Ius Novum
2026, vol. 20, no. 2, pp. 42–53

PEGASUS SOFTWARE AND FAIR CRIMINAL PROCEEDINGS

MIŁOSZ KOŚCIELNIAK-MARSZAŁ*

DOI 10.2478/in-2026-0016

Abstract
The study discusses the functionalities of programmes created to provide special services with the possibility of taking control of mobile devices. By presenting cases of the use of such systems for political purposes and by describing a situation in which incriminating material was fabricated through the use of such systems, the author argues that there is a need for increased judicial oversight of the secret services' activities and for a change in the approach taken by criminal trial authorities to material secured in terminal devices. In view of the possibilities offered by spyware, such material may serve as the basis for findings unfavourable to the accused only after external interference has been excluded, which is all the more difficult because the activities of the secret services are covered by secrecy. The aim of this article is to initiate a discussion on the use of material obtained from the memory of mobile devices in criminal proceedings and to consider the direction in which changes to the law should be undertaken in order to reduce the related threats to fair proceedings.

Keywords: spyware, evidence, surveillance, secret service

In July 2021, representatives of Forbidden Stories, together with 17 media outlets from around the world and with technical support from Amnesty International, conducted an extensive journalistic investigation which found that countries such as Saudi Arabia, Armenia, Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Poland, Rwanda, Togo and the United Arab Emirates (UAE) had acquired software called 'Pegasus' from NSO Group, which was intended to combat the most serious crimes, especially terrorism. However, human rights defenders and those in opposition to state authorities became targets of surveillance using that

* LLD, University of Opole (Poland), e-mail: kancelaria@adwokatmilosz.pl, ORCID: 0000-0002-7261-3389

software. In October 2018, a critic of the Saudi royal family, Jamal Khashoggi, was killed, having been subjected to 'Pegasus' surveillance in the months leading up to his death. More than a thousand phone numbers in Azerbaijan were infected with 'Pegasus'. Journalists, among others, were among those who had been subjected to surveillance. In Armenia, this software was used against journalists as well as human rights defenders. The Hungarian government used it against journalists, opposition politicians, lawyers, university lecturers, prosecutors and social activists. In Greece, around three hundred people were spied on in this manner, including members of the European Parliament and journalists. In Spain, the Prime Minister, the Minister of Defence, the Minister of the Interior and other high-ranking officials, as well as members of the local government of Catalonia, persons belonging to the movement fighting for the independence of Catalonia and members of the European Parliament, lawyers, academics, as well as representatives of civil society, were all subjected to surveillance. Morocco and Rwanda used 'Pegasus' to subject, among others, the President of France, the Prime Minister, the Minister of Defence and the Minister of the Interior of Spain, the Prime Minister of Belgium, the former President of the European Commission, and the former Prime Minister of Italy to surveillance.[1] The Polish secret services used 'Pegasus' against, among others, Senator Krzysztof Brejza during the period when he headed the opposition party's 2019 election staff, Judge Beata Morawiec, who headed the Themis Association of Judges, which criticised the actions of the Ministry of Justice, Prosecutor Ewa Wrzosek, who openly criticised undemocratic changes in the Polish judiciary, as well as advocate Roman Giertych, who opposed the actions of the Minister of Justice.

The purpose and use of the aforementioned software became the subject of the election campaign for the Polish Sejm and Senate in 2023. This was further fostered by a report produced by the Commission of Inquiry on 'Pegasus' appointed by the European Parliament, adopted by recommendation on 15 June 2023. It emphasised that the surveillance carried out with this tool does not meet the requirements outlined in the case law of the ECtHR and the CJEU and therefore remains contrary to the principles provided for in Article 2 of the Treaty on European Union and the fundamental rights enshrined in Article 7 (right to respect for privacy), Article 8 (protection of personal data), Article 11 (right to freedom of expression), Article 17 (right to property), Article 21 (principle of non-discrimination) and Article 47 (right to an effective judicial remedy) of the Charter of Fundamental Rights of the European Union.[2]

Following the seizure of power by the former opposition, the Sejm of the Republic of Poland appointed a Commission of Inquiry to investigate the legality, correctness and expediency of operational and exploratory activities undertaken, *inter alia*, with the use of 'Pegasus' software, by members of the Council of Ministers, the special services, the police, the fiscal and customs control authorities, the authorities responsible for the prosecution of crimes and the prosecutor's office in the period from 16 November 2015 to 20 November 2023. The work of this body

[1] M. Matusiak-Frącczak, 'Konwencyjne standardy legalnej inwigilacji a zastosowanie systemu Pegasus w Polsce', *Europejski Przegląd Sądowy*, 2023, No. 12, pp. 26–28.

