KANCELARIA
SENATU

BIURO ANALIZ,
DOKUMENTACJI
I KORESPONDENCJI

Opinia prawna dotycząca oceny legalności używania do realizacji czynności operacyjno-rozpoznawczych systemu „Pegasus”

Opinie
i ekspertyzy

OE–425

WARSZAWA 2022

Biuro Analiz, Dokumentacji i Korespondencji

Dyrektor – Agata Karwowska-Sokołowska
tel. 22 694 94 32, fax 22 694 94 28,
e-mail: Agata.Karwowska-Sokolowska@senat.gov.pl

Wicedyrektor – Danuta Antoszkiewicz
tel. 22 694 93 21,
e-mail: Danuta.Antoszkiewicz@senat.gov.pl

Dział Analiz i Opracowań Tematycznych
tel. 22 694 95 33, fax 22 694 94 28
Redaktor prowadzący – Urszula Luboińska

Opracowanie graficzno-techniczne
Centrum Informacyjne Senatu
Dział Wydawniczy

Kancelaria Senatu
wrzesień 2022

Dr hab. Dariusz Jagiełło, prof. Uniwersytetu SWPS
SWPS Uniwersytet Humanistycznospołeczny w Warszawie
Katedra Prawa Karnego

Opinia prawna dotycząca oceny legalności używania do realizacji czynności operacyjno-rozpoznawczych systemu „Pegasus”

I. Źródła prawa

- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. z 1997 r., nr 78, poz. 483 z późn. zm.
- Ustawa z dnia 6 czerwca 1997 r., *Kodeks karny*, t. jedn. Dz. U. z 2022 r., poz. 1138 z późn. zm.
- Ustawa z dnia 6 czerwca 1997 r., *Kodeks postępowania karnego*, t. jedn. Dz. U. z 2022 r., poz. 1375 z późn. zm.
- Ustawa z dnia 24 maja 2002 r., *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, t. jedn. Dz. U. z 2022 r., poz. 557.
- Ustawa z dnia 9 czerwca 2006 r., *o Centralnym Biurze Antykorupcyjnym*, t. jedn. Dz. U. z 2022 r, poz. 1900 z późn. zm.
- Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych*, t. jedn. Dz. U. z 2019 r., poz. 742
- Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r., *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego,* Dz. U. z 2011 r., nr 159, poz. 948.

II. Skróty

„ABW”	–	Agencja Bezpieczeństwa Wewnętrznego
„AW”	–	Agencja Wywiadu
„k.k.”	–	Kodeks karny
„Komisja”	–	(Bez dodatkowego dookreślenia) oznacza senacką Komisję Nadzwyczajną do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu

		na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych
„k.p.k.”	–	Kodeks postępowania karnego
„Rozporządzenie”	–	Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r., *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*
„SKW”	–	Służba Kontrwywiadu Wojskowego
„TK”	–	Trybunał Konstytucyjny
„u.o.i.n”	–	Ustawa o ochronie informacji niejawnych

III. Zakres ekspertyzy – wątki badawcze/problemowe wskazane przez Zamawiającego opinię

Treść i zakres merytoryczny ekspertyzy obejmuje odpowiedzi na następujące pytania szczegółowe i rozwinięcie poniższych zagadnień:

- Czy użycie systemu „Pegasus” mieści się w ramach przesłanek o których stanowi art. 17 ustawy o Centralnym Biurze Antykorupcyjnym, w tym w szczególności czy ma on funkcje wykraczające poza to na co pozwala ustawa?
- Czy łamanie zabezpieczeń telefonu systemem „Pegasus” może zostać uznane za kontratyp ustawowy?
- Czy sąd w ramach wnioskowanej kontroli operacyjnej powinien być poinformowany o wnioskowanym użyciu systemu „Pegasus”?
- Czy materiały pozyskane systemem „Pegasus” mogą być dowodem w postępowaniu karnym?
- Analiza faktu, że system „Pegasus” umożliwia pozyskanie korespondencji oraz innej zawartości telefonu, która pochodzą sprzed daty zarządzenia kontroli operacyjnej.
- Analiza problemu związanego z pozyskiwaniem materiałów objętych tajemnicą adwokacką systemem „Pegasus”.
- Analiza problemu przekazywania służbom obcego państwa informacji o zainteresowaniach służb RP.
- Problem certyfikacji systemu „Pegasus” przez ABW/SKW w myśl przepisów ustawy o ochronie informacji niejawnych.

IV. Zastrzeżenie

Niniejsza ekspertyza odnosi się wyłącznie do zagadnień karnoprawnych i karnoprocesowych z wyłączeniem kwestii technicznych, odnośnie

systemu „Pegasus", które nie znajdują się w zakresie zainteresowania badawczego i naukowego opiniującego.

Niemniej w pierwszej kolejności zwrócono uwagę, na te z nich które będą istotne w zakresie opiniowania, a zostały już zgłębione czy to w uprzednio uzyskanych opiniach eksperckich dla Komisji, czy też wystarczająco wyeksplorowane w nauce i literaturze, a mianowicie:

- System „Pegasus" to nazwa oprogramowania szpiegującego (system *spyware*).
- System „Pegasus" można instalować na urządzeniach elektronicznych korzystających z systemu/oprogramowania iOS i Android (w tym zwłaszcza na telefonach komórkowych).
- Producentem systemu „Pegasus" jest izraelska spółka NSO Group Technologies Ltd.
- Instalacja systemu „Pegasus" odbywa się zdalnie bez ingerencji fizycznej (mechanicznej, namacalnej) w sprzęt. Powoduje to, że właściciel urządzenia może być (i często tak jest) nieświadomy zagrożenia, ani też samego faktu zainfekowania.
- O zainfekowaniu systemem „Pegasus" nie wiedzą dostawcy usługi internetowej[1].
- Ingerencja (zainfekowanie sprzętu) daje dostęp do aplikacji, a także informacji znajdujących się na urządzeniu[2], tym samym umożliwia infekującemu pełną wiedzę i nieograniczony dostęp do znajdujących się tam danych.
- Kontrolę nad oprogramowaniem ma licencjodawca[3], co wiąże się z dostępem tego podmiotu do danych gromadzonych i przetwarzanych przez oprogramowanie[4].

