Pojęcia kluczowe: *Pegasus, system szpiegujący, tajemnica adwokacka, tajemnica obrończa, tajemnica zawodowa, inwigilacja, podsłuch*

Miłosz Kościelniak-Marszał

Zagrożenia dla tajemnicy adwokackiej i obrończej wynikające z funkcjonalności współczesnych systemów szpiegujących

Abstrakt

Systemy szpiegujące powstały w celu aktywnej pracy wywiadowczej. Ich funkcjonalność pozwala na implementację danych do urządzenia, modyfikowanie zapisanej w nim zawartości, korzystanie z kont społecznościowych, a nawet totalną inwigilację użytkownika przy wykorzystaniu zintegrowanego mikrofonu i kamery. Z uwagi na charakterystykę takiego oprogramowania, potrzebę zdobywania informacji oraz postęp technologiczny, związanych z tym zagrożeń naruszenia prawem chronionych tajemnic nie da się skutecznie usunąć za pomocą regulacji normatywnych. Do czasu ewentualnego pojawienia się narzędzi blokujących działanie takich programów jedynym rozwiązaniem, które może zmniejszyć wspomniane ryzyko, pozostaje świadome korzystanie ze smartfonów i ograniczenie ich użytkowania w miejscach lub sytuacjach, w których inwigilacja przy ich wykorzystaniu niosłaby szczególne niebezpieczeństwo przełamania tajemnicy.

Smartfony są dziś przedmiotami codziennego użytku, z którymi nie rozstajemy się przez większość czasu. Urządzenia te towarzyszą nam w niemal każdej sytuacji, od wykonywania pracy zawodowej po czynności higieniczne w toalecie. Smartfon jest pierwszym sprzętem, który dotykamy zaraz po zbudzeniu się, i ostatnim, który trzymamy przed zaśnięciem. W ciągu dnia smartfony spoczywają na stole sędziowskim podczas narady nad treścią orzeczenia[1], a w kancelarii adwokackiej leżą pod ręką podczas rozmów z klientami i ustalania strategii obrończej. Dla praktykującego prawnika są źródłem dostępu do poczty elektronicznej, aktualnych przepisów i zdigitalizowanych akt. Przyzwyczailiśmy się do ich obecności do tego stopnia, że czujemy się wręcz nieswojo, gdy okaże się, że smartfona zapomnieliśmy ze sobą zabrać. Niestety,

1 K. Żaczkiewicz-Zborska, *Sędzia Morawiec: Byliśmy niewygodni dla władzy*, https://www.prawo.pl/prawnicy-sady/sedzia-morawiec-bylismy-niewygodni-dla-wladzy,530041.html?utm_source=Eloqua&utm_content=WKPL_MSG_NSL_NRPiA-20-11-24_EML&utm_campaign=WKPL_MSG_NSL_NRPiA-20-11-24_OTH%2FWKC0120011_IEM010&utm_econtactid=CWOLT000027297272&utm_medium=email_newsletter&utm_crmid (dostęp: 26.11.2024 r.).

DOI: 10.54383/0031-0344.2025.06.8

informacje na temat funkcjonalności systemów szpiegujących, które ujawniono podczas prac sejmowej Komisji śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania PEGASUS przez członków rady ministrów, służby specjalne, policję, organy kontroli skarbowej oraz celnoskarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16.11.2015 r. do dnia 20.11.2023 r., uświadamiają związane z tą praktyką zagrożenia dla tajemnicy adwokackiej i obrończej.

