dr Magdalena Matusiak-Frącczak

Autorka jest adiunktem w Katedrze Europejskiego Prawa Konstytucyjnego na Wydziale Prawa i Administracji Uniwersytetu Łódzkiego (ORCID: https://orcid.org/0000-0002-6736-8008).

Konwencyjne standardy legalnej inwigilacji a zastosowanie systemu Pegasus w Polsce

***Słowa kluczowe**: inwigilacja, Pegasus, oprogramowanie szpiegowskie, prawo do prywatności, prawo do sprawiedliwego procesu, prawo do swobody wypowiedzi*

W 2021 r. ujawniono zastosowanie na skalę światową izraelskiego oprogramowania szpiegowskiego o nazwie Pegasus. Okazało się, że było one wykorzystywane nie tylko do zwalczania przestępczości, lecz także do inwigilowania przedstawicieli opozycji, dziennikarzy, prawników czy członków społeczeństwa obywatelskiego. Niniejszy tekst omawia wymogi legalnej inwigilacji na gruncie europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności[1]. Jego zasadniczym celem jest ocena, czy i w jakim zakresie polska praktyka zastosowania Pegasusa była niezgodna z tymi wymogami.

1. Wprowadzenie

Przedmiotem niniejszego opracowania będą standardy dotyczące legalnej inwigilacji w kontekście zastosowania systemu szpiegowskiego *Pegasus*. Inwigilacja istotnie ingeruje w prawa zawarte w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności i w określonych sytuacjach może stanowić przekroczenie granic marginesu swobody przyznanego państwom.

W celu realizacji tematu artykułu w pierwszej kolejności zostaną nakreślone przesłanki legalnej inwigilacji, wypracowane przez Europejski Trybunał Praw Człowieka w bogatym orzecznictwie. Następnie, aby przybliżyć czytelnikowi problem dotyczący Pegasusa, zostanie pokrótce przedstawione zastosowanie tego oprogramowania na świecie oraz skutki ujawnienia użycia tego oprogramowania. Kolejna część skoncentruje się na inwigilacji Pegasusem w Polsce i zostaną poczynione uwagi w przedmiocie zgodności polskiej praktyki w tym zakresie z wymogami konwencyjnymi.

2. Standardy legalnej inwigilacji w świetle orzecznictwa ETPC

Inwigilacja z jednej strony może potencjalnie godzić w takie prawa konwencyjne przysługujące jednostkom, jak prawo do poszanowania prywatności (art. 8 EKPC), czy w określonych okolicznościach również prawo do sprawiedliwego procesu (art. 6 EKPC, jeżeli inwigilacja ingeruje w komunikację jednostki z reprezentującym ją prawnikiem) oraz prawo do swobody wypowiedzi (art. 10 EKPC w przypadku inwigilowania dziennikarzy). Z drugiej strony ma ona na celu zwalczanie przestępczości oraz zwiększa skuteczność organów ścigania w wykrywaniu sprawców przestępstw i pociąganiu ich do odpowiedzialności karnej. Z tych powodów stała się ona przedmiotem licznych orzeczeń Europejskiego Trybunału Praw Człowieka, które w przestrzeni europejskiej nakreślają obecnie standardy legalnej inwigilacji.

Artykuł 8 ust. 1 EKPC gwarantuje każdemu prawo do poszanowania życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Nie jest to prawo absolutne i może być ograniczone w przypadkach przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie m.in. z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne czy ochronę porządku i zapobieganie przestępstwom (art. 8 ust. 2 EKPC). Trybunał dokonał interpretacji ww. warunków ograniczenia prawa do poszanowania prywatności. W pierwszej kolejności zaznaczył, że sformułowanie „w przypadkach przewidzianych przez ustawę" oznacza, że w prawie krajowym powinna istnieć podstawa prawna do stosowania inwigilacji. Ponadto prawo krajowe powinno spełniać pewne wymogi jakościowe, aby uznać, że inwigilacja była zgodna z zasadą praworządności. Owa podstawa prawna musi być dostępna dla jednostki i przewidywalna co do skutków, co w przypadku inwigilacji oznacza, że jednostki powinny być w stanie przewidzieć, kiedy władze publiczne mogą sięgnąć po inwigilację. Prawo to powinno być wystarczająco jasne i szczegółowe oraz dokładnie określać przesłanki, w których organy ścigania

1 Dz.U. z 1993 r. Nr 61, poz. 284 ze zm. – dalej EKPC.

są uprawnione do sięgnięcia po inwigilację, aby uchronić jednostkę przed arbitralnością ze strony władz[2].

Kolejną przesłanką ograniczenia prawa do prywatności jest konieczność inwigilacji w społeczeństwie demokratycznym. Aby przesłanka ta była spełniona, prawo musi zapewniać odpowiednie i skuteczne zabezpieczenia i gwarancje przed nadużyciem ze strony władz publicznych. Dlatego też prawo powinno określać co najmniej poniższe kwestie:

1) naturę przestępstw, w przypadku których można nakazać inwigilację;
2) zdefiniowanie kategorii osób, których komunikacja może być inwigilowana;
3) czasowe ramy inwigilacji;
4) procedurę badania, użycia i przechowywania uzyskanych danych;
5) zabezpieczenia, które należy podjąć przy przekazywaniu zebranych danych innym podmiotom;
6) okoliczności, w których przechowywane dane mogą lub muszą być wykasowane lub zniszczone[3].

Kluczowym wymogiem jest mechanizm skutecznej kontroli nad inwigilacją, która powinna mieć miejsce na trzech etapach: kiedy inwigilacja jest zarządzana po raz pierwszy, kiedy jest wykonywana oraz po jej zakończeniu. W przypadku dwóch pierwszych etapów nadzór odbywa się bez udziału zainteresowanej jednostki, co jest logiczne, gdyż w ten sposób zapewniona jest skuteczność inwigilacji. Istotne jest, aby kontrola była sprawowana przez sąd albo organ sądowy, który daje gwarancje niezależności, bezstronności i przestrzegania stosownych reguł proceduralnych[4].

