Remote Search of IT System in Polish Legislation and Its Importance in Fight Against Cybercrime

Paweł Olber
ORCID: 0000-0002-4614-9527
Police Academy in Szczytno, Poland

Abstract. *The issues of remote access by law enforcement authorities to data in remote IT systems are extremely difficult and controversial. The literature stresses that such activities threaten the right to privacy of the parties involved in the proceedings and the right to a fair trial. However, on the other hand, the dynamic development of new technologies and the need to combat cybercrime effectively require that law enforcement and judicial authorities make use of adequate legal and technical solutions. One such a solution may be a remote search of an IT system, which exists in many European countries, including Belgium, Romania and Germany. In the case of Poland, a search of an IT system as a procedural activity is only allowed in respect of a system in which the person concerned is a dispatcher or user. The Polish legislator has not implemented procedural provisions enabling remote searches via the Internet. In case of the necessity of a system remote search, it will be necessary to conduct a parallel search. Another way of obtaining remote access to data and IT systems may be new methods of covert surveillance, which have been introduced into the Police Act. The new regulations generate a lot of interest among Polish police officers, but at the same time they provoke a lot of discussion. The diversity of the existing approach leads to the development of a uniform interpretation of the introduced regulations, which has been adopted as the subject of this study.*

DOI: 10.5604/01.3001.0013.8288
http://dx.doi.org/10.5604/01.3001.0013.8288

Keywords: covert surveillance, remote search of IT system, remote investigation software, digital evidence.

The main legal act regulating the fight against cybercrime is the Convention on Cybercrime, drafted in Budapest on 23 November 2001 by the Council of Europe. The Convention contains procedural law provisions that can only be applied at national level.[1] The rules contained in this part of the Act oblige the parties to adopt measures which will enable them to effectively conduct criminal proceedings in cases involving new technologies. These include, in particular, legal measures allowing procedural authorities to search and preserve the computer system and to access the content of any data medium. Because of the widespread nature of computer-related crime, it is important to oblige signatory States to introduce a new procedural measure in their national legislation, namely the search of resources of a remote computer system via the Internet.

According to article 19 of the Budapest Convention on Cybercrime, each Party should adopt the appropriate measures necessary to empower the competent national authorities to search or access, by similar means, any information system or part of it, the information technology data stored on it and the medium for storage of information technology data in its territory. In this area, the Polish Code of Criminal Procedure contains relevant regulations, thus guaranteeing the

[1] Raport wyjaśniający do Konwencji o cyberprzestępczości, pkt. 192, p. 33, *Electronic source:* https://rm.coe.int/16800cce5b, *accessed:* 19.07.2019.

possibility of searching the content of an IT system or its part[2]. Competent national authorities should also have adequate resources to allow them to extend a search immediately to another system or to access another system using similar methods. The regulation of how to extend the scope of a search shall be regulated by national law[3].

In Poland, procedural bodies can only use simultaneous search, which consists in conducting correlated activities in different places. Polish law enforcement authorities do not have legal possibilities to carry out extended searches, the essence of which is to extend the scope of activities carried out from the primary system to the secondary one, as well as remote searches. The specificity of a remote search implies that these activities may be classified and concern situations in which it is not possible to inform a person entitled to know that such a search is taking place or is not intentionally informed, in the interest of the proper conduct of the investigation[4].

Remote search of a system as a form of covert policing

In the context of remote access to IT data and search of the IT system, the provisions of the Polish Police Act relating to covert surveillance seem to be important. It is one of the forms of covert policing activities which may be conducted by the Polish Police in a classified manner. Pursuant to article 19(6)(1-5) of the Polish Police Act, the covert surveillance consists in[5]:

1. obtaining and preserving the content of communications conducted using technical means, including telecommunications networks,
2. obtaining and preserving the image or sound of persons from rooms, means of transport or places other than public places,
3. obtaining and preserving the content of correspondence, including correspondence conducted by means of electronic communication,
4. obtaining and preserving data contained in IT data media, telecommunications terminal equipment, IT and ICT systems,
5. accessing and controlling the content of one's shipments.

It should be noted that Article 19(6)(4) of the Police Act provides that covert surveillance consists in obtaining and recording data contained in computer media, terminal equipment, information and communication systems. This provision was introduced by the Act of 15 January 2016 amending the Police Act and certain

[2] Pismo Prokuratury Krajowej nr PK II P 073.81.2016 of 25.07.2018, p. 6. The document in question ia available through Polish police electronic system named Elektroniczny Rejestr Czynności Dochodzeniowo-Śledczych.

[3] Raport wyjaśniający do Konwencji…, pkt. 193, p. 33.