Przedmiot oraz zakres „tajemnicy adwokackiej" wyznaczają przepisy ustawy o adwokaturze oraz Kodeksu etyki adwokackiej. W rozumieniu potocznym „tajemnica" oznacza pewien sekret, charakteryzujący się tajnością i tym, że nie powinien być rozgłaszany, nie powinien wyjść na jaw. Rozumienie to jest właściwie tożsame z rozumieniem tajemnicy w języku prawniczym, w którym używane są również terminy „tajemnica zawodowa" oraz „tajemnica obrończa". Ten pierwszy jest szerszy zakresowo, gdyż prócz adwokatów dotyczy także m.in. radców prawnych, notariuszy, dziennikarzy oraz lekarzy. Tajemnica zawodowa ma charakter dobra korporacyjnego, ustanowionego normatywnie dla ochrony stosunku zaufania między mandantem a przedstawicielem zawodu zaufania publicznego[2]. Drugi termin ma natomiast zakres znacznie węższy, gdyż ograniczony do sytuacji pełnienia funkcji obrońcy w postępowaniu karnym. Tajemnica obrończa stanowi jednak najsilniej chroniony rodzaj tajemnicy. W przeciwieństwie do tajemnicy zawodowej ma bowiem charakter bezwzględny, gdyż żaden organ procesowy nie może jej uchylić, zaś sam obrońca nie może się zwolnić od jej zachowania[3]. Uzasadnienia dla tajemnicy obrończej należy szukać w istocie **stosunku łączącego obrońcę prowadzącego sprawę lub udzielającego porady prawnej z klientem. Jak trafnie zauważa się w literaturze przedmiotu – możliwość procesowej penetracji tego stosunku prowadziłaby do zachwiania zaufania oskarżonych do ich obrońców, wobec których muszą najczęściej przyjąć postawę otwartą, by uzyskać adekwatną poradę prawną lub by optymalnie przygotować stanowisko w procesie i jego argumentację[4].**

Dla zapewnienia utrzymania w tajemnicy uzyskanych informacji, normy deontologiczne nakładają na adwokatów szereg obowiązków. Zgodnie z treścią § 19 Zbioru Zasad Etyki Adwokackiej i Godności Zawodu adwokat zobowiązany jest zachować w tajemnicy oraz zabezpieczyć przed ujawnieniem lub niepożądanym wykorzystaniem wszystko, o czym dowiedział się w związku z wykonywaniem obowiązków zawodowych.

2 Por. Stanowisko Komisji Etyki przy NRA w sprawie odpowiedzi na pytanie: Czy w związku ze zgłoszeniem przez adwokata szkody powstałej na skutek błędu w wykonywaniu czynności pełnomocnika procesowego adwokat jest uprawniony z punktu widzenia obowiązku zachowania tajemnicy adwokackiej przekazać towarzystwu ubezpieczeniowemu dokumentację związaną ze sprawą?, niepubl.z

3 C. Kulesza, *10.5.2.3. Tajemnica obrończa* (w:) *System Prawa Karnego Procesowego*, t. 6, *Strony i inni uczestnicy postępowania karnego*, red. P. Hofmański, C. Kulesza, Warszawa 2016.

4 P. Hofmański, E. Sadzik, K. Zgryzek, *Kodeks postępowania karnego. Komentarz*, Warszawa, 2004, t. 1, s. 745–746.

 DOI: 10.54383/0031-0344.2025.06.8

Musi zobowiązać swoich współpracowników i personel oraz wszelkie osoby zatrudnione przez niego podczas wykonywania działalności zawodowej do przestrzegania obowiązku zachowania tajemnicy zawodowej, a posługując się w pracy zawodowej komputerem lub innymi środkami elektronicznego utrwalania danych, obowiązany jest stosować oprogramowanie i inne środki zabezpieczające dane przed ich niepowołanym ujawnieniem. Także przekazywanie informacji objętych tajemnicą zawodową za pomocą elektronicznych i podobnych środków przekazu wymaga zachowania szczególnej ostrożności i uprzedzenia klienta o ryzyku związanym z zachowaniem poufności przy wykorzystaniu tych środków.

Wymóg czuwania nad zachowaniem w tajemnicy zdobytej wiedzy nabiera jednak zupełnie nowego znaczenia wobec możliwości kontroli totalnej, którą oferują współczesne systemy szpiegujące, ze słynnym „Pegasusem" na czele. Kluczowe w tym zakresie informacje ujawniło posiedzenie wspomnianej komisji sejmowej, jakie odbyło się w dniu 15.03.2024 r., podczas którego przesłuchiwany był Jerzy Kosiński, dyrektor Morskiego Centrum Cyberbezpieczeństwa Wydziału Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej. Świadek, z ramienia polskich władz, w kwietniu 2019 r. brał udział w prezentacji przeprowadzonej przez przedstawicieli NSO Gropu w Izraelu. Spółka ta sprzedawała państwom oprogramowanie, które miało służyć do zwalczania najpoważniejszych przestępstw, zwłaszcza terroryzmu. W gronie jego nabywców znalazło się 16 państw Unii Europejskiej[5], a jak wynika ze śledztwa, które w 2021 r. przeprowadzili dziennikarze Forbidden Stories oraz Amnesty International, prawdopodobnie także: Azerbejdżan, Bahrajn, Kazachstan, Meksyk, Maroko, Rwanda, Arabia Saudyjska, Togo, Indie i Zjednoczone Emiraty Arabskie[6].

