KANCELARIA
SENATU

BIURO ANALIZ,
DOKUMENTACJI
I KORESPONDENCJI

Ekspertyza w przedmiocie: legalności zakupu i wykorzystywania na terytorium Rzeczypospolitej Polskiej systemu „Pegasus”

Opinie
i ekspertyzy

OE–381

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
styczeń 2022

R.pr. dr hab. Mariusz Bidziński
Prof. Uniwersytetu SWPS

Ekspertyza w przedmiocie: legalności zakupu i wykorzystywania na terytorium Rzeczypospolitej Polskiej systemu „Pegasus”

I. Źródła prawa

1. Konstytucja Rzeczypospolitej Polskiej z dn. 2 kwietnia 1997 r. (Dz.U. 1997 r., nr 78, poz. 483 ze zm.);
2. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, sporządzona w Rzymie dn. 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. 1993 r., nr 61, poz. 284 ze zm.);
3. Ustawa z dn. 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. 2020 r., poz. 1740 ze zm.);
4. Ustawa z dn. 6 kwietnia 1990 r. o Policji (Dz.U. 2021 r., poz. 1882 ze zm.);
5. Ustawa z dn. 6 czerwca 1997 r. Kodeks karny (Dz.U. 2021 r., poz. 2345 ze zm.);
6. Ustawa z dn. 6 czerwca 1997 r. Kodeks postępowania karnego (Dz.U. 2021 r., poz. 534 ze zm.);
7. Ustawa z dn. 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz.U. 2021 r., poz. 289 ze zm.);
8. Ustawa z dn. 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. 2021 r., poz. 1671 ze zm.);
9. Ustawa z dn. 27 sierpnia 2009 r. o finansach publicznych (Dz.U. 2021 r., poz. 305 ze zm.);
10. Ustawa z dn. 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz.U. 2021 r., poz. 2234);
11. Uchwała Senatu Rzeczypospolitej Polskiej z dn. 12 stycznia 2022 r. w sprawie powołania Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych.

II. Skróty i akronimy

1.	„CBA”	Centralne Biuro Antykorupcyjne
2.	„EKPC”	Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności
3.	„ETPC”	Europejski Trybunał Praw Człowieka
4.	„k.c.”	Ustawa z dn. 23 kwietnia 1964 r. Kodeks cywilny
5.	„k.k.”	Ustawa z dn. 6 czerwca 1997 r. Kodeks karny
6.	„Konstytucja RP”	Konstytucja Rzeczypospolitej Polskiej z dn. 2 kwietnia 1997 r.
7.	„k.p.k.”	Ustawa z dn. 6 czerwca 1997 r. Kodeks postępowania karnego
8.	„Ustawa o CBA”	Ustawa z dn. 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym

III. Stan faktyczny

„Pegasus” to nazwa oprogramowania szpiegującego, możliwego do zainstalowania na urządzeniach elektronicznych korzystających z systemów iOS i Android (w tym zwłaszcza na telefonach komórkowych), produkowanego przez izraelską spółkę NSO Group Technologies Ltd. Zainstalowanie oprogramowania na urządzeniu odbywa się zdalnie, bez świadomości użytkownika i otwiera podmiotowi infekującemu praktycznie nieograniczony dostęp do urządzenia, umożliwiając m.in.: 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 itp. (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 w dn. 13 stycznia 2022 r.). Innymi słowy, zainfekowanie urządzenia “Pegasusem” daje infekującemu praktycznie całkowitą kontrolę nad urządzeniem, z jego bieżącym używaniem oraz modyfikacją zapisanych w urządzeniu treści włącznie. Stosowanie „Pegasusa” jest niezależne od wiedzy

i zgody operatorów telekomunikacyjnych czy internetowych (J. Trela, *Czy Pegasus może być legalny?*, „Rzeczpospolita", 11 stycznia 2022 r.).

Jednocześnie wskazuje się, że kontrolę nad oprogramowaniem posiada licencjodawca, tj. NSO Group Technologies Ltd. z siedzibą w Herclijji (Izrael), co wiąże się z dostępem tego podmiotu do danych gromadzonych i przetwarzanych przez oprogramowanie (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. 13 stycznia 2022 r.). Dystrybucja licencji na „Pegasusa" jest reglamentowana przez Ministerstwo Obrony Izraela; licencja jest udzielana jedynie podmiotom państwowym (J.A. Gross, *Amid fallout from NSO scandal, Israel imposes new restrictions on cyber exports*, 6 grudnia 2021 r., https://www.timesofisrael.com/, dostęp w dn. 17 stycznia 2021 r.). Z uwagi na ofensywny charakter narzędzia (możliwość ingerencji w funkcjonowanie i zawartość zainfekowanego urządzenia), jest ono nazywane „bronią antyterrorystyczną".

Laboratorium „Citizen Lab" z siedzibą w Munk School of Global Affairs & Public Policy, która znajduje się w strukturach Uniwersytetu Toronto, ustaliło, że „Pegasus" był nabywany i wykorzystywany przez operatora z terenu Rzeczypospolitej Polskiej o nazwie „ORZELBIALY" (B. Marczak i in., *HIDE...*). Dalsze analizy laboratorium doprowadziły do ustalenia, że „Pegasusem" zostały zainfekowane urządzenia m.in. senatora X kadencji Krzysztofa Brejzy (w 2018 r., tj. w chwili infekcji – posła na Sejm VIII kadencji oraz szefa sztabu wyborczego Platformy Obywatelskiej), adw. Romana Giertycha oraz prokurator Ewy Wrzosek. Infekcje „Pegasusem" u ww. osób potwierdziła również organizacja Amnesty International.

