Czym jest system „Pegasus"

Nazwę „Pegasus" stosuje się do oprogramowania szpiegującego, możliwego do zainstalowania na urządzeniach elektronicznych i korzystających z systemów iOS i Android, które wyprodukowane zostało przez izraelską firmę **NSO Group Technologies Ltd**, zwaną w dalszej części Raportu „NSO". Zainstalowanie oprogramowania na urządzeniu odbywa się zdalnie, bez świadomości użytkownika i otwiera podmiotowi infekującemu praktycznie nieograniczony dostęp do urządzenia. Umożliwia mu m. in. : dostęp do wiadomości e-mail oraz SMS i komunikatorów internetowych, śledzenie lokalizacji urządzenia (GPS), dostęp do ustawień urządzenia, zgromadzonych plików, do historii przeglądanych stron internetowych, zapisanych kontaktów, sieci społecznościowych, dokonywanie i przeglądanie wpisów w kalendarzu, dostęp do aparatu i galerii urządzenia, połączeń telefonicznych oraz aplikacji zapisanych na urządzeniu. Jednocześnie oprogramowanie to umożliwia instalowanie w urządzeniu własnych plików oraz modyfikację plików istniejących, modyfikowanie ustawień technicznych urządzenia (w tym dostępu do sieci), wykonywanie połączeń telefonicznych, wysyłanie wiadomości, możliwość wykonywanie zdjęć, filmów i zrzutów ekranu, nagrywanie dźwięku, jak również pozyskiwanie plików z urządzenia (w tym również plików usuniętych). Infekujący ma więc możliwość niczym nieograniczonej ingerencji w urządzenie i przechowywane na nim dane, znacznie przekraczające nawet możliwości prawowitego użytkownika systemu, który może wykonywać wyłącznie operacje dozwolone przez system operacyjny i współdziałające z nim oprogramowanie.[1]

Infekujący urządzenie „Pegasusem" otrzymuje praktycznie całkowitą kontrolę nad urządzeniem – z jego bieżącym używaniem i modyfikacją zapisanych w urządzeniu treści włącznie. [2]

Wyjaśnienie to jest istotne dla ustalenia, czy stosowanie takiego oprogramowania na gruncie prawa polskiego można w ogóle uznać za legalne, mając na uwadze konstytucyjne granice ingerencji w prawa jednostek, ustawowe ramy dla inwigilacji z jednej strony, a opisane wyżej techniczne możliwości systemu z drugiej. Analiza przepisów kodeksu postępowania karnego i ustaw szczególnych prowadzi do wniosku, że nie dają one organom państwa uprawnienia do ingerencji w zawartość urządzeń ani możliwości przejmowania nad

---

[1] Agnieszka Barczak-Opustil Adam Behan, Mikołaj Małecki Szymon Tarapata, Witold Ziomek „Pegasus w Polsce: niedopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych", Czasopismo Prawa Karnego i Nauk Penalnych, Rok 2023, Zeszyt 1, s.11-12

[2] Dr hab. Mariusz Bidziński prof. Uniwersytetu SWPS: Ekspertyza w przedmiocie: legalności zakupu i wykorzystywania na terytorium Rzeczypospolitej Polskiej systemu „Pegasus", s.3

nimi kontroli, bowiem celem inwigilacji procesowej jest pozyskanie określonych informacji, a nie kreowanie, zmiana lub usuwanie danych[3].

Z tego względu „Pegasus" traktowany jest nie jako narządzie operacyjne (do zbierania danych o przestępstwach), ale jako broń (narzędzie do wpływania na postępowanie innych ludzi). W związku z tym, niezależnie od kwestii dopuszczalności stosowania „Pegasusa" w świetle Konstytucji i EKPC, **nie ma prawnej możliwości realizowania przy jego pomocy kontroli przewidzianej w art. 237-242 k.p.k., ani kontroli operacyjnej przewidzianej w ustawach szczególnych (w tym zwłaszcza w art. 17 ustawy o CBA).**[4]

Naruszenia standardów konstytucyjnych

Przepisy Konstytucji RP zawierają normy gwarancyjne, będącą podstawą praw podmiotowych wskazanych przede wszystkim w rozdziale II. Prawie na samym początku tego rozdziału, w art. 31 ust. 3 ustrojodawca zastrzegł, że „***ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw***".

Wymóg wskazania ograniczeń w ustawie jest oczywisty i jasny. Zastrzeżenie, że ograniczenia mogą być ustanawiane tylko wtedy gdy są konieczne w demokratycznym państwie tworzy - zarówno zdaniem doktryny jak i Trybunału Konstytucyjnego - nakaz rozważenia, czy: a) wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków, b) wprowadzona regulacja jest niezbędna dla ochrony interesu publicznego, z którym jest połączona, c) efekty wprowadzonej regulacji pozostają w proporcji do ciężarów nakładanych przez nią na obywatela (proporcjonalność *sensu stricto*)[5]. Należy podkreślić, że negatywne skutki nigdy nie mogą być w przewadze i zawsze muszą prowadzić zamierzonego celu i implementacji wolności i praw, które są gwarantowane przez normy konstytucyjne. Co więcej, obowiązek szanowania wolności i praw innych wiąże się z

---

[3] Katalogi dopuszczalnych czynności operacyjnych zawarte są m. in. w przepisach art. 237 i 241 k.p.k.

[4] Dr hab. Mariusz Bidziński: op.cit. s.8-9

[5] Zob. m.in. orzeczenie TK z 26 kwietnia 1995 r., K. 11/94, OTK w 1995 r., cz. I, poz. 12 oraz wyroki TK z: 28 czerwca 2000 r., K. 34/99, OTK ZU nr 5/2000, poz. 142 i P 14/01, 13 marca 2007 r., K 8/07, OTK ZU nr 3/A/2007, 3 czerwca 2008 r., sygn. K 42/07, OTK ZU nr 5/A/2008, poz. 77.

istotą konstytucyjnych wolności i praw. Odnosi się także do godności człowieka, równości wobec prawa oraz zakazu dyskryminacji[6].