---

1 J. Trela, *Czy Pegasus może być legalny?*, „Rzeczpospolita", 11 stycznia 2022 r.

2 Chodzi m.in. o dostęp do wiadomości e-mail oraz SMS-ów; śledzenie pozycji urządzenia (GPS); modyfikowanie ustawień technicznych urządzenia (w tym dostępu do sieci); dostęp do historii przeglądania stron internetowych, zapisanych kontaktów, sieci społecznościowych; wykonywanie połączeń telefonicznych; dokonywanie i przeglądanie wpisów w kalendarzu; pozyskiwanie plików z urządzenia (w tym usuniętych); instalowanie własnych oraz modyfikacja istniejących plików na urządzeniu; wysyłanie wiadomości; dostęp do aparatu i galerii urządzenia (w tym możliwość wykonywania zdjęć, filmów i zrzutów ekranu); nagrywanie dźwięku. Por. B. Marczak, J. Scott-Railton, S. McKune, B. Abdul Razzak, R. Deibert, HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, 18 września 2018 r., https://citizenlab.ca/, dostęp dnia 14 września 2022 r.).

3 NSO Group Technologies Ltd. z siedzibą w Herclijji (Izrael).

4 Tak A. Zoll w wywiadzie z D. Wysocką-Schnepf, Prof. Zoll: Pegasus? To zbrodnia szpiegostwa. Kamiński, Wąsik, Ziobro, Kaczyński - postawiłbym im ten zarzut, 29 grudnia 2021 r., https://wyborcza.pl/, dostęp w dn. 19 września 2022 r.

– Dystrybucją licencji zajmuje się Ministerstwo Obrony Izraela, a udziela jej wyłącznie państwom[5].
– Charakterystyczne dla systemu Pegasus jest jego działanie ofensywne – możliwość ingerencji w funkcjonowanie i zawartość zainfekowanego urządzenia. Powoduje to, że system określa się mianem „broni antyterrorystycznej"[6].
– Najwyższa Izba Kontroli po realizacji działań kontrolnych stwierdziła, że Ministerstwo Sprawiedliwości złamało prawo przekazując w 2017 r. Centralnemu Biuru Antykorupcyjnemu środki w wysokości 25 mln. złotych pochodzące z Funduszu Sprawiedliwości – co mogło stanowić naruszenie dyscypliny finansów publicznych[7].
– Wątpliwości kontrolerów NIK budziło przekazanie środków na zakup oprogramowania podmiotowi pośredniczącemu (pośrednikiem była: Matic sp. z o.o., a obecnie: Matic S.A.)[8].
– Szereg medialnych wystąpień członków rządu i polityków daje pewność, że służby używały systemu „Pegasus"[9], ale nie jest jasny cel, charakter i skala jego działania.
– Na 35. Posiedzeniu (w dniu 12 stycznia 2022 r.), Senat podjął uchwałę w sprawie powołania Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych[10].

---

5 J.A. Gross, Amid fallout from NSO scandal, Israel imposes new restrictions on cyber exports, 6 grudnia 2021 r., https://www.timesofisrael.com/amid-fallout-from-nso-scandal-israel-imposes-new-restrictions-on-cyber-exports/, dostęp dnia 18 września 2022 r.

6 Materiały NSO wskazują na modele wykorzystania systemu Pegasus, określając je mianem: ekstrakcji początkowej/wstępnej, pasywnego przechwytywania oraz aktywnego zbierania.

7 Pomoc z Funduszu Pomocy Pokrzywdzonym nie dla pokrzywdzonych, 29 czerwca 2018 r., https://www.nik.gov.pl/aktualnosci/fundusz-pomocy-pokrzywdzonym.html, dostęp dnia 17 września 2022 r.; Informacja o wynikach kontroli – Pomoc ofiarom przestępstw w ramach Funduszu Pomoc Pokrzywdzonym (Funduszu Sprawiedliwości), KPB.430.001.2017, Nr ewid. 200/2017/P/17/038/KPB, s. 34.

8 Podmiot otrzymał kwotę 8 mln. zł. NIK ujawnia faktury za „zakup środków techniki specjalnej". Pieniądze CBA otrzymało z Funduszu Sprawiedliwości, https://tvn24.pl/polska/pegasus-inwigilacja-nik-ujawnia-faktury-pieniadze-dla-cba-z-funduszu-sprawiedliwosci-na-zakup-srodkow-techniki-specjalnej-5559012, dostęp dnia 17 września 2022 r.

9 J. Kaczyński: Mamy Pegasusa, ale nie używaliśmy go wobec opozycji, 7 stycznia 2022 r., https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8328416,pegasus-kaczynski-wywiad-brejza-inwigilacja.html, dostęp dnia 14 września 2022 r.

10 Zgodnie z § 2 uchwały, zadaniem Komisji jest m.in. *wyjaśnienie ujawnionych przypadków nielegalnej inwigilacji z użyciem m.in. oprogramowania szpiegowskie-*

W trakcie prac Komisji sporządzono dotychczas opinie, ekspertyzy o podłożu prawno-technicznym, a także konstytucyjnym. Dlatego też w niniejszej opinii pominę wątki, które były już przedmiotem opiniowania uprzednio, wyłącznie je sygnalizując.

