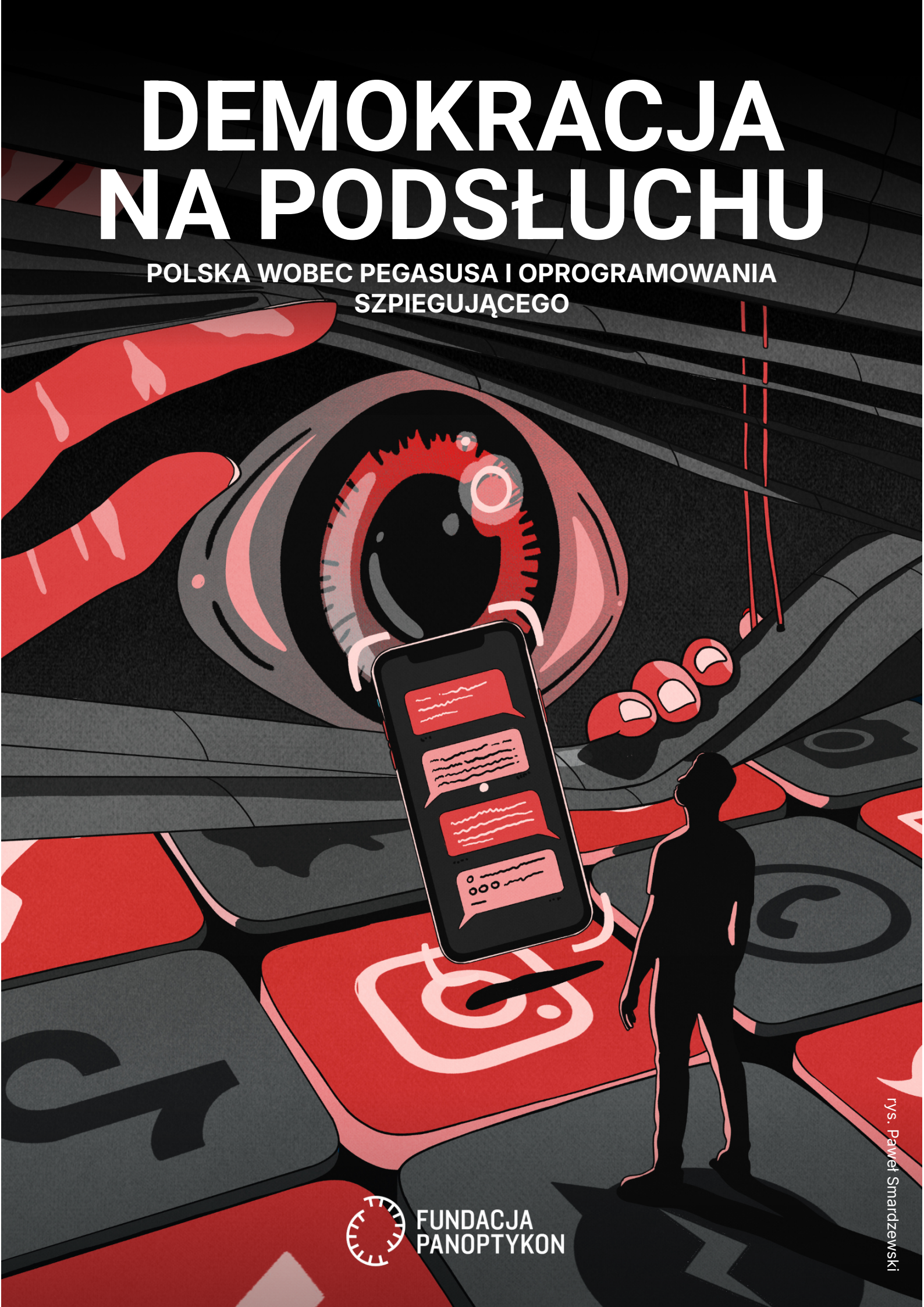
DEMOKRACJA NA PODSŁUCHU

POLSKA WOBEC PEGASUSA I OPROGRAMOWANIA SZPIEGUJĄCEGO



FUNDACJA PANOPTYKON

rys. Paweł Smardzewski

Spis treści

Wstęp

Oprogramowanie szpiegujące to jedno z najważniejszych zagrożeń dla demokracji, praw człowieka i cyberbezpieczeństwa w Unii Europejskiej i na świecie[1]. W rękach niedemokratycznych rządów jest ono jednym z kluczowych narzędzi utrzymania władzy i niszczenia przeciwników i przeciwniczek: dziennikarzy i dziennikarek, opozycjonistów i opozycjonistek czy obrońców i obrończyń praw człowieka.

Możliwości oprogramowania szpiegującego do sięgania w najskrytsze zakamarki urządzenia (w tym do danych objętych tajemnicą dziennikarską, intymnej korespondencji z najbliższymi osobami, aktywności w bankowości elektronicznej i na portalach społecznościowych) i zdalnego kontrolowania mikrofonu czy kamery przy braku jakiejkolwiek kontroli nad jego wykorzystywaniem daje podstawy, żeby uznać je za „broń atomową" odzierającą ofiary z wszelkiej prywatności.

Polskie doświadczenia nie ułatwiają chłodnego spojrzenia na ten problem. W latach 2017-2022 Pegasus był wykorzystywany przez służby do inwigilowania polityków i polityczek, dając władzy nadzwyczajną wiedzę o planach opozycji. Niekontrolowane wykorzystanie takiej technologii to zagrożenie dla praworządności i aktywności obywatelskiej, bo umożliwia podrzucanie „dowodów" – a tym samym wrabianie osób w przestępstwa, których nie popełniły czy kompromitowanie „niewygodnych" dziennikarzy czy aktywistek.

Mimo nagłośnienia nadużyć wciąż dowiadujemy się o nowych przypadkach nieuprawnionego wykorzystania oprogramowania szpiegującego. Po *spyware* sięgają zarówno rządy krajów autorytarnych, jak i demokratycznych. Same państwa często zaprzeczają stosowaniu takiego rodzaju narzędzi lub przyznają się do tego dopiero po ujawnieniu dowodów. Nie wiemy, czy po głośnej „aferze Pegasusa" polskie służby korzystają z takiego oprogramowania, ale potencjalnie jest to możliwe.

Dlaczego? Bo huczne zapowiedzi rozliczeń i zmian w prawie nie zostały zrealizowane.

Przedstawiciele służb przekonują, że potrzebują oprogramowania szpiegującego, żeby skutecznie działać. Główny argument: rosnąca popularność szyfrowanej komunikacji, do której sprawdzania nie wystarczają łatwiej dostępne metody kontrolowania ludzi, jak pozyskiwanie billingów od operatorów telekomunikacyjnych czy zatwierdzony przez sąd

[1] EDRi, *Spyware and state abuse. The case for an EU-wide ban*, https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/.

klasyczny podsłuch. Dlatego już niemal 100 państw na świecie stosuje lub samodzielnie rozwija różne typy oprogramowania szpiegującego[2].

Oprogramowanie szpiegujące jest jak broń atomowa – może rozstrzygnąć o wyniku wojny, ale przy tym narobić gigantycznych szkód. Politycy i polityczki nie mogą dłużej ignorować jego istnienia. Konieczne są ramy prawne, aby nie mogło ono być wykorzystywane w sposób niekontrolowany. Tak jak broń atomowa wymaga adekwatnych gwarancji dla ochrony ludzi, tak oprogramowanie szpiegujące wymaga ich dla praw i wolności obywatelskich.

Ten raport pokazuje, dlaczego konieczne jest zarówno dokończenie rozliczeń „afery Pegasusa", jak i niezwłoczne przyjęcie regulacji prawnych dla oprogramowania szpiegującego i systemowe zmiany w zasadach prowadzenia kontroli operacyjnej przez służby.

Słowniczek

Kontrola operacyjna – prowadzony niejawnie nadzór nad działaniami osoby podejrzewanej o popełnienie lub planowanie przestępstwa. Może obejmować podsłuchy i dostęp do treści korespondencji (SMS-y, maile), ukryte kamery, kontrolę przesyłek i uzyskiwanie dostępu do informatycznych nośników danych. Może być prowadzona przez Policję czy służby specjalne po uzyskaniu zgody prokuratora i sądu.

Oprogramowanie szpiegujące (*spyware*) – oprogramowanie, które pozwala gromadzić wiedzę o użytkowniku czy użytkowniczce zainfekowanego urządzenia i przesyła te informacje bez jego lub jej wiedzy osobom trzecim. W tym raporcie zajmujemy się oprogramowaniem szpiegującym stosowanym przez instytucje państwowe.

Służby specjalne – w Polsce istnieje 5 takich organów: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne. Obok Policji to właśnie służby specjalne prowadzą kontrolę operacyjną[3].

---

[2] Share Foundation, *A privacy nightmare: understanding spyware*, https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf.

[3] Taką możliwość mają też np. Żandarmeria Wojskowa i Straż Graniczna, ale korzystają z niej rzadziej niż Policja, ABW i CBA.

1. Oprogramowanie szpiegujące

W tym rozdziale przeanalizujemy:

- dlaczego oprogramowanie szpiegujące jest zagrożeniem dla praw i wolności,
- na czym polegała „afera Pegasusa”,
- jak obecnie państwa nadużywają oprogramowania szpiegującego.

1.1. Jak działa oprogramowanie szpiegujące

Oprogramowanie szpiegujące pozwala na podejrzenie całej zawartości zainfekowanego urządzenia. Daje wgląd do treści korespondencji prowadzonej za pośrednictwem SMS-ów i szyfrowanych komunikatorów, do listy kontaktów, maili, kalendarza, zdjęć, nagrań, portali społecznościowych, map, aplikacji z muzyką, filmami i newsami, dziennika elektronicznego, menedżera haseł i wszystkich innych rzeczy, które osoba ma na urządzeniu. Pozwala na podsłuchanie rozmów telefonicznych i prowadzonych przez komunikatory internetowe. To tzw. funkcja pasywna oprogramowania szpiegującego.

Diagram pochodzący z dokumentacji NSO Group ilustrujący zakres informacji możliwych do pozyskania z urządzenia zainfekowanego Pegasusem. Źródło: Hacking Team Emails/Citizen Lab, https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-

Niektóre wersje oprogramowania szpiegującego pozwalają też na modyfikowanie zawartości urządzenia, np. zapisywanie i kasowanie plików. To tzw. funkcja aktywna.

Podobnie jak w przypadku typowej kontroli operacyjnej (np. podsłuchu) jedno zainfekowane urządzenie oznacza wgląd w życie nie tylko osoby, do której ten sprzęt należy – ale też wszystkich ludzi, z którymi kiedykolwiek się komunikowała.

Do zainfekowania urządzenia może być potrzebne kliknięcie (jedno!) w złośliwy link przez osobę atakowaną. Ta forma ataku, określana jako *one-click attack*, została wykorzystana przeciwko greckiemu dziennikarzowi śledczemu, którego telefon został zainfekowany Predatorem po tym, jak kliknął w niewinnie wyglądający link do serwisu informacyjnego na temat finansów[4]. Podobnie zaatakowana została pracowniczka greckiego oddziału firmy Meta odpowiedzialna za politykę cyberbezpieczeństwa firmy – kliknęła w link udający potwierdzenie wizyty lekarskiej[5].

Na rynku dostępne są też programy, do których zainstalowania na urządzeniu nie jest potrzebne aktywne działanie ze strony osoby atakowanej (to tzw. *zero-click attack*). W 2020 r. w Hiszpanii doszło do skutecznego zainstalowania Pegasusa na telefonach dwóch prawniczek współpracujących z katalońską organizacją Omnium Cultural. Jedynym śladem pozostawionym na urządzeniu było nieodebrane połączenie przez komunikator WhatsApp[6]. Na rynku dostępne jest też oprogramowanie szpiegujące z funkcją samoniszczącą, które infekuje telefon, nie zostawiając po tym żadnych śladów[7].

1.2. Opozycja i aktywistki prześwietlani Pegasusem

W Polsce najsłynniejsze oprogramowanie szpiegujące Pegasus pojawiło się w 2017 r.[8]. Opinia publiczna usłyszała o nim w 2018 r. dzięki ujawnieniu przez kanadyjską organizację Citizen Lab przypadków wykorzystywania tej technologii w 45 krajach, w tym w Polsce[9]. Sprawę wykorzystania Pegasusa przez Centralne Biuro Antykorupcyjne

---

[4] Raport Komisji śledczej ds. zbadania stosowania oprogramowania Pegasusa i równoważnego oprogramowania szpiegowskiego służącego inwigilacji Parlamentu Europejskiego, pkt 202-211, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html.

[5] Tamże, pkt 232.

[6] Tamże, pkt 286 i 344.

[7] Tamże, pkt 494.

