

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **KOMISJI ŚLEDCZEJ DO ZBADANIA LEGALNOŚCI,
PRAWIDŁOWOŚCI ORAZ CELOWOŚCI
CZYNNOŚCI OPERACYJNO-ROZPOZNAWCZYCH
PODEJMOWANYCH M.IN. Z WYKORZYSTANIEM
OPROGRAMOWANIA PEGASUS PRZEZ CZŁONKÓW
RADY MINISTRÓW, SŁUŻBY SPECJALNE,
POLICJĘ, ORGANY KONTROLI SKARBOWEJ
ORAZ CELNO-SKARBOWEJ, ORGANY POWOŁANE
DO ŚCIGANIA PRZESTĘPSTW I PROKURATURĘ
W OKRESIE OD DNIA 16 LISTOPADA 2015 R.
DO DNIA 20 LISTOPADA 2023 R.
(NR 23)
z dnia 4 września 2024 r.**

Pełny zapis przebiegu posiedzenia Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r. (nr 23)

4 września 2024 r.

Komisja Śledcza do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r., obradująca pod przewodnictwem posła **Magdaleny Sroki (PSL-TD)**, przewodniczącej Komisji, oraz posła **Marcina Bosackiego (KO)**, zastępcy przewodniczącej Komisji, zrealizowała następujący porządek dzienny:

- **przesłuchanie funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego (świadek nr 1), którego dane identyfikujące stanowią informację niejawną, wezwanego w celu złożenia zeznań w toczącym się postępowaniu zmierzającym do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r.;**
- **rozpatrzenie wniosków dowodowych.**

W posiedzeniu udział wzięli: funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego (świadek nr 1), którego dane identyfikujące stanowią informację niejawną – świadek wezwany przez Komisję, **Marcin Bryłka** – pełnomocnik świadka, **Adam Behan**, **Piotr Binas**, **Kamil Krajewski**, **Joanna Martyniuk-Placha**, **Katarzyna Leder Salgueiro**, **Piotr Marciniak**, **Grzegorz Nawrocki**, **Dariusz Pilarz** i **Sławomir Śnieżko** – stali doradcy Komisji.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Sylwia Łaska** i **Mariusz Pawełczyk** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dzień dobry. Witam państwa serdecznie.

Otwieram posiedzenie Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem

oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r.

Na podstawie listy obecności stwierdzam kworum.

Informuję, że na podstawie art. 11a ust. 6 ustawy o sejmowej komisji śledczej na wniosek świadka Marka Bienkowskiego dokonałam poprawek w protokole jego przesłuchania. Były to poprawki jedynie korekcyjne.

Porządek dzienny dzisiejszego posiedzenia Komisji przewiduje przesłuchanie funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego, nazywanego świadkiem nr 1, którego dane identyfikacyjne stanowią informację niejawną, wezwanego w celu złożenia zeznań w sprawie badanej przez Komisję.

Wobec wpływu do Komisji wniosku w sprawie wystąpienia o dokumenty zgłaszam wniosek o rozszerzenie dzisiejszego porządku dziennego Komisji o punkt dotyczący ich rozpatrzenia. Czy jest jakiś sprzeciw? Nie widzę. Rozszerzyliśmy w takim razie porządek dzienny dzisiejszego posiedzenia.

Członków Komisji proszę, w związku z charakterem przesłuchania, o zachowanie dyscypliny zadawania pytań. Pytania ze strony posłów nie mogą nakładać się na odpowiedź świadka, jak również w jednym czasie nie mogą zabierać głosu dwie osoby, ponieważ spowoduje to problemy techniczne i świadek nie będzie słyszał pytań i naszych wypowiedzi.

Informuję, że Komisja uzyskała zgodę szefa Agencji Bezpieczeństwa Wewnętrznego na przesłuchanie funkcjonariusza ABW w trybie jawnym z zachowaniem warunków ochrony wizerunku i danych osobowych, w sposób uniemożliwiający jego identyfikację.

Przystępujemy w takim razie do porządku dziennego dzisiejszego posiedzenia.

Na wezwanie Komisji stawiał się świadek – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego. Komisja przyjmuje określenie „świadek nr 1”. Z treści art. 11d ust. 1 ustawy o sejmowej komisji śledczej w związku z art. 233 § 2 Kodeksu karnego pouczam świadka, iż zeznając przed sejmową komisją śledczą, jest świadek zobowiązany mówić prawdę i tylko prawdę. Zeznanie nieprawdy lub zatajenie prawdy powoduje odpowiedzialność karną na podstawie art. 233 § 1 Kodeksu karnego, który przewiduje sankcję w postaci kary pozbawienia wolności od 6 miesięcy do lat 8.

Wymogi proceduralne obligują mnie do zadania pytania: Czy zrozumiał świadek treść pouczenia?

