Ius Novum
2026, vol. 20, nr 2, s. 41–52

OPROGRAMOWANIE „PEGASUS" A RZETELNY PROCES KARNY

MIŁOSZ KOŚCIELNIAK-MARSZAŁ*

DOI: 10.26399/iusnovum.v20.2.2026.16/m.koscielniak-marszal

Streszczenie
Opracowanie omawia funkcjonalności programów stworzonych w celu zapewnienia służbom specjalnym możliwości przejęcia kontroli nad urządzeniami mobilnymi. Przybliżając przypadki wykorzystania takich systemów w celach politycznych i przedstawiając sytuację spreparowania za ich pomocą obciążających materiałów, autor stawia tezę o konieczności zwiększenia nadzoru sądowego nad dzianiami służb specjalnych oraz zmiany podejścia organów procesu karnego do materiałów zabezpieczonych w urządzeniach końcowych. Wobec możliwości, jakie oferują programy szpiegujące, uczynienie takich materiałów podstawą niekorzystnych dla oskarżonego ustaleń może nastąpić tylko po wykluczeniu ingerencji zewnętrznej, co jest o tyle trudne, że działania służb specjalnych objęte są tajemnicą.

Celem artykułu jest zainicjowanie dyskusji na temat wykorzystania w procesie karnym materiałów pochodzących z pamięci urządzeń mobilnych oraz rozważenie, w jakim kierunku powinny podążyć zmiany prawa, aby ograniczyć związane z tym zagrożenia dla rzetelnego postępowania.

Słowa kluczowe: program szpiegujący, dowody, inwigilacja, służby specjalne

PEGASUS SOFTWARE AND FAIR CRIMINAL PROCEEDINGS

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

* dr, Uniwersytet Opolski (Polska), e-mail: kancelaria@adwokatmilosz.pl, ORCID: 0000-0002-7261-3389

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

W lipcu 2021 roku przedstawiciele organizacji Forbidden Stories z 17 mediami z różnych stron świata i wsparciem technicznym Amnesty International przeprowadzili szeroko zakrojone śledztwo dziennikarskie, które pozwoliło na ustalenie, że takie państwa jak Arabia Saudyjska, Armenia, Azerbejdżan, Bahrajn, Węgry, Indie, Kazachstan, Meksyk, Maroko, Polska, Rwanda, Togo i Zjednoczone Emiraty Arabskie (ZEA) nabyły od spółki NSO Group oprogramowanie o nazwie „Pegasus", które miało być przeznaczone do zwalczania najpoważniejszych przestępstw, zwłaszcza terroryzmu. Obiektami prowadzonej za jego pomocą inwigilacji stali się jednak obrońcy praw człowieka oraz osoby pozostające w opozycji do władz państwowych. W październiku 2018 r. zabito krytyka saudyjskiej rodziny królewskiej Jamala Khashoggiego, który w miesiącach poprzedzających śmierć był inwigilowany „Pegasusem". W Azerbejdżanie zainfekowano nim ponad tysiąc numerów telefonicznych. Wśród inwigilowanych znaleźli się m.in. dziennikarze. W Armenii „Pegasus" stosowano wobec dziennikarzy i wobec obrońców praw człowieka. Rząd węgierski wykorzystał go przeciwko dziennikarzom, politykom opozycji, prawnikom, wykładowcom akademickim, prokuratorom oraz działaczom społecznym. W Grecji szpiegowano w ten sposób około 300 osób, w tym członków Parlamentu Europejskiego i dziennikarzy. W Hiszpanii inwigilowano premiera, ministra obrony narodowej, ministra spraw wewnętrznych oraz innych wysokiej rangi urzędników, a także członków lokalnego rządu Katalonii, osoby należące do ruchu walczącego o niezależność Katalonii oraz członków Parlamentu Europejskiego, prawników, wykładowców akademickich, a także przedstawicieli społeczeństwa obywatelskiego. Maroko i Rwanda inwigilowały „Pegasusem" m.in. prezydenta Francji, premiera, ministra obrony i ministra spraw wewnętrznych Hiszpanii, premiera Belgii, poprzedniego przewodniczącego Komisji Europejskiej, a także byłego premiera Włoch[1]. Polskie służby specjalne użyły „Pegasusa" m.in. wobec senatora Krzysztofa Brejzy w okresie, gdy kierował sztabem wyborczym partii opozycyjnej w 2019 r., wobec sędzi Beaty Morawiec, która kierowała stowarzyszeniem sędziów Themis, atakującego działania resortu sprawiedliwości, a także prokurator Ewy Wrzosek, otwarcie krytykującej niedemokratyczne zmiany w polskim sądownictwie, oraz wobec sprzeciwiającego się działaniom ministra sprawiedliwości adwokata Romana Giertycha.

[1] M. Matusiak-Frącczak, *Konwencyjne standardy legalnej inwigilacji a zastosowanie systemu Pegasus w Polsce*, „Europejski Przegląd Sądowy" 2023, nr 12, s. 26–28.