W roku 2018 Najwyższa Izba Kontroli stwierdziła złamanie prawa polegające na przekazaniu przez Ministerstwo Sprawiedliwości Centralnemu Biuru Antykorupcyjnemu środków w wysokości 25 milionów złotych pochodzących z Funduszu Sprawiedliwości, co nastąpiło w roku 2017 i co mogło stanowić naruszenie dyscypliny finansów publicznych (*Pomoc z Funduszu Pomocy Pokrzywdzonym nie dla pokrzywdzonych*, 29 czerwca 2018 r., https://www.nik.gov.pl/, dostęp w dn. 13 stycznia 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). Wedle dalszych informacji medialnych, środki te zostały przekazane na zakup oprogramowania „Pegasus" przy pomocy podmiotu podstawionego (pośrednika – Matic sp. z o.o.; obecnie: Matic S.A.), który zarobił

na operacji 8 milionów złotych, przy czym fakt ten mają potwierdzać dokumenty w postaci m.in. faktury na zakup licencji (*NIK ujawnia faktury za „zakup środków techniki specjalnej". Pieniądze CBA otrzymało z Funduszu Sprawiedliwości*, 14 stycznia 2022 r., https://tvn24.pl/, dostęp w dn. 17 stycznia 2022 r.).

W pismach z dn. 9 września 2019 r. o znaku VII.519.2.2019.AG, Rzecznik Praw Obywatelskich wystąpił do Mateusza Morawieckiego – Prezesa Rady Ministrów oraz Waldemara Andzela – Przewodniczącego Komisji ds. Służb Specjalnych, wskazując m.in. na konieczność wyjaśnienia sprawy korzystania z „Pegasusa" przez polskie służby specjalne oraz na sprzeczność takiego postępowania z przepisami prawa, w tym Konstytucji RP. W piśmie z dn. 27 września 2019 r. o znaku DNB. WAKS.571.24.2019.BR, Maciej Wąsik – Sekretarz Stanu i Sekretarz Kolegium ds. Służb Specjalnych odmówił podania informacji, czy polskie służby specjalne korzystają z „Pegasusa".

W wywiadzie udzielonym tygodnikowi „Sieci" Jarosław Kaczyński, poseł IX kadencji i Wiceprezes Rady Ministrów, Przewodniczący Komitetu ds. Bezpieczeństwa Narodowego i spraw Obronnych, stwierdził m.in., że *„Źle by było, gdyby polskie służby nie miały tego typu narzędzia"* (tzn. „Pegasusa") oraz że *„Żaden Pegasus, żadne służby, żadne jakieś tajnie pozyskane informacje nie odgrywały w kampanii wyborczej w roku 2019 jakiejkolwiek roli"*. Wywiad ten odbierany jest przez media oraz opinię publiczną jako potwierdzenie, że organy Rzeczypospolitej Polskiej nabyły oprogramowanie „Pegasus" (*Kaczyński: Mamy Pegasusa, ale nie używaliśmy go wobec opozycji*, 7 stycznia 2022 r., https://www.gazetaprawna.pl/, dostęp w dn. 13 stycznia 2022 r.).

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. Zgodnie z § 2 uchwały, zadaniem Komisji jest m.in. wyjaśnienie ujawnionych przypadków nielegalnej inwigilacji z użyciem m.in. oprogramowania szpiegowskiego „Pegasus" oraz naruszeń prawa podczas stosowania przez służby specjalne kontroli operacyjnej.

IV. Analiza prawna

A. Konstytucyjne ramy stosowania instrumentów niejawnego dostępu do urządzeń elektronicznych

Przeprowadzanie w stosunku do danego podmiotu środków inwigilacji w postaci podsłuchu i rejestrowania rozmów, korespondencji, wglądu w dane zapisane na urządzeniu elektronicznym itp. przez aparat państwa bez wątpienia stanowi głęboką ingerencję w prawa i wolności jednostki. W szczególności, stosowanie omawianych środków wiąże się z ingerencją w prawo do życia prywatnego (art. 47 Konstytucji RP – *„Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym"*), tajemnicę komunikowania się (art. 49 Konstytucji RP – *„Zapewnia się wolność i ochronę tajemnicy komunikowania się. Ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony"*) oraz musi pozostawać w zgodzie z zakazem pozyskiwania i gromadzenia informacji zbędnych w demokratycznym państwie prawnym (art. 51 ust. 2 Konstytucji RP – *„Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym"*). Ograniczenie praw wyrażonych lub chronionych przez przywołane przepisy może nastąpić wyłącznie z zachowaniem zasad określonych w art. 31 ust. 3 Konstytucji RP. Granice praktycznej dopuszczalności ingerencji w prawa jednostki zakreślają również zasady legalizmu oraz demokratycznego państwa prawnego (art. 7 i art. 2 Konstytucji RP), jak również zasada przyrodzonej godności człowieka (art. 30 Konstytucji RP).

Trybunał Konstytucyjny w swym orzecznictwie wyznaczył granice stosowania omawianych środków. W wyroku z dn. 12 grudnia 2005 r. o sygn. K 32/04 (OTK-ZU 2005 r., seria „A", nr 11, poz. 132) wskazał przede wszystkim, że regulacja ingerująca w omawiane dobra jednostek musi przejść określony w art. 31 ust. 3 Konstytucji RP test proporcjonalności. Stosowane rozwiązanie musi być konieczne w demokratycznym państwie prawnym, a zatem niewystarczające jest wykazanie samej celowości, pożyteczności, taniości czy łatwości posługiwania się nim przez władzę. Trybunał podkreślił, że *„Bez znaczenia jest też argument porównawczy, że podobne środki w ogóle bywają stosowane w innych państwach"*. Stosowane środki nie mogą nadmiernie ingerować w sferę praw i wolności konstytucyjnych jednostki, a ingerencja musi podlegać kontroli sądowej. Środki nie mogą również

naruszać godności ludzkiej ani pozwalać organom władzy na działania arbitralne.

W przywołanym wyroku, Trybunał Konstytucyjny odwołał się do standardów wypracowanych w orzecznictwie ETPC na gruncie art. 8 EKPC (który wyraża prawo do poszanowania życia prywatnego i rodzinnego), zaaprobował te standardy i wskazał na konieczność dokonywania trójstopniowej oceny (testu) dopuszczalności ingerencji w prawo do prywatności. Polega ona na ustaleniu, czy:

- istnieje dostatecznie precyzyjna i skonkretyzowana podstawa ustawowa dla ograniczenia;
- ingerencja jest konieczna w demokratycznym państwie prawnym (przy czym należy przyjąć standard państwa oświeconego, otwartego, tolerancyjnego, dysponującego odpowiednio fachowym aparatem policyjnym, zdolnym działać w rzetelny, profesjonalny i nie małostkowy czy złośliwy sposób, traktującym wkroczenie w sferę chronionych praw jednostki jako zło konieczne, a nie tylko jako czynnik usprawniający pracę policji);
- jaki jest cel ingerencji (czy mieści się w celach przewidzianych w art. 8 EKPC, jakimi są: bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochrona porządku i zapobieganie przestępstwom, ochrona zdrowia i moralności lub ochrona praw i wolności osób); jeżeli „przy okazji" zbierania danych na ww. cele dochodzi do zbierania innych danych (np. dotyczących kwestii prywatnych, obyczajowych), to oznacza to, że działanie władzy następuje z pogwałceniem omawianego prawa.

