Operational Activities in the Field of Cybersecurity

Justyna Kurek

Abstract The increase in cybercrime and the importance of cyberspace for the preparatory stage of crimes led to the redefinition of operational and exploratory activities. It has become desirable to move away from the concept of targeted surveillance and towards prevention systems used on a massive scale. This trend is manifested in using technological achievements like hacking software for legal purposes. The goal of this article is to define the concept of state-run on-line remote search of information systems, including the use of breakthrough security software like spyware, in the context of procedural- and pre-trial guarantees, the presumption of innocence and protection of privacy. The article attempts to verify the following research hypothesis: that the creation of new appropriate guarantees (institutional, substantive and procedural) for the digital environment is required since the existing safeguards appropriate to the actions in the real world cannot be applied by analogy in the digital environment without influencing the effectiveness of the measures. The legal framework for operational activities in the digital world must take into account the requirement of subsidiarity and necessity of maintaining a balance between effective criminal law and respect for privacy.

1 Foreword

The twenty-first century is described as the information age.¹ The transformation from machinery-based production to an information-based economy, in which the intellectual factor² plays a crucial part, has resulted in the development of the

¹The concept of the *Information Age* was put forward by M. Castells in the thesis entitled “End of Millennium. The Information Age. Economy, Society, and Culture”, Castells (1998). M. Castells’s trilogy was also published in the Polish language—Castells (2010).

²Wang (2010), p. 4.

J. Kurek (✉)

Faculty of National Defence, Akademia Sztuki Wojennej w Warszawie/War Studies University in Warsaw, Warsaw, Poland

e-mail: j.kurek@akademia.mil.pl

information society. The efficiency of the new economy is driven by knowledge. These processes are accompanied by the continued reduction in the costs related to the aggregation of knowledge and the services related to the latest technology.^{3,4} On entering the information age, some cultural changes have been closely related to the evolution and development of communications. A transformation has been evident from the traditional mass media like TV and radio, predominant in the twentieth century,⁵ to horizontal communication networks based on the Internet and wireless communication.⁶ Computer networks, *open-source* software (including Internet protocols), the rapid development of digital connections, and data transmission with telecommunications networks resulted, at the beginning of the 1990s, in the expansion of the Internet and its use for private purposes. At the same time, a revolution started involving communications and the dynamic development of wireless communication.⁷ The Internet and Internet-based technologies also contributed to a revolution in the understanding of traditional legal terms and institutions. T. Hoeren defined these changes as law deconstruction, depersonalisation, distortion, and de-territorialisation.⁸

All these technological developments, and the related social changes, resulted in the establishment of the information society,⁹ based on permanent access to information, which is essential for both businesses and private lives.¹⁰ The establishing of the new social structure was connected with, and resulted from, the massive success of the Internet, and its growing influence, in particular its non-commercial resources. It facilitated the conceptualisation of real phenomena in the digital world.¹¹

2 The Information Society and the Challenges Related to Security

Digitisation processes resulted not only in changes to the economy and private lives, but also to the functioning of criminal groups and types of crime. The increase in cyber threats has had an impact on public expectations regarding the security measures provided by the state and the authorities. Concerns caused by external threats (*inter alia*, terrorism, the spread of organised crime, and cybercrime) have resulted in rising expectations towards the state regarding security, which also

³Picot and Neuburger (2004), p. 6.

⁴Wang (2010), p. 6 et seq.

⁵Broad analyses of mass media—cf. Kocot (2004), p. 13 et seq.; Polański (2007); Polański (2006), p. 241 et seq.; Kuliński (2010); Janowski (2008); Konieczny (2005).

⁶Castells (2010), p. 9.

⁷Castells (2010), p. 16.

⁸Hoeren (2008), p. 2615.

⁹Mickel and Bergmann (2005).

¹⁰Picot and Neuburger (2004), p. 1; Yukins (2004), p. 667 et seq.