[4] Lach A, Przeszukanie na odległość systemu informatycznego. *Prokuratura i Prawo*, 2011, Vol. 9, pp. 68 and 74.

[5] Ustawa z dnia 6 kwietnia 1990 o Policji, Dz.U. 1990, No. 30, item 179 as amended.

other acts[6]. This regulation raised many questions and interpretation doubts as to its practical application by Polish police officers. The discussed problem has also become a subject of discussion in the literature[7].

With regard to this regulation, attention should be drawn to A. Lach's article 'Remote search of IT system' (pol. 'Przeszukanie na odległośc systemu informatycznego'), which contains a critical assessment of the draft amendment to the Police Act, proposing the introduction of a remote search as covert policing. It should be noted that the legislative work regarding the regulation of remote searches has been carried out since 2009. From the beginning it was assumed that these activities would be regulated in the Police Act as covert policing activities[8].

The justification for the draft amendments to the Police Act[9] shows that the necessity to implement the provisions of article 19(6)(1) of the Police Act was caused by the growing interest of 'criminal or terrorist groups in generally available information technologies that enable encryption of communication channels between computers or the disk space of these computers. This encryption makes it practically impossible for services to access the information and content of the calls that have been secured in this way. Breaking such secured calls or data requires the most modern hardware and software and may take a lot of time (days or months, depending on the length of the key used), which in practice destroys the sense of applying covert surveillance to persons using this type of security. The only effective way to remove such barriers is for the police and other services to obtain confidential access to the content of calls and data of interest to these authorities before encryption, which is possible only on the computer used by a potential criminal. This access may be obtained by installing special software on the computer of the person concerned. It will secretly monitor all the activities carried out on that person's computer and the result of that monitoring will be transmitted via the Internet to the concerned services.'

According to A. Lach, that rule is considered to be too general and does not specify the nature of the institution in question. This seems to be a particular form of control and recording of information messages, as well as a form of remote search, as evidenced by the phrase 'recording on an IT data medium' used in the explanatory memorandum. With regard to the above mentioned regulations, questions arise which disqualify the above mentioned provision on the grounds of the need to regulate precisely the interference with the right to privacy. The questions are as follows[10]:

— to what records and to what extent is access possible pursuant to Article 19(6)(4) of the Police Act ?

[6] Ustawa z dnia 15 stycznia 2016 o zmianie ustawy policji oraz niektórych innych ustaw, Dz.U. 2016, item 147.

[7] This issue was discussed by Lach A in the article: Przeszukanie na odległość systemu informatycznego. *Prokuratura i Prawo*, 2011, Vol. 9; Tański P, Warczak W, Czy Policja może stosować oprogramowanie wirusowe? *Policja, Kwartalnik Kadry Kierowniczej Policji,* 2017, Vol. 4.

[8] Lach A, Przeszukanie na odległość systemu…, *op. cit.,* p. 80.

[9] *Electronic source:* https://web.archive.org/web/20090904041844/http://bip.mswia.gov.pl/download.php?s=4&id=5283, *accessed:* 19.07.2019.

[10] *Electronic source:* https://web.archive.org/web/20090904041844/http://bip.mswia.gov.pl/download.php?s=4&id=5283, *accessed:* 19.07.2019.

— what action should be taken after accessing the data (to view, copy the data)?
— is it a single operation, like a traditional search, or can it be carried out through permanent access during the period indicated in the provision?

In addition, in the case of article 19(6)(4) of the Police Act, we deal with duplication of regulations, because the existing provisions concerning covert surveillance, i.e. the provision of article 19(6)(3) of the Police Act regulates the use of control and recording of information messages. There is no basis for duplicating these regulations by introducing another legal element, because the authorisation to control the content of transfers contains a mandate to create technical possibilities for effective implementation of such control. With regard to the standard contained in this provision, it is worth considering the degree of interference with the right to privacy of information systems users. The legislator has not shown that there is an urgent social need for such solutions in Poland, which is a requirement of the European Court of Human Rights with respect to new legal solutions[11].

In order to complete the considerations made by A. Lach concerning the remote search of IT system, a different view expressed in the article 'Can the police use viruses?' by two authors P. Tański and W. Warczak, should be taken into account. The article in question states clearly that the provisions of article 19(6)(4) of the Polish Police Act allow for the possibility of using solutions enabling remote search of the offender's computer, including, inter alia, the use of the following tools[12]:

— a prepared e-mail message containing software that could imitate useful or interesting for the user applications, called trojan or Trojan horse,
— software or a device for recording keys pressed by the user, a so-called keylogger.