Cel i sposób wykorzystywania wspomnianego oprogramowania stały się przedmiotem kampanii wyborczej do Sejmu i Senatu RP w 2023 r. Sprzyjał temu dodatkowo raport, opracowany przez powołaną przez Parlament Europejski komisję śledczą ds. „Pegasusa", przyjęty zaleceniem z 15 czerwca 2023 r. Podkreślono w nim, że prowadzona za pomocą tego narzędzia inwigilacja nie spełnia wymogów nakreślonych w orzecznictwie ETPC i TSUE, w związku z czym pozostaje sprzeczna z zasadami zawartymi w art. 2 Traktatu o Unii Europejskiej 22 oraz prawami podstawowymi zawartymi w art. 7 (prawo do poszanowania prywatności), art. 8 (ochrona danych osobowych), art. 11 (prawo do swobody wypowiedzi), art. 17 (prawo własności), art. 21 (zasada niedyskryminacji) i art. 47 (prawo do skutecznego środka kontroli sądowej) Karty praw podstawowych Unii Europejskiej[2].

Po przejęciu władzy przez dotychczasową opozycję, Sejm RP powołał Komisję śledczą do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych 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. Prace tego gremium ujawniły opinii publicznej wiele informacji na temat funkcjonowania służb specjalnych, do których dostęp był ograniczony w związku z treścią z art. 24 ust. 1 ustawy o CBA, art. 20a ust. 1 ustawy o Policji, art. 35 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego, art. 9c ust. 1 ustawy o Straży Granicznej, art. 131 ust. 1 ustawy o Krajowej Administracji Skarbowej, art. 40 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. Ukształtowane na tym tle orzecznictwo konsekwentnie stało bowiem na stanowisku, że wszystkie informacje, których ujawnienie utrudniłoby wykonywanie służbom ich zadań, w tym wykonywanie czynności operacyjno-rozpoznawczych bez względu na to, czy dotyczą one konkretnych postępowań, podlegają ochronie zasadom ochrony informacji niejawnych[3]. Poznanie charakterystyki narzędzi pracy operacyjnej groziłoby ujawnieniem techniki stosowanej do realizacji czynności i w konsekwencji brakiem faktycznych możliwości realizacji przez nie ustawowych zadań, a co za tym idzie – demontażem tej służby[4]. Niewiedza po stronie osób łamiących prawo ma w tym wypadku charakter prewencyjny, utrudniając działania przestępcze, i w interesie Rzeczypospolitej Polskiej pozostaje, aby uprawnienie jednostki do dostępu do informacji publicznej podlegało w tym zakresie ograniczeniu[5].

Na temat samego „Pegasusa" znany był co prawda, raport, który przedstawiła spółka NSO Group, jednak pochodził on z 2016 r.[6] Informację o możliwościach

---

[2] Ibidem, s. 28.

[3] Wyrok Naczelnego Sądu Administracyjnego z dnia 2 lutego 2018 r., I OSK 668/16, LEX nr 2475548; zob. S. Hoc, P. Szustakiewicz, *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, LEX/el. 2023, Komentarz do art. 24.

[4] P. Opitek, *Kontrola operacyjna urządzenia końcowego*, „Prokuratura i Prawo" 2023, nr 4, s. 60–61.

[5] Wyrok Naczelnego Sądu Administracyjnego z dnia 18 sierpnia 2015 r. I OSK 1679/14, Legalis nr 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 *Pega-*

dalszych wersji tego oprogramowania dostarczyło opinii publicznej dopiero posiedzenie wspomnianej wyżej komisji sejmowej. Świadek Jerzy Kosińskiego, który w 2019 z ramienia polskich władz uczestniczył w prezentacji, zeznał na nim, że system „Pegasus" okazał się narzędziem informatycznym o złożonej funkcjonalności, które pozwalało na przejęcie kontroli nad urządzeniem mobilnym w sposób niesygnalizujący właścicielowi, że kontrola została przez niego utracona[7]. Podczas prezentacji uczestnicy uzyskali możliwość nawiązywania połączeń za pośrednictwem przejętych urządzeń, rozmawiania przez nie, wykonali także próby dotyczące włączania mikrofonu i nasłuchiwania otoczenia, a także mieli bezpośredni dostęp do kamer, które w każdym momencie mogli uruchomić i robić za ich pomocą zdjęcia. Ponieważ telefon przejmowany był kompletnie, więc można było korzystać ze wszystkich jego funkcjonalności i z użyciem narzędzi, które zostały w nim zainstalowane, podszywać się pod jego właściciela, np. w jego imieniu funkcjonować na portalach społecznościowych, na komunikatorach, w systemach bankowości itd.[8] Operator systemu miał ponadto możliwość modyfikowania treści zapisanych w pamięci urządzenia, np. zmieniając treść znajdujących się tam wiadomości tekstowych[9]. Charakterystyczną cechę „Pegasusa" stanowiła trudna wykrywalność, gdyż w odróżnieniu od innych tego typu systemów, ten nie zapisywał się trwale w nośniku, lecz instalował się w pamięci operacyjnej[10]. Jego użycie pozostawiało zatem bardzo mało śladów zainfekowania[11], tak że nawet ekspert miałby trudności z rozróżnieniem, które znajdujące się w nim dane zostały wprowadzone przez operatora systemu, a które z nich pochodziły od właściwego użytkownika tego urządzenia[12].