Trybunał Konstytucyjny kilkukrotnie zajmował się analizą regulacji prawnych, dotyczących kontroli operacyjnej. Głównym przedmiotem badania było zachowanie standardów i granic ingerencji władzy publicznej w prawa i wolności obywatelskie. Sąd konstytucyjny wielokrotnie podkreślał, że prowadzenie inwigilacji może naruszać prawo do prywatności (art. 47 Konstytucji), wolność komunikowania się i związaną z tym ochronę tajemnicy komunikacji (art.49), a także autonomię informacyjną (art.51). Zbyt głęboka, nieproporcjonalna ingerencja w te prawa może prowadzić do naruszenia zasady godności człowieka (art. 30).[7] Trybunał Konstytucyjny nie zakwestionował dopuszczalności prowadzenia kontroli operacyjnej, uzasadnianej ochroną bezpieczeństwa publicznego, lecz wskazał konieczność wprowadzenia szeregu mechanizmów gwarantujących, że wkroczenie w prawa i wolności obywatelskie będzie proporcjonalne. Na płaszczyźnie materialnoprawnej gwarantować mają to przepisy określające sposób wkraczania w prawa i wolności jednostki, precyzujące m.in. kiedy i na jakich zasadach, wobec kogo i jak długo może być stosowana kontrola operacyjna. Proceduralnie natomiast Trybunał wskazał konieczność zapewnienia gwarancji, służących kontroli sposobu realizacji przesłanek materialnoprawnych. Aby uznać, że naruszenie praw i wolności konstytucyjnych jest dopuszczalne, spełnione muszą być przesłanki określone w art. 31 ust.3 Konstytucji, w tym najistotniejsza jest przesłanka proporcjonalności (podjęte przez organy państwa działania ingerujące w określone sfery wolności lub praw musza być absolutnie niezbędne i dostosowane do założonych celów, zaś związana z nimi ingerencja w wolności i prawa nie może być nadmierna). Wielokrotnie podkreślał również, że niedopuszczalna jest zarówno nieograniczona inwigilacja w ramach czynności operacyjnych, jak i możliwość arbitralnego rozpowszechniania zgromadzonych w ten sposób informacji. W wyroku K 54/07[8] Trybunał stwierdził, że sprzeczny z art. 47 i art. 51 w związku z art.31 ust.3 i art.30 Konstytucji jest przepis art. 22 ust.4-7 ustawy o CBA[9], gdyż umożliwia on CBA gromadzenie i przetwarzanie danych wrażliwych w zakresie, w jakim nie jest to niezbędne dla celów ścigania korupcji.

W tym kontekście **stosowanie systemu operacyjnego wobec wszystkich osób, wysłuchanych przez Komisję, naruszało te podstawowe standardy konstytucyjne**.

---

[6] Szerzej M. Chmaj, *Komentarz do Konstytucji RP. Art. 30, 31, 32, 33*, Warszawa 2019, s. 79 i nast.
[7] Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 r. K 32/04
[8] Wyrok Trybunału Konstytucyjnego z dnia 23 czerwca 2009 r. K 54/07
[9] Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U 2021 poz.1671)

Należy w tym miejscu przypomnieć, że stosowanie niejawnej kontroli przez organy państwa uregulowane jest w przepisach, które można podzielić na dwie grupy: podsłuch procesowy oraz tzw. kontrola operacyjna, w tym podsłuch pozaprocesowy. Zasady prowadzenia kontroli operacyjnej regulują ustawy szczególne, w tym pragmatyki służbowe. Ustawodawca przewidział zasadniczo pięć rodzajów kontroli operacyjnej, która polegać może 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. Żadna z ustaw nie przewiduje natomiast dopuszczalności przejmowania kontroli nad urządzeniem czy modyfikacji zapisanych w jego pamięci treści.

Istotne jest, że kontrola operacyjna ma zawsze charakter subsydiarny, co oznacza, że może być zarządzona tylko wtedy, gdy inne środki okazały się bezskuteczne lub nieprzydatne.[10]

Ta generalna niedopuszczalność stosowania systemu „Pegasus" na gruncie prawa polskiego powoduje, że posługiwanie się nim nawet dla realizacji celów prawnie dozwolonych (kontroli operacyjnej) jest niedopuszczalne. Bowiem realizacja celów prawnie dozwolonych jest możliwa jedynie przy zastosowaniu legalnych środków. Dlatego każde stosowanie tego systemu jest działaniem bezprawnym.

Naruszenia przepisów obowiązującego prawa

Zanim zostaną przedstawione szczegółowo naruszenia konkretnych przepisów, należy zwrócić uwagę, że w każdym z wymienionych przypadków następował będzie zbieg z przestępstwem, stypizowanym w art. 231 kodeksu karnego, ujmującym najbardziej charakterystyczne przestępstwa urzędnicze, godzące w autorytet oraz zaufanie społeczne do władz i instytucji, a także w konkretne interesy publiczne lub prywatne, zagrożone lub naruszone przestępnym zachowaniem.[11] Przedmiotem ochrony czynu zabronionego, określonego w art. 231 §1 kk jest przede wszystkim prawidłowe funkcjonowanie instytucji

[10] Dr hab.Mariusz Bidziński op.cit. s.8-9
[11] Jacek Giezek [w] Kodeks karny. Część szczególna. Komentarz red. J.Giezek 2012

państwowych i samorządu terytorialnego oraz powiązany z nim interes władzy publicznej, której wizerunek – w odbiorze społecznym – narażony jest na szwank tego typu działaniem, oznaczającym przekroczenie uprawnień lub niedopełnienie obowiązku. Przekroczenie uprawnień wymaga wykazania, że podjęte przez sprawcę działanie nie wchodziło w zakres jego kompetencji lub było podjęte w ramach uprawnień, ale niezgodnie z przepisami prawa.

Przepis ten stanowi, iż *„Funkcjonariusz publiczny, który przekraczając swoje uprawnienia lub nie dopełniając obowiązków, działa na szkodę interesu publicznego lub prywatnego, podlega karze pozbawienia wolności do lat 3"*.

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 kk. (funkcjonariusze organów powołanych do ochrony bezpieczeństwa publicznego).

Wykorzystywanie przez nich nielegalnego środka do realizacji kontroli operacyjnej stanowić będzie przekroczenie uprawnień przez tych funkcjonariuszy ze szkodą zarówno dla interesu publicznego (naruszenie zaufania do państwa i jego instytucji), jak i prywatnego (naruszenie praw i wolności osób objętych inwigilacją) i może w konsekwencji stanowić podstawę dla ich odpowiedzialności karnej.