V. „Certyfikacja" systemu Pegasus, a realizacja czynności operacyjno-rozpoznawczych

Wszelkie pozyskane w ramach kontroli operacyjnej informacje muszą pozostawać w ścisłej korelacji z treścią ustawy z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych*[11] (dalej: u.o.i.n.). Pozyskane dane, informacje i materiały muszą być tak zabezpieczone, aby nie było możliwe namacalne ingerowanie w ich treść. Nie mogą one zostać udostępnione też osobom postronnym, dla których dane te nie zostały przewidziane. Informacjom nadawana jest odpowiednia klauzula mająca chronić przed ingerencją. W ujęciu konstytucyjnym działanie takie mogłoby naruszyć prawo do prywatności[12].

Nadanie informacjom odpowiedniego statusu chronić ma przed niekontrolowanym wyciekiem informacji, a także zapewnić poufność danych. Dlatego w przepisach u.o.i.n. funkcjonuje określenie certyfikacja, którą odnosi się i definiuje jako proces potwierdzania zdolności urządzenia, narzędzia lub innego środka do ochrony informacji (art. 2 pkt. 11 u.o.i.n.).

Analizując obowiązujące przepisy prawa stwierdzić należy, że art. 49 ust. 9 u.o.i.n. stanowi: *Prezes Rady Ministrów określi, w drodze rozporządzenia, podstawowe wymagania bezpieczeństwa teleinformatycznego, jakim powinny odpowiadać systemy teleinformatyczne, niezbędne dane, jakie powinna zawierać dokumentacja bezpieczeństwa systemów informatycznych oraz sposób opracowania tej dokumentacji.*

Dokumentem tym jest aktualnie obowiązujące Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r., *w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego*[13].

---

go „Pegasus" oraz naruszeń prawa podczas stosowania przez służby specjalne kontroli operacyjnej.

11 Dz. U. z 2019 r., por. 742.

12 Szerzej por. M. Bidziński, *Ekspertyza w przedmiocie: legalności zakupu i wykorzysty wania na terytorium Rzeczypospolitej Polskiej systemu „Pegasus"*, Opinie i ekspertyzy OE-381, Warszawa 2022.

13 Dz. U. z 2011 r., nr 159, poz. 948.

Z jego treści wynika, że: *Poufność informacji niejawnych przekazywanych w formie transmisji poza strefami ochronnymi zapewnia się przez stosowanie urządzeń lub narzędzi kryptograficznych, certyfikowanych zgodnie z art. 50 ust. 2 u.o.i.n. lub dopuszczonych w trybie art. 50 ust. 7 u.o.i.n., odpowiednich do klauzuli tajności przekazywanych informacji* (§ 10 ust. 2 Rozporządzenia).

Urządzenie, narzędzie lub środek przeznaczony do ochrony informacji niejawnych, dla którego został wydany przez Agencję Bezpieczeństwa Wewnętrznego, zwaną dalej „ABW", lub Służbę Kontrwywiadu Wojskowego, zwaną dalej „SKW", certyfikat, o którym mowa wart. 50 ust. 4 u.o.i.n., podlega ochronie do momentu jego zniszczenia lub wycofania, zgodnie z zaleceniami ABW lub SKW (§ 16 Rozporządzenia).

Informacje niejawne przekazywane poza strefę ochronną na informatycznych nośnikach danych chroni się z wykorzystaniem urządzeń lub narzędzi kryptograficznych, certyfikowanych zgodnie z art. 50 ust. 2 u.o.i.n. lub dopuszczonych w trybie art. 50 ust. 7 u.o.i.n., odpowiednich do klauzuli tajności przekazywanych informacji (§ 17 ust. 2 pkt. 1 Rozporządzenia).

Analiza treści Rozporządzenia, a także art. 49-51 u.o.i.n. upoważnia do wniosków, że *ratio* tych przepisów zmierza by system gwarantował poufność. Tę poufność należy interpretować mianem *właściwości określającej, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym* (por. § 2 pkt. 9 Rozporządzenia). Definicję tą należy rozszerzyć na dostęp do danych innych podmiotów.

Biorąc pod uwagę, że **system „Pegasus" od strony technicznej nie jest możliwy do realnej weryfikacji bezpieczeństwa, w tym szczególnie ingerencji obcych państw, a także warunków jego licencji analizując treść ww. przepisów nie jest też możliwe aby mógł on spełnić warunki poufności, o których mowa w ustawie. Z tego też względu jest wysoce prawdopodobne, że nie mógłby uzyskać świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego, o którym mowa w Rozporządzeniu**.

Wydaje się, że jest jeszcze jedna przesłanka techniczna uniemożliwiająca akredytację, a mianowicie integralność o której mowa w § 2 ust. 5 Rozporządzenia, czyli *właściwość określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony*. Jednak analiza tej przesłanki nie jest możliwa dla mnie do analizy z uwagi na brak wiedzy technicznej, co wyłącznie sygnalizuję[14].

14 Szerzej por. A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zolntek, *Ekspertyza. Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasusa),* Kraków 2022

Wszystko to powoduje konieczność przyjęcia i uznania, że system Pegasus nie przeszedłby wymaganej prawem akredytacji. Nie byłoby możliwe zrealizowanie niezbędnych czynności kontrolnych poprzedzających uzyskanie świadectwa akredytacji bezpieczeństwa takich jak: otrzymanie kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego (art. 48 ust. 4 u.o.i.n.) - nie stosuje się do niego wyłączenia z art. 51 u.o.i.n. – nie było też przeprowadzonych testów bezpieczeństwa informacji.