Na trzecim etapie, czyli po zakończeniu inwigilacji, kontrola powinna być sprawowana przy udziale zainteresowanej jednostki. Powyższe może być zrealizowane przez poinformowanie jednostki o zastosowanej inwigilacji w celu umożliwienia jej zaskarżenia stosowania wobec niej kontroli do sądu. Alternatywną ścieżką, na którą wskazuje Trybunał, jest umożliwienie każdemu, kto podejrzewa, że stał się obiektem inwigilacji, złożenia stosownego wniosku do sądu o zbadanie tej kwestii[5].

Należy nadmienić, że inwigilacja może godzić w prawo do obrony i w prawo do sprawiedliwego procesu, jeżeli jej przedmiotem są rozmowy jednostki z adwokatem. W tym zakresie Trybunał podkreśla znaczenie niezależnej kontroli sądowej *ex ante* i *ex post*[6]. Inwigilowanie dziennikarzy może doprowadzić do ujawnienia ich źródeł, czyli do naruszenia tajemnicy dziennikarskiej. W takiej sytuacji ETPC kładzie naciska na kontrolę *ex ante,* ponieważ kontrola sprawowana następczo nie przywróci już poufności informatorów, jeżeli zostaną ujawnieni[7].

W tym miejscu warto zauważyć, że niektóre państwa utworzyły specjalne sądy, które zajmują się wyłącznie kontrolą inwigilacji, zarówno zatwierdzają jej uruchomienie, dokonują jej kontroli w trakcie oraz po jej zakończeniu, jak również jednostki mogą się zwracać do nich o zbadanie, czy nie były obiektem nielegalnej inwigilacji. Przykładowo w Zjednoczonym Królestwie takim sądem jest *Investigatory Powers Tribunal*[8], a w Szwecji *Försvarsunderrättelsedomstolen*[9].

3. Inwigilacja systemem Pegasus na świecie

W 2021 r. śledztwo prowadzone wspólnie przez dziennikarzy Forbidden Stories oraz Amnesty International ujawniło, że spółka NSO Group sprzedawała oprogramowanie o nazwie Pegasus takim państwom, jak Meksyk, Arabia Saudyjska, Azerbejdżan, Armenia, Indie, Maroko, Węgry, Polska. Oficjalnie oprogramowanie to miało służyć do zwalczania najpoważniejszych przestępstw, jak terroryzm, ale w praktyce okazało się, że było wykorzystywane do inwigilacji dziennikarzy, działaczy społecznych, polityków opozycji[10]. Pegasus pozwala na pozyskanie całej zawartości telefonu, nagrywanie rozmów, śledzenie lokalizacji, sekretne włączenie kamery i wykonywanie nagrań oraz zdjęć, a nawet na wgranie zawartości na telefon użytkownika[11].

2 ETPC: wyrok z 4.05.2000 r., 28341/95, Rotaru przeciwko Rumunii, HUDOC, pkt 52; decyzja z 29.06.2006 r., 54934/00, Weber i Saravia przeciwko Niemcom, HUDOC, pkt 93; wyrok z 1.03.2007 r., 5935/02, Heglas przeciwko Czechom, HUDOC, pkt 74; wyrok z 18.05.2010 r., 26839/05, Kennedy przeciwko Zjednoczonemu Królestwu, HUDOC, pkt 151; wyrok z 4.12.2015 r., 47143/06, Zakharov przeciwko Rosji, HUDOC, pkt 228–230; wyrok z 25.05.2021 r., w sprawach połączonych 58170/13, 62322/14 i 24960/15, Big Brother Watch and others przeciwko Zjednoczonemu Królestwu, HUDOC, pkt 332–333; wyrok z 25.05.2021 r., 35252/08, Centrum för Rättvisa przeciwko Szwecji, HUDOC, pkt 246–247.

3 ETPC: decyzja 54934/00, Weber i Saravia przeciwko Niemcom, pkt 95; wyrok z 18.02.2003 r., 58496/00, Prado Bugallo przeciwko Hiszpanii, HUDOC, pkt 30; wyrok 26839/05, Kennedy przeciwko Zjednoczonemu Królestwu, pkt 152; wyrok 47143/06, Zakharov przeciwko Rosji, pkt 231; wyrok w sprawach połączonych 58170/13, 62322/14 i 24960/15, Big Brother Watch and others przeciwko Zjednoczonemu Królestwu, pkt 334–335; wyrok 35252/08, Centrum för Rättvisa przeciwko Szwecji, pkt 248–249.

4 ETPC: wyrok 47143/06, Zakharov przeciwko Rosji, pkt 233; wyrok w sprawach połączonych 58170/13, 62322/14 i 24960/15, Big Brother Watch and others przeciwko Zjednoczonemu Królestwu, pkt 336; wyrok 35252/08, Centrum för Rättvisa przeciwko Szwecji, pkt 250.

5 ETPC: decyzja 54934/00, Weber i Saravia przeciwko Niemcom, pkt 135; wyrok 47143/06, Zakharov przeciwko Rosji, pkt 234; wyrok w sprawach połączonych 58170/13, 62322/14 i 24960/15, Big Brother Watch and others przeciwko Zjednoczonemu Królestwu, pkt 337; wyrok 35252/08, Centrum för Rättvisa przeciwko Szwecji, pkt 251.

6 ETPC: wyrok z 1.12.2015 r., 69436/10, Brito Ferrinho Bexiga Villa-Nova przeciwko Portugalii, HUDOC, pkt 56–59; wyrok z 16.06.2016 r., 49176/11, Versini-Campinchi i Crasnianski przeciwko Francji, HUDOC, pkt 62, 62–74; wyrok z 27.04.2017 r., 73607/13, Sommer przeciwko Niemcom, HUDOC, pkt 62. Zob. też M. Matusiak-Frącczak, *Ochrona poufności komunikacji klienta z adwokatem. Standardy międzynarodowe, standard Unii Europejskiej oraz standardy krajowe wybranych państw a prawo polskie,* Warszawa 2023, s. 234.