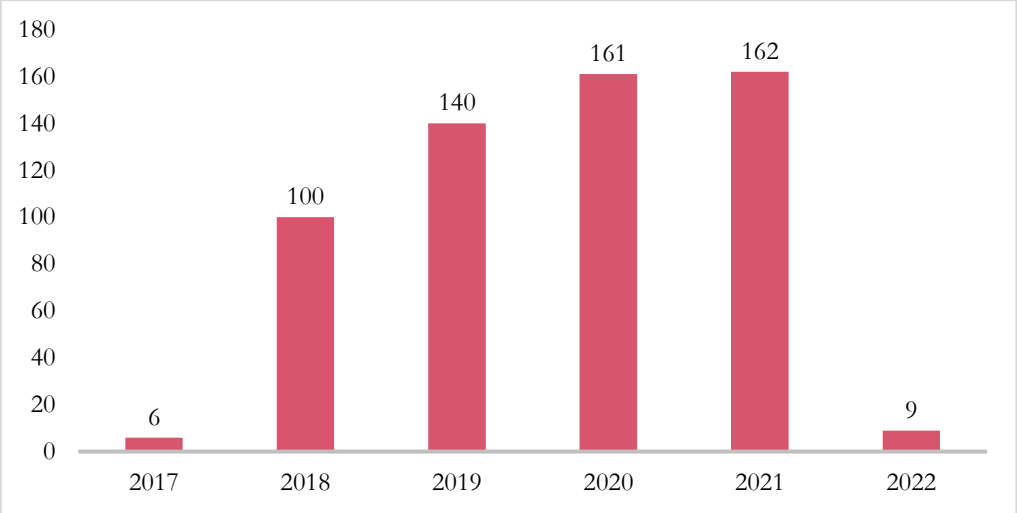
[8] Nie była to pierwsza sytuacja, w której opinia publiczna poznała dowody w sprawie stosowania podobnych narzędzi przez polskie służby. W 2015 r. na jaw wyszła informacja o tym, że Centralne Biuro Antykorupcyjne było klientem firmy Hacking Team, producenta oprogramowania szpiegującego. Faktury wystawione CBA dotyczyły systemu Remote Control System, służącego do infekowania, a następnie zdalnego i ukrytego kontrolowania urządzeń takich jakich komputery i telefony komórkowe.

[9] Citizen Lab, *HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

nagłośnili redaktor naczelny portalu Zaufana Trzecia Strona Adam Haertle oraz dziennikarz śledczy TVN24.pl Robert Zieliński.

Pegasusa stosowano m.in. wobec polityka Krzysztofa Brejzy, adwokata Romana Giertycha, prokuratorki Ewy Wrzosek, jednej z liderek Ogólnopolskiego Strajku Kobiet Klementyny Suchanow czy sędzi Beaty Morawiec.

W kwietniu 2024 r. ówczesny Minister Sprawiedliwości Prokurator Generalny Adam Bodnar poinformował, że w latach 2017-2022 trzy służby stosowały „kontrolę operacyjną urządzenia końcowego" (tj. używały oprogramowania Pegasus) łącznie wobec 578 osób[10]. Lista inwigilowanych miała obejmować „znacznie więcej osób publicznych niż dotychczas ujawniono"[11].



Wykres 1. Liczba osób inwigilowanych w Polsce za pomocą Pegasusa w latach 2017-2022.

Głównym użytkownikiem Pegasusa w Polsce było Centralne Biuro Antykorupcyjne, czyli służba powołana do ścigania przestępstw o charakterze korupcyjnym. To różni nas od innych krajów (np. Hiszpanii), gdzie wykorzystanie tej formy inwigilacji uzasadniano koniecznością zwalczania zagrożeń dla bezpieczeństwa narodowego.

Według informacji podanych przez Adama Bodnara narzędzie to znajdowało się w dyspozycji trzech służb: Centralnego Biura Antykorupcyjnego (CBA), Agencji Bezpieczeństwa Wewnętrznego (ABW) oraz Służby Kontrwywiadu Wojskowego (SKW). Wiadomo również, że Policja korzystała z Pegasusa, lecz nie robiła tego samodzielnie,

[10] Informacja o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej w 2023 r., https://orka.sejm.gov.pl/Druki10ka.nsf/0/7522A4519FE790ACC1258B01003A2A38/%24File/308.pdf.

[11] The Guardian, *Poland launches inquiry into previous government's spyware use*, https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use.

a za pośrednictwem CBA. Nie da się jednak ustalić, jaka dokładnie była częstotliwość wykorzystywania Pegasusa przez każdą ze służb.

Nie ma podstaw, aby twierdzić, że jakiekolwiek inne służby korzystały z Pegasusa.

W opublikowanym we wrześniu 2023 r. raporcie z prac Komisji Nadzwyczajnej powołanej przez Senat w styczniu 2022 r. w celu „wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych" (dalej „komisja senacka") znajdujemy szczegółowe informacje na temat ataków na osoby publiczne. Czytamy, że **inwigilacją objęto też działaczy i działaczki społeczne oraz przedsiębiorców**[12].

Przykładowo, do telefonu adw. Romana Giertycha (pełnomocnika m.in. rodziny Donalda Tuska) włamano się co najmniej 18 razy. Działacza społecznego i politycznego Michała Kołodziejczaka zaatakowano 6 razy. Przedsiębiorców Pawła Tamborskiego oraz Andrzeja Długosza inwigilowanych w związku z prywatyzacją firmy CIECH – odpowiednio 5 i 61 razy[13].

Wśród wszystkich ujawnionych przypadków inwigilacji z wykorzystaniem Pegasusa najgłośniejsza i najbardziej bulwersująca była sprawa polityka Krzysztofa Brejzy. Brejza był szefem sztabu wyborczego Koalicji Obywatelskiej, która w latach 2015-2023 działała w opozycji do rządzącego wówczas PiS-u.

> *Z telefonu „Grzechotnika" [kryptonim nadany przez CBA Krzysztofowi Brejzie] wykradzione zostały następujące dane: 80 tysięcy wiadomości od 2010 do 2019 r., pęk kluczy zawierający wszelkie hasła do ok. 90 usług i serwisów internetowych, pełny dostęp do lokalizacji telefonów, wiadomości e-mail, dokumentów przechodzących przez jego telefony, zdjęcia, nagrania wideo*[14].

W okresie kampanii wyborczej w 2019 r. do telefonu tego polityka włamywano się co najmniej 33 razy, a daty tych działań pokrywają się z kluczowymi momentami tej kampanii. Na podstawie dokumentów operacyjnych CBA komisja senacka ustaliła, że

[12] Raport Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych, https://www.senat.gov.pl/download/gfx/senat/pl/defaultaktualnosci/1924/15764/1/raport_koncowy_z_prac_komisji_nadzwyczajnej.pdf.

[13] Tamże.

[14] Tamże.

z telefonu wykradziono m.in. 80 tys. wiadomości SMS przesyłanych od 2010 r. (czyli inwigilacja objęła okres 9 lat przed atakami).

W kontekście inwigilacji Krzysztofa Brejzy Wojciech Hermeliński, były szef Państwowej Komisji Wyborczej i sędzia Trybunału Konstytucyjnego, ocenił przed komisją senacką:

> *Wybory w 2019 roku, choć nie były sfałszowane, nie były uczciwe*[15].

W przypadkach analizowanych przez komisję senacką żadnej z inwigilowanych osób nie przedstawiono aktu oskarżenia. To by oznaczało, że inwigilacja była prowadzona instrumentalnie, a jej celem nie była walka z przestępczością. Posłanka Magdalena Łośko (w czasie, gdy była inwigilowana Pegasusem: asystentka, koordynatorka i dyrektorka biura Krzysztofa Brejzy) przed komisją senacką powiedziała:

> *Nigdy nie dostałam żadnych zarzutów, te przeszukania i konfiskata sprzętu elektronicznego były po to, by skompromitować rodzinę Brejzów*[16].

W listopadzie 2025 r. w prowadzonym przez prokuraturę postępowaniu dotyczącym nadużyć z wykorzystaniem oprogramowania Pegasus status pokrzywdzonych miało 38 osób[17].

Pełne dane dotyczące rozmiarów inwigilacji nie zostały i najpewniej nigdy nie zostaną udostępnione opinii publicznej.

1.3. Jak inne państwa korzystały (i wciąż korzystają) z oprogramowania szpiegującego

1.3.1. Włochy: inwigilacja krytyków rządu

W styczniu 2025 r. WhatsApp wysłał powiadomienie do ok. 90 włoskich użytkowników i użytkowniczek aplikacji, informując, że mogli zostać zaatakowani oprogramowaniem

[15] Bankier.pl, *Hermeliński: Wybory w 2019 roku, choć nie były sfałszowane, nie były uczciwe,* https://www.bankier.pl/wiadomosc/Hermelinski-Wybory-w-2019-roku-choc-nie-byly-sfalszowane-nie-byly-uczciwe-8266533.html.

[16] Raport komisji senackiej, dz. cyt.

[17] Rzeczpospolita, *Adam Bodnar: Zbigniew Ziobro powinien trafić do aresztu. Zachodzi obawa mataczenia lub ucieczki*, https://www.rp.pl/polityka/art43290211-adam-bodnar-zbigniew-ziobro-powinien-trafic-do-aresztu-zachodzi-obawa-mataczenia-lub-ucieczki.

Graphite. Producent oprogramowania, izraelska firma Paragon, twierdziła, iż jej warunki świadczenia usług zabraniają użycia produktu w sposób nieuprawniony. Jednak w marcu 2026 r. włoska prokuratura potwierdziła, że w 2024 r. celem inwigilacji było dwoje proimigranckich aktywistów oraz dziennikarz śledczy krytykujący rząd Giorgii Meloni.

Podsłuchiwani mieli być też m.in. przyjaźniący się ze zmarłym już papieżem Franciszkiem ksiądz kapelan pracujący na statku ratowniczym należącym do organizacji ratującej osoby migranckie na Morzu Śródziemnym oraz dziennikarz portalu Fanpage.it, który ujawnił powiązania partii premier Włoch ze środowiskami neofaszystowskimi. Ciro Pellegrino zastanawiał się:

> *Dlaczego stałem się celem? Zadaję sobie to pytanie od momentu, gdy otrzymałem zawiadomienie. Zamierzam – i zamierzamy – zadać to pytanie publicznie każdemu, kto ma uprawnienia i obowiązek udzielić na nie odpowiedzi. Odpowiedź należy się… wszystkim, których interesuje, kto w tym kraju zburzył wyraźną granicę między bezpieczeństwem a inwigilacją, między legalnością a nadużyciem*[18].

Z raportu opublikowanego przez włoską komisję parlamentarną ds. bezpieczeństwa wynika, że w latach 2023-2024 włoskie służby wywiadowcze miały podpisane umowy ze wspomnianą firmą Paragon[19]. Nadal nie wiadomo, kto zlecił inwigilację.

1.3.2. Serbia: cyfrowe więzienie

Według Citizen Lab Serbska Agencja Bezpieczeństwa Informacyjnego (BIA) regularnie korzysta z różnych komercyjnych narzędzi szpiegujących, w tym FinFisher od niemieckiej firmy FinFisher GmbH (2014 r.)[20], produktów powiązanej z NSO Group firmy Circles (2020 r.)[21] i Predatora od firmy Cytrox, będącej częścią konsorcjum Intellexa

[18] The Guardian, *Second Italian journalist allegedly targeted with 'mercenary spyware'*, https://www.theguardian.com/world/2025/may/01/second-italian-journalist-allegedly-targeted-with-mercenary-spyware.

[19] Citizen Lab, *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*, https://citizenlab.ca/research/a-first-look-at-paragons-proliferating-spyware-operations/#h-3-whatsapps-paragon-investigation.

[20] Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

[21] Citizen Lab, *Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles*, https://citizenlab.ca/research/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

(2021 r.)[22]. Co najmniej od grudnia 2021 r. Serbia używa również Pegasusa, w tym do inwigilacji przedstawicieli i przedstawicielek społeczeństwa obywatelskiego krytykujących serbski rząd (2023 r.)[23].

W 2024 r. Amnesty International ujawniła stosowanie oprogramowania szpiegującego o nazwie NoviSpy. Z ustaleń eksperckich wynika, że to nowe, lokalnie rozwijane oprogramowanie było wykorzystywane przez organy państwowe wobec dziennikarzy i dziennikarek oraz aktywistek i aktywistów. Całokształt inwigilacji i represji wobec społeczeństwa obywatelskiego w Serbii Amnesty International określiła jako „cyfrowe więzienie". NoviSpy umożliwiało służbom zainfekowanie urządzenia końcowego jedynie przy bezpośrednim kontakcie. Oprogramowanie wgrywano podczas oficjalnych zatrzymań, np. w trakcie antyrządowych demonstracji, gdy urządzenia znajdowały się w rękach służb[24].

1.3.3. Grecja: pierwsze wyroki skazujące

W latach 2021-2022 w Grecji do inwigilacji telefonów ok. 90 osób wykorzystano oprogramowanie szpiegujące o nazwie Predator od grupy Intellexa[25]. To międzynarodowe konsorcjum jest jednym z głównych konkurentów NSO Group, czyli producenta Pegasusa. Działa z Grecji i – jak twierdzi sama firma – jest „podmiotem podlegającym unijnym regulacjom".

Wśród inwigilowanych znaleźli się dziennikarz finansowy, politycy i polityczki opozycji, europoseł, ministrowie, agenci i agentki służb wywiadowczych, prokuratorzy oraz była kierowniczka ds. zaufania i bezpieczeństwa w Meta. Ujawnienie sprawy doprowadziło do poważnego kryzysu politycznego oraz dymisji szefa greckiej agencji wywiadowczej i jednego z najbliższych współpracowników premiera.

W lutym 2026 r. sąd pierwszej instancji skazał cztery osoby z kierownictwa Intellexy na karę 126 lat (w więzieniu spędzą maksymalnie 8 lat, a wykonanie wyroku zostało

---

[22] Citizen Lab, *Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

[23] Access Now, *Spyware in Serbia: civil society under attack*, https://www.accessnow.org/spyware-attack-in-serbia/.

[24] Amnesty International, *Serbia: "A Digital Prison": Surveillance and the suppression of civil society in Serbia*, https://www.amnesty.org/en/documents/eur70/8813/2024/en/.