Powyższe informacje potęgują zastrzeżenia wobec niejawnej inwigilacji, która i tak od dawna budziła kontrowersje[13]. Czynności tego typu w sposób niezwykle silny ingerują bowiem w podstawowe prawa człowieka, takie jak prawo do poszanowania życia prywatnego gwarantowane w przepisach konstytucyjnych (art. 49 Konstytucji RP), jak też międzynarodowych (art. 8 EKPC czy art. 17 MPPOiP). W toku prowadzenia niejawnej inwigilacji niejednokrotnie z jednej strony dochodzi do naruszenia takich konstytucyjnych dóbr prawnych, jak: życie rodzinne, własność, tajemnica korespondencji czy szerzej tajemnica komunikowania się, nienaruszalność

---

susa), „Krakowska Fundacja Prawa Karnego" 2022, s. 7–9, https://kipk.pl/wp-content/uploads/2022/02/ekspertyzapegasus.pdf (dostęp: 10.05.2024).

[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, s. 7, https://orka.sejm.gov.pl/zapisy10.nsf/0/F2D9E8013C0D37E5C1258AEE002C1F7F/%24File/0002610.pdf (dostęp: 26.04.2024).

[8] Ibidem, s. 50.

[9] Ibidem, s. 13.

[10] Ibidem, s. 12.

[11] Ibidem, s. 49–50.

[12] Ibidem, s. 35.

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

mieszkania, autonomia informacyjna bądź nietykalność cielesna. Są to więc narzędzia uważane za bardzo „agresywne"[14].

Z drugiej jednak – bez ich użycia skuteczność organów ścigania czy też organów powołanych do ochrony prawa byłaby zdecydowanie mniejsza. Występuje więc konflikt między potrzebą zapewnienia wielu wolności i praw człowieka a koniecznością naruszania niektórych z nich w określonym zakresie, w celu efektywnego ścigania przestępstw, ochrony bezpieczeństwa powszechnego czy też zapewnienia porządku prawnego[15]. Trudno jednak sobie wyobrazić, aby którekolwiek państwo zrezygnowało z narzędzi pozwalających na elektroniczną inwigilację, gdyż tego rodzaju instrumenty stanowią odpowiedź na kierunek, w jakim rozwija się współczesna przestępczość, zwłaszcza terrorystyczna oraz związana z funkcjonowaniem zorganizowanych grup przestępczych i korupcją[16]. Europejski Trybunał Praw Człowieka w wyroku z 25 maja 2021 r. uznał, że stosowanie przez szwedzkie służby systemu nasłuchu elektromagnetycznego, czyli przechwytywania i analizy treści komunikacji prowadzonej przez miliony obywateli, pozostaje zgodne z prawem. Podobne rozwiązania przewidywał brytyjski Investigatory Powers Act. We Francji służby państwowe przejęły komunikator EncroChat i masowo przechwytywały wiadomości z dziesiątek tysięcy telefonów. Z kolei w Niemczech przepisy przyznają służbom prawo wykorzystania oprogramowania do przełamywania zabezpieczeń telefonów i komputerów oraz do odczytywania zawartości urządzeń użytkowanych przez osoby, którym oficjalnie nie postawiono zarzutów, a są dopiero podejrzewane o popełnienie przestępstwa. Narzędzia takie nazywane są „Staatstrojanern", czyli „trojanami państwowymi", i stosowane do szerszej grupy przestępstw aniżeli tylko terrorystyczne[17].

Możliwości, jakie oferują swoim użytkownikom współczesne systemy szpiegowskie, powodują konieczność rewizji dotychczasowych poglądów. W aktualnej sytuacji chodzi już bowiem nie tyle o opór natury etycznej związany z podstępnym charakterem inwigilacji[18], ile o realne niebezpieczeństwo preparowania materiałów, wykorzystywanych następnie przez organy, które korzystają z ochrony wynikającej z konstytucyjnego domniemania legalności ich działań. Sztandarowym przykładem jest tu przypadek senatora Brejzy, który był inwigilowany „Pegasusem" aż 33 razy, a na jego telefon został wgrany około 1 gigabajt danych, czyli zmieniono zawartość jego telefonu przez dodanie nowych treści[19].

W tym miejscu należy podkreślić, że określenie „Pegasus" stanowi nazwę własną konkretnego systemu. Nie jest jedyny program tego typu. Polska Prokuratura

---

[14] Postanowienie Sądu Najwyższego z 26.04.2007 r. I KZP 6/07, OSNKW 2007/5/37.

[15] Zob. P. Czarnecki, *Czynności operacyjno-rozpoznawcze a postępowanie karne*, „Palestra" 2014, nr 7–8, https://palestra.pl/pl/czasopismo/wydanie/7-8-2014/artykul/czynnosci-operacyjno-rozpoznawcze-a-postepowanie-karne (dostęp: 22.02.2025).

[16] T. Łodziana, *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika*, „Palestra" 2022, nr 9, s. 63, https://palestra.pl/pl/czasopismo/wydanie/9-2022/artykul/kontrola-operacyjna-oraz-uzycie-systemu-pegasus-w-polsce-polemika (dostęp: 25.04.2024).

[17] P. Opitek, *Poważnie kontrolować można nie tylko terrorystów*, „Rzeczpospolita" 2022, 20.01, https://www.rp.pl/opinie-prawne/art19306701-pawel-opitek-powaznie-kontrolowac-mozna-nie-tylko-terrorystow (dostęp: 25.04.2024).