[2] Ibidem, p. 28.

revealed to the public a considerable amount of information on the functioning of the special services, access to which was restricted due to the content of Article 24(1) of the CBA Act, Article 20a(1) of the Police Act, Article 35(1) of the Internal Security Agency Act, Article 9c(1) of the Border Guard Act, Article 131(1) of the National Fiscal Administration Act and Article 40(1) of the Military Police and Military Order Authorities Act. The jurisprudence shaped against this background has consistently taken the position that all information the disclosure of which would hinder the services in the performance of their tasks, including the performance of operational and exploratory activities, regardless of whether it relates to specific proceedings, is subject to protection under the principles governing classified information.[3] Knowledge of the characteristics of the tools of operational work would create a risk of disclosure of the techniques used to carry out operations and, as a consequence, of depriving those services of any real possibility of performing their statutory tasks and, consequently, of dismantling the service.[4] Ignorance on the part of persons breaking the law has, in this case, a preventive character, hindering criminal activities, and it remains in the interest of the Republic of Poland that an individual's right of access to public information be limited in this respect.[5]

On the subject of 'Pegasus' itself, a report presented by NSO Group was indeed known, but it dated back to 2016.[6] Information on the capabilities of later versions of this software was only made available to the public through the session of the aforementioned parliamentary committee. Witness Jerzy Kosiński, who attended the presentation on behalf of the Polish authorities in 2019, testified that, during the presentation, the 'Pegasus' system proved to be an IT tool with complex functionality that allowed control of a mobile device to be taken over in a manner that did not signal to the owner that control had been lost.[7] During the demonstration, participants were given the ability to make calls through the seized devices and talk through them; they also performed tests involving switching on the microphone and listening to the surroundings, as well as obtaining direct access to the cameras, which they could activate at any time and use to take pictures. As the phone was taken over completely, it was possible to use all its functionalities and the tools

---

[3] Judgment of the Supreme Administrative Court of 2 February 2018, I OSK 668/16, LEX no. 2475548; see S. Hoc, P. Szustakiewicz, *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, Warszawa, 2023, commentary to Article 24.

[4] P. Opitek, 'Kontrola operacyjna urządzenia końcowego', *Prokuratura i Prawo*, 2023, No. 4, pp. 60–61.

[5] Judgment of the Supreme Administrative Court of 18 August 2015, I OSK 1679/14, Legalis no. 1361796.

[6] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (*casus *Pegasusa)*, 15 February 2022, pp. 7–9; https://kipk.pl/wp-content/uploads/2022/02/ekspertyzapegasus.pdf (accessed: 10 May 2024).

[7] *Pełny zapis przebiegu posiedzenia Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjnorozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania PEGASUS przez członków rady ministrów, służby specjalne, policję, organy kontroli skarbowej oraz celnoskarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r. (nr 4) z dnia 15 marca 2024 r.*, Kancelaria Sejmu, Biuro Komisji Sejmowych, p. 7; https://orka.sejm.gov.pl/zapisy10.nsf/0/F2D9E8013C0D37E5C1258AEE002C1F-7F/%24File/0002610.pdf (accessed: 26 April 2024).

installed on it to impersonate its owner, for example, to act in his name on social networks, instant messaging services, banking systems, etc.[8] In addition, the system operator was able to modify the content stored in the device's memory, for example, by changing the content of the text messages stored there.[9] A characteristic feature of 'Pegasus' was that it was difficult to detect because, unlike other such systems, it did not permanently write itself to the storage medium, but installed itself in the operating memory.[10] Its use therefore left very few traces of infection,[11] so that even an expert would have difficulty distinguishing which of the data stored on the device had been introduced by the system operator and which came from the actual user of the device.[12]

The above information reinforces reservations concerning covert surveillance, which has in any event long been controversial.[13] This is because activities of this type interfere very strongly with fundamental human rights, such as the right to respect for private life guaranteed by constitutional provisions (Article 49 of the Constitution of the Republic of Poland), as well as international provisions (Article 8 of the ECHR and Article 17 of the ICCPR). In the course of covert surveillance, such constitutional interests as family life, property, secrecy of correspondence or, more broadly, secrecy of communication, inviolability of the home, informational autonomy, and bodily integrity are often violated. These are therefore regarded as very 'aggressive' tools.[14]