¹¹Mik (1999), p. 63.

include, in addition to traditional military actions and non-military activities, protection against crime and violence.¹² With reference to changes taking place in the information society, redefining the objects regarding the protection of public security in the context of individuals' rights appears crucial. As rightly noted by K. Chałubińska-Jentkiewicz and M. Nowikowska, "constitutional rights provide grounds for any restrictions, as well as for activities performed by public administration authorities, and for the use of certain tools by public authorities¹³". Expectations towards the state as a guarantor of security have also led to social acceptance of the infringement of individuals' fundamental rights if such actions serve the purpose of achieving the objective, which is protecting the security of the public.¹⁴

The growth in cybercrime, and the increased significance of cyberspace's providing a preparatory stage for criminal activities, has enforced the redefinition of the operational activities and practices performed by the police and the special services, including in the field of broader prevention.¹⁵ Consequently, departures from targeted surveillance were accepted, and replaced with prevention measures used on a massive scale.¹⁶ This trend is being demonstrated with the use of the latest technological developments by the police and the special services, including spyware. Seizing and securing data carriers or computing equipment is not sufficient for the purpose of the efficient collection and securing of evidence in cyberspace. Law-enforcement authorities taking action in an overt manner would thwart the effects of these operational activities. Moreover, the transferred content is usually encrypted, and the supply of services in the cloud results in the transfer of informational resources outside the physical devices of suspected or accused persons. Efficient operational activities require covert performance, obtaining access, or extracting data remotely, as well as security breaches and hacking to obtain access to encrypted data. To cope with a variety of tasks related to combating crime, the state must employ hackers, and engage in some justifiable activities in terms of legal defence, avoiding the illegality of acts meeting the criteria for hacking. Possible inevitable side-effects of such operational activities, in particular preventive measures taken on a massive scale, often involve interference with the private lives of third parties not engaged in criminal activities. Securing evidence and operational activities can also result in the disclosure of legally protected data and information—providing the foundation for a fair trial—*inter alia*, interfering with the professional secrecy of defence counsels.

Actually, it is difficult to imagine activities in cyberspace, in particular those involving crime combating and prevention, without close cooperation with the

¹²Zalewski (2013), p. 6.

¹³Chałubińska-Jentkiewicz and Nowikowska (2020).

¹⁴Kurek (2016), p. 163.

¹⁵Adamski (2015), p. 2.

¹⁶Working Document 1 on the US and EU Surveillance programmes and their impact on EU citizens fundamental rights. European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Claude Moraes, 11.12.2013 (DT/2012434Pl.doc), p. 2.

private sector, and the use of its infrastructure. It was perfectly expressed by a German philosopher E.-W. Böckenförde, who commented that “a pillar of a democratic and secular state includes values which the state by itself is not able to guarantee. This is a risky undertaking which the state performs in the name of freedom”.¹⁷ Therefore, the system which efficiently provides cybersecurity must include not only state bodies responsible for crime prevention and combating through cybersecurity, but also the network of private businesses supplying services related to the monitoring and identification of potentially dangerous incidents.¹⁸ Numerous regulations impose certain obligations regarding the reporting of incidents, *inter alia*, the Polish law on the national cybersecurity system. Cooperation with the private sector will ensure the supply of information regarding vulnerabilities and incidents. The digital environment provided and controlled by telecommunications operators and Internet-service providers collects transmission data and digital footprints, which are indispensable for the performance of operational activities.

3 Technological Aspects of Covert Operations

The transparent and widely available methods for the collection and acquisition of information from the private sector are not enough. Accordingly, to face challenges related to cybersecurity, the state and its local authorities must also develop certain covert tools which facilitate the gathering of data without the active engagement of the private sector. However, the operational scope of such tools must not be random, and their use should only be justified in view of existential threats. The development of related software can present a significant challenge. It is certain that it cannot be standard software widely available on the market. Moreover, it is necessary to answer some questions regarding the scope of the cooperation established between the law-enforcement authorities and the private sector during the development of such tools. Can the state use ready-made commercial solutions? Or is the development of customised solutions designed for public entities absolutely necessary?

Notably, even in the case of solutions dedicated for law enforcement authorities, their use poses a risk of unauthorised access to the software and difficulties regarding the protection of source codes. Probably, the development of such tools by a specialised department of law-enforcement authorities would provide a safe, but also costly, solution.¹⁹ When analysing these issues, can the key question be answered regarding codes for this software, i.e. can they be handled by the private sector? Can such source codes be made available to the private sector by public

¹⁷*Der freiheitliche, säkularisierte Staat lebt von Voraussetzungen, die er selbst nicht garantieren kann. Das ist das große Wagnis, das er, um der Freiheit willen, eingegangen ist* W: Buchholtz (2016), s. 910 after Böckenförde (1976), p. 60.