[18] R. Skowron, *Kontrola operacyjna a ochrona praw jednostki*, „Studenckie Konferencje Naukowe" 2014, nr 4, s. 136.

[19] M. Matusiak-Frącczak, *Konwencyjne standardy...*, op. cit., s. 28.

Krajowa równolegle dysponowała oprogramowaniem o nazwie „Hermes" – oficjalnie miało ono służyć do zaawansowanego zbierania i analizy danych ze źródeł internetowych, ale jego wszystkie funkcjonalności nie zostały dotąd zbadane[20]. Wiele państw wdrożyło różne podobne metody pracy operacyjnej. Wyspecjalizowany system szpiegujący dla Interpolu oferowała firma niemiecka[21]. Amerykańska agencja ds. leków korzysta m.in. z opracowanego przez firmę Paragon systemu „Graphite", który potrafi przełamywać zabezpieczenia współczesnych smartfonów i omijać szyfrowanie w komunikatorach takich jak WhatsApp czy Signal, wyciągając również dane z chmury[22]. Włoskie służby specjalne w 2019 r. wykorzystywały z kolei oprogramowanie szpiegowskie (spyware) „Hermit"[23]. Ponieważ to właśnie tytułowy „Pegasus", z uwagi na nieznane wcześniej funkcjonalności, stał się punktem zwrotnym zarówno w dyskusji na temat metod pozyskiwania przez organy państwa informacji, jak i procesowego wykorzystywania materiałów pochodzących z mobilnych urządzeń telekomunikacyjnych przeznaczonych do podłączenia bezpośrednio lub pośrednio do zakończeń sieci[24], w dalszej części to określenie będzie wykorzystywane jako egzemplifikacja systemu szpiegującego, dającego możliwość trudno wykrywalnej ingerencji w dane zapisane w urządzeniu końcowym.

Znamienne, że w Polsce tajna inwigilacja jest stosowana na bardzo dużą skalę i wykazuje trend rosnący. O ile w 2011 r. sądy wyraziły zgodę na kontrolę i utrwalanie rozmów lub kontrolę operacyjną w 4863 przypadkach[25], o tyle w roku 2022 liczba takich zgód wyniosła aż 9781. Nie wiadomo przy tym, ile ogółem programów, które pozwalają na kontrolę urządzeń końcowych, posiadają polskie służby. Jednak w latach 2017–2022 trzy z nich wykorzystały „Pegasusa" do kontroli operacyjnej urządzeń końcowych wobec 578 osób. W roku 2017 dotyczyło to 6 osób, w 2018 roku – 100 osób, w 2019 roku – 140 osób, w 2020 roku – 161 osób, w 2021 roku – 162 osób, a w 2022 roku – 9 osób[26]. Warto przy tym zaznaczyć, że w 2017 r. służby wystąpiły ponad 9800 razy o zgodę na kontrolę operacyjną, a sądy odmówiły im tylko w dziewięciu przypadkach[27]. Najwyższa Izba Kontroli, po zbadaniu okresu od 1 stycznia 2017 r. do 31 marca 2023 r., postawiła wniosek, że obowiązujący w Polsce system nadzoru, koordynacji oraz kontroli działalności służb specjalnych jest nieskuteczny

---

[20] https://www.gov.pl/web/pr-rzeszow/komunikat-z-dnia-21-czerwca-2024r (dostęp: 25.06.2024).

[21] Pełny zapis przebiegu posiedzenia Komisji Śledczej…, op. cit., s. 14.

[22] M. Fraser, *Nie skończyć jak NSO Group. Tak producenci spyware zabiegają o przychylność USA*, https://cyberdefence24.pl/biznes-i-finanse/nie-skonczyc-jak-nso-group-tak-producenci-spyware-zabiegaja-o-przychylnosc-usa (dostęp: 6.12.2024).

[23] *Rządowa inwigilacja to nie tylko Pegasus. Spyware Hermit atakuje na Androidzie*, https://cyberdefence24.pl/cyberbezpieczenstwo/rzadowa-inwigilacja-to-nie-tylko-pegasus-spyware-hermit-atakuje-na-androidzie (dostęp: 6.12.2024).

[24] Zob. art. 2 pkt 43 Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. z 2024 r., nr 34.

[25] Źródło: oficjalna strona Prokuratury Generalnej, www.pg.gov.pl (dostęp: 7.09.2012).

[26] M. Kowalewski, *Sąd Najwyższy zgadzał się na stosowanie Pegasusa*, Salon24.pl, https://www.salon24.pl/newsroom/1374074,sad-najwyzszy-zgadzal-sie-na-stosowanie-pegasusa (dostęp: 4.06.2024).

[27] P. Rojek-Socha, *Kontrola operacyjna – sądy weryfikują to co służby chcą?*, https://www.prawo.pl/prawnicy-sady/jak-sady-weryfikuja-wnioski-o-kontrole-operacyjna,263148.html (dostęp: 22.02.2025).

i nie odpowiada standardom obowiązującym w demokratycznych państwach prawa, a w szczególności nie zapewnia efektywnego nadzoru nad realizacją zadań służb oraz nie gwarantuje, że w toku ich wykonywania będą przestrzegane obowiązujące przepisy prawa oraz respektowane prawa i wolności obywatelskie[28].