Zatem na gruncie polskiego prawa, w kontekście używania i certyfikacji systemu Pegasus stwierdzić należy, że:

- Nie może on być używany, gdyż nie jest możliwe jego skuteczne akredytowanie i weryfikacja bezpieczeństwa teleinformatycznego odnośnie do ochrony informacji niejawnych.
- Polskie prawo nie dopuszcza używania programów, których dane poddane zostają niekontrolowanej integralności i poufności.
- Niezgodne z przepisami polskiego prawa jest używanie w ramach działań operacyjnych nieakredytowanych programów komputerowych niezapewniających bezpieczeństwa informacjom niejawnym, a także narażającym (nawet potencjalnie) na ryzyko ich przekazania, czy udostępnienia osobom trzecim.

W kontekście dopuszczalności ewentualnego stosowania systemu Pegasus zwrócić należy uwagę jeszcze na art. 32a ust. 7 i 8 ustawy o ABW i AW[15], wskazujący na uprawnienie ABW w tym zakresie:

Art. 32a, ust. 7: *„ABW może wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b Kodeksu karnego, oraz ich używać w celu określenia podatności ocenianego systemu na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a Kodeksu karnego".*

Art. 32a, ust. 8: *„Używając urządzeń lub programów komputerowych, o których mowa w ust. 7, ABW może uzyskać dostęp do informacji dla niej nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, lub może uzyskać dostęp do całości lub części systemu teleinformatycznego".*

(z datą publikacji 15 kwietnia 2022 r.), https://kipk.pl/ekspertyzy/casus-pegasusa/, s. 13-14.

15 Ustawa z dnia 24 maja 2002 r., *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, t. jedn. Dz. U. z 2022 r., poz. 557.

Ustawodawca dał ABW uprawnienie do stosowania programu takiego jak Pegasus, ale tylko i wyłącznie we wskazanym zakresie jako: *„celu określenia podatności ocenianego systemu na możliwość popełnienia przestępstw…”*. Tylko konkretnych przestępstw wymienionych enumeratywnie w art. 32a, ust. 7 i żadnych innych (sic!). Inny cel działania ABW aniżeli wskazany w przytoczonym przepisie nie jest możliwy do zrealizowania w polskich realiach prawnych. Podkreślić wypada, że tylko w ustawie o ABW znajduje się taki przepis. Innym służbom, które mogą prowadzić kontrolę operacyjną (dopuszczoną ustawowo), tego rodzaju uprawnień nie dano.

Odnośnie do systemu „Pegasus”, w kontekście uprawnień ABW z ewentualnym wykorzystaniem tego systemu, jest to działanie dozwolone w ściśle określonym zakresie, tylko i wyłącznie w celu badania podatności systemu na ataki.

VI. Kontrola operacyjna w ustawie o CBA

Standardy kontroli operacyjnej poza ustawą o CBA (art. 17) zawierają jeszcze inne ustawy[16]. Kontrola ta możliwa jest tylko i wyłącznie do określonego katalogu przestępstw, sprecyzowanego odrębnie w każdej z ustaw. Ponadto, każda z ustaw może przewidywać odrębne cele kontroli operacyjnej. Np. ustawy o CBA (art. 17 ust. 1) a także o ABW (art. 27 ust. 1) stanowią, że można ją wdrożyć w celu ujawnienia mienia zagrożonego przepadkiem. Poszczególne ustawy zawierają przesłanki tożsame, ale nie identyczne. Kontrolę operacyjną można zainicjować dopiero gdy: *„inne środki okazały się bezskuteczne lub też będą nieprzydatne”*. Zatem będzie ona mogła zostać zastosowana gdy nie istnieje inna możliwość zapobiegania, wykrycia, ustalenia sprawców lub pozyskania bądź utrwalenie dowodów przestępstwa. Chodzi o wykorzystanie innych mniej inwazyjnych działań niż inwigilacja (kontrola operacyjna)[17]. Działania w ramach kontroli operacyjnej muszą być adekwatne do celu, któremu kontrola służy. Trzeba także brać pod uwagę stopień ingerencji w dobra prawne osoby kontrolowanej, oraz wagę i stopień popełnienia przestępstwa. Chodzi o jej stosowanie do zapobiegania, czy

16 np. o Policji (art. 19), o ABW (art. 27), o SKW (art. 31), o Krajowej Administracji Skarbowej (art. 118), o Straży Granicznej (art. 9e), o Służbie Ochrony Państwa (art. 42).

17 Pomijam tu przesłankę testu proporcjonalności z art. 31 ust. 3 Konstytucji RP, o której szeroko patrz: M. Bidziński, *Ekspertyza….*, s. 7-8; A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zolntek, Ekspertyza. *Dopuszczalność…*, s. 25 – 27.

wykrywania poważnych przestępstw (przestępstwo zostało, lub mogło zostać popełnione). Niedopuszczalna jest kontrola operacyjna na podstawie abstrakcyjnej.

Przepisy ustawy o CBA art. 17 ust. 5 wskazują rodzaje możliwej kontroli, które mogą zostać wdrożone:

Kontrola operacyjna prowadzona jest niejawnie i polega na:

1. *uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;*
2. *uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;*
3. *uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;*
4. *uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;*
5. *uzyskiwaniu dostępu i kontroli zawartości przesyłek.*

Zaś art. 19 ust. 1 ustawy o CBA stanowi o zakupie kontrolowanym i wymogach z nim związanych w tym o czynności dokumentowania (art. 19 ust. 6 i Rozporządzenie wydane na jego podstawie[18]).