[25] International Consortium of Investigative Journalists, *Greek court convicts Intellexa founder Tal Dilian, three others in wiretapping scandal*, https://www.icij.org/investigations/cyprus-confidential/greek-court-convicts-intellexa-founder-tal-dilian-three-others-in-wiretapping-scandal/ oraz Citizen Lab, *Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

zawieszone do czasu rozpatrzenia apelacji)[26]. Wyroki skazujące mogą doprowadzić do dalszych postępowań karnych przeciwko osobom, które brały udział w procederze, jak również spraw o szpiegostwo.

1.3.4. Wielka Brytania/Arabia Saudyjska: odszkodowanie za inwigilację

Ghanem Al-Masarir, saudyjski aktywista i youtuber polityczny, znalazł się wśród osób inwigilowanych przez saudyjskiego operatora Pegasusa w 2018 r. Aktywista pozwał Królestwo Arabii Saudyjskiej, domagając się odszkodowania oraz zadośćuczynienia za krzywdę psychiczną i utratę zarobków. Brytyjski sąd uznał jego racje i w styczniu 2026 r. nakazał Arabii Saudyjskiej wypłacenie 3 mln funtów m.in. za doznane ból, cierpienie i utratę jakości życia, jak również poniesione straty oraz utracone zarobki[27].

Nie wiadomo, czy Arabia Saudyjska wypłaci zarządzoną skarżącemu sumę, ale zdaniem Al-Masarira – niezależnie od wyniku postępowania sądowego i wypłaty sumy odszkodowania – saudyjski rząd osiągnął swój cel, czyli zablokowanie jego satyrycznej aktywności online:

> *Mam nadzieję, że zastosują się do nakazu i jak najszybciej spłacą dług. Jeśli tego nie zrobią, nie będziemy mieli innego wyjścia, jak tylko podjąć działania egzekucyjne w celu odzyskania pieniędzy z saudyjskich aktywów za granicą – niekoniecznie w Wielkiej Brytanii.*
>
> *To dla nich zwycięstwo, ponieważ uciszyli mnie i nie mogę już wykonywać swojej pracy[28].*

***

Jak wynika z opracowania przygotowanego przez serbską Fundację Share, niemal 100 państw na świecie stosuje któryś z wielu komercyjnych programów szpiegujących

[26] The Record, *Intellexa founder, three others sentenced to 8 years in prison over Greek spyware scandal*, https://therecord.media/spyware-intellexa-greece-sentenced oraz Ekathimerini.com, *Four businesspeople found guilty in 2022 spyware scandal*, https://www.ekathimerini.com/news/1296353/four-businesspeople-found-guilty-in-spyware-trial/.

[27] Wyrok w sprawie Ghanem Al-Masarir przeciwko Królestwu Arabii Saudyjskiej, https://caselaw.nationalarchives.gov.uk/ewhc/kb/2026/119 oraz Citizen Lab, *Saudi Arabia Ordered to Pay £3m to London Dissident Over Pegasus Spying*, https://citizenlab.ca/saudi-arabia-ordered-to-pay-3m-to-london-dissident-over-pegasus-spying/.

[28] The Guardian, *Saudi dissident awarded £3m damages threatens enforcement action if he is not paid*, https://www.theguardian.com/world/2026/jan/30/saudi-dissident-awarded-3m-damages-threatens-enforcement-action-if-he-is-not-paid.

(tzw. *mercenary spyware*) lub samodzielnie rozwija własne narzędzia tego rodzaju[29]. Sprawa wykorzystania oprogramowania Pegasus w Polsce wpisuje się więc w szerszy, międzynarodowy kontekst. W kolejnej części przyjrzymy się argumentom za i przeciw tezie o legalności korzystania z tego rodzaju technologii przez służby.

2. Argumenty przeciwko tezie o legalności Pegasusa

W tym rozdziale:

- rozbrajamy argumentację zwolenników i zwolenniczek tezy o legalności stosowania w Polsce oprogramowania szpiegującego,
- opisujemy, w jaki sposób stosowanie oprogramowania szpiegującego narusza prawo unijne.

2.1. Oprogramowanie szpiegujące nie mieści się w definicji kontroli operacyjnej

Kontrola operacyjna może polegać m.in. na „uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych”[30].

Do tego właśnie służy oprogramowanie szpiegujące – argumentują **zwolennicy i zwolenniczki tezy o legalności Pegasusa. Uważają go za narzędzie kontroli operacyjnej jak każde inne.**

Za taką interpretacją przemawiałoby postanowienie Sądu Najwyższego z 23 kwietnia 2023 r. Zgodnie z nim przepisy regulujące działanie służb wskazują „rodzaje informacji lub danych, jakie mogą być pozyskiwane w trybie kontroli operacyjnej, a nie wskazują środków technicznych”.

Wydaje się, że w dobie szybkiego postępu technologicznego wyliczenie w ustawie takich środków technicznych nie jest możliwe. Przykładowo można wskazać rozwój w obszarze tzw. oprogramowań szpiegujących, nie wymagających współpracy z operatorem GSM, pozwalających poprzez

---

[29] Share Foundation, *A Privacy Nightmare: Understanding Spyware*, https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf.

[30] Zgodnie z art. 17 ust. 5 pkt 4 ustawy o CBA. Analogiczne rozwiązania obowiązują w przypadku innych służb.

„infekowanie telefonów" na kopiowanie wysyłanych lub odbieranych wiadomości, zbieranie zdjęć, nagrywanie rozmów, aktywowanie mikrofonu, aby podsłuchać rozmowy, uruchamianie kamery, aby nagrywać to, co dzieje się wokół danej osoby, umożliwiających dostęp do tzw. materiałów „historycznych", czyli z okresu przed zainstalowaniem takiego oprogramowania, posiadających opcję „samozniszczenia", czyli nie pozostawiających śladów w „zainfekowanym" urządzeniu[31].

Przeciwko takiej interpretacji świadczy po pierwsze to, że użycie Pegasusa i innych programów szpiegujących wiąże się z przełamaniem zabezpieczeń urządzenia i modyfikacją sposobu jego działania. Ani ustawa o CBA, ani żadna inna nie daje służbom prawa do przełamywania zabezpieczeń urządzeń należących do osób, wobec których została zarządzona kontrola operacyjna.

Potwierdził to Sąd Apelacyjny we Wrocławiu w wyroku z 11 maja 2023 r., który nie dopuścił dowodów uzyskanych za pomocą Pegasusa i w związku z tym uniewinnił funkcjonariusza oskarżonego o ujawnienie tajnej informacji.

Oprogramowanie typu spyware *daje pełen dostęp do urządzenia mobilnego, pozwala tym samym na uzyskiwanie i utrwalanie danych z niego. Tyle tylko, że do jego instalacji dochodzi w drodze ominięcia i przełamania zabezpieczeń – włamania na telefon – i to w sposób naruszający jego strukturę. Tymczasem obowiązujące przepisy dotyczące kontroli operacyjnej, w tym omawiany art. 17 ustawy o CBA, nie zezwalają na tego rodzaju działania, nie przewidują takiej możliwości*[32].

Po drugie, oprogramowanie szpiegujące daje możliwość pozyskania i utrwalenia danych historycznych – również z okresu poprzedzającego decyzję o zarządzeniu kontroli i bez ograniczeń czasowych, jeśli tylko dane są dostępne. Tymczasem sąd może zasądzić kontrolę operacyjną na maksymalnie trzy miesiące od zarządzenia kontroli wprzód, nie wstecz.

Jak obrazowo wyjaśnił gen. Krzysztof Bondaryk podczas posiedzenia Sejmowej Komisji Śledczej:

---

[31] Uchwała Sądu Najwyższego z 26 kwietnia 2023 r., sygn. I ZI 50/22, https://www.sn.pl/sites/orzecznictwo/orzeczenia3/i%20zi%2050-22.pdf.

[32] Wyrok z 11 maja 2023 r., sygn. II AKa 480/21, https://www.saos.org.pl/judgments/501168.

Kontrola operacyjna jest w czasie rzeczywistym, nakierowana na przyszłość, czyli od dzisiaj przez trzy miesiące możemy pana czy mnie można podsłuchiwać, a nie od dzisiaj przez np. cztery lata w przeszłość[33].

A to oznacza, że pozyskanie w 2019 r. 80 tysięcy wiadomości z lat 2010-2019 z telefonu należącego do Krzysztofa Brejzy[34] również nie mieściło się w definicji kontroli operacyjnej.

Na ten problem zwrócił też uwagę wrocławski sąd apelacyjny we wspomnianym wyżej wyroku. Interpretując przepisy ustawy o CBA w świetle Konstytucji, sąd doszedł do wniosku, że:

niedopuszczalne jest stosowanie przez służby takich środków kontroli operacyjnej, które wiążą się z (...) uzyskiwaniem dostępu do szerokiego spektrum danych, w tym historycznych, wykraczających poza ramy czasowe zarządzonej kontroli operacyjnej (...), posłużenie się oprogramowaniem szpiegowskim nie może być uznane za zgodny z ustawą, legalny sposób ich pozyskania.

Po trzecie, oprogramowanie szpiegujące daje dostęp nie tylko do danych zapisanych na urządzeniu, ale też do aplikacji i ich historii. Służby mogą dzięki niemu zajrzeć na feed dowolnej aplikacji, do bankowości elektronicznej czy historii zakupów na Vinted osoby inwigilowanej.

Dlatego naszym zdaniem nie ma w tej chwili przewidzianej w przepisach podstawy prawnej, by uznać, że Pegasus lub inne oprogramowanie szpiegujące jest narzędziem służącym do realizacji kontroli operacyjnej.

2.2. Sądy nie mają realnej kontroli nad działaniami służb

Drugim argumentem za legalnością Pegasusa ma być kontrola sądów nad podejmowaniem przez służby działań w zakresie kontroli operacyjnej. Adam Bodnar,

[33] Posiedzenie z 12 lutego 2026 r., https://sejm.gov.pl/Sejm10.nsf/biuletyn.xsp?skrnr=SKPG-126. O pracach sejmowej komisji śledczej piszemy więcej w podrozdziale 3.6.

[34] Raport Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych, https://www.senat.gov.pl/download/gfx/senat/pl/defaultaktualnosci/1924/15764/1/raport_koncowy_z_prac_komisji_nadzwyczajnej.pdf.

jako Minister Sprawiedliwości Prokurator Generalny, potwierdził w Sejmie, iż nie było takiej sytuacji, żeby Pegasus był wykorzystywany bez zgody sądu.

Nie mamy podstaw, by kwestionować tę tezę. **Bardzo możliwe jednak, że w żadnym z 578 przypadków sąd nie wiedział, że zatwierdza użycie właśnie oprogramowania szpiegującego**. Jak mówił w wywiadzie dla Rzeczypospolitej sędzia Sądu Okręgowego w Warszawie Igor Tuleya:

> *To bardzo prawdopodobne, że wydałem zgodę na użycie Pegasusa bez świadomości, jaki system będzie stosowany*[35].

Sędzia Sądu Apelacyjnego w Warszawie Marzanna Piekarska-Drążek przed Sejmową Komisją Śledczą zeznała natomiast:

> *W przypadku zastosowania takich technik operacyjnych typu Pegasus, trudno odnieść to do zapisów ustawowych, ponieważ nikt nie zakładał, że legalnie, czyli w ramach obowiązującego prawa, zostanie zastosowany taki system. Nikt nie przewidywał tego*[36].

Niewiedza sędziów jest symptomem szerszego problemu wadliwości kontroli sądowej nad stosowaniem kontroli operacyjnej. Problemu, któremu przyjrzał się też Europejski Trybunał Praw Człowieka w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce. Trybunał uznał, że „zezwolenie sądowe (...) jest bardzo użytecznym zabezpieczeniem proceduralnym, ale samo w sobie nie wystarcza". Wyrok potwierdza jednocześnie, że w Polsce nie funkcjonuje realny i efektywny mechanizm nadzoru nad stosowaniem kontroli operacyjnej. Na czym polega jego wadliwość?

Po pierwsze, służby do wniosku załączają tylko materiały „uzasadniające" potrzebę prowadzenia kontroli operacyjnej – a nie cały materiał. Jak wskazuje doradca Sejmowej Komisji Śledczej dr Adam Behan:

> *pozwala to służbom „ominąć" niewygodne dla siebie fakty czy kontekst, czy wręcz okoliczności, które uprawdopodobniają brak związku danej*

[35] Rzeczpospolita, *Sędzia Igor Tuleya: Możliwe, że zgodziłem się na Pegasusa*, https://www.rp.pl/sady-i-trybunaly/art39874451-sedzia-igor-tuleya-mozliwe-ze-zgodzilem-sie-na-pegasusa.

[36] Posiedzenie z 12 września 2025 r., https://sejm.gov.pl/Sejm10.nsf/biuletyn.xsp?skrnr=SKPG-102.

osoby ze sprawą, a które – gdyby znalazły się w przedłożonych dokumentach – mogłyby spowodować, iż zgoda nie zostanie wydana[37].

Po drugie, w postępowaniu dotyczącym zarządzenia kontroli operacyjnej nie bierze udziału podmiot reprezentujący prawo do prywatności osoby, której dotyczyć będzie kontrola operacyjna (np. znany z modelu brytyjskiego tzw. adwokat prywatności). W postępowaniu biorą udział tylko służby i prokurator. Jeśli więc sąd wyrazi zgodę na kontrolę operacyjną, nie ma komu zakwestionować słuszności tej decyzji.