On the other hand, however, without their use, the effectiveness of law enforcement agencies or authorities established to protect the law would be significantly reduced. Thus, there is a conflict between the need to ensure many freedoms and human rights and the need to interfere with some of them to a certain extent in order effectively to prosecute crimes, protect public safety or ensure legal order.[15] However, it is difficult to imagine any state giving up tools allowing electronic surveillance, as such instruments are a response to the direction in which modern crime is developing, especially terrorism and crime related to the functioning of organised crime groups and corruption.[16] The European Court of Human Rights, in a judgment of 25 May 2021, ruled that the Swedish service's use of electromagnetic signals intelligence, and therefore the interception and analysis of the content of communications carried out by millions of citizens, remained lawful.

---

[8] Ibidem, p. 50.

[9] Ibidem, p. 13.

[10] Ibidem, p. 12.

[11] Ibidem, pp. 49–50.

[12] Ibidem, p. 35.

[13] Cf. A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin, 2006, p. 346.

[14] Decision of the Supreme Court of 26 April 2007, I KZP 6/07, *OSNKW*, 2007, No. 5, item 37.

[15] See P. Czarnecki, 'Czynności operacyjno-rozpoznawcze a postępowanie karne', *Palestra*, 2014, No. 7–8; https://palestra.pl/pl/czasopismo/wydanie/7-8-2014/artykul/czynnosci-operacyjno-rozpoznawcze-a-postepowanie-karne (accessed: 22 February 2025).

[16] T. Łodziana, 'Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika', *Palestra*, 2022, No. 9, p. 63; https://palestra.pl/pl/czasopismo/wydanie/9-2022/artykul/kontrola-operacyjna-oraz-uzycie-systemu-pegasus-w-polsce-polemika (accessed: 25 April 2024).

The UK's *Investigatory Powers Act* provided for similar solutions. In France, the state services took over the EncroChat messenger and carried out large-scale interception of messages from tens of thousands of phones. In Germany, on the other hand, legislation gives the services the right to use software to break through the security of phones and computers and to read the contents of devices used by people who have not been officially charged but are only suspected of having committed a crime. Such tools are called 'Staatstrojaner', or 'state trojans', and are used for a wider range of crimes than terrorism alone.[17]

The possibilities offered by modern spy systems to their users necessitate a revision of previous views. In the current situation, it is no longer so much a matter of ethical resistance related to the deceitful nature of surveillance,[18] but rather of the real danger of fabricating materials which are then used by authorities enjoying the protection stemming from the constitutional presumption of the legality of their actions. The flagship example here is the case of Senator Brejza, who was subjected to surveillance with 'Pegasus' as many as 33 times and had approximately 1 gigabyte of data uploaded to his phone, that is to say, the content of his phone was altered by the addition of new content.[19]

At this point, it should be emphasised that the term 'Pegasus' is the proper name of a specific system. It is not the only software of this type. The Polish National Public Prosecutor's Office also had, in parallel, software called 'Hermes', which was officially intended for the advanced collection and analysis of data from internet sources, but not all its functionalities have yet been examined.[20] Many countries have implemented various similar methods of operational work. A specialised spying system for Interpol was offered by a German company.[21] The US Drug Enforcement Administration uses, among others, the 'Graphite' system developed by Paragon, which is able to break through the security of modern smartphones and bypass the encryption of messengers such as WhatsApp and Signal, while also extracting data from the cloud.[22] The Italian secret service, in turn, used the spyware 'Hermit' in 2019.[23] Since the eponymous 'Pegasus', owing to its previously unknown functionalities, became a turning point both in the discussion of methods of information extraction by state authorities and in the procedural use of material from mobile telecommunications devices designed to connect directly or indirectly

---

17 P. Opitek, 'Poważnie kontrolować można nie tylko terrorystów', *Rzeczpospolita*, 20 January 2022; https://www.rp.pl/opinie-prawne/art19306701-pawel-opitek-powaznie-kontrolowac-mozna-nie-tylko-terrorystow (accessed: 25 April 2024).