Biorąc pod uwagę brak certyfikacji systemu „Pegasus", a także jego faktyczne możliwości i zakres działania nie mieszczą się one w ramach art. 17 ust. 5 ustawy o CBA. Zdecydowanie przekraczają one kompetencje ustawowe do jego zastosowania. Zatem kontrola operacyjna realizowana przy użyciu systemu „Pegasus" nie spełnia przesłanki ustawowej jej realizacji.

VII. Czy Sąd w ramach wnioskowanej kontroli operacyjnej musi wiedzieć na użycie jakiego urządzenia wyraża zgodę?

Przepisy ustawy o CBA nie precyzują, jakie dokładnie metody i środki techniczne mogą zostać wykorzystane w ramach kontroli operacyjnej. W zakresie opiniowanym nie zawierają w szczególności nazw, czy

18 Rozporządzenie Prezesa Rady Ministrów z dnia 7 września 2006 r. *w sprawie sposobu przeprowadzania przez Centralne Biuro Antykorupcyjne i dokumentowania czynności polegających na dokonaniu w sposób niejawny nabycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przepadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także na przyjęciu lub wręczeniu korzyści majątkowej*, Dz. U. z 2006 r., nr 165, nr 1172.

specyfikacji urządzeń, oprogramowania, które może zostać wykorzystane do inwigilacji. Wydaje się, że z uwagi na standard konstytucyjny i orzecznictwo TK stan taki wątpliwości nie budzi. Chociażby w wyroku z dnia 30 lipca 2014 r., K 23/11 stwierdzono, że ogrom środków stosowanych przez organy państwa powodowałby ich kazuistyczny katalog[19]. Podkreślono, że nie jest przy tym konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie ich parametrów.

Zastanowić się należy nad sytuacją, kiedy złożony został wniosek do sądu o zarządzenie kontroli operacyjnej (zgodnie z obowiązującymi przepisami prawa), a mianowicie czy Sąd musi wiedzieć jakie środki zostaną w ramach kontroli operacyjnej CBA zastosowane?

Rozpocząć należy, że wniosek Szefa CBA o zastosowanie kontroli operacyjnej na podstawie art. 17 ust. 7 ustawy o CBA , zawiera w szczególności:

1. numer sprawy i jej kryptonim, jeżeli został jej nadany;
2. opis przestępstwa z podaniem jego kwalifikacji prawnej;

---

19 OTK-A 2014, nr 7, poz. 80. W pkt. 5.1.3.2. wyroku czytamy: *„niezbędne jest sprecyzowanie sposobu niejawnego wkroczenia w sferę prywatności jednostki. Nie jest przy tym konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie ich parametrów. Mając na uwadze ogromną liczbę środków stosowanych przez organy państwa przydatnych w pracy operacyjno-rozpoznawczej, ustawowy ich katalog musiałby być rozbudowany, a co za tym idzie norma prawna musiałaby być kazuistyczna"*. Rozwiązanie to mogłoby kolidować z wymogiem abstrakcyjności normy prawnej. Jak wielokrotnie wskazywał Trybunał, również w perspektywie określoności przepisów represyjnych, przestrzeganie wymogów wynikających z zasady dostatecznej określoności prawa nie może prowadzić do kazuistyki unormowania (zob. wyroki TK z: 26 listopada 2003 r., sygn. SK 22/02, OTK ZU nr 9/A/2003, poz. 97, cz. III, pkt 4; 5 maja 2004 r., sygn. P 2/03, OTK ZU nr 5/A/2004, poz. 39, cz. III, pkt 3.5; 13 stycznia 2005 r., sygn. P 15/02, OTK ZU nr 1/A/2005, poz. 4, cz. III, pkt 2; 28 czerwca 2005 r., sygn. SK 56/04, OTK ZU nr 6/A/2005, poz. 67, cz. V, pkt 1; 17 grudnia 2008 r., sygn. P 16/08, OTK ZU nr 10/A/2008, poz. 181, cz. IV, pkt 8.2.2; 22 czerwca 2010 r., sygn. SK 25/08, OTK ZU nr 5/A/2010, poz. 51 cz. III, pkt 4.1-4.2; 1 grudnia 2010 r., sygn. K 41/07, OTK ZU nr 10/A/2010, poz. 127, cz. III, pkt 3.2). Podobnie uznał TK w wyroku dotyczącym przepisów regulujących prowadzenie kontroli operacyjnej przez wywiad skarbowy (zob. wyrok TK z 20 czerwca 2005 r., | sygn. K 4/04, cz. V, pkt 2.6), akceptując - po spełnieniu kilku warunków – pewien stopień ogólności unormowania sposobów kontroli operacyjnej prowadzonej przez wywiad skarbowy. *„Należałoby mieć także na uwadze, że w dobie rozwoju technologicznego, wielości form popełniania przestępstw i kanałów komunikowania się przestępców nie wydaje się realne stworzenie zamkniętego katalogu środków technicznych, które mogą być stosowane w celu uzasadnionego konstytucyjnie niejawnego pozyskiwania informacji, bez uszczerbku dla efektywnej walki z zagrożeniami czy dekonspiracji działalności operacyjnej"*.

3. okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków;
4. dane osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania;
5. cel, czas i rodzaj prowadzonej kontroli operacyjnej.

Konieczne jest wskazanie podmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania, a także cel, czas i rodzaj prowadzonej kontroli operacyjnej.

Wydaje się, że w ujęciu zasady określoności prawa konieczne jest wskazanie rodzaju kontroli jaką służba zamierza wdrożyć np. podsłuch rozmów telefonicznych, czy podsłuch i podgląd pomieszczeń bez wskazywania konkretnych parametrów technicznych. Przepisy prawa karnego procesowego wymagają, aby sąd miał wiedzę o przewidywanych do zastosowania (wnioskowanych) rodzajach kontroli operacyjnej. Dlatego, że w art. 17 ust. 7 pkt. 5 mowa jest o rodzaju kontroli operacyjnej, zaś w ustępie poprzedzającym jest alternatywa do wskazania miejsca lub sposobu.