Po trzecie, uzasadnienia wymagają jedynie odmowy zastosowania kontroli operacyjnej. Stanowi to swoistą zachętę dla sędziów, by wyrażać zgodę na stosowanie kontroli. Rząd Koalicji Obywatelskiej próbował nałożyć na sądy obowiązek uzasadniania również zgody na kontrolę operacyjną, ale zrobił to w drodze rozporządzeń, przez co zmiana ta jest nieskuteczna (por. 3.5.1.).

Po czwarte, wnioski rozpatruje tylko jeden (!) sędzia dyżurujący danego dnia, który „ma ograniczone możliwości skontrolowania w terminie jednego albo dwóch dni kilkudziesięciu wniosków o kontrolę operacyjną"[38].

W konsekwencji sądy wyrażają zgody na prowadzenie kontroli operacyjnej w ponad 99% przypadków (por. tabela 1).

Jak twierdzi dr Dominika Czerniak z Biura Rzecznika Praw Obywatelskich, warunki, w jakich sędziowie rozpatrują wnioski służb:

nie są usprawiedliwieniem dla oportunistycznego podejścia do prawa do prywatności i „taśmowego" akceptowania wniosków[39].

Na ile sędziowie mają już dziś realne narzędzia do weryfikacji wniosków służb (ale z nich nie korzystają), a na ile problem leży w dziurawych regulacjach, pozostaje kwestią sporną. Niemniej w aktualnym modelu kontrola sądowa nie stanowi ochrony przed

[37] Prawo.pl, *Kontrola operacyjna wymknęła się... spod kontroli*, https://www.prawo.pl/prawnicy-sady/sedziowie-nie-moga-byc-manipulowani-przez-sluzby,525859.html.

[38] Do Sądu Okręgowego w Warszawie wpływa codziennie – nie wyłączając niedziel i dni wolnych od pracy – średnio ok. 25 wniosków o zarządzenie kontroli operacyjnej. Biuro Rzecznika Praw Obywatelskich, *Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18). Raport w przedmiocie koniecznych zmian w przepisach regulujących pozaprocesową oraz procesową kontrolę i utrwalanie rozmów*, https://bip.brpo.gov.pl/sites/default/files/2025-11/Raport_wykonanie_wyroku_etpc_inwigilacja_3_07_2025.pdf.

[39] Tamże.

nadużyciami – ani w przypadku klasycznych środków kontroli operacyjnej, ani w przypadku stosowania oprogramowania szpiegującego.

Rok	Wnioski służb o kontrolę operacyjną	Odmowa prokuratora (nie ma kontroli operacyjnej)		Zgoda prokuratora (wnioski trafiają do sądu)		Odmowa sądu (nie ma kontroli operacyjnej)		Zgoda sądu (służby prowadzą kontrolę operacyjną)	
	Liczba osób	Liczba osób	%	Liczba osób	%	Liczba osób	%	Liczba osób	%
2024	5818	95	1,63%	5723	98,37%	26	0,454%	5697	**99,55%**
2023	5973	116	1,94%	5857	98,06%	22	0,376%	5835	**99,62%**
2022	6381	129	2,02%	6252	97,98%	38	0,608%	6214	**99,39%**
2021	7071	126	1,78%	6945	98,22%	25	0,360%	6920	**99,64%**
2020	6537	118	1,81%	6419	98,19%	35	0,545%	6384	**99,45%**
2019	5839	103	1,76%	5736	98,24%	25	0,436%	5711	**99,56%**
2018	6088	148	2,43%	5940	97,57%	25	0,421%	5915	**99,58%**
2017	6562	146	2,22%	6416	97,78%	14	0,218%	6402	**99,78%**

Tabela 1. Mimo „afery Pegasusa" sądy wciąż zgadzają się na ponad 99% wniosków o kontrolę operacyjną zatwierdzonych wcześniej przez prokuratora. Opracowanie własne na podstawie rocznych sprawozdań Prokuratora Generalnego.

2.3. Oprogramowanie szpiegujące może być zagrożeniem dla bezpieczeństwa państwa

Pegasus nigdy nie uzyskał akredytacji bezpieczeństwa teleinformatycznego ABW. Zdaniem płk. Przemysława Leśniaka, byłego Dyrektora Departamentu Informacji Niejawnych ABW, „Pegasus nie jest systemem teleinformatycznym i nie przetwarza informacji niejawnych"[40]. Jako taki nie wymagał więc powyższej akredytacji.

Prokuratura Krajowa stwierdziła jednak, że „system Pegasus powinien podlegać akredytacji bezpieczeństwa teleinformatycznego, jednakże świadectwa akredytacji nigdy nie uzyskał"[41]. Oznacza to, że mógł umożliwiać osobom trzecim (np. pracownikom i pracowniczkom NSO Group i izraelskich służb) dostęp do informacji o zainteresowaniach operacyjnych naszego wywiadu[42]. Tezę tę potwierdza również odtajniony dokument wewnętrzny Służby Kontrwywiadu Wojskowego, do którego dotarła Sejmowa Komisja Śledcza. W dokumencie miała znaleźć się informacja dla

[40] Profil płk. Przemysława Leśniaka na X, https://x.com/przemkolesniak/status/2029262770776977767.

[41] Wymóg akredytacji wynika z art. 48 ustawy o ochronie informacji niejawnych, https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20101821228. Prokuratura Krajowa, *ABW: system Pegasus powinien podlegać akredytacji bezpieczeństwa teleinformatycznego*, https://www.gov.pl/web/prokuratura-krajowa/abw-system-pegasus-powinien-podlegac-akredytacji-bezpieczenstwa-teleinformatycznego.

[42] Spider's Web, *Pegasus jest jeszcze bardziej nielegalny, niż się wydawało*, https://spidersweb.pl/2025/05/pegasus-nie-mial-akredytacji-bezpieczenstwa.html.

funkcjonariuszy, że „wykorzystywany system nie wyklucza możliwości zapoznania się z przesyłanymi danymi przez producenta oprogramowania”[43].

Ustalenia zawarte w dokumencie SKW potwierdzają informacje ujawnione przez Adama Haertle, redaktora naczelnego Zaufanej Trzeciej Strony, zgodnie z którymi Pegasus korzystał do transmisji danych z Pegasus Anonymizing Transmission Network (PATN), czyli sieci kontrolowanych przez NSO serwerów rozsianych po całym świecie[44]. Oznacza to, że **informacje pozyskiwane za pośrednictwem tego oprogramowania opuszczały infrastrukturę kontrolowaną przez licencjobiorcę (np. CBA) i trafiały do producenta oprogramowania**.

Ani inwigilowani, ani polskie służby nie mają żadnych narzędzi, żeby zweryfikować, co stało się z danymi, które trafiły do producenta Pegasusa, i jak będą w przyszłości wykorzystane. Co ważne, problem ten wynika z krótkowzrocznej decyzji o zakupie licencji na zewnętrzne oprogramowanie (a nie natury samego oprogramowania).

2.4. Oprogramowanie szpiegujące łamie prawo unijne

Przeciwko stosowaniu oprogramowania szpiegującego w obecnym stanie prawnym opowiada się też Unia Europejska. Komisja PEGA Parlamentu Europejskiego powołana do zbadania wykorzystania Pegasusa w krajach Unii Europejskiej, w tym w Polsce, doszła do wniosku, że pozostaje ono w sprzeczności z prawem unijnym.

Po pierwsze, narusza Kartę Praw Podstawowych Unii Europejskiej (KPP). Umożliwiając pełną, niejawną kontrolę nad urządzeniem, narusza artykuł 7 (prawo do poszanowania życia prywatnego) i 8 (prawo do ochrony danych osobowych) KPP. Zgodnie z art. 52 KPP oraz utrwalonym orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej każda ingerencja w prawa podstawowe musi spełniać wymogi legalności, konieczności i proporcjonalności. Tymczasem Pegasus – ze względu na zakres swoich możliwości – może łatwo doprowadzić do ingerencji przekraczającej to, co zostałoby uznane za proporcjonalne w demokratycznym państwie prawa. Możliwość ingerencji w treść materiału na urządzeniu docelowym podważa też podstawowe gwarancje rzetelnego procesu (art. 47 KPP), podając w wątpliwość zdatność materiału dowodowego przed sądem.

Komisja PEGA podkreśla też nadużywanie przez państwa wytrychu w postaci „bezpieczeństwa narodowego” (art. 4 ust. 2 Traktatu o Unii Europejskiej). Jej zdaniem nie

[43] Przewodnicząca sejmowej komisji śledczej Magdalena Sroka powoływała się na ten dokument podczas posiedzenia 27 czerwca 2026 r.

[44] Zaufana Trzecia Strona, *5 powodów, dla których używanie Pegasusa w Polsce nie mogło być legalne*, https://zaufanatrzeciastrona.pl/post/5-powodow-dla-ktorych-uzywanie-pegasusa-w-polsce-nie-moglo-byc-legalne/.

może ono stanowić powodu do ignorowania praw podstawowych. Również orzecznictwo TSUE jasno wskazuje, że względy bezpieczeństwa narodowego nie uzasadniają nieograniczonych naruszeń praw podstawowych.

Po drugie, wykorzystywanie Pegasusa może naruszać ogólne rozporządzenie o ochronie danych osobowych (RODO). Stosowane bez odpowiedniego nadzoru oprogramowanie szpiegujące może prowadzić do przetwarzania danych osobowych na masową skalę, bez wiedzy i zgody osoby, której dane dotyczą, a także bez spełnienia podstawowych zasad przetwarzania, takich jak minimalizacja danych czy ograniczenie celu.

Po trzecie, narusza ono dyrektywę ePrivacy (dyrektywa 2002/58/WE), która wprowadza zasadę, że przechwytywanie komunikacji elektronicznej oraz uzyskiwanie dostępu do informacji przechowywanych na urządzeniu użytkownika czy użytkowniczki jest dopuszczalne wyłącznie za jego lub jej zgodą lub na podstawie ściśle określonych wyjątków (tj. bezpieczeństwo narodowe, podejrzenie o przestępstwo). Tymczasem działanie *spyware* polega właśnie na uzyskaniu takiego dostępu bez wiedzy i zgody użytkownika i użytkowniczki. Wiemy zaś, że wiele przypadków zastosowania oprogramowania szpiegującego nie miało związku ani z bezpieczeństwem narodowym, ani z uzasadnioną walką z przestępczością.

Wśród sformułowanych przez Parlament Europejski rekomendacji znalazł się postulat opracowania unijnych regulacji prawnych, które pozwolą na kontrolowanie użycia oprogramowania szpiegującego przez organy państw członkowskich[45].

***

Z jednej strony służby przekonujące, że potrzebują narzędzi takich jak Pegasus, i osoby popierające jego stosowanie jako legalne. Z drugiej: nierozliczona afera, liczne argumenty podważające tezę o legalności tego narzędzia i obawy przed drastycznym ograniczeniem praw i wolności. Spór ten dowodzi, że pilnie potrzebujemy regulacji.

W kolejnej części przyjrzymy się, co wydarzyło się w Polsce od wykrycia pierwszych przypadków stosowania Pegasusa przez służby. Dlaczego mówimy o „aferze Pegasusa"? Jakie wyciągnęliśmy z niej wnioski i co zmieniło się w Polsce od ujawnienia inwigilacji?

[45] Zalecenie Parlamentu Europejskiego z 15 czerwca 2023 r. dla Rady i Komisji w następstwie dochodzenia w sprawie zarzutów naruszenia prawa Unii i niewłaściwego administrowania w jego stosowaniu w odniesieniu do oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego (2023/2500(RSP)), pkt 32, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:C_202400494.

3. Co zmieniło się w Polsce od „afery Pegasusa”

W tym rozdziale:

- przypomnimy reakcje polityków i polityczek na ujawnione nadużycia oraz ich obietnice złożone w kampanii,
- podsumujemy, jakie działania podjęto,
- sprawdzimy, czy ktoś został pociągnięty do odpowiedzialności za nadużycia.

3.1. Zapowiedzi wprowadzenia kontroli nad służbami w Polsce

W 2023 r. w Polsce trwała kampania wyborcza do Parlamentu. Pegasus i jego nielegalne wykorzystywanie przez służby były jednymi z tematów poruszanych w jej trakcie. Ówczesny szef opozycji (dziś premier) Donald Tusk zaproponował nawet kreatywne rozwinięcie skrótu PiS: „Przekupstwo Inwigilacja Szantaż”. Krytykując Prawo i Sprawiedliwość, **politycy i polityczki Koalicji Obywatelskiej (a także innych ugrupowań opozycyjnych) deklarowali konieczność zmian w modelu nadzoru nad służbami** (a więc także nad stosowaniem przez nie oprogramowania szpiegującego).

Podczas Kongresu Koalicji Obywatelskiej „100 konkretów” we wrześniu 2023 r. Krzysztof Brejza deklarował:

> *Zapewnimy bezpieczeństwo waszych telefonów, waszej korespondencji (...), każdy z was będzie mógł zgłosić się z pismem z zapytaniem, czy byłem inwigilowany*[46].

Nie był jedyny. Kapitał wyborczy na obietnicy nadzoru nad służbami próbował zbijać również Radosław Sikorski (wówczas europoseł):

[46] Donald Tusk – kanał oficjalny na YouTubie, *Donald Tusk: Kongres 100 konkretów, Tarnów, 9.09.2023*, występ Krzysztofa Brejzy od 1:02:11, https://www.youtube.com/live/rLzOWVm3epo?t=3720s.