18 R. Skowron, 'Kontrola operacyjna a ochrona praw jednostki', *Studenckie Konferencje Naukowe*, 2014, No. 4, p. 136.

19 M. Matusiak-Frącczak, 'Konwencyjne standardy…', op. cit., p. 28.

20 https://www.gov.pl/web/pr-rzeszow/komunikat-z-dnia-21-czerwca-2024r. (accessed: 25 June 2024).

21 *Pełny zapis przebiegu posiedzenia Komisji Śledczej…*, op. cit., p. 14.

22 M. Fraser, 'Nie skończyć jak NSO Group. Tak producenci spyware zabiegają o przychylność USA', *CyberDefence24*, 2 June 2023; https://cyberdefence24.pl/biznes-i-finanse/nie-skonczyc-jak-nso-group-tak-producenci-spyware-zabiegaja-o-przychylnosc-usa (accessed: 6 December 2024).

23 *CyberDefence24*, 'Rządowa inwigilacja to nie tylko Pegasus. Spyware Hermit atakuje na Androidzie', 17 June 2022; https://cyberdefence24.pl/cyberbezpieczenstwo/rzadowa-inwigilacja-to-nie-tylko-pegasus-spyware-hermit-atakuje-na-androidzie (accessed: 6 December 2024).

to network terminations,[24] this term will hereinafter be used as an example of a spyware system offering the possibility of hard-to-detect interference with data stored on the terminal device.

It is significant that in Poland secret surveillance is used on a very large scale and shows an increasing trend. While in 2011 the courts granted authorisation for the interception and recording of conversations, or for operational control, in 4,863 cases,[25] in 2022 the number of such authorisations reached as many as 9,781. At the same time, the exact number of programmes enabling control of terminal devices in the possession of the Polish services remains unknown. However, between 2017 and 2022, three of those services used 'Pegasus' for the operational control of terminal devices in respect of 578 individuals. In 2017, this concerned 6 persons; in 2018, 100 persons; in 2019, 140 persons; in 2020, 161 persons; in 2021, 162 persons; and in 2022, 9 persons.[26] It is worth noting at this point that in 2017 the services applied over 9,800 times for permission for operational control, and the courts refused such applications in only 9 cases.[27] The Supreme Chamber of Control, having examined the period from 1 January 2017 to 31 March 2023, concluded that the current system of supervision, coordination and control of the activities of the special services in Poland is ineffective and does not correspond to the standards in force in democratic states governed by the rule of law and, in particular, does not ensure effective supervision over the implementation of the tasks of the services and does not guarantee that, in the course of their implementation, the applicable laws will be observed and civil rights and liberties will be respected.[28]

Objections to the use of spyware for the purpose of acquiring evidence intended for use in criminal proceedings are, to a large extent, related precisely to the problem of insufficient judicial oversight over covert surveillance carried out by the special services. Indeed, while in 2013 Polish solutions in this regard were considered very restrictive compared with those of other European countries,[29] in the following years the standards of guarantee, and consequently the requirements for this type of activity, increased significantly. In a judgment of 4 May 2000, the European Court of Human Rights emphasised that covert surveillance systems must contain legal (procedural) guarantees applicable to the oversight of the activities of the

---

[24] See Article 2(43) of the Act of 16 July 2004 – Telecommunications Law, Journal of Laws 2024, item 34.

[25] Source: official website of the Public Prosecutor's Office, www.pg.gov.pl (accessed: 7 September 2012).

[26] M. Kowalewski, 'Sąd Najwyższy zgadzał się na stosowanie Pegasusa', *Salon24*, 24 April 2024; https://www.salon24.pl/newsroom/1374074,sad-najwyzszy-zgadzal-sie-na-stosowanie-pegasusa (accessed: 4 June 2024).

[27] P. Rojek-Socha, 'Kontrola operacyjna – sądy weryfikują to co służby chcą?', *Prawo.pl*, 19 July 2018; https://www.prawo.pl/prawnicy-sady/jak-sady-weryfikuja-wnioski-o-kontrole-operacyjna,263148.html (accessed: 22 February 2025).

[28] J. Ojczyk, 'Służby podsłuchują nas bez kontroli, bo pozwala na to prawo. Potwierdził to europejski trybunał', *Business Insider*, 28 May 2024; https://businessinsider.com.pl/prawo/europejski-trybunal-praw-czlowieka-wyda-wyrok-w-sprawie-inwigilacji-w-polsce/3b3e4kh (accessed: 4 June 2024).