Komisja ustaliła, iż doszło do rażącego naruszenia bądź złamania wielu przepisów obowiązującego prawa, w tym zwłaszcza w odniesieniu do procedur zakupu systemu „Pegasus" oraz bezpieczeństwa informacji uzyskanych za pośrednictwem systemu „Pegasus"

1. Naruszenia prawa dokonane przy zakupie systemu „Pegasus". [12]

Sfinansowanie zakupu „Pegasusa" ze źródła znajdującego się poza budżetem Państwa poprzez dofinansowanie służby środkami z Funduszu Sprawiedliwości, co jest **niezgodne z art. 4 ust.1. ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym** zgodnie z którym CBA jest finansowane z budżetu państwa, a środki państwowego funduszu celowego takimi środkami nie są oraz **art.11 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,** jak również naruszenie **art.43 §8 kodeksu karnego wykonawczego**

Opis naruszenia:

[12] Informacji kluczowych w tym zakresie udzieliło 3. posiedzenie Komisji, które odbyło się w dniu 18 stycznia 2022 r. Osobami wysłuchanymi przez Komisję byli wówczas: Senator Krzysztofa Kwiatkowskiego - Prezes Najwyższej Izby Kontroli w latach 2013–19, Marian Banaś – aktualnie urzędujący Prezes Najwyższej Izby Kontroli oraz gen. Marek Bieńkowski - doradca w Departamencie Administracji Publicznej Najwyższej Izby Kontroli.

Dnia 14.09.2017 r. Minister Sprawiedliwości wystąpił do Ministra Finansów o zgodę na przeznaczenie 25.000.000,00 zł z Funduszu Sprawiedliwości na „inne działania, które mają służyć zapobieganiu przestępczości". Pismo podpisał podsekretarz stanu w Ministerstwie Sprawiedliwości, Michał Woś. Fundusz Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej, utworzony na podstawie art. 43 kkw[13] jest ukierunkowany na pomoc pokrzywdzonym i świadkom, przeciwdziałanie przestępczości oraz pomoc postpenitencjarną. Zgodnie z art.43 § 8 k.k.w. Środki Funduszu są przeznaczane na pomoc osobom pokrzywdzonym przestępstwem oraz osobom im najbliższym, zwłaszcza na pomoc medyczną, psychologiczną, rehabilitacyjną, prawną oraz materialną, a także na pomoc postpenitencjarną. Przeznaczenie środków na inny cel – w tym przypadku na zakup systemu operacyjnego, służącego inwigilacji – jest naruszeniem art. 43 § 8 k.k.w.

Już kolejnego dnia, czyli 15.09.2017 r. w porządku obrad posiedzenia sejmowej Komisji Finansów Publicznych dodano punkt: *„zaopiniowanie wniosku Ministra Sprawiedliwości w sprawie zmian w planie finansowym Funduszu Pomocy Pokrzywdzonym oraz Pomocy Penitencjarnej na 2017 r."* W trakcie posiedzenia Komisji obecny na niej Michał Woś tłumaczył, iż „**konieczność** zmiany w planie Funduszu wynika przede wszystkim z wejścia w życie 12.08. 2017 r. ustawy, która nowelizuje zasady finansowania Funduszu(...) w ten sposób, że ustawodawca przewidział rozszerzenie form pomocy. Które mogą być finansowane ze środków funduszu i rozszerzył katalog podmiotów, które taka pomoc mogą świadczyć. (...) , został dodany katalog instytucji z sektora finansów publicznych..." [14] (nie wspomniał o przekazaniu tych środków na rzecz CBA). Komisja Budżetu i Finansów Publicznych pozytywnie zaopiniowała przedstawiony wniosek, nie dysponując pełną wiedzą, na rzecz jakiej „instytucji z sektora finansów publicznych" środki te będą przekazane.

Tego samego dnia szef CBA Ernest Bejda złożył wniosek do Ministerstwa Sprawiedliwości o przekazanie kwoty 25 mln zł, które to środki otrzymał w dwóch transzach. To niespotykane ani wcześniej, ani później przekazanie środków z Funduszu Sprawiedliwości na rzecz służby specjalnej naruszyło przepisy ustawy o Centralnym Biurze Antykorupcyjnym (art.4. ust.1) oraz kilkanaście innych przepisów, dotyczących finansów

---

[13] ustawa z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz.U. 2023 poz.127)

[14] Ministerstwo Sprawiedliwości przedstawiło zmianę zaplanowanych środków finansowych w pozycjach: dotacje o kwotę 20.050 tys. zł z przeznaczeniem na **dotacje na rzecz pomocy pokrzywdzonym i przeciwdziałania skutkom przestępczości**, i w pozycji: koszty własne o 34.514 tys. zł, gdzie wynagrodzenia bezosobowe – wynoszą 600 tys. zł, pochodne od wynagrodzeń, zakup usług oraz działania pozostałe, w tym promocja funduszu (...) – Pełny zapis przebiegu posiedzenia Komisji Finansów Publicznych z dnia 15 września 2017 r. s. 4-5

publicznych.[15] W dniach 9.10.2017 r. i 17.11.2017 r. Ministerstwo Sprawiedliwości dokonało dwóch przelewów w wysokości odpowiednio 13.360.000,00 zł oraz 11.640.000,00 zł z Funduszu Sprawiedliwości na rzecz Centralnego Biura Antykorupcyjnego[16]. Jak wynikało z dostępnych dokumentów, środki te były przeznaczone na rzecz realizacji umowy nr N/2/2017 z dnia 29.09.2017 r., zawartej między CBA a firmą Matic Sp. z o.o. Fakt zawarcia umowy potwierdzają również faktury zaliczkowe wystawione przez wskazaną firmę dnia 03.10.2017 r. i 09.11.2017 r., z opisów których wynika, że dotyczą zakupu systemu współfinansowanego ze środków Funduszu Sprawiedliwości na podstawie umowy nr N/2/2017. Przedmiot umowy nie wynikał z wyżej wymienionych dokumentów. Jednakże w sprawozdaniu z wykonania zadania - Fundusz Sprawiedliwości z dnia 25.01.2018 r., został zamieszczony opis: „zakup środków techniki specjalnej, służącej do wykrywania i zapobiegania przestępczości". Potwierdzone zostało również, że wszystkie z poszczególnych zadań, tj. dostawa sprzętu i oprogramowania, uruchomienie systemu i szkolenia, zostały zrealizowane zgodnie z harmonogramem, co zostało udokumentowane protokołem odbioru. Dokument ten został podpisany przez Dyrektora Biura Finansów CBA - Daniela Arta i Szefa CBA - Ernesta Bejdę, którzy poświadczyli, że informacje zawarte w sprawozdaniu są zgodne z prawdą.[17]

W żadnym miejscu nie została użyta nazwa systemu: „Pegasus", jednak mogło to być spowodowane faktem, iż nikt tą nazwą się w tamtym czasie nie posługiwał i nazwę tę próbowano świadomie ukryć. Osoby, które w tej sprawie podejmowały decyzje i je realizowały, miały świadomość, że naruszają prawo, a przynajmniej działają na granicy prawa.[18] Ponadto środki z Funduszu Sprawiedliwości nie mogły zostać przekazane na rzecz CBA z dwóch powodów: 1) nie jest to cel, na jaki mogą być przeznaczone środki z Funduszu w rozumieniu art.43 §8 punkt 1e) kkw; 2) zgodnie z przepisami art. 4 ust.1 ustawy o CBA[19], działalność Centralnego Biura Antykorupcyjnego jest finansowana z budżetu państwa.