„Jeśli nie chcesz, aby służby mogły podsłuchiwać każdego, kto sprzeciwia się władzy, głosuj na KO" – plakat wyborczy o tej treści opublikował na swoim profilu na X Radosław Sikorski 12 października 2023 r. Wpis opatrzony został hashtagami: #Pegasus #AferyPiS #Inwigilacja #PiStoZło #PiStoWstyd #PolskaWNaszychSercach, https://x.com/sikorskiradek/status/1712440684542599541.

Deklaracje z kampanii przełożyły się na konkrety w umowie koalicyjnej między partiami tworzącymi dziś rząd (Koalicja Obywatelska, Nowa Lewica, Koalicja Polska – Polska 2050 i Koalicja Polska – PSL). **Punkt 19 zawartej umowy zakładał m.in. wprowadzenie skutecznego mechanizmu kontroli wykonywania czynności operacyjno-rozpoznawczych przez służby i przyznanie obywatelom prawa do informacji o zainteresowaniu nimi ze strony służb, w szczególności informacji o prowadzonej wobec nich kontroli operacyjnej**[47].

Oprócz wspomnianego zapisu, umowa koalicyjna odnosiła się szeroko do tematu inwigilacji prowadzonej przez służby. Spodziewaliśmy się więc rychłego regulowania zasad wykorzystania oprogramowania szpiegującego takiego jak Pegasus.

Do tej pory nie doczekaliśmy się realizacji tych obietnic.

[47] Umowa koalicyjna z 10 listopada 2023 r., https://platforma.org/upload/document/203/attachments/433/UmowaKoalicyjna.pdf.

3.2. Senacka komisja nadzwyczajna rekomenduje zmiany

Nieco ponad miesiąc przed wyborami, 6 września 2023 r., zakończyła pracę senacka komisja nadzwyczajna do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych.

Komisja senacka nie miała uprawnień komisji śledczej. Została powołana jeszcze za rządów Prawa i Sprawiedliwości, co było możliwe, gdyż ówczesna opozycja miała większość w Senacie: wszyscy jej członkowie byli związani z ówczesną opozycją, która aktualnie tworzy rząd. Przewodniczący komisji – Marcin Bosacki – jest teraz wiceministrem spraw zagranicznych.

W raporcie podsumowującym prace komisja zarekomendowała systemowe zmiany w obszarze kontroli nad służbami specjalnymi. Podkreślała zwłaszcza konieczność jasnego wskazania niedopuszczalności modyfikacji danych pozyskanych za pomocą zaawansowanych środków kontroli operacyjnej i wprowadzenia obowiązku notyfikacji, czyli przyznania jednostce prawa do informacji o byciu przedmiotem działań operacyjno-rozpoznawczych.

Minęły trzy lata, ale zmiany wciąż nie zostały wprowadzone.

3.3. Kodeks pracy operacyjnej, czyli porzucony pomysł na kontrolę nad służbami

W 2023 r. w środowisku funkcjonariuszy służb specjalnych, z aktywnym udziałem gen. Krzysztofa Bondaryka (szefa ABW w latach 2007-2013), powstał projekt ustawy: Kodeksu pracy operacyjnej. Kodeks miał za zadanie kompleksowo uregulować i uporządkować zagadnienia związane z czynnościami operacyjnymi prowadzonymi przez służby.

Projekt legalizował stosowanie oprogramowania szpiegującego. Pozwalał na przeprowadzenie „niejawnej ingerencji" polegającej na „niejawnym uzyskaniu dostępu do telekomunikacyjnych urządzeń końcowych oraz systemów informatycznych i teleinformatycznych, w celu uzyskania i utrwalenia zawartych w nich danych"[48].

Równolegle projekt wzmacniał mechanizm kontroli sądowej nad działaniami służb (w zakresie kontroli operacyjnej i wykorzystania przez służby oprogramowania szpiegującego). Nakładał też na szefa służby prowadzącej kontrolę operacyjną obowiązek poinformowania osoby, wobec której była zarządzona „niejawna ingerencja",

[48] Projekt ustawy Kodeks pracy operacyjnej z 17 kwietnia 2023 r., https://civitas.edu.pl/wp-content/uploads/2023/05/kodeks-pracy-operacyjnej-projekt-17042023.pdf.

o fakcie jej zastosowania – nie później niż w terminie 12 miesięcy po zakończeniu ingerencji.

Po wyborach w 2023 r. prace nad Kodeksem pracy operacyjnej zostały zarzucone.

3.4. Wyrok w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce – zmiany „priorytetem" rządu

28 maja 2024 r., czyli ponad pół roku po utworzeniu rządu przez nową koalicję, Europejski Trybunał Praw Człowieka wydał wyrok w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce.

Sprawa zainicjowana w 2019 r. przez aktywistki i aktywistę Fundacji Panoptykon (Katarzynę Szymielewicz i Wojciecha Klickiego), Helsińskiej Fundacji Praw Człowieka (Dominikę Bychawską-Siniarską i Barbarę Grabowską-Moroz) oraz adwokata Mikołaja Pietrzaka dotyczyła szerokiego zakresu zagadnień związanych z zasadami prowadzenia kontroli operacyjnej przez polskie służby i sądowego nadzoru nad ich działalnością (nie dotyczyła wprost oprogramowania szpiegującego. Oprogramowanie szpiegujące – jak argumentujemy w rozdziale 2.1. – wykracza poza ramy kontroli operacyjnej. Służby jednak kierowały się do tej pory inną interpretacją. Dlatego analizujemy tu również obietnice i propozycje dotyczące stricte kontroli operacyjnej – por. 3.5.)[49].

Trybunał stwierdził, że system nadzoru nad stosowaniem kontroli operacyjnej przez polskie służby – mimo teoretycznego nadzoru sądów – nie chroni przed nadużyciami (jego szczegóły opisujemy w pkt 2.3).

Wyrok miał stać się – jak stwierdził Minister Sprawiedliwości Adam Bodnar – „istotnym impulsem do dalszych działań". Jak dodał Minister Koordynator Służb Specjalnych Tomasz Siemoniak, jego wykonanie miało być „jednym z priorytetów rządu"[50].

W chwili publikowania tego raportu wyrok nie został wykonany.

3.5. Niewystarczające zmiany legislacyjne

W 2024 r. coś drgnęło, jeśli chodzi o przepisy regulujące nadzór nad służbami. Rząd przyjął **szereg rozporządzeń zmieniających zasady zarządzania kontroli operacyjnej**

---

[49] Fundacja Panoptykon, *Inwigilacja w Polsce narusza twoje prawa. Ważny wyrok Europejskiego Trybunału Praw Człowieka*, https://panoptykon.org/wyrok-ETPC-inwigiliacja-2024.

[50] Ministerstwo Spraw Wewnętrznych i Administracji, *Konferencja prasowa dotycząca orzeczenia ETPC ws. kontroli operacyjnej w Polsce*, https://www.gov.pl/web/mswia/konferencja-prasowa-dotyczaca-orzeczenia-etpc-ws-kontroli-operacyjnej-w-polsce, a także nagranie konferencji (od 7 minuty), https://www.youtube.com/watch?v=ylXp7h0k56A.

przez Policję, Agencję Bezpieczeństwa Wewnętrznego i inne służby[51]. Pod koniec 2025 r. rozpoczęto prace nad **projektem ustawy o zmianie niektórych ustaw „w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną”**[52].

3.5.1. Nieskuteczne rozporządzenia

Rozporządzenia wprowadzają dwie zmiany:

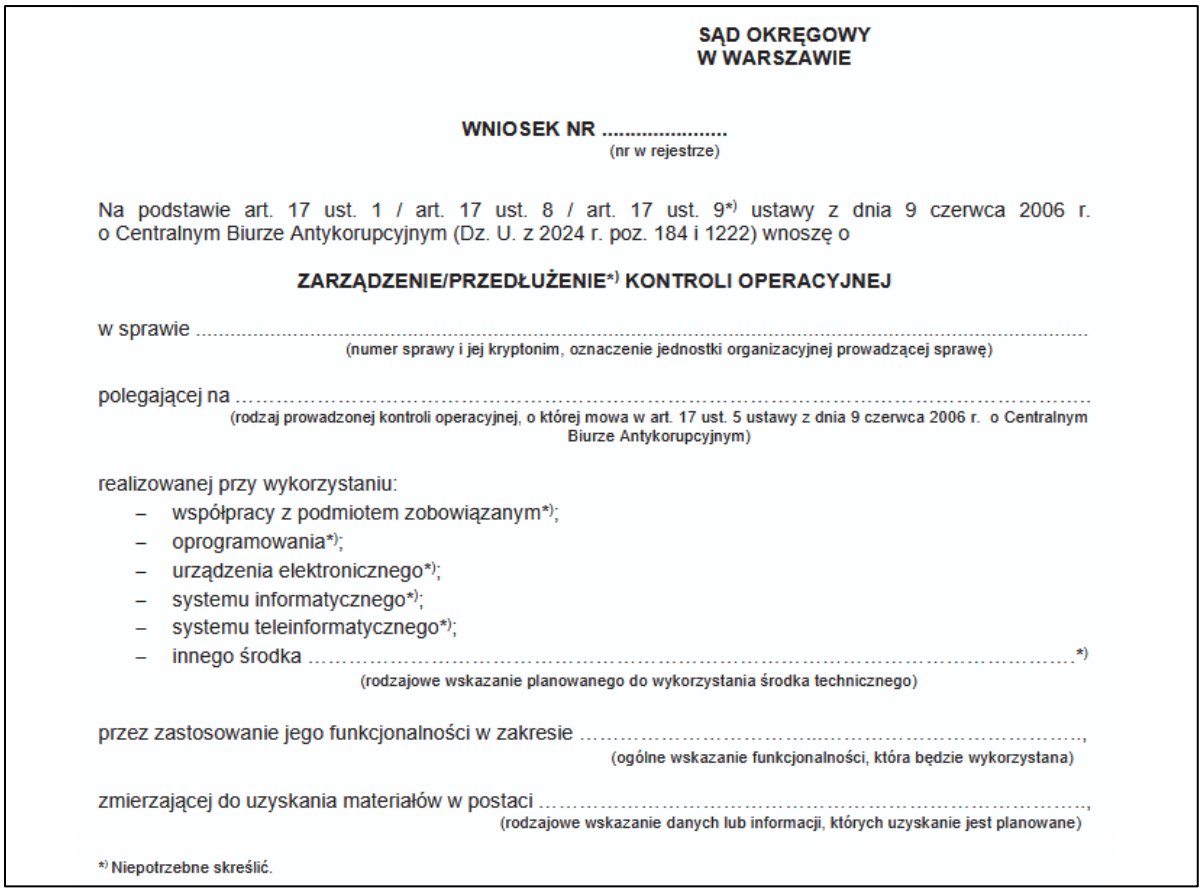
1) służba w uzasadnieniu składanego do sądu wniosku o zgodę na kontrolę operacyjną powinna poinformować, jakiego narzędzia chce użyć do inwigilacji i jakiego typu dane pozyskać za jego pośrednictwem (dzięki temu sąd wie na przykład, czy służba zamierza użyć klasycznego podsłuchu czy oprogramowania szpiegującego);

2) sąd musi uzasadnić zarówno zgodę, jak i odmowę zgody na kontrolę operacyjną (co miało zmniejszać prawdopodobieństwo automatycznego akceptowania wniosków przez sądy, a także realizować jedną z rekomendacji Europejskiego Trybunału Praw Człowieka w wyżej opisanej sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce).

Ocena pierwszej z tych zmian musi być pozytywna: każda zmiana zwiększająca zakres informacji, jakimi dysponują sędziowie rozpatrujący wniosek o wyrażenie zgody na kontrolę operacyjną, pozytywnie wpływa na możliwość sprawowania realnej kontroli przez sędziów nad tym, jakie działania chcą prowadzić służby.

[51] Fundacja Panoptykon, *Wzmocniona kontrola nad działaniami Krajowej Administracji Skarbowej – projekt opublikowany po apelu organizacji*, https://panoptykon.org/krajowa-administracja-skarbowa-po-apelu.

[52] Projekt ustawy o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną, https://sejm.gov.pl/Sejm10.nsf/druk.xsp?documentId=63F5DE808433ECBCC1258DD90031980F, w momencie pisania tego materiału trwały prace sejmowe nad projektem.



SĄD OKRĘGOWY
W WARSZAWIE

WNIOSEK NR .....
(nr w rejestrze)

Na podstawie art. 17 ust. 1 / art. 17 ust. 8 / art. 17 ust. 9*) ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2024 r. poz. 184 i 1222) wnoszę o

ZARZĄDZENIE/PRZEDŁUŻENIE*) KONTROLI OPERACYJNEJ

w sprawie .....
(numer sprawy i jej kryptonim, oznaczenie jednostki organizacyjnej prowadzącej sprawę)

polegającej na .....
(rodzaj prowadzonej kontroli operacyjnej, o której mowa w art. 17 ust. 5 ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym)

realizowanej przy wykorzystaniu:
- współpracy z podmiotem zobowiązanym*);
- oprogramowania*);
- urządzenia elektronicznego*);
- systemu informatycznego*);
- systemu teleinformatycznego*);
- innego środka .....*)
(rodzajowe wskazanie planowanego do wykorzystania środka technicznego)

przez zastosowanie jego funkcjonalności w zakresie .....,
(ogólne wskazanie funkcjonalności, która będzie wykorzystana)

zmierzającej do uzyskania materiałów w postaci .....,
(rodzajowe wskazanie danych lub informacji, których uzyskanie jest planowane)

*) Niepotrzebne skreślić.

