nahm, *Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur*, „Neue Juristische Wochenschrift" 2004, no. 46, p. 3289–3295.
46 Ibidem, p. 3293.

Data Protection (Bundesdatenschutzbeauftragter) at least once every two years. The Tribunal also pointed to the need to increase the transparency of BKA's operation[47]. This may raise justified doubts, as it requires an extension of reporting rules towards Parliament and the public. The Court also emphasised the need to record data acquisition and deletion activities. This is a *sine qua non* for effective subsequent control of data use.

Conclusions

To meet the challenges in cybersecurity, the state and its bodies must develop classified instruments that will enable the acquisition of data without the active involvement of private sector entities. However, the scope of application of such tools should not be arbitrary, and their use should be warranted only in cases of existential threats. Challenges are being faced globally in the legal regulation of classified activities. In the case of Polish legislative activities, one of the significant problems regulators must address is the creation of autonomous solutions for processing and securing personal data. This need results principally from the lack of systemic regulations regarding the management of personal data by security entities. The lack of appropriate guidelines will prevent effective cooperation and exchange of information between other entities due to the lack of an equal level of protection.

The German experience is undoubtedly an interesting example. The BKA-Gesetz regulations certainly needed to be critically analysed. Their comparative analysis, however, allows the Polish legislator to use best practices when creating a comprehensive autonomous regulation regarding the processing of personal data by secret services. By excluding the applicable provisions on the protection of personal data in activities within the national security framework, and comprehensively excluding secret services from the GDPR regime and the provisions implementing Directive 2016/697, the Polish legislator left room for autonomous and comprehensive legal regulation. *De lege ferenda*, this space should be regulated urgently. German examples also show that in a hybrid regulatory environment, the creation of autonomous regulations implementing the level of GDPR protection dedicated to

47 M. Wimers, *Teilweise Verfassungswidrigkeit des BKA-Gesetzes*, „Neue Zeitschrift für Verwaltungsrecht" 2016, no. 12, p. 841.

special services allows the creation of independent and dedicated control over the processing of personal data, which will meet the independence requirements.

Bibliography

Arzt C., *Verbunddateien des Bundeskriminalamts – Zeitgerechte Flurbereinigung*, „Neue Juristische Wochenschrift" 2011, no. 6.

Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, http://online.wsj.com/public/resources/documents/prismfactsheet0608.pdf [access: 28.02.2024].

Kurek J., *Bezpieczeństwo państwa w warunkach hybrydowej regulacji danych osobowych w dobie analizy big data. Aspekty prawne, organizacyjne i systemowe*, Warszawa 2021.

Kurek J., *How to achieve a balance between effective preventing crime and protecting privacy of citizens. Online search as a new challenge for e-Justice*, „Masaryk University Journal of Law and Technology" 2009, vol. 3, no. 3.

Kurek J., *Ocena ustawy o działaniach antyterrorystycznych. Wskazówki wynikające z orzeczenia BVerfG z 20.04.2016 w sprawie 1 BVR 966/09 i 1 BVR 1140/09* [in:] *Polska ustawa antyterrorystyczna jako odpowiedź na zagrożenia współczesnym terroryzmem*, red. K. Jałoszyński, W. Zubrzycki, A. Babiński, Szczytno 2016.

Kurek J., *Ochrona przed niezamówioną korespondencją w komunikacji elektronicznej*, Warszawa 2023.

Kurek J., *Przeszukanie online. Postulaty de lege ferenda* [in:] *System bezpieczeństwa w cyberprzestrzeni RP*, eds. W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, Warszawa 2018.

Kurek J., *Wykorzystanie szpiegowskiego oprogramowania w działalności operacyjnej organów ścigania. Gwarancje konstytucyjne i procesowe z perspektywy doświadczeń niemieckich*, „Przegląd Policyjny" 2016, no. 1.

Kutscha M., *Das Computer-Grundrecht – eine Erfolgsgeschichte*, „Datenschutz und Datensicherheit" 2012, no. 6.

Nahm K., *Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur*, „Neue Juristische Wochenschrift" 2004, no. 46.

NSA Prism program taps in to user data of Apple, Google and others, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:networkfront%20main-2%20Special%20trail:Network%20front%20-%20special%20trail:Position1 [access: 15.01.2024].

Roggan F., *Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur*, „Neue Juristische Wochenschrift" 2009, no. 5.

Rössel M., *Teilweise Verfassungswidrigkeit des BKAG*, „IT-Rechtsberater" 2016.

Siedlecka E., *Polskie służby kupiły hakerskie oprogramowanie, które pozwala włamywać się do komputerów i telefonów?*, 16 May 2014, http://wyborcza.pl/1,76842,15975910,Polskiesluzbykupilyhakerskieoprogramowaniektore.html [access: 10.02.2024].

Soiné M., *Eingriffe in informationstechnische Systeme nach dem Polizeirecht des Bundes und der Länder*, „Neue Zeitschrift für Verwaltungsrecht" 2012, no. 24.

Stadler T., *Zulässigkeit der heimlichen Installation von Überwachungssoftware – Trennung von Onlinedurchsuchungen und Quellen – Telekommunikationsüberwachung möglich?*, MMR 2012, no. 18.

Stettner R. [in:] H. Dreier, *Grundgesetz-Kommentar*, Tübingen 2015.

Sucharzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.

Wimers M., *Teilweise Verfassungswidrigkeit des BKA-Gesetzes*, „Neue Zeitschrift für Verwaltungsrecht" 2016, no. 12.

XKeyscore: NSA tool collects „nearly everything a user does on the internet", http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [access: 20.02.2024].

Ukryte oprogramowanie szpiegowskie w służbie bezpieczeństwa państwa. Aspekty prawne, organizacyjne i systemowe

Streszczenie

Żeby sprostać wyzwaniom cyberbezpieczeństwa, państwo i jego organy muszą wypracować niejawne instrumenty, które umożliwią pozyskiwanie danych bez aktywnego udziału podmiotów sektora prywatnego. Są to programy instalowane na urządzeniu użytkownika bez jego zgody, zbierające i wysyłające informacje o systemie operacyjnym oraz wszelkie informacje w nim zawarte. Celem artykułu nie jest analiza dopuszczalności wykorzystywania narzędzi typowych dla działań przestępczych w świecie cyfrowym do celów związanych z bezpieczeństwem państwa i obywateli. Celem jest rozważenie, jakie gwarancje merytoryczne, proceduralne i instytucjonalne muszą zostać spełnione, żeby zapewnić równowagę pomiędzy ochroną praw człowieka i podstawowymi gwarancjami proceduralnymi (takimi jak domniemanie niewinności) a efektywnością działań w cyberprzestrzeni.

Słowa kluczowe: spyware, bezpieczeństwo państwa, czynności operacyjne, narzędzia hackerskie