[29] J. Mąka, 'Kontrola operacyjna i podsłuch – ocena na tle praktycznego stosowania', *Przegląd Bezpieczeństwa Wewnętrznego*, 2011, No. 4, p. 58.

relevant services. According to the Court, the oversight procedures must adhere as closely as possible to the values of a democratic society, and in particular to the principle of the rule of law. This, in turn, presupposes that interference by the executive authorities with individual rights should be subject to effective oversight.[30] In the cases of *Pietrzak and Bychawska-Siniarska et al. v. Poland*, the European Court of Human Rights noted the lack of sufficient legal guarantees of protection against arbitrariness and abuse in the sphere of operational control, data storage and access to communication data.[31] Every state, and therefore its authorities, must act on the basis of and within the limits of the law, and may not take arbitrary action. Any interference by the state, and thus also electronic interference, with the guarantees of individual rights must be based on the principle of proportionality.[32]

The Polish Constitutional Court has also taken the position that the legislator, in the light of Article 2 of the Constitution, has a constitutional obligation to define the prerequisites for interference in the sphere of privacy as precisely as possible, so as to limit the scope of the discretion left to bodies applying the law, and at the same time is obliged to create appropriate mechanisms for the oversight of acts of public authorities affecting this sphere. When it comes to the restriction of the constitutional freedoms and rights of a human being and a citizen, legislation must be characterised by due precision and clarity. This injunction is functionally related to the principles of legal certainty and security, and to the protection of confidence in the state and the law.[33] In another judgment, the Court stated that an important criterion for assessing the admissibility of equipping a public authority with the power to carry out operational and control activities is the assessment of the functionality of specific activities from the perspective of the tasks carried out by a given authority and the absence of any possibility of the effective performance of those tasks without specific powers in the sphere of operational and control activities. In both these cases, the obligation to demonstrate such expediency and necessity rests with the legislator.[34] On the other hand, in the justification of the judgment of 20 April 2004, the Court indicated that, in the light of the Constitution, the services responsible for security and public order cannot be regarded as having autonomy in the sphere of operational activities. It is therefore not possible, by invoking the requirement of the effectiveness of operational activity, to exclude it from any oversight. Therefore, this activity is not excluded from the limitations which the Constitution imposes on all authorities encroaching upon the sphere of the individual's fundamental rights and freedoms, especially as, by undertaking operational and exploratory activities, police authorities encroach secretly upon the sphere of civil rights and freedoms, as required by the purpose of those activities.

---

30 *Rotaru v. Romania*, Case No. 28341/95.

31 Judgment of 28 May 2024, Chamber (Section I), application nos. 72038/17 and 25237/18.

32 See ECtHR judgment of 7 February 2017 in *Irfan Guzel v. Turkey*, application no. 35285/08, para. 86; ECtHR judgment of 12 January 2016 in *Szabo and Vissy v. Hungary*, application no. 37138/14, paras. 70–72; ECtHR judgment of 4 December 2015 in *Zakharov v. Russia*, application no. 47143/06, para. 260.

33 Judgment of the Constitutional Court of 20 June 2005, K 4/04, OTK-A 2005, No. 6, item 64.

34 Judgment of the Constitutional Court of 17 June 2008, K 8/04, OTK-A 2008, No. 5, item 81.

Such specificity of the said activities requires them to be subjected to a well-thought-out system of oversight: effective and not merely a facade, while certain activities should be applied only to the extent necessary for the realisation of constitutional goals and in a manner characterised by the least possible degree of intrusion for citizens and by the application of specific procedures. Otherwise, the democratic state governed by the rule of law would effectively become a police state.[35] In accordance with this view, the Court of Appeal in Wrocław, in its judgment of 11 May 2023, expressed the opinion that where the court deciding on the accused's criminal liability has no possibility of verifying whether the operational control was lawfully ordered, the evidence obtained as a result must be assessed in the light of the primacy of the norm expressed in Article 5 § 2 of the Code of Criminal Procedure (CCP). Acceptance of a different position would mean that judicial oversight over operational and exploratory activities is in fact illusory and merely a facade, while officers of the competent services conduct these activities and at the same time themselves decide whether they are legal, and whether the materials obtained as a result thereof may be used in the trial.[36] What is more, under the current state of the law, a person under surveillance has no knowledge of the operational activities conducted against them, owing simply to the lack of access to relevant documents or data sets. Unless an indictment is brought against them, that person does not acquire such knowledge even after the completion of the operational activities, and is thus subjected to arbitrary action by the authorities over which they have no influence. Even if they were to acquire such knowledge, they cannot demand an effective review of the legality and reliability of the operational activities carried out, which violates the individual's right to information under Article 51(3) of the Constitution of the Republic of Poland and, consequently, precludes the possibility of lodging a complaint with the court pursuant to Article 78 of the Constitution of the Republic of Poland.[37]