¹⁸Cf. Kurek (2019), p. 152.

¹⁹Kurek (2016), p. 161.

entities for the purpose of setup and upgrade or further development in the context of security?

4 Redefining State Activities—New Tools for Crime Prevention—Spyware in the Service of Security

Due to encryption and cryptographic protection, actions taken by law-enforcement authorities are not limited to acquiring data from telecommunications operators and Internet service providers. Data can be acquired unilaterally, with bypass mechanisms and security breaches using malware, e.g. spyware, trojans, sniffers and keyloggers, i.e. applications which record keystrokes.²⁰ Such software is installed remotely, without the user's consent, to provide information on his or her computer system.²¹ This raises the question not of the deployment of such investigation methods, but of the required logistics and IT-related protection for such operations.

During covert operations, the relevant body should act with due diligence to minimise immissions and safeguard the use of information in forms essential for operational activities. Any information obtained from the system not directly connected with the object of the investigation should be immediately deleted. Moreover, the performance of such activities exposes some gaps and vulnerabilities in the system. The infected system can be more vulnerable to external attacks due to the operation of spyware. In this case, certain solutions adopted by Germany should be considered which oblige the body performing operational activities to provide additional protection for the resources under surveillance. On the completion of operational activities, any security gaps and vulnerabilities should be remedied.²²

The performance of covert operations raises additional questions regarding the right to information in the case of operations performed by the investigating authorities which do not result in the detection of crimes. Should the user of resources be advised accordingly about this surveillance, and his or her security system's being hacked, when there are no charges brought? Considering the analysis regarding potential threats to information resources, the key is the precise documentation of spyware software operation by the body performing the operational activities. For example, the German BKAG law introduced an obligation to log activities. The report must include information regarding the types of technical measures and the times of use thereof; data enabling the identification of the system and any implemented changes; and data enabling the identification of the acquired information.

Another crucial issue is securing the right to privacy. For example, German regulations, in line with recommendations by the BVerfG

²⁰Kurek (2016), p. 161.

²¹Cf. Kurek (2013), p. 66 et seq., and references included therein.

²²A detailed analysis of German solutions in Kurek (2020), s. 225–240.

(*Bundesverfassungsgericht—the highest German Court*), established the principle of a two-level privacy-protection test.²³ First, the employment of any remote-intrusion solution is forbidden when it would only ensure access to information on private lives. Second, the authority responsible for the performance of operational activities should provide conclusive verification that the acquired data do not only relate to private lives, and if they do, any such data should be deleted immediately.²⁴ These solutions are in line with recommendations laid down in European Community strategy and European case law. For example, the European Data Protection Supervisors, on the grounds of case law in the European Court of Justice and the European Court of Human Rights, defined four essential guarantees which should be implemented within national legal systems to minimise interference with private lives to the degree required, and in the scope accepted, in a democratic society, in cases of employed intrusive means of supervision—i.e. (1) processing must be based on transparent, clear, and precise rules; (2) necessity and proportionality must be substantiated with regard to legitimate purposes; (3) an independent supervisory mechanism should be provided; and (4) effective remedies should be available.²⁵

5 Conflicts of Interest Regarding Data Protected by Law

As highlighted by the BVerfG, “State security is essential for public order and peace, and the concomitant respect for human dignity and self-esteem must be guaranteed to ensure public security, as provided by the Constitution’s provisions, and are treated equally with other constitutional rights²⁶”. The protection of public order and national security also contribute to the protection of the rights and freedoms of other people.²⁷ Security should therefore be perceived as a provision contributing to freedom.²⁸ The deployment of spyware in the course of performing operational activities can include not only the surveillance of current and potential criminals, but also of innocent persons.²⁹ Due to the high intrusiveness of such tools and interference with fundamental rights, including the protection of privacy, and the confidentiality of information and trade secrets, legal and public acceptance for such

²³Kutscha (2012), p. 392.