Świadek podał, że zaprezentowany system „Pegasus" okazał się narzędziem informatycznym o złożonej funkcjonalności przeznaczonym do instalacji na systemach iOS i Android. Pierwszy moduł pozwalał na przejęcie kontroli nad urządzeniem mobilnym w sposób niesygnalizujący właścicielowi, że kontrola została przez niego utracona. Drugi umożliwiał zarządzanie tym, co znajduje się w zasobach telefonu. Trzeci przekazywał informacje z przejętego urządzenia na serwer, gdzie były przechowywane. Natomiast czwarty pozwalał na zarządzanie przejętym telefonem[7]. Podczas spotkania uczestnicy otrzymali możliwość nawiązywania połączeń za pośrednictwem przejętych urządzeń oraz prowadzenia przez nie rozmów. Wykonali też próby dotyczące

5 S. Palczewski, *To już potwierdzone: 14 państw UE posiada Pegasusa. Dwóm odebrano licencję, Cyberdefence24 z 2.08.2024*, https://cyberdefence24.pl/polityka-i-prawo/to-juz-potwierdzone-14-panstw-posiada-pegasusa-dwom-krajom-odebrano-licencje (dostęp: 11.02.2025 r.).

6 https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/, dostęp: 11.02.2025 r.

7 Pełny zapis przebiegu posiedzenia Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania PEGASUS przez członków rady ministrów, służby specjalne, policję, organy kontroli skarbowej oraz celnoskarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16.11.2015 r. do dnia 20.11.2023 r. (nr 4) z dnia 15.03.2024 r., Kancelaria Sejmu, Biuro Komisji Sejmowych, s. 7, https://orka.sejm.gov.pl/zapisy10.nsf/0/F2D9E8013C0D37E5C1258AEE002C1F7F/%24File/0002610.pdf (dostęp: 26.04.2024 r.).

włączania mikrofonu i nasłuchiwania otoczenia, jak również mieli bezpośredni dostęp do kamer, które w każdym momencie mogli uruchomić i zdalnie robić za ich pomocą zdjęcia, a więc prowadzić totalną inwigilację. Ponieważ telefon przejmowany był praktycznie kompletnie, można było korzystać ze wszystkich jego funkcjonalności, i z użyciem narzędzi, które zostały zainstalowane na telefonie, podszywać się pod jego właściciela, aby np. w jego imieniu funkcjonować na portalach społecznościowych, na komunikatorach, w systemach bankowości itd.[8] Jeśli telefon komórkowy był zsynchronizowany z innymi urządzeniami mobilnymi typu tablet, laptop czy smartwatch, „Pegasus" dawał możliwość uzyskania danych również z tych urządzeń, a więc wglądu we wszystkie zapisane na nich pliki tekstowe, zdjęcia, filmy itd. Jak wynika ze słów Kosińskiego – operator „Pegasusa" miał w takiej sytuacji więcej możliwości niż właściwy użytkownik urządzenia. W szczególności mógł skopiować całą bazę danych, a następnie odczytać informacje skasowane przez użytkownika, które dla tamtego nie były już dostępne[9]. Mógł także zmodyfikować treści zapisane w pamięci urządzenia, np. zmieniając treść znajdujących się tam wiadomości tekstowych[10].

W tym miejscu należy zaznaczyć, że określenie „Pegasus" jest nazwą własną konkretnego systemu. Nie jest to jedyny dostępny program tego typu. Polska Prokuratura Krajowa równolegle dysponowała oprogramowaniem o nazwie „Hermes", które oficjalnie miało służyć do zaawansowanego zbierania i analizy danych ze źródeł internetowych, ale jego wszystkie funkcjonalności nie zostały dotąd zbadane[11]. Wiele innych państw wdrożyło różne zaawansowane technicznie metody pracy operacyjnej. Wyspecjalizowany system szpiegujący dla Interpolu oferowała firma niemiecka[12]. Włoskie służby specjalne w 2019 r. wykorzystywały oprogramowanie szpiegowskie (*spyware*) „Hermit"[13]. Amerykańska agencja ds. leków ma korzystać m.in. z opracowanego przez izraelską firmę Paragon Solutions systemu „Graphite", który potrafi przełamywać zabezpieczenia współczesnych smartfonów i omijać szyfrowanie w komunikatorach takich jak WhatsApp czy Signal, wyciągając również dane z chmury[14]. Pod koniec stycznia br. należąca do Mety firma WhatsApp poinformowała, że zdołała wykryć i powstrzymać działanie oprogramowania Paragon, przez które poszkodowanych zostało prawie 100 osób usługi, w tym niezależni dziennikarze i przedstawiciele