---

[15] Trzecie posiedzenie Senackiej Komisji Nadzwyczajnej do spraw Inwigilacji w dniu 18.01.2022 r. wyjaśnienia gen. Marka Bieńkowskiego

[16] Dodatkowe informacje, pozyskane w trakcie posiedzenia Komisji, które odbyło się dnia 28 stycznia 2021 r. z wyłączeniem jawności, znajdują się w części niejawnej Raportu

[17] Trzecie posiedzenie Senackiej Komisji Nadzwyczajnej do spraw Inwigilacji w dniu 18.01.2022 r. wyjaśnienia senatora Krzysztofa Kwiatkowskiego , z których wynika, iż na początku 2018 r. NIK przeprowadzała kontrolę wykonania Budżetu Państwa za rok 2017 w części nr 37: „Sprawiedliwość oraz wykonania planów finansowych Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej - Fundusz Sprawiedliwości". W trakcie kontroli natrafiono na kopie faktur zaliczkowych wystawionych przez firmę "Matic Sp. z o.o.", wyciągi bankowe z Narodowego Banku Polskiego, dokumentujące dokonane przelewy oraz sprawozdanie z wykonania zadania - Fundusz Sprawiedliwości.

[18] Trzecie posiedzenie Senackiej Komisji Nadzwyczajnej do spraw Inwigilacji w dniu 18.01.2022 r. wyjaśnienia senatora Krzysztofa Kwiatkowskiego

[19] ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. 2022.0.1900)

Zgodnie natomiast z art.11ust.1 ustawy o finansach publicznych[20] jednostkami budżetowymi są jednostki organizacyjne sektora finansów publicznych nieposiadające osobowości prawnej, które pokrywają swoje wydatki bezpośrednio z budżetu. W związku z tym istnieje ustawowy zakaz finansowania jednostki sektora finansów publicznych z innych źródeł niż budżet państwa, których na podstawie art.29 ustawy o finansach publicznych nie stanowią państwowe fundusze celowe.[21]

Najwyższa Izba Kontroli przeprowadzała w 2018 r. kontrolę, której celem była ocena wykonania ustawy budżetowej na rok 2017 z dnia 16 grudnia 2016 r. w części 37 – Sprawiedliwość, a także planów finansowych Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej – Funduszu Sprawiedliwości i Funduszu Aktywizacji Zawodowej Skazanych oraz Rozwoju Przywięziennych Zakładów Pracy.[22] Zdaniem NIK środki Funduszu Sprawiedliwości w wysokości 25 000 tys. zł (nieobjęte naborem wniosków lub programem) nie mogły zostać przekazane Centralnemu Biuru Antykorupcyjnemu, gdyż w myśl art. 4 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym działalność CBA jest finansowana wyłącznie ze środków budżetu państwa, a środki państwowego funduszu celowego nie są środkami tego rodzaju

W konsekwencji Najwyższa Izba Kontroli po przedstawieniu ustaleń kontroli i wniosków o złamaniu dyscypliny finansów publicznych CBA i Ministerstwu Sprawiedliwości, następnie oddaleniu zastrzeżeń tych ostatnich, w dniu 18.07.2018 r. złożyła zawiadomienie do Rzecznika Dyscypliny Finansów Publicznych o możliwości naruszenia dyscypliny finansów publicznych przez szefa CBA Ernesta Bejdę i wiceministra sprawiedliwości Michała Wosia. Po odmowie wszczęcia postępowania wyjaśniającego NIK złożyła zażalenie do Głównego Rzecznika Dyscypliny Finansów Publicznych. Ostatecznie decyzją z 14 września 2020 r. Rzecznik Dyscypliny Finansów Publicznych Piotr Patkowski wydał postanowienie o odmowie wszczęcia postępowania wobec CBA, ustalając, że

[20] ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U.2023.0.1270)

[21] Raport Najwyższej Izby Kontroli***

[22]. W ocenie NIK przepis art. 43 Kkw nie może być traktowany jako przepis szczególny uprawniający do modyfikacji ustawy ustrojowej o CBA, a podkreślić należy, że zastrzeżenie w odniesieniu do finansowania służb specjalnych środkami budżetu państwa wprowadzono do wszystkich ustaw ustrojowych tych formacji. Wątpliwości NIK budzi także charakter prawny umowy zawartej pomiędzy Ministrem Sprawiedliwości jako dysponentem Funduszu Sprawiedliwości a Szefem CBA, gdyż powoduje to sytuację, w której Skarb Państwa zawarł umowę sam ze sobą (na gruncie prawa cywilnego oba te podmioty działają jako *statio fisci* Skarbu Państwa). Wątpliwość NIK budzi również możliwość uznania zawartej umowy za rodzaj porozumienia administracyjnego, gdyż przepisy dotyczące Funduszu nie przewidują takiej formy przekazywania środków. Skutkiem zawartej umowy było odejście od zasad ewidencjonowania środków zgodnie z przepisami wykonawczymi do ufp, ustawy o rachunkowości i ustawy Pzp. – Informacja o wynikach kontroli wykonania budżetu państwa w 2017 r. w części 37 – Sprawiedliwość oraz wykonania planów finansowych Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej – Funduszu Sprawiedliwości i Funduszu Aktywizacji Zawodowej Skazanych oraz Rozwoju Przywięziennych Zakładów Pracy; KPB.430.003.2018

wprawdzie **do naruszenia dyscypliny finansów publicznych doszło, ale była to znikoma szkodliwość czynu dla finansów publicznych**.[23] W stosunku do tych Ernesta Bejdy i Michała Wosia zostały również złożone wnioski do prokuratury, lecz bez procesowych rezultatów.

Wysłuchanie kontrolera i Prezesów NIK doprowadziło Komisję do wniosku, że zakup „Pegasusa" został sfinansowany nielegalnie, co zostało potwierdzone przez Kolegium Najwyższej Izby Kontroli oraz co do zasady przez Rzecznika Dyscypliny Finansów Publicznych. Ten ostatni uznał, że naruszenie dyscypliny finansów publicznych o kwotę 25 mln zł stanowi znikomą szkodliwość dla finansów publicznych. O zamiarze ukrycia transakcji zakupu systemu świadczą opisane wyżej zabiegi – gdyby nie było takiego zamiaru, można byłoby legalnie przeprowadzić całą procedurę zakupu systemu, uzyskując niezbędne opinie oraz finansując go zgodnie z przepisami prawa.