7 ETPC: wyrok z 14.09.2010 r., 38224/03, Sanoma Uitgevers B.V. przeciwko Niderlandom, HUDOC, pkt 95–100; wyrok z 16.07.2013 r., 73469/10, Nagla przeciwko Łotwie, HUDOC, pkt 87–90. Zob. też M. Matusiak-Frącczak, *Ochrona…*, s. 56.

8 Sekcje 65–70, Regulaction of Investigatory Powers Act 2000, https://www.legislation.gov.uk/ukpga/2000/23/introduction (dostęp: 12.07.2023 r.).

9 Lag (2009:966) om Försvarsunderrättelsedomstol, https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2009966-om-forsvarsunderrattelsedomstol_sfs-2009–966/ (dostęp: 12.07.2023 r.).

10 L. Richard, S. Rigaud, *Pegasus. The Story of the World's Most Dangerous Spyware,* London 2023; T. Kaldani, Z. Prokopets, *Pegasus spyware and its impact on human rights,* Strasbourg 2022, s. 15–20; G. Sartor, A. Loreggia, *Wpływ oprogramowania Pegasus na prawa podstawowe i procesy demokratyczne,* Bruksela 2023, s. 37.

11 Wysoki Komisarz ds. Praw Człowieka ONZ, *The right to privacy in the digital age,* 4.08.2022 r., A/HRC/51/17; zob. też G. Sartor, A. Loreggia, *Wpływ...*, s. 27–28; M.R. Woźniak, *Pegasus: gorzej niż podsłuch. Umożliwia podrzucanie dowodów. Giertych, Wrzosek, Brejza, kto jeszcze...*, 26.12.2021 r., https://oko.press/pegasus-gorzej-niz-podsluch-potrafi-tez-podrzucac-dowody/ (dostęp: 11.07.2023 r.); A. Wolska, M. Kucharczyk, *Pegasus: Jak działa oprogramowanie do szpiegowania?*, 24.12.2021 r., https://www.euractiv.pl/section/gospodarka/news/pegasus-giertych-wrzosek-brejza-macron-izrael-usa-polska-wegry-podsluch-cyberatak-pis-ziobro-cba-sluzby/ (dostęp: 11.07.2023 r.); Radio Free Europe, *Azerbaijan suspected of Spying on Reporters, Activists by Using Software to Access Phones,* 18.07.2021, https://www.rferl.org/a/azerbaijan-pegasus-spying-nso/31365076.html (dostęp: 11.07.2023 r.).

Na początku zainfekowanie telefonu Pegasusem wymagało działania ze strony użytkownika telefonu. Taki użytkownik otrzymywał wiadomością (przez SMS, WhattsApp, Messenger itp.) link, a po kliknięciu w ten link Pegasus instalował się na telefonie. Z czasem technologia Pegasusa została ulepszona do mechanizmu określanego jako zero-click, przy którym nie była wymagana żadna akcja ze strony użytkownika telefonu, wystarczyło, że na urządzenie przyszła wiadomość i Pegasus sam się instalował[12].

Można wskazać na kilka przykładów zastosowania Pegasusa przez wspomniane państwa. Pierwszym klientem NSO Group był Meksyk i do dzisiaj pozostaje on państwem, który najczęściej sięga po inwigilację Pegasusem. To właśnie Pegasus przyczynił się do schwytania narkotykowego barona Meksyku znanego jako El Chapo. Niestety, często obiektami inwigilacji stali się obrońcy praw człowieka czy osoby pozostające w politycznej opozycji do władz państwowych. Chociaż prezydent Meksyku Andrés Manuel López zapowiedział zakończenie nielegalnej inwigilacji niewinnych ludzi, praktyka ta jest kontynuowana[13].

W październiku 2018 r. w Istambule został zabity reporter Jamal Khashoggi, najprawdopodobniej na rozkaz saudyjskiego księcia koronnego. Khashoggi był znanym krytykiem saudyjskiej rodziny królewskiej i był postrzegany jako zagrożenie dla saudyjskiego dziedzica. Analiza jego telefonu oraz telefonów bliskich mu osób wykazała inwigilację tych osób w miesiącach poprzedzających jego śmierć i następujących po jego zabiciu. Wdowa po J. Khashoggi'm zapowiedziała pozew przeciwko NSO Group[14].

W Azerbejdżanie ujawniono ponad 1000 numerów zainfekowanych Pegasusem. Wśród tych osób byli dziennikarze, jak Khadija Ismailova z Radio Free Europe, która przez kilka lat miała sądowy zakaz opuszczania kraju. W Armenii inwigilacja Pegasusem była stosowana zarówno wobec dziennikarzy, jak i obrońców praw człowieka. W obu tych państwach zauważono szczególną aktywność inwigilacyjną w związku z konfliktem o Nagorny Karabach[15].

W Indiach w sprawie Pegasusa miał już okazję wypowiedzieć się indyjski Sąd Najwyższy (*Supreme Court of India),* który uznał, że inwigilacja oraz podejrzenie, że można być nią objętym, wpływa na jednostkę, która decyduje o tym, czy skorzystać ze swoich praw, czy też nie. Taka sytuacja może doprowadzić do autocenzury. Ma to szczególne znaczenie dla wolności prasy, która jest istotnym filarem demokracji. Taki efekt mrożący dla swobody wypowiedzi stanowi zamach na żywotną rolę prasy jako strażnika i może podważyć zdolność mediów do dostarczania dokładnej i wiarygodnej informacji. Ponieważ sprawa, ze względu na swoją wagę dla praw podstawowych, wymagała dalszego zbadania, indyjski sąd utworzył komitet ekspertów do zbadania, czy Pegasus został użyty przeciwko obywatelom Indii w celu uzyskania dostępu do danych, podsłuchiwania rozmów, uzyskiwania informacji lub w innym celu oraz do ustalenia danych ofiar ataku przy użyciu oprogramowania szpiegowskiego[16].