In the light of the above-mentioned judgments and the current legal regulation, it remains particularly pertinent that, despite the exceptionally far-reaching capabilities of the 'Pegasus' system, the court, when considering an application for permission to conduct operational control, does not obtain knowledge of the technical aspects of the planned undertakings and thus, unless it conducts additional explanatory proceedings, will not know what tools the special services intend to use to carry out the requested control. Having possibly given its consent, it also does not have at its disposal any instruments for the ongoing supervision of the course of the control conducted, which at this stage is left to the exclusive discretion of the special services. In such a context, the systemic legal principle of legality, stemming

---

[35] Judgment of the Constitutional Court of 20 April 2004, K 45/02, OTK-A 2004, No. 4, item 30.

[36] Judgment of the Court of Appeal in Wrocław of 11 May 2023, II AKa 480/21, LEX no. 3652572.

[37] R. Rynkun-Werner, 'Kontrola operacyjna bez kontroli – kilka refleksji na kanwie postanowienia Trybunału Konstytucyjnego z 28.06.2022 r. (SK 60/21)', *Palestra*, 2023, No. 4; https://palestra.pl/pl/czasopismo/wydanie/4-2023/artykul/kontrola-operacyjna-bez-kontroli-kilka-refleksji-na-kanwie-postanowienia-trybunalu-konstytucyjnego-z-28.06.2022-r.-sk-60-21 (accessed: 22 February 2025).

from Article 7 of the Constitution of the Republic of Poland, assumes particular significance, imposing certain obligations both on public authorities applying the law and on those enacting it, on the basis of the relevant competence, procedural and substantive provisions. The point, however, is that Article 7 of the Constitution also forms the basis for the legal presumption that actions taken by state authorities comply with the law.[38] And although this presumption is rebuttable, the party advancing the thesis of an infringement of the law by a sovereign act of public authorities is, as a rule, obliged to demonstrate that the given action went beyond the framework provided by law,[39] which, in view of the secret nature of the actions of the secret services, will in most cases be an impossible task.

The functionality of 'Pegasus', which allows the modification of data stored on the terminal device or even the implantation of data into the device's memory, that is to say, interference by the system operator with the content of the data stored on the terminal device, in the absence of effective judicial oversight of the course of surveillance, necessitates a change in the approach to all material originating from terminal devices, and in particular to the possibility of its use as evidence in a criminal trial. When securing a data carrier, as a general rule, a binary copy is first made, after connecting a suitable write blocker to prevent overwriting and modification of the secured data, from which a checksum is calculated in order to ensure that the data analysed by the expert is the same as the data on the secured carrier and that no change in the data occurs as a result of the analysis undertaken. However, such action is irrelevant if the data on the device is changed before the copy is made. A situation in which software is installed on the device (the 'Pegasus' agent), giving its user the ability to modify the data stored there before the device is officially secured for the purposes of the investigation, affects the assessment of the reliability of the material contained therein.[40] The ability to edit data stored on the device, initiate calls, exchange messages or send messages, or use the phone owner's social media accounts results in data from the mobile device appearing to have limited procedural usefulness. Even if one considers that this does not yet disqualify such evidence, it certainly undermines the conclusion that until now has generally been taken for granted, namely that the information secured from the terminal device was created by its user or by the persons with whom he or she exchanged it. Now, whenever this data is challenged, there must be justified doubt as to by whom the secured material was introduced into the terminal device.[41] It is

---

[38] See resolution of a panel of seven judges of the Supreme Court of 9 October 2007, III CZP 46/07, or judgment of the Supreme Court of 20 May 2011, IV CSK 563/10, in relation to administrative decisions; decision of the Supreme Court of 11 April 2014, I CSK 324/13, in relation to court records; judgment of the Supreme Administrative Court of 10 October 2013, I OSK 1573/13, in relation to the validity of court decisions; or judgment of the Supreme Court of 8 January 2014, IV KK 183/13, and judgment of the NSA of 13 September 2013, II FSK 2644/11, in relation to the independent refusal of public authorities to apply the applicable law.