W ocenie Komisji, biorąc pod uwagę wyniki wskazanej wyżej kontroli NIK istnieje uzasadnione podejrzenie, że osoby podejmujące decyzje w tej sprawie, zarówno ze strony Ministerstwa Sprawiedliwości, jak i Centralnego Biura Antykorupcyjnego popełniły przestępstwo przekroczenia uprawnień na szkodę interesu publicznego, określonego w art. 231 §1 kk.

Komisja podjęła decyzję o zawiadomieniu prokuratury o możliwości popełnienia takiego przestępstwa przez funkcjonariuszy organów władzy publicznej, którzy w omawianym okresie byli zaangażowani w procedurę przekazania środków, ich przyjęcia oraz dokonania zakupu systemu. Byli to:

Michał WOŚ – pełniący funkcję sekretarza stanu w Ministerstwie Sprawiedliwości, który pełnił również rolę Dysponenta Funduszu Sprawiedliwości *(art.231§1 kk. w zw. z art.11 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych i art.43 §8 kkw)* ; [24]

Ernest BEJDA – pełniący funkcję szefa CBA *(art.231§1 kk. w zw. z art. 4 ust.1. ustawy z dnia 9 czerwca 2006 r. o CBA i art.11 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych)*

Daniel ART – pełniący funkcję Dyrektora Biura Finansów CBA *(art.231§1 kk. w zw. z art. 4 ust.1. ustawy z dnia 9 czerwca 2006 r. o CBA i art.11 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych)*

---

[23] Wyjaśnienia gen. Marka Bieńkowskiego
[24] Część niejawna Raportu

Piotr PATKOWSKI – pełniący funkcję Rzecznika Dyscypliny Finansów Publicznych przy szefie KPRM *(art.231§1 kk.)*

Zadaniem prokuratury będzie weryfikacja, czy doszło do popełnienia przestępstwa, wskazanego w niniejszym akapicie i kto za to ponosi odpowiedzialność. Nie jest wykluczone, że prokuratura dojdzie do wniosku, że zarzutami z art.231§1 kk należy objąć szerszy krąg zaangażowanych w tę operację osób.

2. Naruszenia bezpieczeństwa informacji uzyskanych za pośrednictwem systemu „Pegasus"

Komisja ustaliła, iż doszło do złamania dyspozycji art.48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz wydanego na mocy art. 49 ust.9 tej ustawy rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. Nr 159, poz.948)

Opis naruszenia:

Na mocy art. 48 ustawy o ochronie informacji niejawnych systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego, którego dokonać winna Agencja Bezpieczeństwa Wewnętrznego lub Służba Kontrwywiadu Wojskowego. Wydanie takiej akredytacji poprzedzić ma kompletny dokument szczegółowych wymagań bezpieczeństwa systemu teleinformatycznego (art.48 ust. 4 ustawy), który winien być opracowywany już na etapie projektowania samej aplikacji. Nie sposób – również ze względów technologicznych – udzielić wymaganej prawem akredytacji bez przeprowadzenia miarodajnych testów programu i uzyskania dostępu do kodów źródłowych i infrastruktury całego systemu.

Z uwagi na niemożność zrealizowania określonej w ustawie prawidłowej i skutecznej akredytacji i weryfikacji podstawowych wymagań bezpieczeństwa teleinformatycznego , związanego z ochroną informacji niejawnych, **Pegasus nie może być więc stosowany na gruncie polskiego prawa.** Polski system prawny nie dopuszcza bowiem stosowania programów, w ramach których pozyskiwane dane operacyjne transferowane są za pośrednictwem niekontrolowanych przez właściwe służby kanałów transmisji, gdyż rodzi to ryzyko naruszenia ich integralności oraz nie zapewnia im wymaganej przez prawo poufności.

W konsekwencji niezgodne z przepisami polskiego prawa są wszelkie działania operacyjne z wykorzystaniem nieakredytowanych programów komputerowych, które nie zapewniają bezpieczeństwa informacji niejawnych lub których użycie wiąże się z udostępnianiem tych danych osobom trzecim nieuprawnionym do dostępu do informacji niejawnych.

Jak wynika z opracowań NSO[25], dla zapewnienia bezpieczeństwa informacji pozyskiwane z atakowanego urządzenia dane przesyłane są na serwer operatora za pośrednictwem zanonimizowanej sieci transmisji, przy wykorzystaniu rozproszonej geograficznie sieci połączeń. Oznacza to, że dane pozyskane na terenie Polski transmitowane są także poza obszar Rzeczypospolitej Polskiej. Warto zauważyć, że będące w gestii NSO zewnętrzne serwery można wyposażyć w oprogramowanie, które daje możliwość przesyłania transmitowanych danych również do siedziby NSO. Według polskiego prawa systemy informatyczne służące do kontroli operacyjnej muszą spełniać rygorystyczne wymogi bezpieczeństwa teleinformatycznego, nakładane przez ustawę o ochronie informacji niejawnych i wydane na jej podstawie rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. System taki gwarantować winien w szczególności poufność, czyli taką właściwość systemu, która powoduje, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym, co w przypadku braku pełnej kontroli nad infrastrukturą służącą do transmisji danych nie może być skutecznie zagwarantowana. Innymi słowy, pozyskane w wyniku kontroli operacyjnej dane pozostają pod szczególną ochroną określoną w ustawie o ochronie informacji niejawnych i jako takie nie mogą być bez określonej w prawie kompetencji przekazywane osobom trzecim, nieuprawnionym do dostępu czy przetwarzania informacji, objętych klauzulą tajności. Opisany sposób transmisji danych pozyskanych za pośrednictwem „Pegasusa", zakładający od strony technicznej brak możliwości realnej weryfikacji bezpieczeństwa tego systemu wobec służb państwa obcego czy NSO, uniemożliwia spełnienie warunku poufności, w związku z czym system ten nie mógł i nie może uzyskać świadectwa akredytacji bezpieczeństwa informatycznego.