Zastrzeżenia wobec stosowania oprogramowania szpiegującego w celu zdobywaniu materiałów dowodowych przeznaczonych do wykorzystania w postępowaniu karnym w znacznej mierze wiążą się właśnie z problemem niedostatecznej kontroli sądowej nad niejawną inwigilacją realizowaną przez służb specjalne. O ile bowiem w 2013 r. polskie rozwiązania w tym zakresie uważano za bardzo restrykcyjne na tle innych krajów Europy[29], o tyle w kolejnych latach standardy gwarancyjne, a w ślad za tym wymagania w stosunku do tego rodzaju działań, znacząco wzrosły. W wyroku z 4 maja 2000 r. Europejski Trybunał Praw Człowieka podkreślił, że systemy niejawnej inwigilacji muszą zawierać gwarancje prawne (proceduralne) stosowane do kontroli działań właściwych służb. Zdaniem Trybunału procedury kontrolne muszą odpowiadać wartościom demokratycznego społeczeństwa tak wiernie, jak to możliwe, a w szczególności zasadzie rządów prawa. Ta z kolei zakłada, że ingerencja ze strony organów władzy wykonawczej w prawa jednostki powinna być przedmiotem skutecznej kontroli[30]. W sprawach Pietrzak oraz Bychawska-Siniarska i inni *v.* Polska Europejski Trybunał Praw Człowieka zwrócił uwagę na brak wystarczających gwarancji prawnych ochrony przed arbitralnością i nadużyciami w sferze kontroli operacyjnej, przechowywania danych i dostępu do danych komunikacyjnych[31]. Każde państwo, a zatem jego organy, muszą bowiem działać na podstawie i w granicach prawa, w tym nie mogą podejmować działań arbitralnych. Wszelka ingerencja państwa, a zatem także elektroniczna, w gwarancje dla praw jednostki musi odbywać się na zasadzie proporcjonalności[32].

Również polski Trybunał Konstytucyjny stanął na stanowisku, że ustawodawca w świetle art. 2 Konstytucji ma konstytucyjny obowiązek określić przesłanki ingerencji w sferę prywatności w sposób możliwie precyzyjny, tak aby ograniczyć zakres swobody decyzyjnej pozostawionej organom stosującym prawo, a jednocześnie ma obowiązek stworzyć odpowiednie mechanizmy kontroli nad aktami organów władzy publicznej dotykającymi tej sfery. Jeśli chodzi o ograniczenie konstytucyjnych wolności i praw człowieka i obywatela, przepisy muszą charakteryzować się należytą precyzją i jasnością. Nakaz ten jest funkcjonalnie związany z zasadami pewności i bezpieczeństwa prawnego oraz ochrony zaufania do państwa i prawa[33].

---

[28] J. Ojczyk, *Służby podsłuchują nas bez kontroli, bo pozwala na to prawo. Potwierdził to europejski trybunał*, „Business Insider" 2024, 28.05, https://businessinsider.com.pl/prawo/europejski-trybunal-praw-czlowieka-wyda-wyrok-w-sprawie-inwigilacji-w-polsce/3b3e4kh (dostęp: 4.06.2024).

[29] J. Mąka, *Kontrola operacyjna i podsłuch – ocena na tle praktycznego stosowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, s. 58.

[30] Rotaru przeciwko Rumunii, sprawa nr 28341/95.

[31] Wyrok z 28 maja 2024 r., Izba (Sekcja I), skargi nr 72038/17 i 25237/18.

[32] Zob. wyrok ETPCz z 7.02.2017 r. w sprawie Irfan Guzel v. Turcja, skarga nr 35285/08, § 86; wyrok ETPCz z 12.01.2016 r. Szabo i Vissy v. Węgry, skarga nr 37138/14, § 7072; wyrok ETPCz z 4.12.2015 r. w sprawie Zakharov v. Rosja, skarga nr 47143/06, § 260.

[33] Wyrok TK z dnia 20 czerwca 2005 r., K 4/04, OTK-A 2005/6/64.