Wzór formularza zawierającego wniosek Szefa CBA do Sądu Okręgowego w Warszawie o zarządzenie lub przedłużenie kontroli operacyjnej. Sąd uzyska informację np. o tym, że służba chce wykorzystać oprogramowanie oraz jakie jego funkcjonalności będą wykorzystywane.

Te zmiany to za mało. Bez wprowadzenia takich rozwiązań, jak np. adwokat prywatności, postępowanie wciąż ma charakter jednostronny, bo nikt nie występuje w obronie prawa do prywatności osoby poddawanej kontroli.

Co więcej, zdaniem niektórych sędziów, druga zmiana została wprowadzona z pominięciem hierarchii aktów prawnych i przez to jest nieskuteczna.

Kodeks postępowania karnego mówi, że „nie wymaga uzasadnienia (...) uwzględnienie wniosku, któremu inna strona nie sprzeciwiła się, chyba że orzeczenie podlega zaskarżeniu" (art. 98 § 3 kpk). W postępowaniu o wyrażenie zgody na prowadzenie kontroli operacyjnej nie ma „innej strony", a postanowienie o zgodzie na podsłuch nie podlega zaskarżeniu.

Ponieważ kodeks postępowania karnego jest ustawą i ma pierwszeństwo nad rozporządzeniem – jak poinformowała Prezes Sądu Okręgowego w Warszawie (czyli tego, który wydaje zgody na podsłuchy prowadzone przez służby specjalne) Beata

Najjar – część sędziów zignorowała zmiany w rozporządzeniach i nie uzasadnia postanowień, w których zgadza się na wnioskowany przez służbę zakres kontroli[53].

Jednocześnie sam obowiązek przygotowania uzasadnienia nie rozwiązuje problemu ograniczonego czasu, jaki sędziowie poświęcają na sprawy, w których zarządzają kontrolę operacyjną. Jak poinformowała wspomniana Prezes Sądu Okręgowego, część sędziów posługuje się pieczątką, która zastępuje uzasadnienie postanowienia o zarządzeniu kontroli operacyjnej.

3.5.2. Projekt ustawy o kontroli nad służbami nie rozwiązuje problemu

Projekt ustawy o zmianie niektórych ustaw „w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną”[54] ma za zadanie przede wszystkim wprowadzić obowiązek uzasadnienia postanowień w sprawie wniosków o zarządzenie kontroli operacyjnej (bez względu na to, czy sąd je zaakceptował, czy się sprzeciwił) – co nieskutecznie próbowano wprowadzić w drodze rozporządzeń. Przewiduje też możliwość nadzoru sądu nad już zarządzoną kontrolą operacyjną: sąd mógłby zażądać dostępu do materiałów zebranych w ramach kontroli operacyjnej i po ich analizie wydać postanowienie o przerwaniu działania służb.

Rząd zastrzega, że projekt nie ma na celu wykonania wyroku Europejskiego Trybunału Praw Człowieka:

> *[P]oszczególne rozwiązania zawarte w projekcie mogą odpowiadać na problemy dostrzeżone przez Europejski Trybunał Praw Człowieka w przywoływanym wyroku w sprawie Pietrzak i Bychawska-Siniarska i inni p. Polsce. Niemniej sam projekt ustawy nie aspiruje do miana regulacji wykonującej to orzeczenie[55].*

Wbrew tym deklaracjom projekt powstał w związku z nieformalnymi konsultacjami pomiędzy Ministerstwem Sprawiedliwości, Ministrem Koordynatorem Służb Specjalnych a przedstawicielami skarżących dotyczącymi właśnie wykonania wyroku.

---

[53] Biuro Rzecznika Praw Obywatelskich na YouTubie, *Konferencja: Pod nadzorem/bez nadzoru. Kontrola operacyjna w państwie prawa*, występ SSO Beaty Najjar od 4:37:20, https://www.youtube.com/watch?v=UW8ASvZbM6U.

[54] Projekt ustawy o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną, dz. cyt.

[55] Protokół rozbieżności załączony do pisma z 3 lutego 2026 r. przekazującego projekt ustawy UD278 o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną na Stały Komitet Rady Ministrów, https://legislacja.rcl.gov.pl/projekt/12404202.

Tam też jego zarys był po raz pierwszy przedstawiony jednemu z autorów tej analizy. Według naszej wiedzy inne prace nad wdrożeniem wyroku obecnie nie są prowadzone.

Projekt – by jego deklarowane cele nie pozostały wyłącznie na papierze – wymaga solidnego dopracowania.

Po pierwsze, sąd **może** weryfikować trwającą kontrolę operacyjną, ale **nie musi** tego robić. Przepis powinien wprowadzać obowiązek weryfikacji działań służb, nawet jeśli miałoby to dotyczyć tylko niektórych spraw.

Po drugie, w projekcie nie przewidziano zasobów umożliwiających realizację nowego zadania (np. w postaci nowych stanowisk sędziowskich w sądach, zwłaszcza w Sądzie Okręgowym w Warszawie – dlaczego to ważne, wyjaśniliśmy w podrozdziale 2.2.).

Po trzecie, możliwość udostępnienia sądowi – na jego żądanie – materiałów zebranych w toku prowadzenia kontroli operacyjnej może skończyć się zasypaniem go nieprzetworzoną przez funkcjonariuszy i funkcjonariuszki ilością materiałów, których sąd nie będzie w stanie ocenić, by na tej podstawie zweryfikować, czy wciąż istnieje konieczność prowadzenia kontroli operacyjnej[56].

Tezę **o pozorności proponowanych rozwiązań potwierdza wypowiedź sędzi Beaty Najjar**, Prezes Sądu Okręgowego w Warszawie, podczas konferencji w Biurze Rzecznika Praw Obywatelskich:

> *Aby decyzja o przerwaniu kontroli operacyjnej mogła zapaść, sąd musiałby ocenić najpierw jej wyniki, czyli musiałby zapoznać się z materiałem, który został na przestrzeni tego czasu – od momentu zarządzenia kontroli do momentu weryfikacji – zgromadzony. (...) Nie wyobrażam sobie tego organizacyjnie do zrobienia (...) przy naszych obecnych możliwościach kadrowych, przy liczbie sędziów, przy obciążeniu obowiązkami*[57].

[56] Opinia Fundacji Panoptykon z 30 kwietnia 2026 r. w sprawie projektu ustawy o zmianie niektórych ustaw w celu wzmocnienia sądowego nadzoru nad kontrolą operacyjną (druk sejmowy 2411), https://panoptykon.org/sites/default/files/2026-05/opinia-fundacji-panoptykon.pdf.

[57] Biuro Rzecznika Praw Obywatelskich na YouTubie, *Konferencja: Pod nadzorem/bez nadzoru. Kontrola operacyjna w państwie prawa*, występ SSO Beaty Najjar od 4:37:20, https://www.youtube.com/watch?v=UW8ASvZbM6U.

3.6. Nikt nie poniósł odpowiedzialności za „aferę Pegasusa”

W trakcie kampanii wyborczej w 2023 r. politycy i polityczki podkreślali również konieczność rozliczenia osób odpowiedzialnych za wykorzystanie Pegasusa do inwigilacji osób publicznych.

Pomijając to, że zapowiedzi te mogły mieć na celu przede wszystkim wygranie wyborów, uważamy, że takie rozliczenie jest potrzebne. Jego rolą jest przede wszystkim zniechęcenie kierownictwa i funkcjonariuszy służb do popełniania kolejnych nadużyć.

Rozliczeniami zajmują się Sejmowa Komisja Śledcza oraz Zespół Śledczy nr 3 w Prokuraturze Krajowej. Oba ta podmioty mają za zadanie wyjaśnić aferę, przy czym Komisja obraduje – co do zasady – jawnie, a Prokuratura nie.

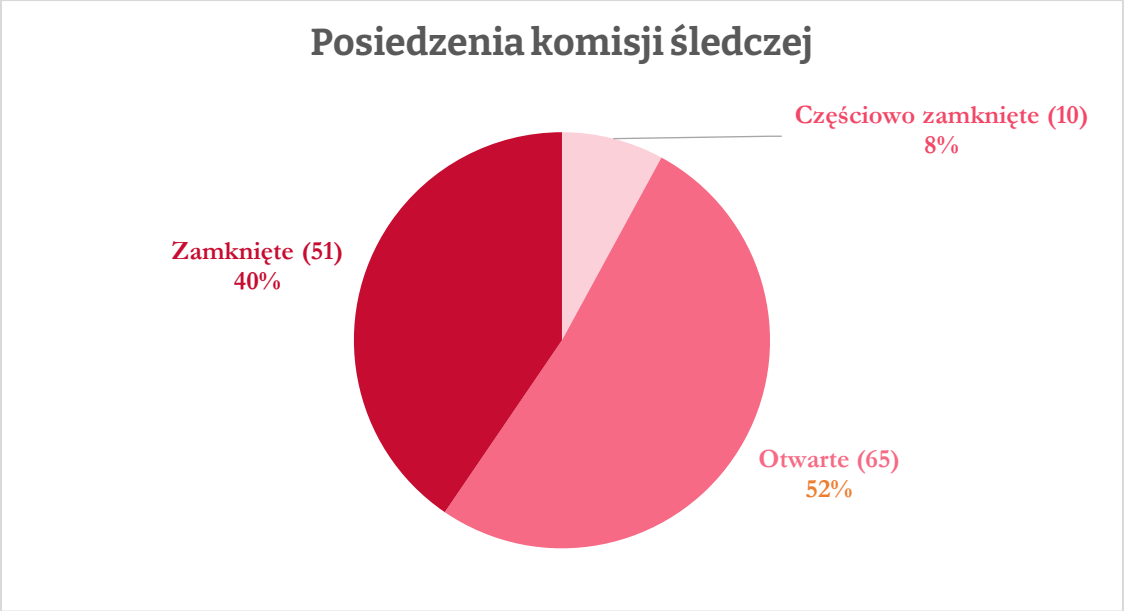
3.6.1. Przeciągające się prace Sejmowej Komisji Śledczej

Sejmowej Komisji Śledczej powierzono zbadanie „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 celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r.”.

Komisja pod przewodnictwem posłanki Magdaleny Sroki rozpoczęła prace w 2024 r. Odbyła ona dotychczas 126 posiedzeń, z których 77 miało charakter merytoryczny (tj. przesłuchano na nich świadka bądź odebrano opinię biegłego).

Komisja zajmowała się zarówno badaniem prawidłowości samych czynności operacyjno-rozpoznawczych, jak i oceną legalności i celowości zakupu oprogramowania Pegasus. Starała się wyjaśnić okoliczności zastosowania systemu Pegasus oraz określić liczbę przeprowadzonych za jego pośrednictwem interwencji. Badała również kwestię potencjalnego szpiegostwa i starała się ustalić, czy doszło do nielegalnego ujawnienia danych na temat zainteresowań polskich służb specjalnych obcym wywiadom poprzez nieprawidłowe, nielegalne lub niecelowe wykorzystywanie oprogramowania Pegasus lub innego systemu.

Mimo kontrowersji związanych z legalnością Komisji[58] i wynikającymi z tego problemami ze stawiennictwem niektórych świadków[59], **Komisja przesłuchała ostatecznie 79 osób, z czego dane 22 zostały utajnione**. 61 ze 126 posiedzeń miało charakter zamknięty lub częściowo zamknięty, aby przesłuchiwani podczas nich świadkowie mogli przekazać posłom i posłankom informacje mające charakter niejawny.



Wykres 2. Opracowanie własne na podstawie informacji ze strony sejmu: https://sejm.gov.pl/Sejm10.nsf/PosKomZrealizowane.xsp?komisja=SKPG.

W momencie pisania niniejszego raportu Komisja nie opublikowała jeszcze sprawozdania końcowego ze swoich prac. Według oficjalnych doniesień raport końcowy zostanie podzielony na część jawną, tajną i ściśle tajną (opinia publiczna będzie mogła zapoznać się jedynie z jawną częścią raportu). Raport miał ukazać się jeszcze w kwietniu 2026 r., natomiast opóźnienie w jego publikacji ma wynikać właśnie z dużej ilości tajnych materiałów[60].

[58] Prokuratura Okręgowa w Warszawie, *Sejmowa Komisja Śledcza ds. Pegasusa legalna. Odmowa wszczęcia śledztwa z uwagi na brak znamion czynu zabronionego*, https://www.gov.pl/web/po-warszawa/sejmowa-komisja-sledcza-ds-pegasusa-legalna-odmowa-wszczecia-sledztwa-z-uwagi-na-brak-znamion-czynu-zabronionego.

[59] PAP, *Były szef CBA nie stawił się na komisji ds. Pegasusa. Będzie wniosek o karę i doprowadzenie*, https://www.pap.pl/aktualnosci/byly-szef-cba-nie-stawil-sie-na-komisji-ds-pegasusa-bedzie-wniosek-o-kare-i.

[60] TVP Info, *Komisja Pegasusa kończy prace. Raport podzielony na część jawną i tajną*, https://www.tvp.info/92515418/sejmowa-komisja-ds-pegasusa-ujawni-czesc-raportu-czesc-pozostanie-tajna.

3.6.2. Zespół Śledczy Prokuratury Krajowej nie przedstawił aktów oskarżenia

Zespół Śledczy Prokuratury Krajowej prowadzi śledztwo od marca 2024 r.[61]. Jego zadaniem jest zbadanie legalności, zasadności i prawidłowości wykorzystania Pegasusa przez funkcjonariuszy publicznych. Zespół prokuratorski miał rozpoznać również zawiadomienie o podejrzeniu popełnienia przestępstwa, które zostało złożone w wyniku prac senackiej komisji nadzwyczajnej (por. część 2. raportu komisji).