W ocenie Komisji istnieje uzasadnione podejrzenie, że osoby podejmujące decyzje o podjęciu działań operacyjnych z wykorzystaniem nieakredytowanego programu nie zapewniającego bezpieczeństwa informacji niejawnych lub których użycie wiązało się z udostępnianiem tych danych osobom trzecim nieuprawnionym do dostępu do informacji niejawnych, popełniły przestępstwo niedopełnienia obowiązków oraz przekroczenia

---

[25] NSO Group Technologies Ltd z siedzibą w Herclijji (Izrael)

uprawnień na szkodę interesu publicznego oraz interesu prywatnego, określonego w art. 231 §1 kk. Komisja podjęła decyzję o zawiadomieniu prokuratury o możliwości popełnienia takiego przestępstwa przez funkcjonariuszy organów władzy publicznej, którzy w omawianym okresie podejmowali takie decyzje. Byli to:

Ernest BEJDA – pełniący funkcję szefa CBA *(art.231§1 kk. w zw. z art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych)*

Mariusz KAMIŃSKI – pełniący funkcję Ministra Spraw Wewnętrznych i Administracji i Koordynatora Służb Specjalnych *(art.231§1 kk)*

Zadaniem prokuratury będzie weryfikacja, czy doszło do popełnienia przestępstwa, wskazanego w tym akapicie i kto ponosi odpowiedzialność za to przestępstwo. Nie jest wykluczone, że prokuratura dojdzie do wniosku, że zarzutem z art.231§1 kk należy objąć szerszy krąg zaangażowanych w tę operację osób.

NARUSZENIE:

Art.267 §1-3 kodeksu karnego

Opis naruszenia:

Zgodnie z treścią art. 267 kodeksu karnego, *uzyskanie bez uprawnienia dostępu do informacji nieprzeznaczonej dla uzyskującego dostęp, poprzez otwarcie zamkniętego pisma lub podłączenie się do sieci telekomunikacyjnej lub przełamanie albo ominięcie elektroniczne magnetyczne, informatyczne lub inne szczególne jej zabezpieczenia, uzyskanie dostępu do całości lub części systemu informatycznego lub założenie lub posłużenie się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem, jak również ujawnienie w ten sposób informacji innej osobie, jest przestępstwem, zagrożonym karą pozbawienia wolności do lat 2.* Ściganie tego przestępstwa następuje na wniosek pokrzywdzonego.

Posłużenie się systemem, którego użytkowanie w polskim systemie prawnym jest niedopuszczalne, powoduje, że czyn ten może wyczerpywać również znamiona nieuprawnionego dostępu do informacji. Osobnym zagadnieniem jest również brak przesłanek merytorycznych, uzasadniających uzyskanie tego typu informacji. Jak wynika z przekazanych przez senatora Krzysztofa Brejzę informacji, w czasie ataków na jego urządzenie za pomocą systemu „Pegasus", zostały z tego urządzenia pobrane wiadomości SMS od 2010 r. (czyli 9 lat wstecz, licząc od daty ataków). Było to około 85.000 wiadomości, jak również hasła zabezpieczające do wszystkich komunikatorów

elektronicznych. Jednocześnie wgrano do jego urządzenia ok 1 Gb danych. Cała operację nadzorował – jak wynika z wyjaśnień Senatora Krzysztofa Brejzy – ówczesny szef delegatury CBA w Bydgoszczy.[26] Zaangażowana w te działania wobec Senatora Krzysztofa Brejzy była również Zuzanna Mrozowska, pełniąca wówczas funkcję naczelnika tej samej delegatury CBA w Bydgoszczy.[27] W działaniach wobec senatora Krzysztofa Brejzy brał udział również Maciej Wybult. Wszyscy agenci CBA, którzy prowadzili operację wobec Senatora Krzysztofa Brejzy, odeszli ze służby: dwoje do PKN Orlen, trzeci z nich na emeryturę. omijając możliwość popełnienia przy tej okazji innych przestępstw, w tym takich, które nie stanowią przedmiotu prac Komisji, stwierdzić należy, że pozyskanie tych informacji wyczerpuje znamiona art. 267 §1, §2 i §3 kodeksu karnego, a przekazywanie tych informacji również §4 kodeksu karnego.

W ocenie Komisji istnieje uzasadnione podejrzenie, że osoby podejmujące decyzje o posłużeniu się systemem, którego użytkowanie w polskim systemie prawnym jest niedopuszczalne – w celu inwigilacji wskazanych w I części Raportu osób, popełniły przestępstwo przekroczenia uprawnień na szkodę interesu publicznego oraz interesu prywatnego, określonego w art. 231 §1 kk.

Komisja również w tym przypadku podjęła decyzję o zawiadomieniu prokuratury o możliwości popełnienia takiego przestępstwa przez funkcjonariuszy organów władzy publicznej, którzy w omawianym okresie podejmowali takie decyzje. Byli to:

Ernest BEJDA – pełniący funkcję szefa CBA *(art.231§1 kk. w zw. z art. 267 kk)*

Mariusz KAMIŃSKI – pełniący funkcję Ministra Spraw Wewnętrznych i Administracji i Koordynatora Służb Specjalnych *(art.231§1 kk)*

Jarosław SZMYT – pełniący funkcję szefa delegatury CBA w Bydgoszczy, nadzorujący operację wobec Senatora Krzysztofa Brejzy *(art.231§1 kk. w zw. z art. 267 kk)*

Zuzanna MROZOWSKA – pełniąca funkcję naczelnika delegatury CBA w Bydgoszczy, uczestnicząca w operacji wobec Senatora Krzysztofa Brejzy *(art.231§1 kk. w zw. z art. 267 kk)*

Maciej WYBULT – agent CBA w Bydgoszczy, uczestniczący w operacji wobec Senatora Krzysztofa Brejzy *(art.231§1 kk. w zw. z art. 267 kk)*

---

[26] Wkrótce po powstaniu senackiej Nadzwyczajnej Komisji, Jarosław Szmyt odszedł z CBA i rozpoczął pracę w PKN Orlen na stanowisku dyrektora Biura Analiz.

[27] Zuzanna Mrozowska również odeszła z CBA i we wrześniu 2022 r. rozpoczęła pracę w Biurze Analiz PKN Orlen, w którym dyrektorem jest Jarosław Szmyt.

Zadaniem prokuratury będzie weryfikacja, czy doszło do popełnienia przestępstwa, wskazanego w tym akapicie i kto ponosi odpowiedzialność za to przestępstwo. Nie jest wykluczone, że prokuratura dojdzie do wniosku, że zarzutem z art.231§1 kk należy objąć szerszy krąg zaangażowanych w tę operację osób.