8 Pełny zapis przebiegu posiedzenia Komisji Śledczej..., s. 50.

9 Pełny zapis przebiegu posiedzenia Komisji Śledczej..., s. 9–10, 40.

10 Pełny zapis przebiegu posiedzenia Komisji Śledczej..., s. 13.

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

12 Pełny zapis przebiegu posiedzenia Komisji Śledczej..., s. 14.

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

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

 DOI: 10.54383/0031-0344.2025.06.8

społeczeństwa obywatelskiego, których prywatność mogła zostać naruszona[15]. Podczas ataków wykorzystano złośliwe pliki PDF, które rozsyłane były za pośrednictwem publicznych grup WhatsApp. Ataki zostały wykryte w grudniu, ale nie wiadomo, jak długo użytkownicy byli na nie narażeni[16].

Mimo rozwoju technologii szpiegowskch, przepisy k.p.k. z 1997 r. nadal nie przewidują regulacji, które *expressis verbis* zabraniałyby kontroli i utrwalania rozmów z obrońcą lub adwokatem czy radcą działającym na podstawie art. 245 k.p.k. Kwestie związane z kontrolą i utrwalaniem rozmów telefonicznych, innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną, regulują kompleksowo z jednej strony przepisy zgrupowane w rozdziale 26 k.p.k., zatytułowanym „Kontrola i utrwalanie rozmów", z drugiej zaś przepisy szczególne zawarte w ustawach dotyczących organów ochrony bezpieczeństwa i porządku prawnego, określających zasady tzw. podsłuchu pozaprocesowego. Otwierający wskazany rozdział 26 k.p.k. przepis art. 237 § 1 k.p.k. stwarza podstawy do zarządzenia przez sąd na wniosek prokuratora, po wszczęciu postępowania karnego, kontroli i utrwalania treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa. Przepis art. 237 § 3 k.p.k. zawiera katalog przestępstw, w przypadku których możliwe jest zarządzenie kontroli i utrwalania rozmów. Regulację dotyczącą kontroli i utrwalania rozmów telefonicznych zawartą w art. 237–240 stosuje się na mocy art. 241 k.p.k. odpowiednio do kontroli i utrwalania innych niż telefoniczne rozmów oraz przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną. Wedle treści art. 237 § 4 k.p.k.: „kontrola i utrwalanie treści rozmów telefonicznych są dopuszczalne 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". Treść art. 237 § 4 k.p.k. nie zawiera żadnego ograniczenia kręgu podmiotów, co do których możliwe jest zainstalowanie podsłuchu – jest on praktycznie nieograniczony i, z punktu widzenia wskazanego przepisu, obejmuje także obrońcę oraz jego mandanta[17].

W literaturze przedmiotu panuje zgoda co do niemożności wykorzystywania zdobytych w ten sposób materiałów[18]. Dominujące stanowisko wychodzi z założenia, że – podobnie jak w przypadku art. 225 § 3 k.p.k. – regulacje zawarte w rozdziale 26

15 S. Kirchgaessner, *WhatsApp says journalists and civil society members were targets of Israeli spyware*, „The Guardian" z 31.01.2025 r., https://www.theguardian.com/technology/2025/jan/31/whatsapp-israel-spyware (dostęp: 11.02.2025 r.).

16 J. Szczepaniak, *WhatsApp miał swojego Pegasusa?*, https://android.com.pl/tech/878887-whatsapp-inwigilacja-paragon-pegasus/ (dostęp: 11.02.2025 r.).

17 P. Kardas, *Ochrona tajemnicy obrończej. Kilka uwag o dopuszczalności kontroli i utrwalania treści rozmów oraz przekazów informacji realizowanych przy użyciu środków technicznych pomiędzy obrońcą a mandantem*, „Czasopismo Prawa Karnego i Nauk Penalnych", Rok XV: 2011, z. 4, s. 11.