Nie dostrzegam przeszkód, aby Sąd zapytał wnioskodawcę o przewidywany rodzaj środków technicznych. Może zwrócić się do niego z prośbą o wyjaśnienie celu, konieczności czy proporcjonalności, jeśli takie wątpliwości będzie miał.

Problemem jest, czy można wskazać miejsce, w którym będzie stosowany system „Pegasus". Jeśli jest to możliwe, to biorąc pod uwagę określany w logice prawniczej, mianem funktora alternatywy nierozłącznej do spójnika „lub" (użyty w art. 17 ust. 7 pkt. 4 ustawy o CBA) oznacza on możliwość zastosowania tego, co przed funktorem, tego, co za nim, albo też obu elementów łącznie.

Jeśli nie zaistnieje konieczność wskazania na jego użycie wystarczające będzie sformułowanie „kontrola i utrwalania rozmów...". Warto jednak zauważyć, że wykorzystanie „Pegasusa" daje również możliwość ingerencji w urządzenie, na którym go zainstalowano. Zatem gdy wnioskodawca ma możliwość wskazania miejsca wykonywania kontroli operacyjnej np. miejsca w którym stosował będzie urządzenie podsłuchowe, wtedy nie musi obligatoryjnie wskazywać nazwy stosowanego urządzenia, choć oczywiście może to zrobić. Musi także udzielić stosownej informacji sądowi, który by o taką informację poprosił.

Gdy chodzi o system „Pegasus" wskazanie miejsca – wydaje się – być niemożliwe, bowiem jego stosowanie nie jest związane z żadnym miejscem, inaczej niż np. podsłuch tzw. „pluskwa" w konkretnym miejscu,

pod konkretnym przedmiotem – np. biurkiem. Wtedy winno zostać wskazane jakim systemem będzie kontrola realizowana, czyli w takim wypadku wskazać należy, że zastosowany zostanie system „Pegasus".

Sposób to nie tylko „urządzenie elektroniczne" trzeba też wskazać, jakie to urządzenie. A jeżeli byłoby to określone zbyt mało precyzyjnie, wtedy sąd może żądać doprecyzowania, wyjaśnienia - jakie to będzie urządzenie.

Wskazanie miejsca jest niemożliwe, ale przedmiot już tak np. smartfon o numerze ...., albo wręcz numer .... Ale wtedy nie mamy do czynienia z miejscem, zatem potwierdza to, iż Sąd winien wiedzę odnośnie do sposobu kontroli – urządzenia, systemu – uzyskać.

Dla zbadania zasady proporcjonalności, a także przejrzystości stosowania kontroli operacyjnej zasadne jest, by we wniosku wskazać środki techniczne (certyfikowane), którymi zamierza się daną kontrolę realizować.

Wiedza odnośnie do stosowania systemu „Pegasus" uzupełnia ogólny pogląd na temat zamierzeń wnioskodawcy, w szczególności, że jest to program, który certyfikacji nie uzyskał i nie ma stosownego świadectwa wystawionego przez ABW.

VIII. Materiał uzyskany za pomocą systemu „Pegasus", a dowód w procesie karnym

Abstrahując od certyfikacji i braku możliwości wykorzystania systemu Pegasus w polskim systemie prawa należy odnieść się do sytuacji dysponowania dowodami za jego pomocą uzyskanymi. W szczególności zastanowić się należy, czy dowodu takiego nie będzie można wykorzystać w procesie karnym biorąc pod uwagę treść art. 168a k.p.k.: *„Dowodu nie można uznać za niedopuszczalny wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 k.k., chyba że dowód został uzyskany w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności".*

Wydaje się, że prawo nie stoi na przeszkodzie by sąd wziął pod uwagę ewentualny złożonego przez oskarżyciela dowód **uzyskany za jego pomocą. Jednak musi się on odnosić do katalogu przestępstw w nim zamieszczonych.**

Art. 168a k.p.k. nie wyklucza użycia takiego dowodu w procesie. Przepis stanowi *„nie można uznać za niedopuszczalny wyłącznie na*

***tej podstawie ….”.* Nawet jeżeli funkcjonariusz publiczny wie, że nie może użyć tego urządzenia, a mimo to go użyje, to nadal działanie to nie spełni przesłanki z art. 168a k.p.k. Wtedy wprowadzone byłoby to do procesu jako legalnie pozyskany dowód, pomimo nieuprawnionego użycia systemu „Pegasus”.**

Dodatkowo powstaje wątpliwość, czy biegły w zakresie informatyki/analizy informatycznej byłby w stanie wykonać analizę prawdziwości dowodu, w tym w szczególności, czy nie miała miejsca nieuprawniona ingerencja w jego treść.

IX. Zakres informacji objętych tajemnicą adwokacką, a użycie systemu „Pegasus”

Przepisy prawa karnego procesowego w art. 178 k.p.k. stanowią zakaz dowodowy. Nie wolno bowiem przesłuchiwać jako świadków: obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 § 1, co do faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę (art. 178 pkt. 1 k.p.k.).