Podobne stanowisko zostało przedstawione przez Trybunał Konstytucyjny w wyroku z dn. 23 czerwca 2009 r. o sygn. K 54/07 (OTK-ZU 2009 r., seria „A", nr 6, poz. 86), gdzie wskazano, że niedopuszczalne jest przyjmowanie mechanizmów niezapewniających możliwości kontroli gromadzenia danych w sposób niejawny. Podkreślono, że *„Obserwacja winna mieścić się w granicach niezbędności dla założonego celu obserwacji. Te trzy ograniczenia (celowości, subsydiarności działania, niezbędności prowadzonej obserwacji) służą minimalizacji niekoniecznych – z punktu widzenia celu działalności operacyjnej – wkroczeń w prywatność. Realizacja tej zasady wymaga ponadto efektywnej kontroli zapobiegającej ekscesowi"* (w tej materii, zob. również T.M. Miłkowski, *Czynności operacyjno-rozpoznawcze a prawa i wolności jednostki*, Warszawa 2020, LEX/el., rozdział 1, pkt 2 oraz P. Wiliński, *Proces karny w świetle konstytucji*, Warszawa 2011, LEX/el., rozdział 8, pkt 7).

B. Ustawowe ramy stosowania instrumentów niejawnego dostępu do urządzeń elektronicznych

Stosowanie podsłuchów i – szerzej ujmując – niejawnej kontroli przez organy państwa uregulowane jest w przepisach, które można podzielić na dwie grupy. Pierwsza odnosi się do tzw. podsłuchu procesowego (uregulowanego w art. 237–242 k.p.k.), druga – do tzw. kontroli operacyjnej, w tym podsłuchu pozaprocesowego (uregulowanej w ustawach szczególnych, dedykowanych działalności poszczególnych służb).

Artykuły 237–242 k.p.k. przewidują możliwość zarządzenia przez sąd (a w przypadkach niecierpiących zwłoki – prokuratora) *„kontroli i utrwalania treści rozmów telefonicznych w celu wykrycia i uzyskania dowodów dla toczącego się postępowania lub zapobieżenia popełnieniu nowego przestępstwa”* (art. 237 § 1 k.p.k.); dopuszczalne jest również wyrażenie zgody na kontrolę i utrwalanie *„treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną”* (art. 241 k.p.k.). Kontrola może zatem zostać zastosowana wyłącznie w przypadku wszczęcia postępowania (A.R. Stefański, S. Zabłocki, *Kodeks postępowania karnego. Tom II. Komentarz do art. 167-296*, Warszawa 2019, LEX/el., komentarz do art. 237 k.p.k., pkt 4). W art. 237 § 4 k.p.k. zakreślony został ograniczony krąg osób, które mogą być objęte podsłuchem procesowym. Są to: osoba podejrzana, oskarżony, pokrzywdzony lub inna osoba, z którą może się kontaktować oskarżony albo która może mieć związek ze sprawcą lub z grożącym przestępstwem. Ustawa nie przewiduje możliwości samej kontroli treści rozmów/przekazów informacji – konieczne jest prowadzenie kontroli połączonej z nagrywaniem (przechwytywaniem) przekazu (tamże, pkt 3). Kodeks nie określa podmiotów, które wykonują postanowienie o kontroli, ale nakłada na określone urzędy, instytucje i przedsiębiorców obowiązek umożliwienia wykonania postanowienia. Na gruncie art. 241 k.p.k. dopuszczalne jest poddawanie kontroli tylko tych informacji, których przejęcie nastąpiło, zanim zostały zapisane na nośniku informacji (R. Stefański, S. Zabłocki, *Kodeks...*, komentarz do art. 241 k.p.k., pkt 1). Z powyższego wynika, że podsłuch procesowy może być stosowany do przechwytywania treści rozmów na bieżąco, nie zaś – do uzyskiwania wglądu w pamięć urządzenia służącego do przekazu informacji.

Zasady prowadzenia kontroli operacyjnej (w tym podsłuchu operacyjnego) regulują ustawy szczególne, w tym zwłaszcza pragmatyki służbowe. Wskazać można w tym zakresie np. na art. 17 Ustawy o CBA, art. 19 ustawy z dn. 6 kwietnia 1990 r. o Policji czy art. 9 ustawy z dn. 10 czerwca 2016 r. o działaniach antyterrorystycznych. Ustawodawca

przewidział zasadniczo pięć rodzajów kontroli operacyjnej, która może polegać 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.

Wskazuje się, że *„Stosowanie środków technicznych umożliwia uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych"* (S. Hoc, P. Szustakiewicz, *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, LEX/el. 2012, komentarz do art. 17 Ustawy o CBA, pkt 5). Ustawy nie przewidują natomiast dopuszczalności przejmowania kontroli nad urządzeniem czy modyfikacji zapisanych w jego pamięci treści (co do uzyskiwania i utrwalania danych zawartych na nośnikach danych por. szerzej M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz*, Warszawa 2018, komentarz do art. 9 ustawy o działaniach antyterrorystycznych, pkt. 22–29).

Kontrola operacyjna, podobnie jak podsłuch procesowy, wymaga uzyskania postanowienia sądu o zarządzeniu kontroli (albo zarządzenia następczego, zatwierdzającego kontrolę przeprowadzoną w warunkach niecierpiących zwłoki) i może być prowadzona przez daną służbę jedynie w związku z określonymi w danej ustawie przestępstwami. Kontrola ma zawsze charakter subsydiarny, co oznacza, że może być zarządzona tylko wtedy, gdy inne środki okazały się bezskuteczne lub są nieprzydatne (M. Rogalski, *Podsłuch procesowy i pozaprocesowy. Kontrola i utrwalanie rozmów na podstawie kpk oraz ustaw szczególnych*, Warszawa 2019, LEX/el., rozdział III, pkt 2).