18 J. Machlańska, *Dowód z podsłuchu procesowego a ochrona tajemnicy obrończej*, „Palestra" 2016/1–2, s. 77–78 i podane tam poglądy doktryny.

k.p.k. są uzupełniane poprzez zakazy dowodowe, a więc wykorzystanie takich materiałów wiązałoby się z obejściem art. 178 pkt 1 k.p.k. Natomiast drugi pogląd odwołuje się do treści art. 226 k.p.k. (w zw. z art. 178 § 1 pkt 1 k.p.k.) stanowiącego w zd. 1, że w kwestii wykorzystania dokumentów zawierających informacje niejawne lub tajemnicę zawodową, jako dowodów w postępowaniu karnym, stosuje się odpowiednio zakazy i ograniczenia określone w art. 178–181 k.p.k. W oparciu o poglądy D. Szumiło-Kulczyckiej[19] przyjmuje się, że mimo wąskiego ujęcia treści art. 178 w zw. z art. 226 k.p.k. wynika z niego niedopuszczalność wykorzystywania w procesie uzyskanych w następstwie kontroli operacyjnej lub podsłuchu procesowego nagrań obejmujących rozmowy pomiędzy sprawcą a adwokatem lub obecnie także radcą prawnym[20].

Trzeba jednak zauważyć, że niemożność procesowego użytku ze zdobytej informacji nie jest tym samym co wprost wyrażony zakaz prowadzenia inwigilacji. Dodatkowo brak w polskim porządku prawnym jednoznacznej regulacji kwestii tzw. owoców zatrutego drzewa może skłaniać do pozyskiwania wiedzy przydatnej operacyjnie, choćby nawet bez możliwości jej późniejszego bezpośredniego wykorzystania w procesie karnym. Na tym tle interesujące stanowisko przedstawił P. Kosmaty, wywodząc, że choć przepisy rozdziału 26 k.p.k. nie przewidują uregulowań, które pozwalałyby na wyłączenie określonych osób z prowadzenia względem nich podsłuchu, to z kręgu podmiotów, wobec których może być stosowany podsłuch telefoniczny, wyłączyć należy osoby, co do których istnieje bezwzględny zakaz dowodowy przesłuchania ich w charakterze świadka (art. 178 k.p.k.). Zatem nie wolno kontrolować obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 § 1 k.p.k. co do faktów, o których dowiedział się, udzielając porady prawnej lub prowadząc sprawę[21]. Pogląd ten koreluje z wcześniejszymi wypowiedziami przedstawicieli polskiej doktryny[22] i orzecznictwa[23]. Warte odnotowania jest także stanowisko Rzecznika Praw Obywatelskich, który uznał, że kontrola treści rozmów, kontaktów podejrzanego z jego obrońcą dokonywana przez organy władzy publicznej – poza wyjątkami przewidzianymi w § 2 i 3 art. 73 k.p.k. – jest niedopuszczalna i nielegalna na poziomie norm konstytucyjnych, jak i rozwiązań ustawowych zawartych w Kodeksie

19 D. Szumiło-Kulczycka, *Tajemnica obrończa a podsłuch procesowy i kontrola operacyjna*, „Palestra" 2013/1–2, s. 90–100.

20 K. Eichstaedt (w:) D. Świecki (red.), B. Augustyniak, K. Eichstaedt, M. Kurowski, *Kodeks postępowania karnego*, Warszawa 2015, t. 1, s. 739.

21 P. Kosmaty, *Wybrane problemy procesowej kontroli i utrwalania rozmów*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2023/2 (50), s. 75.

22 R. A. Stefański (w:) J. Bratoszewski, L. Gardocki, Z. Gostyński, S. M. Przyjemski, R. A. Stefański, S. Zabłocki, *Kodeks postępowania karnego. Komentarz*, Warszawa 2003, t. 1, s. 1020; T. Grzegorczyk, *Kodeks postępowania karnego oraz ustawa o świadku koronnym. Komentarz*, Warszawa 2008, s. 518; P. Kardas, *Ochrona…*, s. 31, którzy zakaz podejmowania takich działań wyprowadzają przede wszystkim z norm konstytucyjnych.

23 Zob. postanowienie z 26.10.2011 r. (I KZP 12/11), w którym Sąd Najwyższy wskazał: „Obrońca jest też oczywiście poza kręgiem osób, wobec których dopuszcza się kontrolę i utrwalanie rozmów (art. 237 § 4 k.p.k.)", OSNKW 2011/10, poz. 90.