Przepis art. 178 k.p.k. formułuje bezwzględne zakazy dowodowe, które w żadnych warunkach nie mogą być uchylone, co oznacza, że osoby te co do tych okoliczności nie mogą zostać przesłuchane, a gdyby zostały wezwane w charakterze świadków, mają prawo i obowiązek odmowy złożenia w tym zakresie zeznań. Zakazu tego nie uchyla nawet zgoda wszystkich zainteresowanych osób. W orzecznictwie trafnie zauważa się, że ani osoba wnioskodawcy, ani kierunek przesłuchania (na korzyść oskarżonego) nie pozwalają na obejście tego zakazu dowodowego[20]. Zakaz dotyczy organu, nie osoby znającej tajemnicę.

Co do zakresu tajemnicy obrończej formułuje się dość powszechnie pogląd, że – mimo wąskiego ujęcia treści art. 178 w zw. z art. 226 – występuje niedopuszczalność wykorzystywania w procesie treści uzyskanych w następstwie kontroli operacyjnej lub podsłuchu procesowego nagrań obejmujących rozmowy pomiędzy sprawcą a adwokatem, także w sytuacji, gdy w chwili ich odbywania adwokat nie był jeszcze formalnie obrońcą, a nawet gdy ostatecznie w ogóle nim nie zostanie[21].

---

20 Por. Wyrok Sądu Apelacyjnego w Szczecinie z dnia 18 lutego 2015 r., LEX nr 1668674.

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

Ustawa o CBA w art. 15f odnosi się do owych informacji (przewiduje tryb postępowania). Jeżeli pozyskane informacje zawierają dane, o których mowa w art. 178 k.p.k., Szef CBA zarządza ich niezwłoczne, komisyjne i protokolarne zniszczenie. Zatem w ogóle nie można legalnie nagrać kontaktu oskarżonego ze swoim obrońcą, a nagrany przypadkowo nie może być legalnie użyty. Ustawa o CBA przewiduje tryb postępowania z takim dowodem, nie wskazuje jednak co zrobić w sytuacji, kiedy na tej podstawie służba pozyskała inny kolejny dowód (np. ciało, narkotyki itp.).

Nie budzi wątpliwości, że osób tych nie wolno przesłuchiwać co do faktów określonych w art. 178 k.p.k., tylko gdy są świadkami, jednak zakaz ten nie dotyczy przesłuchiwania ich w charakterze oskarżonych czy podejrzanych[22], a gdyby doszło do przesłuchania takiego świadka co do takich okoliczności, to ta część zeznań nie mogłaby stanowić dowodu w sprawie. Nie dostrzegam jednak przeszkód do wykorzystania takich informacji dla uzyskania i przeprowadzenia innych dowodów co do tych okoliczności (faktów) lub wykorzystania ich w działaniach operacyjnych organów ścigania[23]. **Gdyby zatem stosować system „Pegasus" tylko do podsłuchiwania klienta i adwokata, czy stosowania podsłuchu telefonicznego, działanie to jest niewątpliwie nielegalne i z tym dyskutować nie można.**

Ale jeśli na tej podstawie uzyskam inny dowód istotny dla postępowania (on ma swój początek z dowodu uzyskanego systemem „Pegasus"), w mojej ocenie, eliminacji podlegać będzie tylko i wyłącznie ten dowód, który został pozyskany nielegalnie. Dowód kolejny wprowadzamy do procesu tak jak każdy inny fizyczny dowód rzeczowy (wobec wąskiego i enumeratywnie wymienionego katalogu z art. 168a k.p.k.), który należy uznać za legalny.

Wniosek taki płynie z faktu, że w Polsce nie funkcjonuje teoria owoców zatrutego drzewa (*The Fruit of the Poisonous Tree doctrine*), zatem tę rozmowę eliminujemy, ale to co dalej zostało ustalone dowodowo w procesie zaistnieje i będzie mogło stanowić materiał dowodowy.

---

22 Uchwała Sądu Najwyższego z dnia 29 listopada 1962 r., VI KO 61/62, OSNKW1963, nr 7-8, poz. 157; M. Kucharczyk, *Kwestia ujawnienia tajemnicy państwowej, służbowej, zawodowej i funkcyjnej w wyjaśnieniach oskarżonego,* „Państwo i Prawo" 2005, nr 2, s. 78.

23 Tak. też por. L. K. Paprzycki (red), *Komentarz aktualizowany do art. 1-424 Kodeksu postępowania karnego,* LEX/el 2015, Pkt. 6.

X. Działanie systemu „Pegasus" a kontratyp ustawowy

W zleceniu do wydania opinii znalazło się zagadnienie: Czy łamanie zabezpieczeń telefonu systemem „Pegasus" może zostać uznane za kontratyp ustawowy? Nie wskazano w kierunku jakiego kontratypu analizę przeprowadzić ma opiniujący.

Na wstępie należy podkreślić, że kontratyp to *„(...) te i tylko te okoliczności, które, mimo, że czyn wykazuje ustawowe znamiona czynu zabronionego przez ustawę pod groźbą kary, jednak powodują, że nie jest społecznie szkodliwy (ew. jest dodatni), a tym samym bezprawny; są to więc okoliczności legalizujące czyn, generalnie uznany za bezprawny*[24]*"*. A. Zoll przyjmuje jako podstawę dla wszystkich kontratypów *wystąpienie kolizji dóbr, z czego wyprowadza dwa dalsze warunki zachowania kontratypowego: konieczność poświęcenia dobra mającego wartość społeczną oraz społeczną opłacalność poświęcenia określonego dobra*[25].