This view, as already mentioned, takes into account the opinions expressed by A. Lach and is grounded on the Constitutional Court stand as expressed in the judgment of 30 July 2014. According to the Constitutional Court, the specific nature of new technologies and the assessment of threats related to them justifies entrusting specialised public authorities (police services and state security services) with adequate powers, thanks to which they will be able to prevent and detect crimes, prosecute their perpetrators, and provide information on threats to legally protected assets. Democratic state governed by the rule of law cannot ignore the growing importance of new technologies and, moreover, the scale of their use, including infringing the law. Current situation requires that these services be equipped with appropriate powers and that they be provided with financial and organisational means to combat infringements effectively. Public authorities should have the legal and factual capacity to detect crimes committed and activities directed against the State or its constitutional bodies. They should also be able to anticipate the actions of violators, preventing the occurrence of threats. In the conditions of global crime and terrorism or organised crime crossing borders, it is also important to prevent threats whose occurrence may cause irreparable losses to legally protected goods. Lack of opportunities to exploit the achievements of modern technology by police services, or even equipping them in such a possibility but to an insufficient extent, may mean that the state does not fulfil

[11] Lach A, Przeszukanie na odległość systemu…, *op. cit.,* p. 82.
[12] Tański P, Warczak W, Czy Policja …, p. 32.

its constitutional task of guarding the independence and inviolability of the Polish territory, and ensuring the safety of citizens, as well as violating the principle of efficiency of public institutions. Sometimes this may result in Poland violating its obligations under international agreements and commitments to cooperate in the fight against international crime and terrorism[13].

According to the Constitutional Court, one of the commonly recognized instruments for detecting threats and prosecuting infringements of the law are covert policing activities, which include covert surveillance, in particular with the use of technical means enabling to obtain information and evidence in a secret manner and to record them, transmitted via telecommunications networks, as well as collection and processing of telecommunications data. These activities are therefore intended to make it possible to prevent and combat risks to an extent that is unprecedented and unattainable by traditional methods. Analysis of materials collected by the means of surveillance or analysis of telecommunications data enables to obtain information of unique significance, allowing for precise reconstruction of decision making processes in criminal groups and interrelationships between communicating persons. The analysis of such data also allows for rapid detection of the perpetrators of threats to important goods such as the life or health of individuals. It is also important to note that new technologies used in the course of covert policing activities make it possible to record and subsequently reconstruct the content of voice, text or multimedia messages transmitted via telecommunications networks. Thanks to them, it is possible to obtain knowledge that was previously unavailable to the state authorities. New technologies are basically the only way to combat cybercrime in its broadest sense. The use of covert policing activities is not so much an improvement in covert policing as it is in most cases the only way to prevent crime or to detect the perpetrators of crime[14].

The view of P. Tański and W. Warczak is based on the claim that the provision of Article 19(6)(4) of the Police Act is a statutory provision, thus enabling lawful activities to be undertaken by law enforcement agencies in the face of activities infringing the constitutional rights of an individual. In addition, as stressed by the Constitutional Court judges, with regard to surveillance, there is no need to indicate in law specific measures of covert surveillance and even less their defined parameters[15]. This statement gave grounds for concluding by P. Tański and W. Warczak that law enforcement authorities are free to use specific technical means and to determine their parameters, provided that they are used within the framework of the closed catalogue of methods of covert surveillance provided for in the law, specified in article 19(6) of the Police Act.

Besides the above mentioned decisions, the authors also pointed out technical issues requiring regulation in order to enable police officers to apply the above mentioned covert surveillance mode, i.e.[16]:

— equipping the Polish Police with specialist software,

[13] Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014, sygn. akt K 23/11, Dz.U. 2014, item 1055, p. 52. *Electronic source:* https://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/dokumenty/wyroki_trybunalu/k_23_11.pdf, *accessed:* 20.07.2019.

[14] Wyrok Trybunału Konstytucyjnego…, *op. cit.,* p. 53.

[15] *Ibid.,* p. 72.

[16] Tański P, Warczak W, Czy Policja …, *op. cit.*, p. 32.

— the use of solutions which interfere minimally with the media and data belonging to the controlled persons,
— full recognition (documentation) of the manner of operation of the IT software in order to use the materials collected (by means of it) in the preparatory proceedings,
— identification of a division within the Polish Police unit responsible for the technical application of IT tools, in which officers with specialist IT knowledge will be employed,
— the establishment of common methods for the collection of data obtained by the above mentioned measures,
— providing Polish Police officers with appropriate tools, service system and classified positions (with limited access), allowing for a permanent and ongoing analysis of the materials obtained within the framework of the control.