 DOI: 10.54383/0031-0344.2025.06.8

postępowania karnego oraz Prawa o adwokaturze[24]. Pogląd taki znajduje wyraźne odbicie w orzeczeniu z 25.03.1992 r., w którym Europejski Trybunał Praw Człowieka podkreślił, że każda osoba, która potrzebuje porady adwokata, powinna mieć możliwość jej zasięgnięcia w warunkach pozwalających na swobodną rozmowę. Właśnie dlatego kontakty klient–adwokat muszą być uprzywilejowane[25]. Wynika z tego, że ograniczenie dopuszczalności inwigilacji ma charakter mieszany, tj. podmiotwo-przedmiotowy, gdyż nie oznacza zakazu inwigilowania *sui generis* adwokata, natomiast dotyczy wszelkich sytuacji, kiedy tenże adwokat udziela pomocy prawnej jako obrońca lub w trybie art. 245 § 1 k.p.k. Rozróżnienie to jest o tyle istotne, że nawet w przypadku wdrożenia inwigilacji miejsca lub osoby działania takie nie mogą być realizowane w sytuacjach, kiedy miałyby objąć rejestrację czynności związanych z realizacją prawa do obrony.

A należy zaznaczyć, że w Polsce tajna inwigilacja jest stosowana na ogromną skalę – w samym tylko 2022 r. krajowe sądy wydały zgody na podsłuchy w ponad 99% wnioskowanych przypadków, a policja zastosowała je aż 9781 razy. Jednocześnie Najwyższa Izba Kontroli, po zbadaniu okresu od 1.01.2017 r. do 31.03.2023 r. postawiła wniosek, że obowiązujący w Polsce system nadzoru, koordynacji oraz kontroli działalności służb specjalnych jest nieskuteczny i nie odpowiada standardom obowiązującym w demokratycznych państwach prawa. W szczególności nie zapewnia efektywnego nadzoru nad realizacją zadań służb oraz nie gwarantuje, że w toku ich wykonywania będą przestrzegane obowiązujące przepisy prawa oraz respektowane prawa i wolności obywatelskie[26]. Choć nie wiadomo, ile programów, które pozwalają na kontrolę urządzeń końcowych, posiadają polskie służby, to ujawniono, że w latach 2017–2022 trzy z nich wykorzystały „Pegasusa" podczas kontroli operacyjnej urządzeń końcowych wobec 578 osób. W roku 2017 dotyczyło to 6 osób, w 2018 roku 100 osób, w 2019 roku 140 osób, w 2020 roku 161 osób, w 2021 roku 162 osób, a w 2022 roku 9 osób[27].

Dane te ukazują jednak zaledwie wierzchołek problemu związanego z możliwością prowadzenia totalnej inwigilacji. Ilustrują bowiem wyłącznie przypadki prowadzenia kontroli operacyjnej przez polskie służby. Tymczasem wyniki śledztwa dziennikarskiego, o którym była już mowa, nasuwają wniosek, że systemy szpiegujące funkcjonują bez ograniczeń terytorialnych, co oznacza, że mogą być wykorzystywane zarówno poza granicami kraju posiadającego licencję na jego użytkowanie, jak i wobec osób niebędących jego obywatelami ani rezydentami. Dla przykładu, Maroko i Rwanda inwigilowały „Pegasusem" m.in. prezydenta Francji, premiera, ministra

24 Stanowisko Rzecznika Praw Obywatelskich w sprawie skargi konstytucyjnej SK 7/10, Warszawa 25 X 2010 r., s. 6.

25 Sprawa Campbell przeciwko Zjednoczonemu Królestwu, skarga nr 13590/88.

26 J. Ojczyk, *Służby podsłuchują nas bez kontroli, bo pozwala na to prawo. Potwierdził to europejski trybunał*, „Business Insider" z 28.05.2024 r., https://businessinsider.com.pl/prawo/europejski-trybunal-praw-czlowieka-wyda-wyrok-w-sprawie-inwigilacji-w-polsce/3b3e4kh (dostęp: 4.06.2024 r.).

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

obrony i ministra spraw wewnętrznych Hiszpanii, premiera Belgii, poprzedniego przewodniczącego Komisji Europejskiej, a także byłego premiera Włoch[28]. Tym samym nawet hipotetycznie mając informację o braku inwigilacji adwokata przez polskie służby specjalne, nie da się wykluczyć, że takie działania zostały wobec niego przeprowadzone przez organy zagraniczne.