W innym judykacie Trybunał stwierdził, iż istotnym kryterium oceny dopuszczalności wyposażenia organu władzy publicznej w uprawnienie do przeprowadzania czynności operacyjno-kontrolnych jest ocena funkcjonalności określonych czynności w perspektywie realizowanych przez dany organ zadań oraz brak możliwości efektywnego wykonania tych zadań bez posiadania konkretnych uprawnień z zakresu czynności operacyjno-kontrolnych. W obu tych przypadkach obowiązek wykazania owej celowości i konieczności spoczywa na ustawodawcy[34]. Natomiast w uzasadnieniu wyroku z dnia 20 kwietnia 2004 r. Trybunał zaznaczył, że w świetle Konstytucji, służby odpowiedzialne za bezpieczeństwo i porządek publiczny nie mogą być uznane za dysponujące autonomią w zakresie czynności operacyjnych. Nie można więc, w powołaniu na wymóg skuteczności działalności operacyjnej, wyłączać jej spod jakiejkolwiek kontroli. Dlatego działalność ta nie jest wyłączona spod ograniczeń, jakie Konstytucja nakłada na wszystkie władze, wkraczające w dziedzinę podstawowych praw i wolności jednostki, zwłaszcza że podejmując czynności operacyjno-rozpoznawcze, organy policji wkraczają w sposób tajny w sferę praw i wolności obywatelskich, czego wymaga cel tych czynności. Tego rodzaju specyfika wspomnianych czynności wymaga poddania ich przemyślanemu systemowi kontroli: efektywnej i niefasadowej, i należy stosować określone działania tylko w zakresie koniecznym dla realizacji konstytucyjnych celów oraz w sposób charakteryzujący się jak najmniejszym stopniem dolegliwości dla obywateli i z zastosowaniem określonych procedur. W przeciwnym razie demokratyczne państwo prawne stałoby się w rzeczywistości państwem policyjnym[35]. W zgodzie z tym zapatrywaniem, Sąd Apelacyjny we Wrocławiu w wyroku z dnia 11 maja 2023 r. wyraził pogląd, że brak możliwości zweryfikowania przez sąd rozstrzygający o odpowiedzialności karnej oskarżonego, prawidłowości zarządzenia kontroli operacyjnej, powoduje, że zdobyty w jej wyniku materiał dowodowy musi być oceniany przez pryzmat normy wyrażonej w art. 5 § 2 k.p.k. Zaakceptowanie innego stanowiska oznaczałoby bowiem, że kontrola sądowa nad czynnościami operacyjno-rozpoznawczymi jest w istocie iluzoryczna i ma fasadowy charakter, a funkcjonariusze właściwych służb prowadzą te czynności i jednocześnie sami decydują o tym, czy są one legalne oraz czy uzyskane w ich wyniku materiały mogą być wykorzystane w procesie[36]. Co więcej, w obowiązującym stanie prawnym osoba inwigilowana nie ma wiedzy o prowadzonych przeciwko sobie czynnościach operacyjnych, poprzez brak dostępu do odpowiednich dokumentów lub zbiorów danych. O ile nie zostanie skierowany przeciwko niej akt oskarżenia, nie pozyskuje takiej wiedzy również po zakończeniu czynności operacyjnych, a tym samym poddana zostaje arbitralnemu działaniu władz, na które nie ma żadnego wpływu. Gdyby nawet powzięła taką wiedzę, to nie może zażądać skutecznego sprawdzenia legalności i rzetelności przeprowadzonych działań operacyjnych, co narusza prawo jednostki do informacji wynikające z art. 51 ust. 3 Konstytucji RP,

[34] Wyrok TK z dnia 17 czerwca 2008 r., K 8/04, OTK-A 2008/5/81.
[35] Wyrok TK z dnia 20 kwietnia 2004 r., K 45/02, OTK-A 2004/4/30.
[36] Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 11 maja 2023 r., II AKa 480/21, LEX nr 3652572.

a w konsekwencji blokuje możliwość wniesienia do sądu zażalenia, o czym mowa jest w art. 78 Konstytucji RP[37].

W świetle tych orzeczeń oraz obecnej regulacji prawnej szczególnie relewantne pozostaje, że mimo wyjątkowo daleko idących możliwości systemu „Pegasus", sąd, rozpoznając wniosek w przedmiocie zgody na prowadzenie kontroli operacyjnej, nie uzyskuje wiedzy o technicznej stronie planowanych przedsięwzięć, a więc, o ile nie przeprowadzi dodatkowych wyjaśniających, nie będzie wiedział, za pomocą jakich narzędzi służby specjalne zamierzają realizować wnioskowaną kontrolę. Po ewentualnym wyrażeniu zgody nie dysponuje też żadnymi instrumentami służącymi do bieżącego nadzoru nad przebiegiem prowadzonej kontroli, które to czynności na tym etapie pozostają w wyłącznej gestii służb specjalnych. W takim kontekście szczególnego znaczenia nabiera wynikająca z art. 7 Konstytucji RP ustrojowa zasada prawna legalizmu, nakładająca określone obowiązki zarówno na organy władzy publicznej stosujące prawo, jak i na te, które je tworzą, na podstawie odpowiednich przepisów kompetencyjnych, proceduralnych i materialnych. Rzecz jednak w tym, że art. 7 konstytucji stanowi jednocześnie podstawę domniemania prawnego, iż działania pochodzące od organów państwa cieszą się domniemaniem zgodności ich z prawem[38]. I chociaż presumpcja ta jest podważalna, to na podmiocie przedstawiającym tezę o naruszeniu prawa przez władcze działanie organów władzy publicznej ciąży, co do zasady, obowiązek wykazania, że dana czynność wykroczyła poza ramy przewidziane prawem[39], co wobec tajnego charakteru działań służb specjalnych w większości przypadków będzie zadaniem niewykonalnym.

Funkcjonalność „Pegasusa", która pozwala na modyfikację zapisanych w urządzeniu końcowym danych lub nawet implementowanie danych do pamięci urządzenia, a więc ingerowania przez operatora systemu w treść danych znajdujących się w urządzeniu końcowym, wobec braku skutecznego nadzoru sądowego nad przebiegiem inwigilacji, rodzi konieczność zmiany podejścia do wszelkich materiałów pochodzących z urządzeń końcowych, a szczególności możliwości ich wykorzystania jako dowodów w procesie karnym. W przypadku zabezpieczania nośnika danych, co do zasady, najpierw jest wykonywana – po wcześniejszym podłączeniu stosownego blokera zapisu (celem uniemożliwienia nadpisania i modyfikacji zabezpieczonych danych) – kopia binarna, z której obliczana jest suma kontrolna mająca zagwarantować, że dane poddane analizie przez biegłego będą tożsame z danymi znajdującymi się na zabezpieczonym nośniku i nie dojdzie do

---

[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, nr 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 (dostęp: 22.02.2025).