Conclusions

The author argues that the position of P. Tański and W. Warczak on the provision of article 19(6)(4) of the Polish Police Act being a statutory provision should be agreed on. It therefore enables Polish law enforcement agencies to undertake legal activities in the field of obtaining and preserving data contained in IT media, telecommunication terminal equipment, IT and ICT systems. However, in relation to the above statement, the full judgment (unlike the above mentioned) of the Constitutional Court should be quoted, according to which 'it is necessary to specify the manner of secret entry into the sphere of privacy of an individual. It is not necessary, however, for the legislation to specify the specific measures of covert surveillance or, even less, to define their parameters. Taking into account the huge number of funds used by the state authorities for covert policing activities, the legal catalogue would have to be extended and the legal norm would have to be casuistic. This solution could conflict with the requirement for an abstract legal norm. It should also be noted that in the era of technological development, the multiplicity of forms of crime and criminal channels of communication, it does not seem realistic to create a closed catalogue of technical means that can be used to obtain information in a constitutionally justified, secret manner, without prejudice to the effective fight against threats or to covert policing disclosure[17]. In the light of the opinions the Constitutional Court rules that, with regard to covert policing activities, 'it is necessary to specify the manner in which an intrusion into the sphere of privacy of the individual is classified'. In the author's opinion A Lach's comments should be taken into account. Therefore, it is still necessary to specify the type of provisions and the scope of access to data within the framework of covert policing activities carried out on the basis of Article 19(6)(4) of the Police Act. It is also necessary to define the scope of activities that can be performed by Polish investigators after obtaining remote access to data/information system and to indicate whether a remote search should be a one-time activity or a kind of monitoring of an information system.

[17] Wyrok Trybunału Konstytucyjnego…, *op. cit.,* pp. 72–73.

It also seems reasonable to assume that the Polish Police authorities should have trained personnel and adequate technical facilities necessary to apply the above-mentioned covert surveillance procedure. It seems, however, that this issue needs to be further developed. First of all a reference should be made to the statement that it is necessary to indicate a division in the Polish Police responsible for technical application of IT tools in which officers with specialist IT knowledge will be employed. It should be noted that at present, in the case of Polish police authorities, 'specialist knowledge' (as determined by law) in the field of information technology is the domain of computer forensic experts from police forensic laboratories only. 'Specialist knowledge' may be the result of specialised training and must be distinguished from knowledge of a particular field acquired during studies and further training courses[18]. Depending on the decisions taken (in accordance with A. Lach's comments) as to the scope of the actions to be taken after remote access to data, a decision would have to be taken as to whether the implementation of such technical actions really requires 'specialised knowledge'. There is no doubt that these are covert policing activities and should therefore be performed by specialists/officers of the Cybercrime Departments. Police officers/specialists employed in these departments should have appropriate IT knowledge and practical skills as well as appropriate qualifications (confirming their skills) to perform the tasks referred to in the art. 19(6)(4) of the Police Act. The necessary qualifications should be obtained, as in the case of computer forensic experts, after completion of an internal training courses, developed and approved in advance, which end in an examination and certification. With regard to the claim that it is necessary to equip Polish Police with specialist software, one should consider who should be the author of IT tools for covert surveillance: officers/staff of police authorities or an external company ? However, there is no doubt that the operation of this type of software should be transparent for Polish law enforcement agencies and thus should automatically record the processes and tasks performed. Besides providing police authorities with appropriate software, tools and system for handling classified positions, it would also be necessary to provide appropriate IT infrastructure enabling collection of huge sets of data with broadband Internet access.

References

1. Lach A, Computer system remote search, *Prokuratura i Prawo*, 2011, Nr 9, p. 67.
2. Raport wyjaśniający do Konwencji Rady Europy o cyberprzestępczości. *Electronic source:* https://rm.coe.int/16800cce5b.
3. Tański P, Warczak W, Czy Policja może stosować oprogramowanie wirusowe? *Policja. Kwartalnik Kadry Kierowniczej Policji,* 2017, Vol. 4.
4. Ustawa z dnia 15 stycznia 2016 o zmianie ustawy o Policji oraz niektórych innych ustaw, Dz.U. 2016, item 147.

[18] Wyrok Sądu Najwyższego z dnia 15 kwietnia 1976, SN II KR 48/76, OSNKW 1976, No. 10–11, item 133; Wyrok Sądu Najwyższego z dnia 23 listopada 1982, SN II KR 186/82, OSNPG 1983, No. 5, item 59.