Domniemywam, że pytanie to i ewentualna wątpliwość wzięły się z faktu, że funkcjonuje kontratyp ustawowy do pojęcia prowokacji. Prowokacja znajduje się w treści art. 24 k.k., zaś w ustawie o policji jest tzw. „czysta prowokacja", lecz prawem dozwolona. Są to uprawnienia policji w zakresie kontroli operacyjnej. Zatem legalny podsłuch telefoniczny jest kontratypem stosowanym gdy *inne środki okazały się bezskuteczne albo będą nieprzydatne*. Można je stosować dopiero wtedy, kiedy inne środki techniki zawodzą. To ustalenie daje *asumpt* do ubiegania się o zgodę na przekroczenie konstytucyjnego pojęcia prawa do wolności z art. 31 ust. 1 Konstytucji RP, wyrażoną w wystąpieniu do Sądu o jej zastosowanie.

W realiach systemu „Pegasus" jego zakresu działania, gromadzenia danych, żadna okoliczność kontratypowa nie może być zastosowana. Już z uwagi na to, że brak **jest możliwości uzyskania certyfikatu dla urządzenia wykluczona jest możliwość analizy jakiegokolwiek działania w ramach kontratypu oraz nie można zastosować go w ramach kontroli operacyjnej. Nie może być mowy o szczególnym kontratypie do art. 231 k.k., czyli przekroczenia uprawnień przez funkcjonariusza.**

---

24 W. Wolter, *Nauka o przestępstwie,* Warszawa 1973, s. 163

25 A. Zoll, *Okoliczności wyłączające bezprawność czynu (Zagadnienia ogólne),* Warszawa 1982, s. 104.

XI. Przekazywanie służbom obcego państwa informacji o zainteresowaniach służb RP

Odpowiedź na to pytanie wymaga wiedzy, czy przez włączenie systemu „Pegasus", jego operator, jak mniemam, w Izraelu, może wiedzę taką pozyskać?, Czy mogą wiedzieć do jakiego aparatu (model, numer, symbol) system „Pegasus" został zastosowany lub kto jest jego właścicielem aparatu?

Jeżeli te służby – pierwotny operator „Pegasusa" w Izraelu – mogą wiedzieć, do czego/kogo/numeru/osoby jest zastosowany, to nie wolno tego robić. Nie wolno przekazywać takich informacji państwu. Bo państwu, na podstawie umowy o wzajemnej pomocy prawnej pomiędzy państwami, można przekazywać tylko te informacje, o które wyraźnie państwo wnioskuje.

W umowach o wzajemnej pomocy prawnej znajduje się zwrot: „informacje o toczących się postępowaniach, podejrzeniach, wolno przekazywać na prośbę. Państwo się musi zwrócić. Jeżeli „Pegasus" daje uzyskanie tej możliwości, to działanie takie jest nielegalne.

Jest prawdopodobne, że operator w Izraelu może wiedzieć do kogo został „Pegasus" włączony. Jeśli może wiedzieć, to jest to działanie niewątpliwie nielegalne. Wypełnione zostałyby znamiona przestępstwa przekroczenia uprawnień przez funkcjonariusza. A niekiedy nawet (w określonym stanie faktycznym) mogłoby to wypełnić znamiona przestępstwa szpiegostwa art. 130 k.k.

XII. Pozyskanie danych sprzed daty zarządzenie kontroli operacyjnej

Kontrola operacyjna rozpoczyna się z dniem udzielenia zgody na jej realizację. Jest ona pasywna bez możliwości tworzenia, fabrykowania dowodów. Takie działanie jest przestępstwem. Z systemem „Pegasus" wiąże się pierwszy problem polegający na tym, że pozwala on działać nie tylko pasywnie, ale także aktywnie, czyli wprowadzać zmiany w nośniku.

Toteż można sobie wyobrazić hipotetyczną (pozostaję z nadzieja, że tylko taką!) sytuację, że system wprowadza zmiany polegające na wprowadzeniu niedozwolonych treści na nośniku, np. pornografia dziecięca.

Wątpliwe jest, czy biegły będzie w stanie ustalić, czy jest to informacja, plik na nośniku, który został wprowadzony z zewnątrz i ewentualnie kiedy? Przepis art. 202 § 4a k.k. mówi o posiadaniu treści

pornograficznych z udziałem małoletniego, zatem samo istnienie zainfekowanego pliku wypełnia już znamiona przestępstwa.

Jeśli taka możliwość ingerencji (aktywnej) nie jest możliwa do wykrycia, ustalenia przez biegłego, nie ma znaczenia, czy dowody pochodzą sprzed zarządzenia kontroli, czy też po jej zarządzeniu. Chyba, że jasno i wprost wynika z treści nagrania - data, czasookres, kontekst sytuacyjny. Wtedy mamy do czynienia z przekroczeniem uprawnień, a dowody te w ramach kontroli operacyjnej wprowadzone do procesu być nie mogą.

Na podstawie art. 168b k.p.k. dowody zgromadzone przez jeden podsłuch – za zgodą prokuratora – można wykorzystać w innej sprawie. Ale musi być on legalny i nie wprowadzać (aktywnie) zmian w telefonie.

W związku z tak kontrowersyjnym charakterem (bardzo wąskim) przepisu 168a k.p.k., co do rzeczy, które działy się przed włączeniem „Pegasusa", nie można ich użyć. Jeśli jesteśmy w stanie rozgraniczyć, które dane powstały wcześniej.

Ze względu na zasadę praworządności (art. 7 Konstytucji RP, a także art. 6 k.p.k.) można wykorzystać te dowody, które w związku z zastosowaniem „Pegasusa" datowane są po jego wprowadzeniu, a to co przed – nie może być wprowadzone do procesu. Zgodnie z zasadą praworządności art. 168a k.p.k. działania takiego nie wyłącza, zaś art. 168b k.p.k. pozwala stosować za zgodą prokuratora do wszystkiego. Niemniej cały czas chodzi o urządzenia certyfikowane i dopuszczone do działania w ramach kontroli operacyjnej. System „Pegasus" certyfikowany nie jest.