Co więcej, według ujawnionych informacji, jak dotąd, użytkownikami oprogramowania szpiegującego oferowanego przez NSO Gropu czy „Paragon Solutions" byli wyłącznie klienci rządowi. Wynikało to jednak wyłącznie z przyjętej polityki firmowej[29]. Nie sposób natomiast wykluczyć, że popularyzacja wspomnianej technologii, przełamanie monopolu dostawców czy wreszcie zmiana strategii rozwoju spółek spowodują zmianę podejścia do tego tematu, w wyniku czego system szpiegujący trafi do rąk podmiotów pozarządowych. W grę wchodzą zwłaszcza zorganizowane grupy przestępcze, które dysponują środkami finansowymi pozwalającymi na zakup oprogramowania szpiegującego. Dla przykładu – wspomniany wyżej system „Hermit" już dziś jest dostępny na zasadach komercyjnych, co oznacza, że w praktyce nie ma żadnej kontroli nad tym, kto go użyje i przeciwko komu. Ślady tego oprogramowania, pierwotnie wykorzystywanego przez włoskie służby specjalne w ramach akcji antykorupcyjnej, wykryto m.in. w północno-wschodniej Syrii i w Kazachstanie[30].

Niezależnie przy tym od kroków prawnych, które zostaną podjęte w celu zwiększenia kontroli nad użyciem tego typu oprogramowania, trudno sobie wyobrazić, żeby omawiany kierunek rozwoju technologii został zarzucony, gdyż systemy szpiegowskie zostały opracowane jako narzędzia do aktywnej pracy wywiadowczej[31], służące zdobywaniu informacji, której posiadanie pozwala na uzyskanie przewagi nad przeciwnikiem. W interesie służb każdego państwa jest posiadanie informacji, które pozwolą na zapewnienie bezpieczeństwa publicznego i skuteczną walkę z przestępczością, a ewentualne pozbawienie się, w imię ochrony praw człowieka, przewagi technologicznej, jaką zapewnia oprogramowanie szpiegujące, nie wydaje się realne, zwłaszcza że byłoby równoznaczne z oddaniem pola służbom specjalnym obcych państw. Tym samym należy mieć świadomość, że w najbliższym czasie ewentualności zastosowania systemów o możliwościach takich, jakie posiada m.in. „Pegasus", nie uda się definitywnie wyeliminować, niezależnie od tego, jakie kroki prawne zostaną podjęte – czy to na płaszczyźnie krajowej, czy nawet międzynarodowej. Mimo związanych z tym poważnych zagrożeń dla praw jednostki, trzeba przyjąć, że takie niebezpieczeństwo

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

29 M. Jeżewski, *Producent oprogramowania szpiegującego Paragon potwierdza, że USA korzystają z jego usług*, https://ithardware.pl/aktualnosci/paragon_oprogramowanie_szpiegujace_usa-38736.html (dostęp: 13.02.2025 r.).

30 *Rządowa inwigilacja to nie tylko Pegasus. Spyware Hermit atakuje na Androidzie*, https://cyberdefence24.pl/cyberbezpieczenstwo/rzadowa-inwigilacja-to-nie-tylko-pegasus-spyware-hermit-atakuje-na-androidzie (dostęp: 15.01.2025 r.).

31 Pełny zapis przebiegu posiedzenia Komisji Śledczej…, s. 46.

 DOI: 10.54383/0031-0344.2025.06.8

będzie nam towarzyszyło aż do momentu upowszechnienia się technologii blokujących, na wzór swoistego antywirusa. Do tego czasu istnieje tylko jedno rozwiązanie, które może zmniejszyć związane z takimi systemami ryzyko naruszenia tajemnicy wynikającej z roli adwokata. Jest nim świadome korzystanie ze smartfonów oraz innych urządzeń końcowych poprzez ograniczenie ich użytkowania, a nawet noszenia, w miejscach i w sytuacjach, w których ewentualnie wdrożona przy ich wykorzystaniu inwigilacja niosłaby realne niebezpieczeństwo załamania prawem chronionych tajemnic lub mogłaby doprowadzić do nieproporcjonalnego zagrożenia dla interesów posiadacza aparatu bądź osób trzecich. Trzeba mieć bowiem w pamięci, że tak użyteczny w codziennej praktyce zawodowej smartfon może być równocześnie narzędziem szpiegującym, za pomocą którego odbywa się niejawny podsłuch lub podgląd otoczenia, a więc totalna inwigilacja.

adw. dr Miłosz Kościelniak-Marszał

Doktor, adwokat w Izbie Adwokackiej w Częstochowie, adiunkt w Katedrze Prawa Karnego Uniwersytetu Opolskiego.