5. Ustawa z dnia 6 kwietnia 1990 o Policji, Dz.U. 1990, No. 30, item 179 as amended.
6. Uzasadnienie projektu zmian ustawy o Policji. *Electronic source:* https://web.archive.org/web/20090904041844/http://bip.mswia.gov.pl/download.php?s=4&id=5283.
7. Wyrok Sądu Najwyższego z dnia 15 kwietnia 1976, SN II KR 48/76, OSNKW 1976, Vol. 10–11, item 133.
8. Wyrok Sądu Najwyższego z dnia 23 listopada 1982, SN II KR 186/82, OSNPG 1983, Vol. 5, item 59.
9. Wyrok Trybunału Konstytucyjnego z dnia 30 lipca 2014, sygn. akt K 23/11, Dz.U. p2014, item 1055. *Electronic source:* https://www.senat.gov.pl/gfx/senat/userfiles/_public/k8/dokumenty/wyroki_trybunalu/k_23_11.pdf
10. Pismo Prokuratury Krajowej nr PK II P 073.81.2016 of 25.07.2018.

About the Author

***Paweł Olber**, PhD, lieutenant, senior lecturer at the Institute for Legal Sciences, Faculty of Security and Legal Sciences at the Police Academy in Szczytno, Poland. His research interests are: computer forensics, in particular the study of digital evidence and issues related to the legal and technical aspects of IT data security and cybercrime. E-mail: p.olber@wspol.edu.pl*

***Streszczenie.** Zagadnienia dotyczące uzyskiwania zdalnego dostępu przez organy ścigania do danych znajdujących się w odległych systemach informatycznych są niezwykle trudne i kontrowersyjne. W literaturze przedmiotu podkreśla się, że tego rodzaju czynności zagrażają prawu do prywatności uczestników postępowania oraz prawu do rzetelnego procesu. Jednocześnie dynamiczny rozwój nowych technologii oraz potrzeba skutecznego zwalczania cyberprzestępczości wymagają, by organy ścigania i wymiaru sprawiedliwości wykorzystywały adekwatne rozwiązania prawne i techniczne. Jednym z takich rozwiązań może być instytucja zdalnego przeszukania systemu informatycznego, która funkcjonuje w wielu państwach europejskich, w tym między innymi w Belgii, Rumunii oraz w Niemczech. W przypadku Polski, przeszukanie systemu informatycznego jako czynność procesowa jest dopuszczalne wyłącznie w zakresie systemu, którego dana osoba jest dysponentem lub użytkownikiem. Polski ustawodawca nie wdrożył przepisów procesowych umożliwiających przeprowadzenie przeszukania na odległość za pośrednictwem sieci Internet. W przypadku zaistnienia konieczności przeszukania systemu odległego, niezbędne będzie przeprowadzenie przeszukania prowadzonego równolegle. Innym sposobem uzyskiwania zdalnego dostępu do danych i systemów informatycznych mogą okazać się nowe metody kontroli operacyjnej, które zostały wprowadzone do ustawy o Policji. Nowe przepisy wzbudzają szerokie zainteresowanie wśród funkcjonariuszy polskiej Policji, wywołując jednocześnie wiele dyskusji. Różnorodność istniejącego podejścia do omawianej problematyk, skłania więc do wypracowania jednolitej interpretacji wprowadzonych przepisów, co przyjęto za przedmiot niniejszego opracowania.*

***Резюме.** Вопросы, связанные с удаленным доступом правоохранительных органов к данным, размещенным в удаленных ИТ-системах, являются чрезвычайно сложными и спорными. В литературе подчеркивается, что такая деятельность ставит под угрозу право на неприкосновенность частной жизни участников судебного процесса и на справедливое судебное разбирательство. Одновременно, динамичное развитие новых технологий и необходимость эффективной борьбы с киберпреступностью требуют от правоохранительных и судебных органов использования надлежащих правовых и технических решений. Одним из таких решений может оказаться система удаленного поиска в ИТ-системе, которая работает во многих европейских странах, в том числе в Бельгии, Румынии и Германии. В Польше поиск в системе ИТ в качестве процессуальной деятельности разрешается только в рамках системы, которой данное лицо является владельцем или пользователем. Польский законодатель до сих пор не ввел процессуальные положения, предусматривающие возможность удаленного поиска с использованием сети Интернет. В случае необходимости*

проведения поиска в удаленной системе, следует провести параллельный поиск. Другим способом получения дистанционного доступа к данным и ИТ-системам могут оказаться новые методы оперативной проверки, которые были внесены в Закон о полиции. Эти новые положения вызывают большой интерес среди сотрудников польской полиции и одновременно — дискуссию. Разный подход к рассматриваемому вопросу требует разработки единого понимания вводимых правоположений, что и стало основной темой настоящей статьи.