Prowadzone przez Prokuraturę Krajową śledztwo obejmuje trzy rodzaje przypadków:

1) przekroczenia uprawnień lub niedopełnienia obowiązków przez funkcjonariuszy publicznych, czyli sytuacji bezprawnego wykorzystania programu Pegasus jako środka realizowania kontroli operacyjnej, a także bezprawnego wykorzystania materiałów uzyskanych na jej skutek,

2) podżegania lub pomocnictwa do nieuzasadnionego wykorzystania Pegasusa,

3) wprowadzenia w błąd innych organów w celu wykorzystania programu Pegasus w konkretnych sprawach.

Dotychczas postawiono zarzuty przekroczenia uprawnień (polegającego m.in. na „podstępnym" wprowadzeniu sądu w błąd „co do istnienia przesłanek do zastosowania i przedłużenia kontroli operacyjnej") lub niedopełnienia obowiązków służbowych (w związku z nieuzyskaniem wymaganej akredytacji ABW na stosowanie Pegasusa): byłym szefom ABW, SKW, CBA, byłemu Zastępcy Szefa CBA oraz dwóm byłym funkcjonariuszom CBA.

Nikt nie usłyszał aktu oskarżenia.

***

Podsumowując, przeprowadzone dotychczas zmiany sprowadzają się do rozporządzeń zwiększających zakres informacji, na podstawie których sąd zarządza kontrolę operacyjną (lub odrzuca wniosek o jej zarządzenie). Rozporządzenia nakładające obowiązek uzasadnienia decyzji przez sąd są nieskuteczne, prace nad Kodeksem pracy operacyjnej zostały zarzucone, a wyrok Europejskiego Trybunału Praw Człowieka jest wdrażany w bardzo okrojonym zakresie.

[61] Prokuratura Krajowa, *Komunikat o zespole śledczym ds. Pegasusa*, https://www.gov.pl/web/prokuratura-krajowa/komunikat-o-zespole-sledczym-ds-pegasusa.

Zmieniły się jedynie realia personalne. Po 2023 r. na czele wszystkich służb specjalnych stanęły nowe osoby. Ich poprzedni szefowie i osoby zaangażowane w aferę Pegasusa wciąż nie poniosły odpowiedzialności.

Politycy i polityczki nie zrealizowali zapowiedzi wprowadzenia kontroli nad działaniami służb. Oznacza to też, że nie zmieniły się ramy prawne stosowania oprogramowania szpiegującego. W kolejnej części piszemy, co powinno się zmienić.

4. Rekomendacje ram prawnych dla oprogramowania szpiegującego

W tym rozdziale:

- wyjaśniamy, dlaczego służby chcą używać oprogramowania szpiegującego,
- prezentujemy listę koniecznych zmian w polskim prawie jeśli chodzi o oprogramowanie szpiegujące i – szerzej – kontrolę operacyjną.

4.1. Dlaczego służby powinny móc legalnie używać oprogramowania szpiegującego

Koronny argument za tym, że Pegasus jest dopuszczalny w polskim systemie prawnym, sprowadza się do stwierdzenia, że służby potrzebują go do skutecznego działania. Podnoszą go przede wszystkim politycy Prawa i Sprawiedliwości oraz osoby odpowiedzialne za kierowanie służbami specjalnymi w okresie rządów PiS. Jak przekonują byli szefowie polskich służb w apelu do rządu:

> *Zapewnienie służbom technologii niezbędnych do skutecznej realizacji zadań jest nie tylko powinnością, ale wręcz obowiązkiem Szefów Służb Specjalnych*[62].

Jak wynika z rekomendacji grupy roboczej wysokiego szczebla w sprawie dostępu do danych dla skutecznego egzekwowania prawa, już w 2019 r. ponad 22% wiadomości było przesyłanych za pośrednictwem komunikatorów szyfrowanych *end-to-end*, co czyniło je niedostępnymi dla organów ścigania. Udział tego typu komunikatorów w codziennej

[62] Profil Stanisława Żaryna na X, https://x.com/StZaryn/status/2028417655468650894?s=20.

komunikacji skokowo rośnie. Aktualnie ok. 90% komunikacji odbywa się za pośrednictwem komunikatorów – w tym takich, które szyfrują komunikację domyślnie[63].

To właśnie rosnąca popularność szyfrowanej komunikacji jest najczęściej podawanym argumentem za korzystaniem przez służby z oprogramowania szpiegującego[64].

Przygotowanie rozwiązań technologicznych, które „umożliwiłyby organom ścigania dostęp do zaszyfrowanych danych w sposób zgodny z prawem, chroniąc cyberbezpieczeństwo i prawa podstawowe", zapowiedziała już Komisja Europejska w Europejskiej Strategii Bezpieczeństwa Wewnętrznego ProtectEU[65].

Polski rząd również zapowiada opracowanie systemu „umożliwiającego skuteczne utrwalanie treści generowanych przez osoby zaangażowane w działalność terrorystyczną z wykorzystaniem komunikatorów internetowych" oraz precyzyjne uregulowanie zasad stosowania „ofensywnych cybernarzędzi wobec współcześnie wykorzystywanych narzędzi komunikacyjnych, w tym komunikacji interpersonalnej". Towarzyszyć ma temu rozwój potencjału technicznego w tym zakresie[66].

Jesteśmy przekonani, że polskie służby już dziś mają narzędzia technologiczne, które umożliwiają im uzyskiwanie dostępu do szyfrowanej komunikacji *end-to-end*. Takie możliwości daje oprogramowanie szpiegujące.

Jednocześnie polski system prawny nie daje podstaw, żeby korzystać z takiego oprogramowania. Mimo szumnych zapowiedzi, władze nie wprowadziły zmian prawnych pozwalających je stosować, a system nadzoru sądowego nad kontrolą operacyjną pozostaje wysoce wadliwy. Oznacza to, że polskie służby działają w niejasnym otoczeniu prawnym, a obywatele i obywatelki nie są chronieni przed nadużyciami.

Jeśli służby mają skutecznie realizować swoje zadania, a przy tym nie naruszać prawa, potrzebne są:

---

[63] Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en.

[64] Trudność w dyskutowaniu z tym argumentem tkwi w tym, że alternatywa w postaci osłabienia szyfrowania komunikacji (proponowana np. w kontekście regulacji przeciwko wykorzystaniu dzieci – Child Sexual Abuse Regulation) jest znacznie bardziej niebezpieczna, bo dotyczy wszystkich.

[65] Komisja Europejska, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148.

[66] Uchwała nr 92 Rady Ministrów z 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, https://monitorpolski.gov.pl/M2026000030901.pdf.

1) systemowe zmiany w nadzorze nad prowadzeniem kontroli operacyjnej przez służby,

2) precyzyjne ramy prawne dla stosowania oprogramowania szpiegującego.

Naszym zdaniem **oprogramowanie szpiegujące powinno być szczególną, wyodrębnioną formą prowadzenia niejawnej ingerencji w prywatność obywateli i obywatelek**. Dlatego proponujemy dwie warstwy zmian:

1) w generalnych zasadach stosowania kontroli operacyjnej, które dotyczyć powinny zarówno tradycyjnych podsłuchów, jak i oprogramowania szpiegującego (por. 4.2),

2) w zakresie uregulowania **konkretnie** oprogramowania szpiegującego (por. 4.3).

4.2. Zmiany w zakresie stosowania kontroli operacyjnej

4.2.1. Realna kontrola wstępna

Model pozyskiwania zgody sądu na prowadzenie kontroli operacyjnej następujących zmian:

1) Sędzia powinien mieć możliwość zapoznania się z całym materiałem dotyczącym sprawy, a nie tylko tą częścią, która uzasadnia potrzebę prowadzenia kontroli operacyjnej.

2) Sędzia powinien mieć zapewnione odpowiednie zasoby (czas, wsparcie techniczne i administracyjne) oraz wiedzę techniczną, żeby dokładnie przyjrzeć się każdej sprawie.

3) Postępowanie powinno być zrównoważone przez obecność adwokata prywatności broniącego prawa osoby, której dotyczy wniosek, mającego możliwość zaskarżenia decyzji sądu o zgodzie na prowadzenie kontroli operacyjnej.

4) Wniosek o kontrolę operacyjną kierowany do sądu powinien jednoznacznie określać cele, zakres i sposób kontroli, w tym informacje o tym, jakie funkcjonalności mają być wykorzystane, jakie dane będą pozyskane oraz czy będą pozyskane dane historyczne.

4.2.2. Obowiązek informowania o inwigilacji i możliwość zaskarżenia

Fundamentalne znaczenie ma także **przyznanie jednostce:**

1) prawa do informacji o byciu przedmiotem zainteresowania ze strony uprawnionych instytucji,

2) prawa dostępu do przetwarzanych przez nie danych osobowych.

Obowiązek poinformowania osoby, względem której została zarządzona kontrola operacyjna, o tym fakcie, powinien być – co do zasady – realizowany po 12 miesiącach od zakończenia kontroli. Oczywiście możliwe są wyjątki od tej zasady np. ze względu na bezpieczeństwo państwa (pod warunkiem uzyskania zgody sądu).

Konsekwencją poinformowania powinna być także możliwość zaskarżenia decyzji sądu.

4.2.3. Kontrola następcza ze strony wyspecjalizowanego organu lub sądu

Ponadto niezbędne jest wprowadzenie **mechanizmu skutecznej weryfikacji działania służb w trakcie prowadzenia przez nie kontroli operacyjnej**.

Naszym zdaniem optymalnym rozwiązaniem byłoby stworzenie wyspecjalizowanej instytucji kontrolnej (koncepcja ta jest szczegółowo opisana w raporcie *Osiodłać Pegaza. Przestrzeganie praw obywatelskich w działalności służb specjalnych – założenia reformy*[67]).

Dopiero wprowadzenie łącznie tych trzech zmian wzmocni kontrolę nad działaniami służb.

4.3. Szczególne regulacje dotyczące oprogramowania szpiegującego

Postulujemy również przyjęcie szczególnych regulacji dotyczących konkretnie oprogramowania szpiegującego. **Przepisy powinny:**

1) **rozróżniać funkcję pasywną od aktywnej takiego oprogramowania** (por. podrozdział 1.1.) oraz zakazywać stosowania tej drugiej,

2) **dopuszczać stosowanie oprogramowania szpiegującego tylko w sprawach o szczególnej wadze**, np. związanych z terroryzmem (katalog takich sytuacji powinien być zamknięty i ograniczony do najpoważniejszych przestępstw),

3) **gwarantować bezpieczeństwo danych pozyskiwanych za pośrednictwem oprogramowania szpiegującego tak, by uniemożliwić dostęp niezaufanym**

[67] Fundacja Panoptykon, *Osiodłać Pegaza. Przestrzeganie praw obywatelskich w działalności służb specjalnych – założenia reformy*, https://panoptykon.org/sites/default/files/osiodlac_pegaza_-_jak_powinien_wygladac_nadzor_nad_sluzbami._raport_ekspertow.pdf.

dostawcom tych technologii. Być może rozwiązaniem w tym obszarze jest sygnalizowany w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej zamiar stworzenia krajowego narzędzia umożliwiającego dostęp do treści zawartych w telefonach osób zaangażowanych w działalność terrorystyczną czy szpiegowską.

***

Powyższe rekomendacje obejmują najważniejsze zmiany niezbędne do tego, by możliwe było zalegalizowanie działań z wykorzystaniem oprogramowania szpiegującego oraz by nadzór nad stosowaniem kontroli operacyjnej w Polsce gwarantował odpowiednią równowagę pomiędzy koniecznością zapewnienia skuteczności działania służb a zminimalizowaniem ryzyka nadużyć. Traktujemy je jako punkt wyjścia do koniecznej dyskusji.

Szczegółowe propozycje zmian znajdują się m.in. w opracowaniu Rzecznika Praw Obywatelskich *Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18). Raport w przedmiocie koniecznych zmian w przepisach regulujących pozaprocesową oraz procesową kontrolę i utrwalanie rozmów*[68] oraz w raporcie *Osiodłać Pegaza*. Ważnym punktem odniesienia jest także projekt ustawy Kodeksu pracy operacyjnej, który odpowiada na wiele opisanych wyżej wyzwań.

Nasze rekomendacje nie obejmują natomiast innych problemów, które w obszarze działania służb wymagają rozwiązania, np. kwestii dostępu do danych telekomunikacyjnych. W tym zakresie odsyłamy do właściwego raportu Rzecznika Praw Obywatelskich[69].

Ponieważ rekomendacje adresowane są do polskiego ustawodawcy, nie poruszamy też tutaj problemów, których rozwiązanie leży w gestii Unii Europejskiej, a które opisane są szczegółowo w raporcie komisji śledczej PEGA oraz w przywoływanym stanowisku EDRi.

---

[68] Biuro Rzecznika Praw Obywatelskich, *Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18). Raport w przedmiocie koniecznych zmian w przepisach regulujących pozaprocesową oraz procesową kontrolę i utrwalanie rozmów*, https://bip.brpo.gov.pl/sites/default/files/2025-11/Raport_wykonanie_wyroku_etpc_inwigilacja_3_07_2025.pdf.

[69] Biuro Rzecznika Praw Obywatelskich, *Opinia RPO ws. pozyskiwania danych telekomunikacyjnych obywateli przez służby specjalne i policję. Odpowiedź MC*, https://bip.brpo.gov.pl/pl/content/rpo-retencja-danych-policja-sluzby-koordynator-mswia-ms-mc.