[39] M. Zubik, W. Sokolewicz, in: Garlicki L. (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Vol. I, Warszawa, 2016, Article 7.

[40] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność*…, op. cit., p. 46.

[41] Cf. D. Drajewicz, 'Dowodowe wykorzystanie wyników kontroli operacyjnej w postępowaniu karnym', *Prokuratura i Prawo*, 2010, No. 7–8, p. 177, and the footnotes cited therein.

difficult to imagine that this will not affect trial practice, which has often accepted information from the memory of smartphones and similar devices as the primary source of information about the circumstances of an incident. Meanwhile, in the current situation, such material can only remain the basis for the conclusion that specific content found its way onto the terminal device, while the assumption that it was introduced by the user of that device requires the authorities to carry out separate procedural findings that categorically exclude the possibility that this occurred through third parties.

Pursuant to Article 2 § 2 CCP, the basis for all decisions in a criminal trial should be true factual findings. In view of the directive contained in Article 5 § 2 CCP, making material from terminal devices the basis for findings unfavourable to the accused therefore requires an examination of whether there has been any external interference with the data contained therein. This means that, in order not to violate the criteria of a fair trial, in the event of any objections to the authorship of the secured data, the trial authorities are faced with the necessity, at the very least, of admitting evidence in the form of an expert opinion from an IT specialist in any proceedings in which a conviction would be based on material from the terminal device. Regardless of the expert findings, however, it must be borne in mind that the 2019 version of the 'Pegasus' software left very few traces of infection. It may be assumed, with confidence bordering on certainty, that it has undergone further development since then and that the instruments used to examine the terminal device may fail to detect its latest versions.[42] This circumstance provides a weighty argument for the need for trial authorities to exercise great caution as to the reliability of data from terminal devices, up to and including deprecating it as a source of trial findings, because of the real risk of arbitrariness and abuse.

In summary, advances in covert information-acquisition methods, exemplified by the titular 'Pegasus', have given rise to legitimate concerns about the reliability of evidence obtained from devices vulnerable to attacks carried out by such systems. State authorities have thus, on the one hand, gained very effective surveillance tools that allow for the effective identification of criminal environments and the targeting of preventive actions and possible trial activities, but, on the other hand, as a consequence of technological development in a manner that gives the system operator the possibility of interfering with the content of the data stored on the device, reservations have arisen concerning the trial use of data from terminal devices. This does not reflect negatively on the spyware itself, but rather on its use contrary to the purpose intended by its creators. Indeed, the system was developed as a tool for active intelligence work and was intended for the operational collection of information, regardless of the aspect of its subsequent evidential use.[43]

In the absence of a legal framework ensuring full judicial supervision over the course of operational control, a situation in which there is no possibility of determining unequivocally who – that is to say, whether it was the subject of surveillance or the

---

[42] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność*…, op. cit., p. 45.

[43] *Pełny zapis przebiegu posiedzenia Komisji Śledczej*…, op. cit., p. 46.

operator of the spying system – placed, modified or removed specific content from the device, must lead to the conclusion that the use of such material as a source of findings unfavourable to the accused would mean that the criminal trial, assessed as a whole, could not be considered fair in the light of Article 45 of the Constitution of the Republic of Poland and Article 6(1) of the ECHR.[44] *De lege ferenda*, it should be postulated that solutions in the area of operational and exploratory activities should take into account national and European safeguard standards and ensure effective, ongoing judicial supervision over the course of their implementation by state services, along with a mechanism for eliminating unlawfully collected data.

BIBLIOGRAPHY

Barczak-Oplustil A., Małecki M., Tarapata S., Behan A., Zontek W., *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych* (casus *Pegasusa)*, 15 February 2022; https://kipk.pl/wp-content/uploads/2022/02/ekspertyza-pegasus.pdf (accessed: 13 April 2026).

CyberDefence24, 'Rządowa inwigilacja to nie tylko Pegasus. Spyware Hermit atakuje na Androidzie', 17 June 2022; https://cyberdefence24.pl/cyberbezpieczenstwo/rzadowa-inwigilacja-to-nie-tylko-pegasus-spyware-hermit-atakuje-na-androidzie (accessed: 25 June 2024).