Naruszenie:

Art. 269b § 1 kodeksu karnego w związku **z art.32a ust.7 i 8 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu** (Dz.U. 2020 poz.27)

Opis naruszenia:

Oceniając dopuszczalność wykorzystywania oprogramowania, które ma możliwość przejęcia kontroli nad urządzeniem końcowym, należy zadać pytanie, czy jakakolwiek agencja posiada tego typu kompetencje w świetle przepisów polskiego prawa. Art. 32a ust.7 przyznaje taką kompetencję ABW, lecz w ściśle określonym przypadku, mianowicie „*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 lub § 2 w związku z § 1, art. 269 § 2 lub 269a kodeksu karnego.*"

Wniosek: w polskim porządku prawnym jedynie ABW posiada uprawnienie do korzystania z tego typu programów, lecz w wąskim, ściśle sprecyzowanym celu, nie można więc wytwarzać, pozyskiwać lub używać tego typu programów w jakimkolwiek innym celu. Brak również przepisów, które dopuszczałyby wykorzystywanie takiego oprogramowania przez jakąkolwiek inną służbę, posiadającą uprawnienie do kontroli operacyjnej. Pozyskanie więc takiego oprogramowania przez inny podmiot wyczerpuje znamiona czynu zabronionego opisanego w art. 269b § 1 kodeksu karnego.

Sprawców czynu z art. 269b § 1 kk poszukiwać należy nie tylko w gronie kierownictwa i funkcjonariuszy oraz pracowników CBA biorących udział w transakcji nabycia systemu, ale również po stronie pośrednika przy nabyciu licencji oraz względem kierownictwa i pracowników Ministerstwa Sprawiedliwości – z uwagi na pomoc przy nabyciu oprogramowania, znajdującą wyraz w przekazaniu środków na ten cel z Funduszu Sprawiedliwości.

Odpowiedzialność karna związana z obrotem oprogramowaniem przystosowanym do nielegalnej inwigilacji jest niezależna od ewentualnej odpowiedzialności za złamanie

dyscypliny finansów publicznych, a w szczególności możliwość naruszenia zakazu finansowania CBA ze źródeł znajdujących się poza budżetem państwa.

Naruszenie:

Art.130 §2 kodeksu karnego

Opis naruszenia:

W tym miejscu nie sposób nie zwrócić uwagi na inny jeszcze, ale być może najistotniejszy i mogący nieść najpoważniejsze konsekwencje, aspekt braku zrealizowania ustawowo przewidzianej weryfikacji podstawowych wymagań systemu informatycznego i możliwości dostępu osób trzecich, również zagranicznych, do transferowanych danych wrażliwych. Aby zrozumieć istotę wypełnienia znamion zbrodni z art.130 § 2 kk, należy jeszcze raz zwrócić uwagę na sposób przekazywania danych pozyskiwanych za pomocą systemu „Pegasus". Jak już wcześniej wskazano, dla zapewnienia bezpieczeństwa informacji pozyskane dane przesyłane są z atakowanego urządzenia na serwer operatora za pośrednictwem zanonimizowanej sieci transmisji, przy wykorzystaniu rozproszonej geograficznie sieci połączeń, transferujących dane od atakowanego urządzenia do miejsca lokalizacji serwera danej instalacji (np. CBA), także poza obszar Rzeczypospolitej Polskiej. Jeżeli więc zaatakowane urządzenie końcowe znajduje się np. w Inowrocławiu, a serwer CBA w Warszawie, to całość danych przesłana zostanie np. do Londynu, potem np. do San Francisco, potem przez np. Kair dopiero do Warszawy. Nie sposób pominąć faktu, że będące w gestii NSO zewnętrzne serwery można było wyposażyć w oprogramowanie, które transmitowane dane przesyłałoby również do samego NSO.[28]

Skoro ze stosowaniem oprogramowania „Pegasus" wiąże się zautomatyzowane przetwarzanie przynajmniej części danych przez podmiot zewnętrzny – NSO Group Technologies Ltd z siedzibą w Herclijji (Izrael) – w sytuacji, gdy kontrolę nad udzielaniem licencji podmiotom zagranicznym posiada Ministerstwo Obrony Izraela, istnieje wysokie prawdopodobieństwo, że doszło do uzyskania dostępu do tych danych przez służby specjalne państwa Izrael.[29] Mogło więc dojść do przekazania ważnych dla państwa informacji obcemu wywiadowi. Są to informacje o charakterze zarówno publicznoprawnym, niejednoktrotnie objęte tajemnicą (prokurator Ewa Wrzosek, adwokat Roman Giertych), jak i informacje o charakterze prywatnym, często intymnym (dotyczy to wszystkich osób inwigilowanych w czasie trwania ataków na urządzenia). Przepis art.130 § 2 kodeksu karnego, wskazując

[28] A.Barczak-Opustil (...) op.cit. s.11-12
[29] Dr hab.Mariusz Bidziński op.cit. s.3-4 i 21-22

znamiona zbrodni szpiegostwa, stanowi iż *„kto działając na rzecz obcego wywiadu udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, ...”*

W tym kontekście osoby, które podejmowały decyzje w sprawie zakupu, a następnie wykorzystywania „Pegasusa” musiały mieć świadomość mechanizmu działania tego narzędzia i co najmniej wysokiego prawdopodobieństwa posiadania dostępu do pozyskanych danych przez służby specjalne obcego państwa – przez co zarówno podjęcie decyzji o zakupie, jak i wykorzystywania tego systemu może być zakwalifikowane jako „działanie na rzecz obcego wywiadu” w rozumieniu art. 130 § 2 kk. Ciężar gatunkowy zbrodni szpiegostwa jest ogromny, informacje, które mogły wejść w posiadanie służb obcego państwa, szczególnie informacje wrażliwe, mogą posłużyć tym służbom w przyszłości i wyrządzić niepowetowaną szkodę interesom Rzeczypospolitej Polskiej.

Po wypowiedziach w przestrzeni publicznej autorytetów w zakresie prawa karnego, w tym prof. Andrzeja Zolla[30] prokuratora ma konstytucyjny obowiązek wszczęcia postępowania celem ustalenia, czy nie zostały wypełnione znamiona przestępstwa z art. 130§ 2 kk.