[38] Zob. uchwała składu siedmiu sędziów SN z 9 października 2007 r., III CZP 46/07 czy wyrok SN z 20 maja 2011 r., IV CSK 563/10 w odniesieniu do decyzji administracyjnych; postanowienie SN z 11 kwietnia 2014 r., I CSK 324/13 w odniesieniu do akt sądowych; wyrok NSA z 10 października 2013 r., I OSK 1573/13, w odniesieniu do prawomocności orzeczeń sądowych czy wyrok SN z 8 stycznia 2014 r., IV KK 183/13 i wyrok NSA z 13 września 2013 r., II FSK 2644/11 w odniesieniu do samodzielnej odmowy stosowania obowiązujących przepisów prawa przez organy władzy publicznej.

[39] M. Zubik, W. Sokolewicz, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom I*, red. L. Garlicki, Warszawa 2016, art. 7.

jakiejkolwiek zmiany danych na skutek wdrożonej analizy. Działanie takie nie ma jednak znaczenia w razie zmiany danych w urządzeniu przed wykonaniem kopii. Przypadek, w którym na urządzeniu instalowany jest program (agent „Pegasusa"), dający swojemu użytkownikowi uprawnienia, które pozwalają na modyfikowanie zgromadzonych tam danych przed oficjalnym zabezpieczeniem urządzenia na potrzeby postępowania, wpływa na ocenę wiarygodności znajdujących się w nim materiałów[40]. Możliwość edycji danych zapisanych w urządzeniu, inicjowanie połączeń, wymiana wiadomości wysyłki wiadomości czy korzystanie z kont właściciela aparatu w social mediach powodują, że dane pochodzące z urządzenia mobilnego okazują się mieć ograniczoną przydatność procesową. Nawet jeśli uznać, że nie dyskwalifikuje to jeszcze takich dowodów, to z całą pewnością podważa wniosek, który dotąd z reguły traktowany był jako pewnik – że zabezpieczone z urządzenia końcowego informacje zostały wytworzone przez jego użytkownika lub osoby, z którymi je wymieniał. Obecnie, w każdym przypadku zakwestionowania tych danych, musi pojawić się usprawiedliwiona wątpliwość co do tego, przez kogo został wprowadzony do urządzenia końcowego zabezpieczony materiał[41]. Trudno sobie wyobrazić, aby nie wpłynęło to na praktykę procesową, która informacje z pamięci smartfonów i podobnych urządzeń często przyjmowała jako podstawowe źródło informacji o okolicznościach zdarzenia. Tymczasem w aktualnej sytuacji takie materiały mogą pozostawać jedynie podstawą wniosku, że określona treść znalazła się w urządzeniu końcowym, natomiast przyjęcie, że została ona wprowadzona przez użytkownika tego urządzenia, wymaga przeprowadzenia przez organy odrębnych ustaleń procesowych, kategorycznie wykluczających możliwość, że stało się tak za sprawą osób trzecich.

Stosownie do art. 2 § 2 k.p.k., podstawę wszelkich rozstrzygnięć w procesie karnym powinny stanowić prawdziwe ustalenia faktyczne. Wobec dyrektywy zawartej w art. 5 § 2 k.p.k., uczynienie materiałów z urządzeń końcowych podstawą niekorzystnych dla oskarżonego ustaleń wymaga zatem zbadania, czy nie doszło do zewnętrznej ingerencji w znajdujące się w nim dane. Oznacza to, że aby nie uchybić kryteriom rzetelnego procesu, w razie pojawienia się jakichkolwiek zastrzeżeń co do autorstwa zabezpieczonych danych, organy procesowe stoją co najmniej przed koniecznością dopuszczenia dowodu z opinii biegłego informatyka w każdym postępowaniu, w którym skazanie miałoby się opierać na materiale pochodzącym z urządzenia końcowego. Niezależnie jednak od wyników ekspertyz, trzeba mieć w polu widzenia, że oprogramowanie typu „Pegasus" w wersji z 2019 r. pozostawiało bardzo mało śladów zainfekowania. Z przekonaniem graniczącym z pewnością można założyć, że od tego czasu nastąpił jego dalszy rozwój, a instrumenty służące do badania urządzenia końcowego mogą nie wykrywać jego najnowszych wersji[42]. Powyższa okoliczność stanowi ważny argument za koniecznością bardzo

---

[40] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej…*, op. cit., s. 46.

[41] Por. D. Drajewicz, *Dowodowe wykorzystanie wyników kontroli operacyjnej w postępowaniu karnym*, „Prokuratura i Prawo" 2010, nr 7–8, s. 177, i podawane tam przypisy.

[42] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej…*, op. cit., s. 45.

ostrożnego podchodzenia przez organy procesowe do wiarygodności danych pochodzących z urządzeń końcowych, aż po ich deprecjację jako źródła ustaleń procesowych włącznie, z uwagi na realne ryzyko arbitralności i nadużyć.