Trybunał Konstytucyjny w wyroku z dn. 30 lipca 2014 r. o sygn. K 23/11 (OTK-ZU 2014 r., seria „A", nr 7, poz. 80) wskazał, że przy stosowaniu środków kontroli operacyjnej, niezbędna jest ich indywidualizacja, albowiem organy mogą stosować jedynie te środki, które są

prawnie dopuszczalne. W kontekście tej wypowiedzi Trybunału należy zauważyć, że o ile sądy powinny kontrolować środki techniczne, które zamierzają wykorzystywać służby, to ustawy nie przyznają im kompetencji do legalizowania stosowania środków technicznych, których stosowanie jest generalnie albo w danych warunkach niedopuszczalne.

C. Dopuszczalność stosowania oprogramowania „Pegasus" w prawie polskim – uwagi ogólne

Uwzględniając konstytucyjne granice ingerencji w prawa jednostek (w tym zwłaszcza prawo do prywatności i prawa z nią związane), ustawowe ramy dla inwigilacji z jednej strony oraz możliwości techniczne i sposób funkcjonowania „Pegasusa" z drugiej, dojść należy do wniosku, że jego stosowanie jest na gruncie prawa polskiego **niedopuszczalne.**

Po pierwsze, „Pegasus" jako ofensywne narzędzie totalnej inwigilacji, nie wpisuje się w ramy istniejących instytucji procesowych. Zainfekowanie urządzenia takim oprogramowaniem skutkuje uzyskaniem przez infekującego nie tylko **pełnego dostępu do wszystkich danych** znajdujących się na urządzeniu, ale również **możliwości kontroli urządzenia,** w tym **zmiany zawartości pamięci urządzenia.** Przepisy ustaw (tj. art. 237 i 241 k.p.k. oraz przepisy ustaw szczególnych) zawierają katalogi dopuszczalnych czynności operacyjnych (kontrola i utrwalanie rozmów, uzyskiwanie i utrwalanie treści korespondencji itd.), natomiast nie wskazują na konkretne środki służące do realizacji tych czynności (np. poprzez wskazanie technicznej metody podsłuchu). Nie ulega przy tym wątpliwości, że wyrażenie przez właściwy organ zgody na daną czynność stanowi upoważnienie tylko i wyłącznie do realizowania jej przy pomocy środków adekwatnych. Dopuszczalne jest stosowanie tylko takich środków, które nie prowadzą do dalszej ingerencji w prawa jednostki, niż jest to niezbędne do zamierzonego celu (reguła instrumentalnego nakazu). Ani przepisy k.p.k., ani ustaw szczególnych, nie dają organom państwa uprawnienia do ingerencji w zawartość urządzeń ani możliwości przejmowania nad nimi kontroli, albowiem celem inwigilacji procesowej jest uzyskanie określonych informacji (danych) – i to w formie możliwie nieinwazyjnej, a nie kreowanie, zmiana albo usuwanie danych. Z tego, wszakże względu „Pegasus" traktowany jest nie jako narzędzie operacyjne (do zbierania danych o przestępstwach), ale jako broń (narzędzie do wpływania na postępowanie przestępców i podmiotów wrogich). Fakt ten powoduje, że niezależnie od kwestii dopuszczalności stosowania „Pegasusa" w świetle

konstytucji i EKPC (o czym dalej), nie ma prawnej możliwości realizowania przy jego pomocy ani kontroli przewidzianej w art. 237 – 242 k.p.k., ani kontroli operacyjnej przewidzianej w ustawach szczególnych (w tym zwłaszcza art. 17 Ustawy o CBA).

Co więcej, obowiązujące przepisy prawa nie pozwalają żadnemu z organów państwowych na przełamywanie zabezpieczeń (*hacking*) i przechwytywanie oraz wykorzystywanie treści przekazów komunikacyjnych (tak Rzecznik Praw Obywatelskich w wystąpieniu z dn. 9 września 2019 r. o znaku VII.519.2.2019.AG, s. 4). Potwierdza to fakt, że **na gruncie obecnie obowiązujących regulacji stosowania kontroli sądowej oraz operacyjnej, stosowanie „Pegasusa" nie może mieć miejsca.**

Należy jednocześnie podkreślić, że włamanie się do urządzenia przy użyciu „Pegasusa" wiąże się z ingerencją w strukturę danych urządzenia. W połączeniu z możliwością niekontrolowanej ingerencji w funkcjonowanie i pamięć urządzenia (a zatem możliwość zmiany treści utrwalonych na nim plików oraz wykonywania wszelkiego rodzaju czynności bez zgody i wiedzy użytkownika telefonu), wartość dowodowa danych pozyskanych przy pomocy „Pegasusa" jest znikoma, jeżeli nie zerowa. Nigdy bowiem nie ma pewności, że zawartość urządzenia nie została zmodyfikowana przez organ stosujący „Pegasusa" na niekorzyść podmiotu inwigilowanego. Również ten aspekt funkcjonowania systemu wyłącza dopuszczalność jego stosowania **– z uwagi na nieprzydatność na gruncie procesowym.**

W kontekście powyższego należy ponadto zasygnalizować, że zgoda sądu na podjęcie określonych czynności operacyjnych **nie oznacza zgody** na wykorzystanie przez inwigilującego dowolnych środków technicznych, w tym „Pegasusa", choćby nawet podmiot zamierzający go stosować poinformował o tym sąd. Jak zostało wyżej wskazane, sąd nie posiada kompetencji do legalizowania stosowania środków, których stosowanie w świetle prawa jest niedopuszczalne (czy to generalnie, czy też w indywidualnym przypadku). W konsekwencji, nawet wydanie przez sąd zgody na przeprowadzenie kontroli procesowej lub operacyjnej w określony sposób i przy wykorzystaniu określonych środków technicznych nie prowadzi do dekryminalizacji zastosowania „Pegasusa".