Komisja nie posiada wiedzy, czy takie postępowanie zostało wszczęte, w związku z czym podjęła decyzję o zawiadomieniu prokuratury o możliwości popełnienia zbrodni z art. 130§ 2 kk przez funkcjonariuszy organów władzy publicznej, którzy w omawianym okresie podjęli stosowne decyzje oraz wykonywali opisane czynności. Byli to:

Ernest BEJDA – pełniący funkcję szefa CBA *(art.231§1 kk. w zw. z art. 130 kk)*

Mariusz KAMIŃSKI – pełniący funkcję Ministra Spraw Wewnętrznych i Administracji i Koordynatora Służb Specjalnych *(art.231§1 kk w zw. z art. 130 kk)*

Michał KIERSKI – Prokurator Okręgowy w Gdańsku *(art.231§1 kk w zw. z art. 130 kk)*

Grzegorz OCIECZEK - pełniący funkcję wiceszefa CBA *(art.231§1 kk w zw. z art. 130 kk)*

Bogdan ŚWIĘCZKOWSKI – Prokurator Krajowy *(art.231§1 kk w zw. z art. 130 kk)*

---

[30] W wywiadzie, którego udzielił prof. Andrzej Zoll Gazecie Wyborczej dnia 29.12.2021 r. stwierdził między innymi: „Bo te informacje, które są zdobywane przez Pegasusa na terenie używającego ten system państwa – w tym wypadku Polski - niewątpliwie trafiają też w ręce służb specjalnych Izraela. A więc korzystanie z tego ma pewne cechy szpiegostwa. Bo to jest dostarczanie obcym służbom specjalnym informacji, które mogą zagrażać państwu polskiemu (...)Wykorzystanie tego, ze względu właśnie na możliwość czy nie tylko możliwość, ale w całej procedurze stosowania tego urządzenia jest przekazywanie czy umożliwienie przekazania obcemu wywiadowi informacji, które zostały zebrane przez Pegasus. Te informacje są ważne, przecież to są informacje o cechach osobowości, o wiadomościach, o przekazywaniu wiadomości przez osoby pełniące ważne funkcje państwowe. Można sobie świetnie wyobrazić, że te osoby, które były namierzone przez Pegasus, będą po przyszłych wyborach pełnić funkcje premierów, prezydenta, bardzo poważne urzędy w państwie. I to może być bardzo dobry materiał do stosowania wobec tych osób szantażu. Różne wiadomości zostały przekazane służbom Izraela..”

Jarosław SZMYT – pełniący funkcję szefa delegatury CBA w Bydgoszczy, nadzorujący operację wobec Senatora Krzysztofa Brejzy *(art.231§1 kk. w zw. z art. 130 kk)*

Naruszenie:

Przestępstwa wskazane w Rozdziale XXX kodeksu karnego: Przestępstwa przeciwko wymiarowi sprawiedliwości, w tym: z art. 234 kk (fałszywe oskarżenie), 235 kk (tworzenie fałszywych dowodów), 239 § 1 kk (zacieranie śladów przestępstwa) oraz 276 kk (niszczenie, uszkodzenie, czynienie bezużytecznym, ukrywanie lub usuwanie dokumentu, którym nie ma się prawa wyłącznie rozporządzać)

Z wyjaśnień osób inwigilowanych systemem „Pegasus", które stawiły się przed Komisją wynika, że wnioski o wyrażenie zgody na kontrolę operacyjną, jakie za pośrednictwem Prokuratora Krajowego składano do sądu, zawierały zmanipulowane informacje i sfabrykowane dowody, wprowadzające sąd w błąd co do zasadności przeprowadzenia takiej kontroli. Jak wyjaśnił senator Krzysztof Brejza, informacje, które CBA podało do sądu, nie zostały potwierdzone w trakcie kontroli operacyjnej.[31] Następnie już po wygaśnięciu zgody na kontrolę operacyjną wielokrotnie dokonywano ataków na telefon senatora Krzysztofa Brejzy. Wreszcie dowody, świadczące o popełnieniu tych czynów, są niszczone. Informację tę przekazał Komisji Senator Krzysztof Brejza w trakcie 21 posiedzenia Komisji.[32] Senator Brejza potwierdził, że posiada informacje, iż połamana została płyta, na której znajdowały się dane, pobrane z jego telefonu podczas pierwszego ataku systemem „Pegasus" w dniu 26 kwietnia 2019 r. Porównanie tej płyty ze stanem telefonu Krzysztofa Brejzy w późniejszym okresie mogło stanowić dowód na to, iż BBA nie tylko pobierała dane z telefonu, ale również wgrywała na urządzenie określone treści.

W ocenie Komisji istnieje uzasadnione podejrzenie, że osoby podejmujące decyzje o podjęciu tego typu działań, jak i zaangażowane w te działania, popełniły przestępstwa, wskazane w Rozdziale XXX Kodeksu karnego, a więc art.234 kk, 235 kk, 239 § 1kk, 276 kk.

---

[31] Wysłuchanie senatora Krzysztofa Brejzy w trakcie 21 posiedzenia Komisji w dniu 12 maja 2023 r.

[32] „Otóż uzyskałem informację, że w postępowaniu, w którym przeciwko mnie użyto cyberbroni Pegasus w trakcie kampanii wyborczej, kiedy kierowałem kampanią Koalicji Obywatelskiej, niszczone są dowody. Oświadczam państwu, że zniszczono płytę, jedną z kilku płyt, na którą pozyskano materiał pochodzący z mojego telefonu systemem cybernetycznym Pegasus. Była to płyta włączona w postępowanie z oryginalną zawartością telefonu, tzw. pierwszy strzał z systemu cyber Pegasus. Zniszczona płyta była płytą unikalną. Dane nie dają się odtworzyć, nie ma kopii 1:1, wiąże się to oczywiście z tym, że ten system jest nielegalny i niecertyfikowany przez polskie służby, ale – co istotne – zniszczenie tej płyty nie pozwala ustalić tego, co do telefonu było wgrywane w kolejnych strzałach, a uzyskaliśmy też informację z Citizen Lab, że służby PiS wgrały do moich telefonów ok. 1 GB danych." – fragment wypowiedzi senatora Krzysztofa Brejzy

Komisja również w tym przypadku podjęła decyzję o zawiadomieniu prokuratury o możliwości popełnienia takiego przestępstwa przez funkcjonariuszy organów władzy publicznej, którzy w omawianym okresie podejmowali takie decyzje. Byli to:

Ernest BEJDA – pełniący funkcję szefa CBA *(art.231§1 kk. w zw. z art. 234 kk w zw. zart.235 kk)*

Mariusz KAMIŃSKI – pełniący funkcję Ministra Spraw Wewnętrznych i Administracji i Koordynatora Służb Specjalnych *(art.231§1 kk w zw. z art. 234 kk w zw. z art. 235 kk)*

Bogdan ŚWIĘCZKOWSKI – Prokurator Krajowy *(art.231§1 kk w zw. z art. 234 kk w zw. z art. 235 kk)*