Po ujawnieniu informacji o stosowaniu inwigilacji Pegasusem wobec osób niezwiązanych z działalnością przestępczą różne instytucje Izraela (Ministerstwo Spraw Zagranicznych, Ministerstwo Sprawiedliwości, Mossad, wywiad wojskowy) zaczęły analizować działania spółki NSO Group[17]. Ostatecznie 65 państw (w tym Polska i Węgry) zostały wykreślone przez Izrael z listy państw, którym można sprzedawać oprogramowanie szpiegowskie, ponieważ zostały uznane za reżimy autokratyczne[18].

Eksperci ONZ wystosowali w 2021 r. apel do wszystkich państw o nałożenie globalnego moratorium na sprzedaż i transfer technologii inwigilacyjnych do czasu opracowania regulacji, które gwarantowałyby zgodność używania tych technologii z prawami człowieka. Zdaniem ekspertów narzędzia szpiegowskie naruszają prawo do swobody wypowiedzi, prawo prywatności, podważają demokrację, pokój i bezpieczeństwo oraz współpracę międzynarodową[19].

W ramach Unii Europejskiej Parlament Europejski powołał komisję śledczą ds. Pegasusa[20]. Komisja opracowała raport, który został przyjęty przez Parlament zaleceniem z 15.06.2023 r.[21], w którym stwierdzono, że omawiana inwigilacja nie spełnia wymogów nakreślonych w orzecznictwie ETPC i TSUE, w związku z czym jest sprzeczna z zasadami zawartymi w art. 2

12 Wysoki Komisarz ds. Praw Człowieka ONZ, *The right…*, A/HRC/51/17; T. Kaldani, Z. Prokopets, *Pegasus…*, s. 7. Szczegółowy opis, jak może dojść do infekcji, oraz sposoby wykrycia infekcji Pegasusem są opisane w: Amnesty International, *Forensic Methodology Report. How to Catch NSO Group's Pegasus,* London 2021.

13 N. Kitroeff, R. Bergman, *How Mexico Became the Biggest User of the World's Most Notorious Spy Tool,* 18.04.2023 r., https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html (dostęp: 11.07.2023 r.); https://www.timesofisrael.com/mexico-continues-to-target-activists-with-israeli-made-pegasus-spyware-ny-times/ (dostęp: 11.07.2023 r.).

14 D. Boffey, *Jamal Khashoggi's wife to sue NSO Group over Pegasus spyware,* 22.09.2022 r., https://www.theguardian.com/world/2022/sep/22/jamal-khashoggis-wife-to-sue-nso-group-over-pegasus-spyware (dostęp: 11.07.2023 r.); S. Kirchgaessner, *Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests,* 18.07.2021 r., https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus (dostęp: 11.07.2023 r.).

15 Amnesty International, *Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict,* 25.05.2023 r., https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/ (dostęp: 11.07.2023 r.).

16 Supreme Court of India, Manohar Lal Sharma vs Union Of India, wyrok z 27.10.2021 r.

17 P. Howell O'Neill, *Israel begins investigation into NSO Group spyware abuse,* MIT Technology Review, 28.07.2021 r., https://www.technologyreview.com/2021/07/28/1030244/israel-investigation-nso-group-pegasus-spyware/ (dostęp: 11.07.2023 r.).

18 K. Sobczak, *Izrael: Polska jako „autokracja" nie kupi Pegasusa,* 26.11.2021 r., https://www.prawo.pl/prawo/pegazus-izralel-nie-sprzeda-polsce,511996.html (dostęp: 11.07.2023 r.).

19 Pod apelem podpisał się specjalny sprawozdawca ONZ ds. promowania i ochrony prawa do swobody wypowiedzi, specjalny sprawozdawca ONZ ds. sytuacji obrońców praw człowieka, specjalny sprawozdawca ONZ ds. praw do pokojowych zgromadzeń i stowarzyszeń, grupa robocza ONZ ds. praw człowieka i korporacji transnarodowych oraz innych przedsiębiorców. Zob. ONZ, *Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech,* 12.08.2021 r., https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening (dostęp: 11.07.2023 r.).

20 Decyzja Parlamentu Europejskiego (UE) 2022/480 z 10.03.2022 r. w sprawie powołania komisji śledczej w celu zbadania stosowania oprogramowania Pegasus i równoważnego oprogramowania szpiegowskiego służącego inwigilacji oraz określenia przedmiotu dochodzenia, a także zakresu odpowiedzialności, składu liczbowego i czasu trwania mandatu komisji (Dz.Urz. UE Nr 98, s. 72).

21 Parlament Europejski zalecenie z 15.06.2023 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, P9_TA(2023)0244 (2023/2500(RSP)).

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[23]. W raporcie tym stwierdzono między innymi, że rząd węgierski osłabił i wyeliminował prawne zabezpieczenia pozwalające osobom inwigilowanym na skorzystanie ze środka kontroli sądowej, zaś Pegasus był stosowany w celach politycznych przeciwko dziennikarzom, politykom opozycji, prawnikom, wykładowcom akademickim, prokuratorom, działaczom społecznym. W przypadku Grecji doszło do szpiegowania greckich członków PE oraz dziennikarzy (łącznie około 300 osób[24]). W Hiszpanii inwigilowano premiera, ministra obrony narodowej, ministra spraw wewnętrznych oraz innych wysokiej rangi urzędników, jak również członków lokalnego rządu Katalonii, członków ruchu walczącego o niezależność Katalonii, członków PE, prawników, wykładowców akademickich oraz przedstawicieli społeczeństwa obywatelskiego. Zauważono też, że takie państwa jak Maroko czy Rwanda inwigilowały m.in. prezydenta Francji, premiera, ministra obrony i ministra spraw wewnętrznych Hiszpanii, premiera Belgii, poprzedniego przewodniczącego Komisji Europejskiej, byłego premiera Włoch.