Czarnecki P., 'Czynności operacyjno-rozpoznawcze a postępowanie karne', *Palestra*, 2014, No. 7–8; https://palestra.pl/pl/czasopismo/wydanie/7-8-2014/artykul/czynnosci-operacyjno-rozpoznawcze-a-postepowanie-karne (accessed: 22 February 2025).

Drajewicz D., 'Dowodowe wykorzystanie wyników kontroli operacyjnej w postępowaniu karnym', *Prokuratura i Prawo*, 2010, No. 7–8.

Fraser M., 'Nie skończyć jak NSO Group. Tak producenci spyware zabiegają o przychylność USA', *CyberDefence24*, 2 June 2023; https://cyberdefence24.pl/biznes-i-finanse/nie-skonczyc-jak-nso-group-tak-producenci-spyware-zabiegaja-o-przychylnosc-usa (accessed: 13 April 2026).

Garlicki L. (ed.), *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom I*, Warszawa, 2016.

Hoc S., Szustakiewicz P., *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, Warszawa, 2023.

Kowalewski M., 'Sąd Najwyższy zgadzał się na stosowanie Pegasusa', *Salon24*, 24 April 2024; https://www.salon24.pl/newsroom/1374074,sad-najwyzszy-zgadzal-sie-na-stosowanie-pegasusa (accessed: 13 April 2026).

Łodziana T., 'Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika', *Palestra*, 2022, No. 9; https://palestra.pl/pl/czasopismo/wydanie/9-2022/artykul/kontrola-operacyjna-oraz-uzycie-systemu-pegasus-w-polsce-polemika (accessed: 25 April 2024).

Matusiak-Frącczak M., 'Kontrola operacyjna oraz użycie systemu Pegasus w Polsce', *Palestra*, 2022, No. 7–8.

Matusiak-Frącczak M., 'Konwencyjne standardy legalnej inwigilacji a zastosowanie systemu Pegasus w Polsce', *Europejski Przegląd Sądowy*, 2023, No. 12.

Mąka J., 'Kontrola operacyjna i podsłuch – ocena na tle praktycznego stosowania', *Przegląd Bezpieczeństwa Wewnętrznego*, 2011, No. 4.

[44] M. Matusiak-Frącczak, 'Kontrola operacyjna oraz użycie systemu Pegasus w Polsce', *Palestra*, 2022, No. 7–8, pp. 19–20.

Ojczyk J., 'Służby podsłuchują nas bez kontroli, bo pozwala na to prawo. Potwierdził to europejski trybunał', *Business Insider*, 28 May 2024; https://businessinsider.com.pl/prawo/europejski-trybunal-praw-czlowieka-wyda-wyrok-w-sprawie-inwigilacji-w-polsce/3b3e4kh (accessed: 13 April 2026).

Opitek P., 'Kontrola operacyjna urządzenia końcowego', *Prokuratura i Prawo*, 2023, No. 4.

Opitek P., 'Poważnie kontrolować można nie tylko terrorystów', *Rzeczpospolita*, 20 January 2022; https://www.rp.pl/opinie-prawne/art19306701-pawel-opitek-powaznie-kontrolowac-mozna-nie-tylko-terrorystow (accessed: 13 April 2026).

Rojek-Socha P., 'Kontrola operacyjna – sądy weryfikują to co służby chcą?', *Prawo.pl*, 19 July 2018; https://www.prawo.pl/prawnicy-sady/jak-sady-weryfikuja-wnioski-o-kontrole-operacyjna,263148.html (accessed: 13 April 2026).

Rynkun-Werner R., 'Kontrola operacyjna bez kontroli – kilka refleksji na kanwie postanowienia Trybunału Konstytucyjnego z 28.06.2022 r. (SK 60/21)', *Palestra*, 2023, No. 4; https://palestra.pl/pl/czasopismo/wydanie/4-2023/artykul/kontrola-operacyjna-bez-kontroli-kilka-refleksji-na-kanwie-postanowienia-trybunalu-konstytucyjnego-z-28.06.2022-r.-sk-60-21 (accessed: 22 February 2025).

Skowron R., 'Kontrola operacyjna a ochrona praw jednostki', *Studenckie Konferencje Naukowe*, 2014, No. 4.

Taracha A., *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin, 2006.

Cite as:

Kościelniak-Marszał M. (2026), *Pegasus Software and Fair Criminal Proceedings*, Ius Novum (Vol. 20) 2, 42–53. DOI 10.2478/in-2026-0016