W ocenie Eksperta, stosowanie „Pegasusa" jest nie do pogodzenia z wartościami wyrażonymi w art. 47, art. 49 i art. 51 ust. 2 Konstytucji RP oraz art. 8 EKPC, albowiem stanowi zbyt daleko idącą, rażąco nieproporcjonalną ingerencję w prawa jednostek. Jakkolwiek na gruncie Konstytucji RP jest dopuszczalne nawet daleko idące ograniczenie prawa do prywatności oraz tajemnicy komunikacji, to ingerencja ta nie

może godzić w istotę tych praw. Zainfekowanie urządzenia „Pegasusem" sprawia, że służby uzyskują całkowitą kontrolę nad urządzeniem, co przy roli telefonów komórkowych oznacza praktycznie przejęcie kontroli nad życiem prywatnym (możliwość dostępu do wszystkich zalogowanych serwisów, dokonywania dyspozycji majątkowych, korespondowania z innymi ludźmi pod przykrywką użytkownika telefonu, podsłuchiwania i podglądania w każdym czasie i miejscu itd.; w istocie: kradzież tożsamości). Jest to nie tylko naruszenie prywatności w wymiarze powzięcia wiedzy o życiu prywatnym, ale również w wymiarze nieuświadomionej inwigilowanemu najgłębszej ingerencji w jego życie osobiste. Tak głęboka ingerencja w sferę prywatności (a nawet głębiej: intymności) człowieka narusza istotę prawa wyrażonego w art. 47 Konstytucji RP oraz narusza przyrodzoną godność człowieka (art. 30 Konstytucji RP), albowiem czyni człowieka jedynie instrumentem w urzeczywistnianiu celów organu władzy (por. wyrok Trybunału Konstytucyjnego z dn. 9 lipca 2009 r., sygn. SK 48/05, OTK-ZU 2009 r., seria „A", nr 7, poz. 108).

Ciężko sobie wyobrazić sytuacje, w których stosowanie „Pegasusa" i związana z tym ingerencja w prywatność i tajemnicę komunikacji, będą mogły być uznane za proporcjonalne w stosunku do celów, którym inwigilacja ma służyć. Wobec wykorzystywania omawianego oprogramowania bez podstawy prawnej nie da się prawidłowo przeprowadzić testu proporcjonalności. Przyjmując nawet założenie, że potencjalnym uzasadnieniem dla inwigilacji może być chęć zagwarantowania zewnętrznego lub wewnętrznego bezpieczeństwa państwa oraz zapobieżenia przestępstwom, to ochrona tych wartości ma przecież swoje granice. Totalna inwigilacja, połączona z możliwością niejawnego wpływania na życie inwigilowanego (sterowania nim), charakteryzuje państwa totalitarne i nie może być stosowana w państwach demokratycznych. Takie działanie nie służy bowiem ochronie obywateli oraz ich godności, która stanowi źródło innych praw podmiotowych, ale służy ochronie aparatu państwowego przed samymi obywatelami.

Jak zostało wyżej wskazane, „Pegasus" nie jest uznawany za narzędzie kontroli operacyjnej, ale jako broń cybernetyczna w walce z zagrożeniami dla bezpieczeństwa kraju. Z tego względu, można teoretycznie wyobrazić sobie stosowanie „Pegasusa" przez organy władzy publicznej w stosunku do wrogów Rzeczypospolitej, w warunkach bojowych albo w przypadku rzeczywistego zagrożenia popełnienia najcięższych gatunkowo przestępstw (terroryzmu, zbrodni ściganych na mocy konwencji międzynarodowych), w stosunku do obywateli państw obcych (którzy nie podlegają ochronie na gruncie art. 51 ust. 2 Konstytucji RP).

Przyjmując założenie, że w tych wyjątkowych, ekstraordynaryjnych sytuacjach stosowanie „Pegasusa" będzie w świetle Konstytucji RP i EKPC dopuszczalne, to pozostaje to bez znaczenia dla sytuacji analizowanej w realiach nin. ekspertyzy. Wyżej opisane przypadki nie stanowią przypadków kontroli (sądowej, operacyjnej) przeprowadzanej przez służby w celu zapobiegania czy wykrywania przestępstw, ale przypadki działań ofensywnych w stosunku do wrogów państwa. W konsekwencji, nawet, jeżeli wykorzystywanie rzeczonego oprogramowania może być wyjątkowo dopuszczalne przy działaniach bojowych czy antyterrorystycznych, to te działania nie mieszczą się w kategorii kontroli operacyjnej, a przy tym – nie należą do określonych w art. 1 i 2 Ustawy o CBA zadań Centralnego Biura Antykorupcyjnego, któremu zarzuca się nabycie i wykorzystywanie „Pegasusa" (tak samo Rzecznik Praw Obywatelskich w wystąpieniu z dn. 9 września 2019 r. o znaku VII.519.2.2019.AG, s. 4).

D. Stosowanie oprogramowania „Pegasus" a odpowiedzialność karna

Z uwagi na wskazaną wyżej generalną niedopuszczalność stosowania systemu „Pegasus" na gruncie prawa polskiego, posługiwanie się nim nawet dla realizacji celów prawnie dozwolonych (kontroli operacyjnej) jest niedopuszczalne. Jak zostało bowiem wyjaśnione, realizacja celów prawnie dozwolonych może następować jedynie przy wykorzystaniu legalnych środków. W konsekwencji, każde stosowanie systemu „Pegasus" dla celów określonych w k.p.k. i ustawach szczególnych stanowić będzie działanie penalizowane.

Nawet gdyby zgodzić się z prezentowanym niekiedy stanowiskiem, że teoretycznie, w wyjątkowych przypadkach związanych ze zwalczaniem terroryzmu, w przypadku operacji polegających wyłącznie na inwigilacji obywateli państw obcych, stosowanie oprogramowania „Pegasus" może być uznane za spełniające wyżej opisane testy zgodności z Konstytucją RP i aktami prawa międzynarodowego (abstrahując od konieczności uprzedniego ustanowienia ustawowych ram dla stosowania tego rodzaju środka, których obecnie brak), to wciąż jego typowe użycie, zwłaszcza zaś – użycie przeciwko obywatelowi polskiemu, będzie stanowiło działanie bezprawne. Należy mieć na uwadze, że do wyłączenia bezprawności podsłuchu (czy innych form inwigilacji) niezbędne jest działanie w ramach przepisów stanowiących ramy procesowej i pozaprocesowej kontroli (por. M. Rogalski, *Podsłuch*..., rozdział III, pkt 2 oraz wyrok SN z dn. 13 listopada 2002 r., sygn. I CKN 1150/00, LEX nr 75292).