4. Inwigilacja systemem Pegasus w Polsce

W przypadku Polski mówi się o zastosowaniu Pegasusa co najmniej wobec senatora opozycji Krzysztofa Brejzy w czasie, kiedy ten był szefem sztabu wyborczego jednej z partii opozycyjnych w wyborach parlamentarnych w 2019 r. (co nasuwa skojarzenia z aferą Watergate w Stanach Zjednoczonych), prokurator Ewy Wrzosek, która otwarcie krytykuje niedemokratyczne zmiany w polskim sądownictwie, czy adwokata Romana Giertycha[25]. Tylko senator Brejza był inwigilowany 33 razy, a dodatkowo na jego telefon zostały przez Pegasusa wgrane dane (ok. 1 gigabajt), czyli zmieniono zawartość jego telefonu przez dodanie nowej zawartości. W 2023 r. doszło w prokuraturze do zniszczenia dowodu w postaci płyty DVD, na której zapisano nielegalnie pozyskane dane z telefonu senatora[26].

We wspomnianym w poprzedniej części opracowania zaleceniu Parlamentu Europejskiego z 2023 r. zauważono, że rząd polski, podobnie jak węgierski, osłabił i wyeliminował prawne zabezpieczenia pozwalające osobom inwigilowanym na skorzystanie ze środka kontroli sądowej, zaś Pegasus był stosowany w celach politycznych przeciwko dziennikarzom, politykom opozycji, prawnikom, prokuratorom, działaczom społecznym. W dokumencie tym Polska została wezwana m.in. do tego, żeby Prokurator Generalny wszczął postępowanie w sprawie nadużyć przy wykorzystaniu oprogramowania szpiegowskiego, do przywrócenia wystarczających gwarancji proceduralnych i prawnych, w szczególności efektywnej kontroli *ex ante* i *ex post*, do wprowadzenia prawodawstwa chroniącego obywateli, bez względu na to, jaki podmiot prowadzi inwigilację, do wypełnienia wyroku TK z 30.07.2014 r., K 23/11[27], do dostosowania się do opinii Komisji Weneckiej[28], do dostosowania polskiej praktyki do wymogów nakreślonych w wyroku ETPC w sprawie 47143/06, Zakharov przeciwko Rosji, do dostosowania się do orzecznictwa TSUE i ETPC w przedmiocie niezależności sądownictwa polskiego czy do usunięcia art. 168a Kodeksu postępowania karnego[29] pozwalającego na wykorzystywanie w procesie karnym tzw. owoców zatrutego drzewa.

Ponieważ użycie Pegasusa obejmuje kontrolę i utrwalanie rozmów telefonicznych, powinny się one odbywać zgodnie z warunkami nakreślonymi w art. 237–241 k.p.k. Taką kontrolę może zarządzić sąd na wniosek prokuratora w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa (art. 237 § 1 k.p.k.), w dodatku tylko w przypadku podejrzenia popełnienia określonej kategorii przestępstw (art. 237 § 3 k.p.k.). Jest ona ponadto dopuszczalna jedynie w stosunku do osoby podejrzanej, oskarżonego oraz w stosunku do pokrzywdzonego lub innej osoby, z którą może się kontaktować oskarżony albo która może mieć związek ze sprawcą lub z grożącym przestępstwem (art. 237 § 4 k.p.k.). Ogłoszenie postanowienia osobie, wobec której stosowano kontrolę, podlega odroczeniu najpóźniej do dnia zakończenia postępowania przygotowawczego (art. 239 § 1 i 2 k.p.k.), osobie tej przysługuje prawo do wniesienia zażalenia (art. 240 k.p.k.). Ponadto Pegasus mógł być stosowany w ramach kontroli operacyjnej, którą regulują przepisy ustaw o: Policji[30], Straży Granicznej[31], Agencji Bezpieczeństwa Wewnętrznego[32], Żandarmerii Wojskowej[33], Służbie Kontrwywiadu Wojskowego[34], Centralnym Biurze Antykorupcyjnym[35], a także Krajowej Administracji Skarbo-

22 Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 13.

23 Wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 389. Podobnie: G. Sartor, A. Loreggia, *Wpływ…*, s. 30.

24 G. Sartor, A. Loreggia, *Wpływ...*, s. 37.

25 P. Malinowski, *Roman Giertych i prokurator Ewa Wrzosek byli szpiegowani Pegasusem*, 10.12.2021 r., https://www.rp.pl/kraj/art19215811-roman-giertych-i-prokurator-ewa-wrzosek-byli-szpiegowani-pegasusem (dostęp: 12.07.2023 r.); M. Mikowski, M. Rawicz, P. Śmiłowicz, *Ekspert Citizen Lab: Mamy pewność, senator Brejza był bardzo szeroko monitorowany*, 17.01.2022 r., https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8335172,brejza-inwigilacja-pegasus-senat.html (dostęp: 12.07.2023 r.).

26 Zob. G. Sartor, A. Loreggia, *Wpływ...*, s. 37; D. Drob, *Afera z Pegasusem. Brejza twierdzi, że zniszczono dowody. „Płyta z pierwszego ataku jest złamana”*, 12.05.2023 r., https://wiadomosci.gazeta.pl/wiadomosci/7,114884,29753841,afera-z-pegasusem-brejza-twierdzi-ze-zniszczono-dowody-plyta.html (dostęp: 12.07.2023 r.).

27 LEX nr 1491305. W wyroku tym stwierdzono, że przepisy różnych ustaw polskich pozwalających różnym służbom na inwigilację są niezgodne z polską Konstytucją przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, nie przewidują gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne, nie przewidują zniszczenia danych niemających znaczenia dla prowadzonego postępowania, zezwalają na zachowanie materiałów innych niż zawierające informacje mające znaczenie dla postępowania.

28 Komisja Wenecka, *Opinion no. 839/2016 on the Act of 15 January 2016 amending the Police Act and certain other acts,* 13.06.2013 r., CDL-AD(2016)012.