Podsumowując, na skutek postępu w dziedzinie metod niejawnego zdobywania informacji, którego egzemplifikację stanowi tytułowy „Pegasus", mamy uzasadnione obawy co do wiarygodności dowodów pozyskiwanych z urządzeń podatnych na ataki przeprowadzane za pomocą takich systemów. Organy państwa z jednej strony zyskały zatem bardzo efektywne narzędzia inwigilacji, pozwalające na skuteczne rozpoznanie środowisk kryminalnych oraz ukierunkowanie działań prewencyjnych i ewentualnych czynności procesowych, ale z drugiej – konsekwencją rozwoju technologii w sposób dający możliwość ingerencji operatora systemu w treść zapisanych w urządzeniu danych stały się zastrzeżenia co do procesowego wykorzystania danych pochodzących z urządzeń końcowych. Nie świadczy to negatywnie o samym oprogramowaniu szpiegowskim, lecz o jego wykorzystaniu niezgodnie z zakładanym przez twórców przeznaczeniem. System ten powstał bowiem jako narzędzie aktywnej pracy wywiadowczej i był przeznaczony do operacyjnego zbierania informacji, bez względu na aspekt ich późniejszego, dowodowego wykorzystania[43].

Wobec braku regulacji, która zapewniała pełny nadzór sądowy nad przebiegiem kontroli operacyjnej, sytuacja, gdy nie ma możliwości jednoznacznego ustalenia kto, a więc obiekt inwigilowany czy operator systemu szpiegującego, umieścił, zmodyfikował lub usunął dane treści z urządzenia, musi skutkować konkluzją, że wykorzystanie takich materiałów jako źródła niekorzystnych dla oskarżonego ustaleń powodowałoby, że proces karny, oceniany jako całość, nie daje się zostać uznany za sprawiedliwy w świetle art. 45 Konstytucji RP oraz art. 6 ust. 1 EKPC[44]. *De lege ferenda* należy więc postulować, aby rozwiązania w zakresie czynności operacyjno-rozpoznawczych uwzględniały krajowe i europejskie standardy gwarancyjne oraz zapewniały efektywny, bieżący nadzór sądowy nad przebiegiem ich realizacji przez służby państwowe, wraz mechanizmem eliminowania danych zgromadzonych niezgodnie z prawem.

BIBLIOGRAFIA

Barczak-Oplustil A., Małecki W., Tarapata S., Behan A., Zontek W., *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (*casus *Pegasusa)*, „Krakowska Fundacja Prawa Karnego" 2022.

Czarnecki P., *Czynności operacyjno-rozpoznawcze a postępowanie karne*, „Palestra" 2014, nr 7–8.

Drajewicz D., *Dowodowe wykorzystanie wyników kontroli operacyjnej w postępowaniu karnym*, „Prokuratura i Prawo" 2010, nr 7–8.

Fraser M., *Nie skończyć jak NSO Group. Tak producenci spyware zabiegają o przychylność USA*, https://cyberdefence24.pl.

---

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

[44] M. Matusiak-Frącczak, *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce*, „Palestra" 2022, nr 7–8, s. 19–20.

Hoc S., Szustakiewicz P., *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, LEX 2023.
Konstytucja Rzeczypospolitej Polskiej. Komentarz. Tom I, red. L. Garlicki, Warszawa 2016.
Kowalewski M., *Sąd Najwyższy zgadzał się na stosowanie Pegasusa*, Salon24.pl.
Łodziana T., *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika*, „Palestra" 2022, nr 9.
Matusiak-Frącczak M., *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce*, „Palestra" 2022, nr 7–8.
Matusiak-Frącczak M., *Konwencyjne standardy legalnej inwigilacji a zastosowanie systemu Pegasus w Polsce*, „Europejski Przegląd Sądowy" 2023, nr 12.
Mąka J., *Kontrola operacyjna i podsłuch – ocena na tle praktycznego stosowania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013.
Ojczyk J., *Służby podsłuchują nas bez kontroli, bo pozwala na to prawo. Potwierdził to europejski trybunał*, „Business Insider" 2024, 28.05.
Opitek P., *Kontrola operacyjna urządzenia końcowego*, „Prokuratura i Prawo" 2023, nr 4.
Opitek P., *Poważnie kontrolować można nie tylko terrorystów*, „Rzeczpospolita" 2022, 20.01.
Rojek-Socha P., *Kontrola operacyjna – sądy weryfikują to co służby chcą?*, https://www.prawo.pl.
Rynkun-Werner R., *Kontrola operacyjna bez kontroli – kilka refleksji na kanwie postanowienia Trybunału Konstytucyjnego z 28.06.2022 r. (SK 60/21)*, „Palestra" 2023, nr 4.
Skowron R., *Kontrola operacyjna a ochrona praw jednostki*, „Studenckie Konferencje Naukowe" 2014, nr 4.
Taracha A., *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin 2006.

Cytuj jako:

Kościelniak-Marszał M., *Oprogramowanie „Pegasus" a rzetelny proces karny*, „Ius Novum" 2026, nr 2(20), s. 41–52. DOI: 10.26399/iusnovum.v20.2.2026.16/m.koscielniak-marszal