²⁴Roggan (2009), p. 262.

²⁵Working Document 1/2016 of 13.04.2016 (16/EN/WP/237) on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data—European Essential Guarantees.

²⁶Point 100 of BVerfG ruling in cases No. BVR 966/09 and 1 BvR 1140/09.

²⁷Point 53—ECJ ruling of 15 February 2016 in case No. C-601/15.

²⁸Buchholtz (2016), p. 909.

²⁹Also in Adamski (2015), p. 2.

activities requires the establishing of institutional, substantive, and procedural rules.³⁰

An axiological basis for legal regulations concerning covert operations performed by investigating authorities using spyware is provided, *inter alia*, by case law in German courts. The ruling of BVerfG of 20 April 2016 regarding cases No. 1 BvR 966/09 and 1 BvR 1140/09³¹ indicated that the special services' rights whose scope interferes with private lives shall be limited to security matters and the enhancement of essential legitimate interests, i.e. it should be exercised exclusively in cases of serious crimes, and for the protection of life, health, freedom, and national security. The criterion fulfilling this unique condition is the safeguarding of values fundamental to the common interest.³² So, the BVerfG sustained the previous case-law line, for example, in the ruling of 27 February 2008 regarding case No. 1 BvR 370/07, when, examining the right to use online surveillance, it cited the relevance and proportionality rules, and stated that the deployment of surveillance measures highly interfering with private lives might follow only if the method in question was one which could prevent a hazard posed to legally protected rights. Therefore, online surveillance must relate to unique means whose use shall be justified in cases of utmost importance. The German Supreme Court also alluded to the proportionality rule. The BGH's ruling of 31 January 2007 regarding case No. StB 18/06³³ indicated clearly that these means could be employed only if a serious crime is suspected, and thus their use should be subjected to very restricted formal procedures.

The ruling of 20 April 2016 regarding cases No. 1 BvR 966/09 and 1 BvR 1140/09 BVerfG also highlighted the protection of the private lives of persons who, by accident, were within the range of operational measures. The Court cited the issue of third parties not being targeted by the special services, but who are accompanying a suspect (a targeted person). Such persons may be closest persons, family members, friends in close relationships with the suspect, or criminal, whose correspondence, due to its nature (e.g. defence counsels, lawyers) shall be under protection.

6 Summary

In the light of the changes in society, redefining the law enforcement authorities' activities involving the prevention and combating of serious crime seems to be inevitable. Ensuring adequate protection is now impossible without engaging the

³⁰Cf. Kurek (2018).

³¹BVerfG ruling of 20 April 2016 in case No. 1 BvR 966/09 i 1 BvR 1140/09, <https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2016/04/rs20160420_1bvr096609.html>, accessed 1.10.2020 r.

³²Rössel (2016), p. 149.

³³BGH ruling of 31 January 2007 in case No. StB 18/06, <<http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2007&Sort=3&nr=38779&linked=bes&Blank=1&file=dokument.pdf>>, accessed on 1.10.2020.

private sector or interfering with business and human rights. The functioning of the state under such conditions, and the activities conducted by its authorities to combat crime, require the employment of technology related to surveillance and technological advancements, also including the use of operational measures enabling surveillance on a large-scale. The efficient prevention and combating of crime in the digital environment includes the use of *spyware* tools. This should be based on the assumption that protection cannot be ensured at an adequate level without monitoring private computer resources, and includes the surveillance of current and potential criminals, as well as innocent people.³⁴ Due to the high intrusiveness of such tools and interference with the fundamental rights, including the protection of privacy, the confidentiality of information and trade secrets, the legal and public acceptance of such activities requires the establishing of institutional, substantive, and procedural rules.³⁵