29 Ustawa z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2022 r. poz. 1375 ze zm.) – dalej k.p.k.

30 Art. 19 ustawy z 6.04.1990 r. o Policji (Dz.U. z 2023 r. poz. 171 ze zm.).

31 Art. 9e ustawy z 12.10.1990 r. o Straży Granicznej (Dz.U. z 2023 r. poz. 1080 ze zm.).

32 Art. 27 ustawy z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2023 r. poz. 1136 ze zm.).

33 Art. 31 ustawy z 24.08.2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz.U. z 2023 r. poz. 1266 ze zm.).

34 Art. 31 ustawy z 9.06.2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U. z 2023 r. poz. 81 ze zm.).

35 Art. 17 ustawy z 9.06.2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2022 r. poz. 1900 ze zm.).

wej[36]. Stosowanie takiej kontroli jest uzależnione od zgody właściwego sądu okręgowego, ma ona ograniczenia czasowe (3 miesiące do maksymalnie 12 miesięcy)[37]. W przypadku kontroli operacyjnej osoba, wobec której stosowano inwigilację, nie jest o niej informowana, może się o niej dowiedzieć jedynie przy okazji końcowego zaznajomienia z aktami postępowania przygotowawczego (art. 321 k.p.k.), nie ma więc ona jakiejkolwiek możliwości zainicjowania kontroli *ex post* postanowień o zastosowaniu wobec niej takiego rodzaju inwigilacji.

Jak wynika z powyższego, kontrola inwigilacji *ex post* jest ograniczona wyłącznie do przypadków kontroli i utrwalania rozmów telefonicznych (art. 240 k.p.k.), nie istnieje w przypadku inwigilacji prowadzonej w innym zakresie. Natomiast kontrola *ex ante* bywa iluzoryczna, ponieważ wnioski do sądów często są anonimizowane, obejmują kryptonim sprawy, a sąd nie ma możliwości weryfikacji, wobec kogo *de facto* taka inwigilacja ma być prowadzona[38]. W Polsce nie ma takich mechanizmów, jak te istniejące w Zjednoczonym Królestwie i Szwecji, które pozwalałyby osobom podejrzewającym, że były inwigilowanie, na wszczęcie procedury sądowej, która miałaby na celu zbadanie tej okoliczności.

Problem w przypadku użycia oprogramowania Pegasus w Polsce leży jednak nie tylko w ograniczonym zakresie kontroli sądowej wykonywanej *ex ante*. Brak jest obecnie informacji, czy kontrola wobec wcześniej wskazanych osób była w ogóle zatwierdzana przez sąd, a jeżeli była, to na podstawie jakich informacji przekazanych przez służby. Nic nie wiadomo o jakimkolwiek postępowaniu karnym, w ramach którego przeciwko tym osobom można byłoby zastosować kontrolę operacyjną, nie wiadomo więc, czy była ona dopuszczalna *ratione personae* i *ratione materiae*[39]. Niewątpliwe natomiast jest, że materiały uzyskane z telefonu senatora Brejzy zostały w toku kampanii wyborczej zmodyfikowane i zmanipulowane, a następnie pokazane widzom TVP[40], czyli użycie tych materiałów miało *stricte* polityczny kontekst, a nie prawnokarny.

Jeżeli ta kontrola nie była legalna, bo przeprowadzona poza proceduralnymi ramami zatwierdzania zastosowania takiej kontroli przez sądy, to wszelkie materiały zdobyte w jej toku stają się automatycznie dowodami, o którym mowa w art. 168a k.p.k. W tym kontekście należy zauważyć, że w świetle polskiego orzecznictwa nie jest do końca jasne, czy takie dowody byłyby dopuszczone. Jak wskazał Sąd Najwyższy w wyroku z 2.02.2022 r., I KK 4/22[41], „art. 168a k.p.k. nie może stanowić podstawy prawnej przeprowadzenia dowodu uzyskanego z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, jedynie wówczas, gdy przeprowadzenie takiego dowodu czyniłoby proces nierzetelnym w rozumieniu art. 6 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności". Z kolei w wyroku z 3.11.2021 r., III KK 373/20[42], SN uznał, że „decyzja o uznaniu dowodu za niedopuszczalny (art. 170 § 1 pkt 1 w zw. z art. 168a k.p.k.), z uwagi na uzyskanie go z naruszeniem prawa, musi być rezultatem skrupulatnego ważenia pozostających w konflikcie wartości, jakimi są: z jednej strony prawda materialna oraz potrzeba urzeczywistnienia zasady trafnej reakcji karnej (art. 2 § 1 pkt 1 i § 2 k.p.k.), a z drugiej strony konieczność przestrzegania konstytucyjnej zasady legalizmu, a więc wymogu działania organów procesowych na podstawie i w granicach prawa (art. 7 Konstytucji RP) oraz pozostałych reguł rzetelnego procesu, co jest niezbędne do osiągnięcia stanu sprawiedliwości proceduralnej".

Jeżeli jednak organy ścigania z premedytacją naruszają przepisy chroniące jednostki przed nieuzasadnioną ingerencją ze strony władz państwowych, jak przepisy o konieczności uzyskania zgody sądowej, to nie sposób wyobrazić sobie sytuację, w której tak przeprowadzony proces byłby rzetelny. Należy zgodzić się z E. Plebanek, że art. 168a k.p.k. mógłby co najwyżej służyć do zaakceptowania dowodów zdobytych nielegalnie przez podmioty prywatne, gdyż w tym przypadku możliwe jest pogodzenie przeprowadzenia takiego dowodu z wymogami konstytucyjnymi, natomiast całkowicie powinny zostać wykluczone ze stosowania tego przepisu dowody uzyskane nielegalnie przez instytucje i funkcjonariuszy publicznych[43].