Wskazać należy na art. 231 § 1 k.k., zgodnie z którym *„Funkcjonariusz publiczny, który, przekraczając swoje uprawnienia lub nie dopełniając obowiązków, działa na szkodę interesu publicznego lub prywatnego, podlega karze pozbawienia wolności do lat 3”*. Paragraf 2 tego artykułu zaostrza odpowiedzialność w przypadku popełnienia przestępstwa w celu osiągnięcia korzyści majątkowej lub osobistej (zgodnie z art. 115 § 4 k.k., chodzi tu o korzyść dla siebie lub osoby trzeciej; może być to również korzyść o charakterze politycznym – zob.np. J. Giezek, [w:] J. Giezek (red.), *Kodeks karny. Część ogólna. Komentarz*, Warszawa 2021, LEX/el., komentarz do art. 115 k.k., pkt 6). Funkcjonariusze służb, które mogą mieć dostęp do systemu „Pegasus” i próbować wykorzystywać go w ramach czynności operacyjnych, są funkcjonariuszami publicznymi w rozumieniu art. 115 § 13 pkt 7 k.k. (funkcjonariusze organów powołanych do ochrony bezpieczeństwa publicznego). Wykorzystanie nielegalnego środka do realizacji kontroli operacyjnej stanowić będzie zatem przekroczenie uprawnień tych funkcjonariuszy ze szkodą zarówno dla interesu publicznego (w tym zwłaszcza z uwagi na naruszenie zaufania do państwa i jego instytucji w kontekście zasady legalizmu), jak również prywatnego (naruszenie praw i wolności osób objętych inwigilacją), przez co stanowić może podstawę dla ich odpowiedzialności karnej.

Artykuł 267 k.k. stanowi:

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Stosowanie „Pegasusa” nierozerwalnie wiąże się z ingerencją większą, niż zakreślona przepisami k.p.k. i ustaw szczególnych, co zresztą sprawia, że jest to środek nieproporcjonalny do ochrony wartości, które mają uzasadniać jego stosowanie.

W szczególności, z uwagi na uzyskanie w wyniku zainfekowania urządzenia „Pegasusem" dostępu do wszelkich danych zapisanych w pamięci urządzenia, możliwości ich modyfikacji oraz możliwości kontrolowania urządzenia w sposób niemal całkowicie dowolny, każde zastosowanie analizowanego oprogramowania musi prowadzić do uzyskania przez stosujący je organ dostępu do danych i informacji dla niego nieprzeznaczonych, niemogących wchodzić w ustawowy zakres kontroli. Co więcej, każde zastosowanie „Pegasusa" wiąże się z przełamaniem zabezpieczeń urządzenia. Z tego względu, każdorazowe skorzystanie z „Pegasusa" wypełniać będzie znamiona przestępstw opisanych w § 1–3 omawianego artykułu. Nawet przy przyjęciu względniejszej interpretacji, dopuszczającej warunkowe, wyjątkowe korzystanie z „Pegasusa" w przypadkach terroryzmu, to wciąż jego stosowanie wobec obywateli Rzeczypospolitej Polskiej, zwłaszcza zaś stosowanie nieproporcjonalne, w związku z podejrzeniem popełnienia przestępstw o niższym niż najwyższy ciężar gatunkowy, tym bardziej – stosowanie mogące prowadzić do uzyskania informacji niepodlegających ujawnieniu (np. objętych tajemnicą adwokacką, w tym obrończą, tajemnicą postępowania przygotowawczego itp.) będzie wypełniać znamiona opisanych czynów.

Zgodnie z § 4 omawianego artykułu, karze podlega również ten, kto ujawnia informację uzyskaną w warunkach § 1–3 innej osobie. Z uwagi na sposób funkcjonowania systemu „Pegasus", który wymaga zaangażowania podmiotu trzeciego (dostawcy systemu – NSO Group Technologies Ltd. albo podmiotów przez niego upoważnionych), z wysokim prawdopodobieństwem można przyjąć, że informacje pozyskiwane w drodze stosowania „Pegasusa" są przynajmniej częściowo przetwarzane przez osoby trzecie, w tym zwłaszcza zagraniczną spółkę prawa handlowego. Takie działanie kwalifikować należy jako ujawnienie pozyskanej nielegalnie informacji innej osobie, co wypełnia znamiona czynu opisanego w omawianym przepisie.

Stosownie do treści art. 130 § 2 k.k., *„Kto, biorąc udział w obcym wywiadzie albo działając na jego rzecz, udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 3"*. Jak zostało wyżej wskazane, ze stosowaniem oprogramowania „Pegasus" immanentnie wiąże się zautomatyzowane przetwarzanie przynajmniej części pozyskiwanych za pomocą oprogramowania danych przez podmiot zewnętrzny, tj. NSO Group Technologies Ltd., przy czym kontrolę nad udzielaniem licencji podmiotom zagranicznym posiada Ministerstwo Obrony Izraela. W takiej sytuacji, z wysokim prawdopodobieństwem można przyjąć, że dostęp do przetwarzanych informacji

posiadają również służby specjalne państwa Izrael. Korzystanie z „Pegasusa" prowadzić musi zatem do automatycznego udzielania obcemu wywiadowi informacji, pośród których mogą być dane, których przekazanie może – choćby teoretycznie – wyrządzić szkodę Rzeczypospolitej Polskiej. Będzie tak np. w sytuacji, gdy obcy wywiad uzyska dostęp do informacji niejawnych, do których dostęp posiada poseł (senator), adwokat czy prokurator, w szczególności wiążących się z prowadzoną kampanią wyborczą czy postępowaniami (karnymi, administracyjnymi, a nawet – cywilnymi) z udziałem osób piastujących funkcje w organach władzy publicznej. Wykorzystanie takich informacji przez obcy wywiad ze szkodą dla Rzeczypospolitej Polskiej jest nie tylko oczywiście możliwe, ale również wysoce prawdopodobne. Jednocześnie, osoby wykorzystujące „Pegasusa" muszą mieć świadomość mechanizmu działania narzędzia oraz co najmniej wysokiego prawdopodobieństwa posiadania dostępu do pozyskiwanych danych przez służby specjalne obcego państwa, przez co korzystanie z „Pegasusa" kwalifikować należy jako „działanie na rzecz" obcego wywiadu w rozumieniu przywołanego przepisu. W konsekwencji, nie można obecnie wykluczyć, że osoby dokonujące kontroli operacyjnej przy pomocy oprogramowania „Pegasus" dopuścić się mogły zbrodni szpiegostwa.