Źródła

1. EDRi, *Spyware and state abuse. The case for an EU-wide ban*, https://edri.org/our-work/spyware-and-state-abuse-the-case-for-an-eu-wide-ban-position-paper/.

2. Share Foundation, *A privacy nightmare: understanding spyware*, https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf.

3. Raport Komisji śledczej ds. zbadania stosowania oprogramowania Pegasusa i równoważnego oprogramowania szpiegowskiego służącego inwigilacji Parlamentu Europejskiego, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html.

4. Citizen Lab, *HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, https://citizenlab.ca/research/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

5. Informacja o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej w 2023 r., https://orka.sejm.gov.pl/Druki10ka.nsf/0/7522A4519FE790ACC1258B01003A2A38/%24File/308.pdf.

6. The Guardian, *Poland launches inquiry into previous government's spyware use*, https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use.

7. Raport Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych, https://www.senat.gov.pl/download/gfx/senat/pl/defaultaktualnosci/1924/15764/1/raport_koncowy_z_prac_komisji_nadzwyczajnej.pdf.

8. Bankier.pl, *Hermeliński: Wybory w 2019 roku, choć nie były sfałszowane, nie były uczciwe,* https://www.bankier.pl/wiadomosc/Hermelinski-Wybory-w-2019-roku-choc-nie-byly-sfalszowane-nie-byly-uczciwe-8266533.html.

9. Rzeczpospolita, *Adam Bodnar: Zbigniew Ziobro powinien trafić do aresztu. Zachodzi obawa mataczenia lub ucieczki*, https://www.rp.pl/polityka/art43290211-adam-bodnar-zbigniew-ziobro-powinien-trafic-do-aresztu-zachodzi-obawa-mataczenia-lub-ucieczki.

10. The Guardian, *Second Italian journalist allegedly targeted with 'mercenary spyware'*, https://www.theguardian.com/world/2025/may/01/second-italian-journalist-allegedly-targeted-with-mercenary-spyware.

11. Citizen Lab, *Virtue or Vice? A First Look at Paragon's Proliferating Spyware Operations*, https://citizenlab.ca/research/a-first-look-at-paragons-proliferating-spyware-operations/#h-3-whatsapps-paragon-investigation.

12. Citizen Lab, *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation*, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/.

13. Citizen Lab, *Running in Circles. Uncovering the Clients of Cyberespionage Firm Circles*, https://citizenlab.ca/research/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/.

14. Citizen Lab, *Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

15. Access Now, *Spyware in Serbia: civil society under attack*, https://www.accessnow.org/spyware-attack-in-serbia/.

16. Amnesty International, *Serbia: "A Digital Prison": Surveillance and the suppression of civil society in Serbia*, https://www.amnesty.org/en/documents/eur70/8813/2024/en/.

17. International Consortium of Investigative Journalists, *Greek court convicts Intellexa founder Tal Dilian, three others in wiretapping scandal*, https://www.icij.org/investigations/cyprus-confidential/greek-court-convicts-intellexa-founder-tal-dilian-three-others-in-wiretapping-scandal/.

18. Citizen Lab, *Pegasus vs. Predator. Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware*, https://citizenlab.ca/research/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

19. The Record, *Intellexa founder, three others sentenced to 8 years in prison over Greek spyware scandal*, https://therecord.media/spyware-intellexa-greece-sentenced.

20. Ekathimerini.com, *Four businesspeople found guilty in 2022 spyware scandal*, https://www.ekathimerini.com/news/1296353/four-businesspeople-found-guilty-in-spyware-trial/.

21. Citizen Lab, *Saudi Arabia Ordered to Pay £3m to London Dissident Over Pegasus Spying*, https://citizenlab.ca/saudi-arabia-ordered-to-pay-3m-to-london-dissident-over-pegasus-spying/.

22. Wyrok w sprawie Ghanem Al-Masarir przeciwko Królestwu Arabii Saudyjskiej, https://caselaw.nationalarchives.gov.uk/ewhc/kb/2026/119.

23. The Guardian, *Saudi dissident awarded £3m damages threatens enforcement action if he is not paid*, https://www.theguardian.com/world/2026/jan/30/saudi-dissident-awarded-3m-damages-threatens-enforcement-action-if-he-is-not-paid.

24. Share Foundation, *A Privacy Nightmare: Understanding Spyware*, https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf.

25. Uchwała Sądu Najwyższego z 26 kwietnia 2023 r., sygn. I ZI 50/22, https://www.sn.pl/sites/orzecznictwo/orzeczenia3/i%20zi%2050-22.pdf.

26. Wyrok z 11 maja 2023 r., sygn. II AKa 480/21, https://www.saos.org.pl/judgments/501168.

27. Sejmowa Komisja Śledcza 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 celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r. (SKPG), https://sejm.gov.pl/Sejm10.nsf/agent.xsp?symbol=KOMISJASL&NrKadencji=10&KodKom=SKPG.

28. Rzeczpospolita, *Sędzia Igor Tuleya: Możliwe, że zgodziłem się na Pegasusa*, https://www.rp.pl/sady-i-trybunaly/art39874451-sedzia-igor-tuleya-mozliwe-ze-zgodzilem-sie-na-pegasusa.

29. Prawo.pl, *Kontrola operacyjna wymknęła się... spod kontroli*, https://www.prawo.pl/prawnicy-sady/sedziowie-nie-moga-byc-manipulowani-przez-sluzby,525859.html.

30. Biuro Rzecznika Praw Obywatelskich, *Wykonanie wyroku Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak i Bychawska-Siniarska i inni przeciwko Polsce (sprawa nr 72038/17 i 25237/18). Raport w przedmiocie koniecznych zmian w przepisach regulujących pozaprocesową oraz procesową kontrolę i utrwalanie rozmów*, https://bip.brpo.gov.pl/sites/default/files/2025-11/Raport_wykonanie_wyroku_etpc_inwigilacja_3_07_2025.pdf.

31. Profil płk. Przemysława Leśniaka na X, https://x.com/przemkolesniak/status/2029262770776977767.

32. Prokuratura Krajowa, *ABW: system Pegasus powinien podlegać akredytacji bezpieczeństwa teleinformatycznego*, https://www.gov.pl/web/prokuratura-krajowa/abw-system-pegasus-powinien-podlegac-akredytacji-bezpieczenstwa-teleinformatycznego.

33. Spider's Web, *Pegasus jest jeszcze bardziej nielegalny, niż się wydawało*, https://spidersweb.pl/2025/05/pegasus-nie-mial-akredytacji-bezpieczenstwa.html.

34. Zaufana Trzecia Strona, *5 powodów, dla których używanie Pegasusa w Polsce nie mogło być legalne*, https://zaufanatrzeciastrona.pl/post/5-powodow-dla-ktorych-uzywanie-pegasusa-w-polsce-nie-moglo-byc-legalne/.

35. Zalecenie Parlamentu Europejskiego z 15 czerwca 2023 r. dla Rady i Komisji w następstwie dochodzenia w sprawie zarzutów naruszenia prawa Unii i niewłaściwego administrowania w jego stosowaniu w odniesieniu do oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego (2023/2500(RSP)), pkt 32, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:C_202400494.

36. Donald Tusk – kanał oficjalny na YouTubie, *Donald Tusk: Kongres 100 konkretów, Tarnów, 9.09.2023*, https://www.youtube.com/live/rLzOWVm3epo?t=3720s.

37. Profil Radosława Sikorskiego na X, *https://x.com/sikorskiradek/status/1712440684542599541*.

38. Umowa koalicyjna z 10 listopada 2023 r., https://platforma.org/upload/document/203/attachments/433/UmowaKoalicyjna.pdf.

39. Projekt ustawy Kodeks pracy operacyjnej z 17 kwietnia 2023 r., https://civitas.edu.pl/wp-content/uploads/2023/05/kodeks-pracy-operacyjnej-projekt-17042023.pdf.

40. Fundacja Panoptykon, *Inwigilacja w Polsce narusza twoje prawa. Ważny wyrok Europejskiego Trybunału Praw Człowieka*, https://panoptykon.org/wyrok-ETPC-inwigiliacja-2024.

41. Ministerstwo Spraw Wewnętrznych i Administracji, *Konferencja prasowa dotycząca orzeczenia ETPC ws. kontroli operacyjnej w Polsce*, https://www.gov.pl/web/mswia/konferencja-prasowa-dotyczaca-orzeczenia-etpc-ws-kontroli-operacyjnej-w-polsce.

42. Fundacja Panoptykon, *Wzmocniona kontrola nad działaniami Krajowej Administracji Skarbowej – projekt opublikowany po apelu organizacji*, https://panoptykon.org/krajowa-administracja-skarbowa-po-apelu.

43. Projekt ustawy o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną, https://sejm.gov.pl/Sejm10.nsf/druk.xsp?documentId=63F5DE808433ECBCC1258DD90031980F.

44. Biuro Rzecznika Praw Obywatelskich na YouTubie, *Konferencja: Pod nadzorem/bez nadzoru. Kontrola operacyjna w państwie prawa*, https://www.youtube.com/watch?v=UW8ASvZbM6U.

45. Protokół rozbieżności załączony do pisma z 3 lutego 2026 r. przekazującego projekt ustawy UD278 o zmianie niektórych ustaw w celu wzmocnienia nadzoru sądowego nad kontrolą operacyjną na Stały Komitet Rady Ministrów, https://legislacja.rcl.gov.pl/projekt/12404202.

46. Fundacja Panoptykon, opinia w sprawie projektu ustawy o zmianie niektórych ustaw w celu wzmocnienia sądowego nadzoru nad kontrolą operacyjną (druk sejmowy 2411) z 30 kwietnia 2026 r., https://panoptykon.org/sites/default/files/2026-05/opinia-fundacji-panoptykon.pdf.

47. Prokuratura Okręgowa w Warszawie, *Sejmowa Komisja Śledcza ds. Pegasusa legalna. Odmowa wszczęcia śledztwa z uwagi na brak znamion czynu zabronionego*, https://www.gov.pl/web/po-warszawa/sejmowa-komisja-sledcza-ds-pegasusa-legalna-odmowa-wszczecia-sledztwa-z-uwagi-na-brak-znamion-czynu-zabronionego.

48. PAP, *Były szef CBA nie stawił się na komisji ds. Pegasusa. Będzie wniosek o karę i doprowadzenie*, https://www.pap.pl/aktualnosci/byly-szef-cba-nie-stawil-sie-na-komisji-ds-pegasusa-bedzie-wniosek-o-kare-i.

49. TVP Info, *Komisja Pegasusa kończy prace. Raport podzielony na część jawną i tajną*, https://www.tvp.info/92515418/sejmowa-komisja-ds-pegasusa-ujawni-czesc-raportu-czesc-pozostanie-tajna.

50. Prokuratura Krajowa, *Komunikat o zespole śledczym ds. Pegasusa*, https://www.gov.pl/web/prokuratura-krajowa/komunikat-o-zespole-sledczym-ds-pegasusa.

51. Profil Stanisława Żaryna na X, https://x.com/StZaryn/status/2028417655468650894?s=20.

52. Recommendations of the High-Level Group on Access to Data for Effective Law Enforcement, https://home-affairs.ec.europa.eu/document/download/1105a0ef-535c-44a7-a6d4-a8478fce1d29_en.

53. Komisja Europejska, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0148.

54. Uchwała nr 92 Rady Ministrów z 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, https://monitorpolski.gov.pl/M2026000030901.pdf.

55. Fundacja Panoptykon, *Osiodłać Pegaza. Przestrzeganie praw obywatelskich w działalności służb specjalnych – założenia reformy*, https://panoptykon.org/sites/default/files/osiodlac_pegaza_-_jak_powinien_wygladac_nadzor_nad_sluzbami._raport_ekspertow.pdf.

56. Biuro Rzecznika Praw Obywatelskich, *Opinia RPO ws. pozyskiwania danych telekomunikacyjnych obywateli przez służby specjalne i policję. Odpowiedź MC*, https://bip.brpo.gov.pl/pl/content/rpo-retencja-danych-policja-sluzby-koordynator-mswia-ms-mc.

O Fundacji Panoptykon

W Fundacji Panoptykon od 2009 r. walczymy o prawo chroniące wolność i prywatność. Patrzymy na ręce państwu i korporacjom, ujawniamy nadużycia, pokazujemy, jak świadomie żyć w cyfrowym świecie.

Działamy po to, by nowe technologie służyły społeczeństwu, a ludzie mieli kontrolę nad tym, w jaki sposób wykorzystywane są ich dane.

Od ponad 17 lat walczymy o kontrolę nad działaniami służb. W 2010 r. ujawniliśmy statystyki dotyczące pozyskiwania przez polskie służby billingów i innych danych telekomunikacyjnych. W 2024 r. doprowadziliśmy do wydania przez Europejski Trybunał Praw Człowieka wyroku wskazującego, że polskie przepisy dotyczące kontroli operacyjnej wymagają systemowych zmian. Współpracowaliśmy z Komisją PEGA Parlamentu Europejskiego oraz senacką komisją nadzwyczajną, wyjaśniającymi przypadki wykorzystywania Pegasusa do inwigilacji obywateli i obywatelek.

Jeśli cenisz sobie wolność i prywatność, przekaż nam darowiznę lub 1,5% podatku.

Więcej informacji: panoptykon.org/wspieraj

KRS: 0000327613

***

Opracowanie: Wojciech Klicki, Anna Obem, Zuzanna Rżysko

Korekta: Hanna Prorok-Ali

Okładka: Paweł Smardzewski

Fundacja Panoptykon

Panoptykon.org

Maj 2026

FUNDACJA PANOPTYKON