Załóżmy jednak, że służby złożyły stosowne wnioski do sądów i zostały one uwzględnione. W takiej sytuacji nie można tracić z pola widzenia faktu wgrania na telefon senatora Brejzy około 1 gigabajt danych. Wartość dowodowa materiału uzyskanego przy pomocy programu, który pozwala dowolnie zmieniać zawartość telefonu przez wgrywanie lub usuwanie danych, jest *de facto* żadna, chociaż obecnie można sobie wyobrazić prawne dopuszczenie takiego dowodu na skutek zastosowania art. 168a k.p.k. Rację ma więc Rzecznik Praw Obywatelskich, że z tego właśnie powodu użycie Pegasusa jest w ogóle nie do pogodzenia z polskimi wymogami konstytucyjnymi[44].

Wykorzystanie systemu Pegasus w Polsce było również sprzeczne z wymogami konwencyjnymi, opisanymi w pierwszej części niniejszego opracowania. Mając je na względzie, należy skonstatować, że nie wiadomo, jaka była natura rzekomych przestępstw, w przypadku których sięgnięto po Pegasusa, coraz więcej wskazuje na to, że wykorzystano to oprogramowanie bez związku z jakimkolwiek przestępstwem. Osoby inwigilowane nie były podejrzanymi, oskarżonymi, pokrzywdzonymi ani innymi osobami, z którymi mógłby kontaktować się sprawca przestępstwa, byli to przedstawiciele opozycji oraz prawnicy sprzeciwiający się niedemokratycznym zmianom w sądownictwie. Nie wiadomo, jakie były czasowe ramy owej inwigilacji, była ona natomiast intensywna i wielokrotna. Brak jest informacji o tym, jak zostały zabezpieczone dane przy przekazywaniu ich innym podmiotom, skoro część z nich w wersji zmodyfikowanej została opublikowana w TVP. Najprawdopodobniej nie było również kontroli *ex ante* wniosków o zastosowanie

36 Art. 122 ustawy z 16.11.2016 r. o Krajowej Administracji Skarbowej (Dz.U. z 2023 r. poz. 615 ze zm.).

37 Szerzej na ten temat: M. Matusiak-Frącczak, *Ochrona*..., s. 314–318.

38 G.J. Leśniak, *Tajemnica zawodowa nie przeszkadza służbom w podsłuchiwaniu*, 23.11.2018 r., https://www.prawo.pl/prawnicy-sady/tajemnica-zawodowa-sluzby-naruszaja-mimo-zakazu,332166.html (dostęp: 12.07.2023 r.); M. Matusiak-Frącczak, *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce,* „Palestra" 2022/7–8, s. 14–15.

39 M. Matusiak-Frącczak, *Kontrola*..., s. 16.

40 P. Szostak, *Inwigilacja Pegasusem i spreparowane SMSy Brejzy w TVP? Operacja dezinformacyjna jak z rosyjskiego podręcznika,* 29.12.2021 r., https://wyborcza.biz/biznes/7,177150,27954283,inwigilacja-pegasusem-i-spreparowane-sms-y-brejzy-w-tvp-operacja.html?disableRedirects=true (dostęp: 12.07.2023 r.).

41 LEX nr 3397391.

42 LEX nr 3306162.

43 E. Plebanek, *Kilka uwag na temat znaczenia przepisu art. 168a k.p.k. dla dopuszczalności wykorzystania w postępowaniu sądowym dowodu pozyskanego z naruszeniem rygorów ustawowych*, „Palestra" 2018/10, s. 37.

44 M. Domagalski, *RPO: Polskie sądy nie mogą wyrażać zgody na Pegasusa*, 9.01.2022 r., https://www.rp.pl/prawo-dla-ciebie/art19265491-rpo-polskie-sady-nie-moga-wyrazac-zgody-na-pegasusa (dostęp: 12.07.2023 r.).

Pegasusa, z drugiej strony wiadomo, że pokrzywdzonym przez tę inwigilację osobom nie przysługiwał żaden środek kontroli sądowej i nigdy nie otrzymały one postanowienia zarządzającego taką inwigilację. Po 30 latach stosowania Konwencji w Polsce mamy więc do czynienia z przypadkiem, kiedy reguły konwencyjne dotyczące inwigilacji zostały całkowicie zdeptane.

5. Podsumowanie

W przypadku inwigilacji tak inwazyjnym oprogramowaniem, jakim jest Pegasus, aktualne pozostaje pytanie *quis custodiet ipsos custodes*. Ponieważ Pegasus jest w stanie zainfekować telefon bez żadnej akcji ze strony użytkownika urządzenia, jednostki są całkowicie bezbronne wobec zastosowania tego programu. Niewątpliwie, może być on bardzo przydatny w zwalczaniu przestępczości zorganizowanej czy terroryzmu. Z drugiej strony, jak pokazały wydarzenia ostatnich lat, może być wykorzystywany przez autorytarne władze do nielegalnej inwigilacji przeciwników politycznych, dziennikarzy, prawników, członków społeczeństwa obywatelskiego.

Europejski Trybunał Praw Człowieka nakreślił prawne przesłanki legalności inwigilacji. Dotyczą one treści prawa, które zezwala na inwigilację i powinno ściśle określać kryteria, kiedy, jak długo i przeciwko komu kontrola może być stosowana. Ponadto powinny istnieć mechanizmy skutecznej kontroli inwigilacji *ex ante* i *ex post*. Sprawa Pegasusa pokazała w soczewce, jak wygląda przestrzeganie wymogów konwencyjnych po 30 latach od przystąpienia Polski do EKPC – polskie służby ignorują te wymogi całkowicie, naruszając prawa podstawowe, jak prawo do prywatności, prawo do sprawiedliwego procesu czy prawo do swobody wypowiedzi. Przede wszystkim zauważalny jest brak mechanizmów skutecznej kontroli sądowej, dlatego zasadne wydawałoby się utworzenie w Polsce specjalnych sądów, na wzór brytyjskiego i szwedzkiego, które badałyby sprawy inwigilacji. Ponadto, biorąc pod uwagę, że Pegasus pozwala wgrywać dane na telefon użytkownika, użycie akurat tego oprogramowania powinno zostać w Polsce zakazane.