References

- Adamski A (2015) Dane telekomunikacyjne jako środek inwigilacji masowej w demokratycznym państwie prawa. In: Majewski J (ed) *Przeciwdziałanie przestępczości. Jawność i jej ograniczenia*, vol X
- Böckenförde E-W (1976) *Staat, Gesellschaft, Freiheit*, Frankfurt
- Buchholtz G (2016) Kein Sonderopfer für die Sicherheits BVerfG erklärt BKAG für verfassungswidrig, NVwZ
- Castells M (1998) *End of millennium. The information age. Economy, society, and culture*, Oxford
- Castells M (2010) *Wiek Informacji. Ekonomia, społeczeństwo i kultura*, Warsaw
- Chałubińska-Jentkiewicz K, Nowikowska M (2020) *Bezpieczeństwo, prywatność, tożsamość – aspekty prawne*, Warsaw
- Hoeren T (2008) Das Pferd frisst keinen Gurkensalat – Überlegungen zur Internet Governance, NJW, No. 36
- Janowski J (2008) *Elektroniczny obrót prawny*, Warsaw
- Kocot W (2004) *Wpływ Internetu na prawo umów*, Warsaw
- Konieczny P (2005) *Komunikacja od mowy do internetu*. <http://histmag.org/?id=744>. Accessed 1 Oct 2020
- Kuliński M (2010) *Regulacje komunikacji elektronicznej w rozwoju społeczeństwa informacyjnego Unii Europejskiej*, Warsaw
- Kurek J (2013) *Ochrona przed niezamówioną korespondencją w komunikacji elektronicznej*, Warsaw
- Kurek J (2016) Wykorzystanie szpiegowskiego oprogramowania w działalności operacyjnej organów ścigania. Gwarancje konstytucyjne i procesowe z perspektywy doświadczeń niemieckich, *Przegląd Policyjny* 1
- Kurek J (2018) Online search. Postulaty de lege ferenda. In: Kitler W, Chałubińska-Jentkiewicz K, Badźmirowska-Masłowska K (eds) *System Bezpieczeństwa w Cyberprzestrzeni*, Warsaw
- Kurek J (2019) Cyberprzestrzeń jako sfera aktywności normatywnej państwa - analiza w kontekście przeciwdziałania przestępczości. In: Taczowska-Olszewska J, Oręziak B, Wielec M (eds) *Zarządzanie ludźmi w organizacji*, Warsaw

³⁴Also in Adamski (2015), p. 2.

³⁵Cf. Kurek (2018).

- Kurek J (2020) Prawne bezpieczeństwo rozwiązań w zakresie przeszukań on-line. Nowe ramy regulacyjne w Niemczech BKA - Gesetz 2017. In: Kosiński J, Krasnodębski G (eds) *Przestępczość teleinformatyczna 2019* / - Gdynia
- Kutscha M (2012) *Das Computer-Grundrecht — eine Erfolgsgeschichte, Datenschutz und Datensicherheit* 6
- Mickel WW, Bergmann J (2005) *Handlexikon der Europäischen Union*, Warsaw
- Mik C (1999) *Media masowe w europejskim prawie wspólnotowym*, Toruń
- Picot A, Neuburger R (2004) In: Hoeren T, Sieber U (eds) *Handbuch Multimedia-Recht München*
- Polański P (2006) Usługi społeczeństwa informacyjnego na tle reformy usług w Unii Europejskiej. Quo Vadis Europo, Warsaw
- Polański P (2007) Customary law of the internet, in the search for a supranational cyberspace law, Hague
- Roggan F (2009) Das neue BKA-Gesetz — Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, *Neue Juristische Wochenschrift* 5
- Rössel M (2016) Teilweise Verfassungswidrigkeit des BKAG. *ITRB*
- Wang FF (2010) Internet jurisdiction and choice of law. Legal practices in EU, US and China, Cambridge
- Yukins ChR (2004) Making federal information technology accessible: a case study in social policy and procurement, *Public Contract Law Journal* 33
- Zalewski S (2013) *Bezpieczeństwo Polityczne. Zarys Problematyki*, Siedlce

Justyna Kurek PhD, an attorney at law and adjunct at the National Security Faculty of the War Studies University in Warsaw. Justyna Kurek is a lecturer in the field of international crime fighting, the law of new technologies, security of electronic communication, protection of classified information, and protection of personal data. Dr Kurek was a long-term employee of central public administration bodies—the Office of Competition and Consumer Protection and the Office of Electronic Communications. She is the author of the scientific monograph “Protection against spam in electronic communication” (2013), over 20 chapters in other scientific monographs, and over 30 scientific articles.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.