Doctor of law, advocate at the District Bar Association in Częstochowa, assistant professor at the Department of Criminal Law of the University of Opole

ORCID: 0000-0002-7261-3389

Abstract

Keywords: *Pegasus, spyware, advocate-client privilege, defence counsel-client privilege, professional privilege, surveillance, wire-tapping*

Threats to legal professional privilege resulting from the functionality of contemporary spyware

Spyware was developed for the purposes of active intelligence-gathering work. Their functionality enables implementing information into a device, modifying content stored on it, using social media accounts, and even total surveillance of the user by means of the integrated microphone and camera. Considering the features of such software tools, the need to gather information, as well as the technologi-

cal advances, it is impossible to efficiently remove the related risks of violation of secrets protected by law by means of normative regulations. Unless and until tools capable of blocking the operation of such software are developed, the only solution that might mitigate the aforementioned risks is security-conscious use of smartphones and limiting their use in places or situations where smartphone surveillance might involve heightened risk of confidential information being revealed.

Bibliografia

1. **Bratoszewski Jerzy, Gardocki Lech, Gostyński Zbigniew, Przyjemski Stanisław, Stefański Ryszard, Zabłocki Stanisław,** *Kodeks postępowania karnego. Komentarz*, Warszawa 2003, t. 1
2. **Fraser Małgorzata,** *Nie skończyć jak NSO Group. Tak producenci spyware zabiegają o przychylność USA*, Cyberdefence24
3. **Grzegorczyk Tomasz,** *Kodeks postępowania karnego oraz ustawa o świadku koronnym. Komentarz*, Warszawa 2008
4. **Hofmański Piotr, Sadzik Elżbieta, Zgryzek Kazimierz,** *Kodeks postępowania karnego. Komentarz*, Warszawa 2004, t. 1
5. **Hofmański Piotr, Kulesza Cezary,** *System Prawa Karnego Procesowego*, t. 6, *Strony i inni uczestnicy postępowania karnego*, Warszawa 2016
6. **Jeżewski Marcin,** *Rządowa inwigilacja to nie tylko Pegasus. Spyware Hermit atakuje na Androidzie*, Ithardware.pl
7. **Kardas Piotr,** *Ochrona tajemnicy obrończej. Kilka uwag o dopuszczalności kontroli i utrwalania treści rozmów oraz przekazów informacji realizowanych przy użyciu środków technicznych pomiędzy obrońcą a mandantem*, „Czasopismo Prawa Karnego i Nauk Penalnych", Rok XV: 2011, z. 4
8. **Kirchgaessner Stephanie,** *WhatsApp says journalists and civil society members were targets of Israeli spyware*, „The Guardian" z 31.01.2025 r.
9. **Kosmaty Piotr,** *Wybrane problemy procesowej kontroli i utrwalania rozmów*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2023/2(50)
10. **Kowalewski Mariusz,** *Sąd Najwyższy zgadzał się na stosowanie Pegasusa*, Salon24.pl.
11. **Machlańska Joanna,** *Dowód z podsłuchu procesowego a ochrona tajemnicy obrończej*, „Palestra" 2016/1–2
12. **Matusiak-Frącczak Magdalena,** *Konwencyjne standardy legalnej inwigilacji a zastosowanie systemu Pegasus w Polsce*, „Europejski Przegląd Sądowy" 2023/12

DOI: 10.54383/0031-0344.2025.06.8

13. **Ojczyk Jolanta,** *Służby podsłuchują nas bez kontroli, bo pozwala na to prawo. Potwierdził to europejski trybunał*, „Business Insider" z 28.05.2024 r.
14. **Palczewski Szymon,** *To już potwierdzone: 14 państw UE posiada Pegasusa. Dwóm odebrano licencję*, Cyberdefence24.
15. **Szczepaniak Jolanta,** *WhatsApp miał swojego Pegasusa?*, Android.com.pl.
16. **Szumiło-Kulczycka Dobrosława,** *Tajemnica obrończa a podsłuch procesowy i kontrola operacyjna*, „Palestra" 2013/1–2
17. **Świecki Dariusz** (red.), Augustyniak Barbara, Eichstaedt Krzysztof, Kurowski Michał, *Kodeks postępowania karnego*, Warszawa 2015, t. 1, s. 739
18. **Żaczkiewicz-Zborska Katarzyna,** *Sędzia Morawiec: Byliśmy niewygodni dla władzy*, Prawo.pl.