Abstract

dr Magdalena Matusiak-Frącczak

The author is an assistant professor at the Department of European Constitutional Law, Faculty of Law and Administration, University of Lodz, Poland (ORCID: https://orcid.org/0000-0002-6736-8008).

ECHR Standards of Legal Surveillance and the Use of the Pegasus System in Poland

Keywords: *surveillance, Pegasus, spyware, right to privacy, right to a fair trial, freedom of expression*

In 2021, it was revealed that the Israeli spyware Pegasus was applied worldwide. However, it was not only used to combat organized crime, but also to surveil political opposition members, journalists, lawyers, or members of democratic society. The article describes the conditions of legal invigilation stemming from the European Convention for the Protection of Human Rights and Fundamental Freedoms. Its main aim is to assess whether and to what extent the Polish practice of using Pegasus spyware was contrary to these conditions.

Bibliografia/References

Boffey D., *Jamal Khashoggi's wife to sue NSO Group over Pegasus spyware,* 22.09.2022 r., https://www.theguardian.com/world/2022/sep/22/jamal-khashoggis-wife-to-sue-nso-group-over-pegasus-spyware (dostęp: 11.07.2023 r.).

Domagalski M., *RPO: Polskie sądy nie mogą wyrażać zgody na Pegasusa*, 9.01.2022 r., https://www.rp.pl/prawo-dla-ciebie/art19265491-rpo-polskie-sady-nie-moga-wyrazac-zgody-na-pegasusa (dostęp: 12.07.2023 r.).

Drob D., *Afera z Pegasusem. Brejza twierdzi, że zniszczono dowody. „Płyta z pierwszego ataku jest złamana",* 12.05.2023 r., https://wiadomosci.gazeta.pl/wiadomosci/7,114884,29753841,afera-z-pegasusem-brejza-twierdzi-ze-zniszczono-dowody-plyta.html (dostęp: 12.07.2023 r.).

Howell O'Neill P., *Israel begins investigation into NSO Group spyware abuse,* 28.07.2021 r., https://www.technologyreview.com/2021/07/28/1030244/israel-investigation-nso-group-pegasus-spyware/ (dostęp: 11.07.2023 r.).

Kaldani T., Prokopets Z., *Pegasus spyware and its impact on human rights,* Strasbourg 2022.

Kirchgaessner S., *Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests,* 18.07.2021 r., https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus (dostęp: 11.07.2023 r.).

Kitroeff N., Bergman R., *How Mexico Became the Biggest User of the World's Most Notorious Spy Tool,* 18.04.2023 r., https://www.nytimes.com/2023/04/18/world/americas/pegasus-spyware-mexico.html (dostęp: 11.07.2023 r.).

Leśniak G.J., *Tajemnica zawodowa nie przeszkadza służbom w podsłuchiwaniu*, 23.11.2018 r., https://www.prawo.pl/prawnicy-sady/tajemnica-zawodowa-sluzby-naruszaja-mimo-zakazu,332166.html (dostęp: 12.07.2023 r.).

Malinowski P., *Roman Giertych i prokurator Ewa Wrzosek byli szpiegowani Pegasusem*, 10.12.2021 r., https://www.rp.pl/kraj/art19215811-roman-giertych-i-prokurator-ewa-wrzosek-byli-szpiegowani-pegasusem (dostęp: 12.07.2023 r.).

Matusiak-Frącczak M., *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce,* „Palestra" 2022/7–8.

Matusiak-Frącczak M., *Ochrona poufności komunikacji klienta z adwokatem. Standardy międzynarodowe, standard Unii Europejskiej oraz standardy krajowe wybranych państw a prawo polskie,* Warszawa 2023.

Mikowski M., Rawicz M., Śmiłowicz P., *Ekspert Citizen Lab: Mamy pewność, senator Brejza był bardzo szeroko monitorowany*, 17.01.2022 r., https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8335172,brejza-inwigilacja-pegasus-senat.html (dostęp: 12.07.2023 r.).

Plebanek E., *Kilka uwag na temat znaczenia przepisu art. 168a k.p.k. dla dopuszczalności wykorzystania w postępowaniu sądowym dowodu pozyskanego z naruszeniem rygorów ustawowych*, „Palestra" 2018/10.

Richard L., Rigaud S., *Pegasus. The Story of the World's Most Dangerous Spyware,* London 2023.

Sartor G., Loreggia A., *Wpływ oprogramowania Pegasus na prawa podstawowe i procesy demokratyczne,* Bruksela 2023.

Sobczak K., *Izrael: Polska jako „autokracja" nie kupi Pegasusa,* 26.11.2021 r., https://www.prawo.pl/prawo/pegazus-izralel-nie-sprzeda-polsce,511996.html (dostęp: 11.07.2023 r.).

Szostak P., *Inwigilacja Pegasusem i spreparowane SMSy Brejzy w TVP? Operacja dezinformacyjna jak z rosyjskiego podręcznika*, 29.12.2021 r., https://wyborcza.biz/biznes/7,177150,27954283,inwigilacja-pegasusem-i-spreparowane-sms-y-brejzy-w-tvp-operacja.html?disableRedirects=true (dostęp: 12.07.2023 r.).
Wolska A., Kucharczyk M., *Pegasus: Jak działa oprogramowanie do szpiegowania?*, 24.12.2021 r., https://www.euractiv.pl/section/gospodarka/news/pegasus-giertych-wrzosek-brejza-macron-izrael-usa-polska-wegry-podsluch-cyberatak-pis-ziobrocba-sluzby/ (dostęp: 11.07.2023 r.).
Woźniak M.R., *Pegasus: gorzej niż podsłuch. Umożliwia podrzucanie dowodów. Giertych, Wrzosek, Brejza, kto jeszcze...*, 26.12.2021 r., https://oko.press/pegasus-gorzej-niz-podsluch-potrafi-tez-podrzucac-dowody/ (dostęp: 11.07.2023 r.).