Co oczywiste, odpowiedzialność za wyżej wskazane czyny zabronione ponosić mogą nie tylko funkcjonariusze i pracownicy służb bezpośrednio odpowiedzialni za obsługę i stosowanie „Pegasusa", ale również ich przełożeni, w tym kierownictwo służb, osoby piastujące funkcje w innych organach państwa (np. odpowiedzialne za nadzór nad służbami czy sfinansowanie nabycia licencji na „Pegasusa") oraz beneficjenci inwigilacji. Podmioty te mogą odpowiadać jako współsprawcy, ale również z uwagi na pomocnictwo, podżeganie lub sprawstwo kierownicze.

Z uwagi na brak pełnej wiedzy o faktycznym zasięgu i przypadkach stosowania systemu „Pegasus" przez polskie organy bezpieczeństwa publicznego, nie można na ten moment wykluczyć popełnienia przez ww. osoby również innych czynów zabronionych ustawą karną. Należy podkreślić, że niezależnie od odpowiedzialności karnej, osoby zaangażowane w proceder inwigilacji „Pegasusem" podlegają również odpowiedzialności dyscyplinarnej, przewidzianej w ustawach pragmatycznych.

E. Dopuszczalność nabycia oprogramowania „Pegasus"

Stosownie do art. 269b § 1 k.k., zabronione pod groźbą kary pozbawienia wolności jest wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie

innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstw określonych w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 lub 2 albo art. 269a k.k., a także haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej. Zgodnie z § 1a tego artykułu, nie popełnia przestępstwa ten, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia. Zgodnie zaś z § 2, *„W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy"*.

Jak zostało wyżej wskazane, na gruncie prawa polskiego praktycznie nie jest możliwe korzystanie z systemu „Pegasus" w sposób legalny, a z pewnością – nie jest możliwe korzystanie z niego w celach kontroli sądowej lub operacyjnej. „Pegasus" z natury rzeczy umożliwia nie tylko popełnienie przestępstwa określonego w art. 267 § 3 k.k., ale również określonego w art. 268a § 1 i 2 (przestępstwo niszczenia, uszkadzania, usuwania, zmieniania lub utrudniania dostępu do danych) oraz w art. 269 § 1 i 2 (przestępstwo niszczenia, uszkadzania lub zmieniania danych o szczególnym znaczeniu dla kraju). Umożliwia on bowiem wykonywanie operacji na cudzym urządzeniu w wymiarze przekraczającym konstytucyjnie i ustawowo ograniczony zakres czynności operacyjnych. W konsekwencji, „Pegasus" umożliwia – choćby potencjalne – wykonywanie operacji w zakresie, w jakim organ państwa nawet teoretycznie nie może być uprawniony, a zatem „Pegasus" jest oprogramowaniem, o którym mowa w art. 268b § 1 k.k. Skoro brak jest przepisów prawa, które umożliwiałyby organom państwa korzystanie z „Pegasusa" (poza sytuacją opisaną w art. 268b § 2 k.k.), to nie sposób wskazać na przepisy prawa, które dawałyby podstawę do zakupu tego rodzaju oprogramowania. W konsekwencji, wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie „Pegasusa" stanowi wyżej opisane przestępstwo.

Mając na uwadze schemat domniemanego nabycia licencji na „Pegasusa" przez Centralne Biuro Antykorupcyjne, podkreślić należy, że sprawców czynu z art. 269b § 1 k.k. należy poszukiwać nie tylko w gronie kierownictwa oraz funkcjonariuszy i pracowników CBA biorących udział w transakcji, ale również po stronie pośrednika przy nabyciu licencji (piastunów organów oraz pracowników spółki pośredniczącej) – jako zbywcy oprogramowania względem CBA oraz pośród kierownictwa

i pracowników Ministerstwa Sprawiedliwości – z uwagi na pomoc przy nabyciu oprogramowania, znajdującą wyraz w przekazaniu środków na ten cel z Funduszu Sprawiedliwości.

Należy podkreślić, że odpowiedzialność karna związana z obrotem oprogramowania przystosowanego do nielegalnej inwigilacji jest niezależna od ewentualnej a zasygnalizowanej przez Najwyższą Izbę Kontroli i Rzecznika Praw Obywatelskich odpowiedzialności za złamanie dyscypliny finansów publicznych. W szczególności należy zwrócić uwagę na możliwość złamania zakazu finansowania CBA ze źródeł znajdujących się poza budżetem państwa, poprzez dofinansowanie służby środkami z Funduszu Sprawiedliwości, co stoi w sprzeczności z art. 4 ust. 1 Ustawy o CBA oraz art. 11 ustawy z dn. 27 sierpnia 2009 r. o finansach publicznych i co może stanowić naruszenie w rozumieniu art. 11 ust. 1 ustawy z dn. 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych przez dysponenta Funduszu. Na obecnym etapie sprawy, niewykluczone jest stwierdzenie naruszeń dyscypliny również przez inne podmioty zaangażowane w procedurę przekazania funduszy do CBA.

Wynikający z art. 269b § 1 k.k. zakaz obrotu oprogramowaniem i sprzętem służącym do nielegalnej inwigilacji lub innego rodzaju *hackingu* sprawia, że oprogramowanie „Pegasus" stanowi *res extra commercium* – rzecz wyłączoną z obrotu cywilnego (por. szerzej A. Obłąk, *„Rzeczy wyłączone z obrotu"* (res extra commercium) *w polskim porządku prawnym*, [w:] J. Jezioro, K. Zagrobelny (red.), *Wybrane zagadnienia polskiego prawa prywatnego. Księga pamiątkowa ku czci Doktora Józefa Kremisa i Doktora Jerzego Strzebinczyka*, Wrocław 2019, s. 185–195). W tym kontekście należy wskazać na konsekwencje zawarcia i wykonania umowy, której przedmiotem jest odpłatne nabycie rzeczy wyłączonej z obrotu (tutaj: udzielenie licencji na korzystanie z oprogramowania wyłączonego z obrotu). Tego rodzaju umowa jest bezwzględnie nieważna (art. 58 k.c.), co może otwierać drogę do dochodzenia przez Skarb Państwa od kontrahenta CBA (pośrednika w nabyciu licencji) zwrotu świadczenia pieniężnego uiszczonego w zamian za przeniesienie licencji czy też udzielenie dalszej licencji.

V. Konkluzje

1. Stosowanie wszelkich środków kontroli operacyjnej wiąże się w ingerencją w konstytucyjne i konwencyjne prawa jednostki, w tym zwłaszcza prawo do życia prywatnego, tajemnicę korespondencji

oraz zakaz pozyskiwania i gromadzenia przez państwo informacji zbędnych w demokratycznym państwie prawnym (art. 47, art. 49 i art. 51 ust. 2 Konstytucji oraz art. 8 EKPC).

2. Korzystanie z kontroli operacyjnej nie może prowadzić do naruszenia godności ludzkiej (art. 30 Konstytucji RP) oraz może następować wyłącznie w granicach zakreślonych zasadą legalizmu oraz demokratycznego państwa prawnego (art. 7 i art. 2 Konstytucji RP).
3. Zgodnie z orzecznictwem Trybunału Konstytucyjnego, ograniczenie praw i wolności jednostki w drodze kontroli operacyjnej może nastąpić tylko w przypadku, gdy istnieje ku temu precyzyjna podstawa ustawowa, ingerencja jest konieczna w demokratycznym państwie prawnym, zaś cel ingerencji stanowi istotną wartość konstytucyjną.
4. Ograniczenie praw i wolności musi przejść test proporcjonalności wynikający z art. 31 ust. 3 Konstytucji.
5. Ingerencja w prawa i wolności musi być celowa, subsydiarna i niezbędna oraz podlegać efektywnej kontroli, w tym sądowej.
6. Oprogramowanie „Pegasus" umożliwia inwigilującemu pełny (totalny) dostęp do urządzenia elektronicznego (telefonu) osoby inwigilowanej, w tym m. in. na podsłuchiwanie rozmów, ingerencje w wiadomości, modyfikowanie, usuwanie i dodawanie plików w pamięci urządzenia, zmianę ustawień technicznych itp.
7. Stosowanie „Pegasusa" jest na gruncie prawa polskiego niedopuszczalne z racji, iż umożliwia niekontrolowany dostęp do sfery intymnej człowieka, przyznając inwigilującemu możliwość niejawnego wpływania na tok życia inwigilowanego, w tym kradzież jego tożsamości.
8. W systemie prawnym Rzeczpospolitej Polskiej stosowanie „Pegasusa" nie jest dopuszczalne. Brak jest jakichkolwiek ram ustawowych, które pozwalałyby służbom na prowadzenie działań operacyjnych połączonych z przełamywaniem zabezpieczeń i uzyskiwaniem kontroli nad urządzeniem elektronicznym.
9. Uregulowana w k.p.k. instytucja podsłuchu sądowego oraz warianty uregulowanej w ustawach szczególnych kontroli operacyjnej pozwalają jedynie na kontrolowanie i rejestrowanie – od chwili uzyskania sądowej zgody – rozmów i korespondencji inwigilowanych oraz kopiowanie zawartości nośników danych. Zakres ingerencji systemu „Pegasus" wykracza poza jakiekolwiek znane w polskim systemie prawnym normy.
10. Wobec braku ram ustawowych dla legalnego stosowania „Pegasusa", każde jego wykorzystanie przez funkcjonariuszy organów państwa klasyfikować należy jako przekroczenie uprawnień ze szkodą dla

interesu publicznego i prywatnego, co stanowi czyn opisany w art. 231 § 1 k.k.

11. Stosowanie „Pegasusa" wypełnia znamiona przestępstw opisanych w art. 267 § 1–3 k.k. (nieuprawnione uzyskiwanie dostępu do informacji, systemu informatycznego oraz posługiwanie się urządzeniem podsłuchowym).
12. Z uwagi na fakt, że wykorzystywanie „Pegasusa" związane jest z przetwarzaniem przynajmniej części pozyskiwanych danych przez podmiot zewnętrzny (administratora systemu i licencjodawcę – NSO Group Technologies Ltd.), stanowi to czyn opisany w art. 267 § 4 k.k.
13. Eksport licencji na „Pegasusa" podlega kontroli Ministerstwa Obrony Izraela, co wskazuje na bardzo wysokie prawdopodobieństwo, że dostęp do pozyskiwanych przez użytkowników oprogramowania danych posiadają służby specjalne tego państwa. Fakt ten może wypełniać znamiona zbrodni szpiegostwa (art. 130 § 2 k.k.), poprzez działanie na rzecz obcego wywiadu, polegające na zbieraniu i przekazywaniu danych istotnych z punktu widzenia bezpieczeństwa Rzeczypospolitej Polskiej.
14. Z uwagi na brak możliwości korzystania przez służb z „Pegasusa" na cele kontroli operacyjnej, zakup licencji na to oprogramowanie był i jest niedopuszczalny, zaś fakt zakupu wypełnia znamiona określone w art. 269b § 1 k.k. (obrót oprogramowaniem przystosowanym do prowadzenia inwigilacji w wymiarze prawnie zakazanym).
15. Jeżeli zakup licencji na „Pegasusa" został dokonany przez CBA, za pośrednictwem spółki prawa handlowego, ze środków przekazanych służbie z Funduszu Sprawiedliwości, to operacja ta nastąpiła w warunkach naruszenia dyscypliny finansów publicznych. Zgodnie z obowiązującymi przepisami zakazane jest finansowanie Centralnego Biura Antykorupcyjnego spoza budżetu państwa.
16. W świetle art. 269b k.k., licencję na oprogramowanie „Pegasus" należy traktować jako rzecz wyłączoną z obrotu, co skutkuje nieważnością umowy pomiędzy Skarbem Państwa – Centralnym Biurem Antykorupcyjnym a pośrednikiem. Otwiera to drogę do dochodzenia od niego zwrotu uiszczonego przez CBA świadczenia pieniężnego.