Świadek nr 1:

Tak, zrozumiałem.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Zgodnie z treścią art. 11c ust. 1 i 2 oraz art. 17 ust. 1 ustawy o sejmowej komisji śledczej pouczam świadka o następujących prawach, które świadkowi przysługują: uchylenia się od odpowiedzi na pytanie, jeżeli jej udzielenie miałoby narazić świadka lub osobę dla świadka najbliższą w rozumieniu art. 115 § 11 Kodeksu karnego na odpowiedzialność za przestępstwo lub przestępstwo skarbowe; odmowy zeznań, gdy jest świadek osobą podejrzaną o popełnienie przestępstwa pozostającego w ścisłym związku z czynem stanowiącym przedmiot postępowania albo gdy za to przestępstwo został świadek skazany; żądania, aby przesłuchano świadka na posiedzeniu zamkniętym, jeżeli treść zeznań miałaby narazić na hańbę świadka lub osobę dla świadka najbliższą w rozumieniu art. 115 § 11 Kodeksu karnego; odmowy zeznań co do okoliczności, na które rozciąga się ciężący na świadku obowiązek zachowania tajemnicy ustawowo chronionej, w przypadkach określonych w przepisach ustawy o sejmowej komisji śledczej; zgłoszenia wniosku o zarządzenie przerwy w posiedzeniu komisji; zwrócenia się z wnioskiem o umożliwienie swobodnej wypowiedzi w objętej przesłuchaniem sprawie; zwrócenia się z wnioskiem o udzielenie pytania... uchylenie pytania, które w świadka ocenie sugeruje treść odpowiedzi, jest nieistotne bądź niestosowne; złożenia wniosku o dokonanie czynności, które komisja może lub ma obowiązek podejmować z urzędu; oraz złożenia wniosku o wyłączenie członka komisji w trybie art. 5 albo art. 6 ustawy o sejmowej komisji śledczej.

Przypominam, że przebieg przesłuchania jest utrwalany za pomocy urządzenia rejestrującego dźwięk i obraz z zachowaniem zasad pełnej anonimizacji.

W dalszej kolejności na podstawie art. 11b ustawy o sejmowej komisji śledczej zwracam się do świadka z pytaniem: Czy ustanowił świadek pełnomocnika?

Świadek nr 1:

Tak, ustanowiłem pełnomocnika, pana Marcina Bryłkę.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Proszę o zgłoszenie pełnomocnictwa do protokołu.

Czy Komisja... członkowie Komisji wnoszą jakiekolwiek zastrzeżenia co do przedłożonego do protokołu pełnomocnictwa? Nie widzę. Komisja nie wnosi w takim razie zastrzeżeń co do przedłożonego pełnomocnictwa.

Oświadczam, że dane identyfikujące oraz dane dotyczące miejsca zamieszkania świadka znane są Komisji i znajdują się w aktach sprawy opatrzonej klauzulą niejawności.

Czy był świadek prawomocnie składany za składanie... skazany za składanie fałszywych zeznań lub oskarżenie?

Świadek nr 1:

Nie.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Proszę o w takim razie wszystkich o powstanie. Zgodnie z treścią art. 11d ustawy o sejmowej komisji śledczej nastąpi teraz odebranie od świadka przyrzeczenia.

Proszę powtarzać za mną:

„Świadomy znaczenia moich słów...

Świadek nr 1:

„Świadomy znaczenia moich słów...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

...i odpowiedzialności przed prawem...

Świadek nr 1:

...i odpowiedzialności przed prawem...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

...przyrzekam uroczyście...

Świadek nr 1:

...przyrzekam uroczyście...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

...że będę mówił szczerą prawdę...

Świadek nr 1:

...że będę mówił szczerą prawdę...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

...niczego nie ukrywając z tego, co jest mi wiadome”.

Świadek nr 1:

...niczego nie ukrywając z tego, co jest mi wiadome”.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję. Możemy usiąść.

Zgodnie z art. 11i ustawy o sejmowej komisji śledczej w związku z art. 171 § 1 Kodeksu postępowania karnego może świadek swobodnie wypowiedzieć się w sprawie będącej przedmiotem badań Komisji. Czy chce świadek skorzystać z tego prawa?

Świadek nr 1:

Nie, dziękuję.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję uprzejmie. W tej chwili przechodzimy w takim razie do zadawania pytań.

Szanowni państwo, do tej pory odnośnie dopuszczenia systemu Pegasus do stosowania przez polskie służby mogliśmy opierać się na doniesieniach medialnych. Ostatnie prace naszej Komisji i przesłuchania, dowody, które żeśmy do tej pory zebrali, wskazują, że system Pegasus i jego integralna część, bez której nie mogłaby nastąpić infekcja urządzenia, znajdowały się poza granicami naszego kraju, w państwie, z którego zakupiono system Pegasus, tzn. w Izraelu.

Czy w takim razie system i osoby, które podjęły decyzję o tym, żeby dopuścić ten system do użytkowania, miały pełną świadomość tego, jak wygląda jego architektura? Czy dane pozyskiwane przy pomocy tego systemu są bezpieczne? Ja dzisiaj mam przekonanie, że nasze dane nie były bezpieczne. Dlatego dzisiejsze przesłuchanie... mam nadzieję, że pozwoli nam odpowiedzieć na kwestie dotyczące akredytacji, czyli czy Agencja Bezpieczeństwa Wewnętrznego, która takie akredytacje przy tego typu narzędziach pracy operacyjnej wykonała, a jeżeli nie, to dlaczego nie przeprowadzono takiej akredytacji.

Bardzo proszę powiedzieć i odpowiedzieć na pytanie. Bardzo proszę świadka, na czym polega akredytacja bezpieczeństwa teleinformatycznego systemów teleinformatycznych przeznaczanych do przetwarzania informacji niejawnych? Jak wygląda ta procedura?

Świadek nr 1:

Akredytacja bezpieczeństwa systemu... systemów teleinformatycznych prowadzona w trybie art. 48 i tak naprawdę całego rozdziału 8 ustawy o ochronie informacji niejawnych polega na kompleksowej ocenie bezpieczeństwa systemów teleinformatycznych. Chciałbym jednak w tym miejscu sprecyzować jedną drobną rzecz. Otóż w rozumieniu ustawy systemem teleinformatycznym jest tak naprawdę zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Musimy...

Świadek nr 1:

To nie jest...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Przepraszam, musimy mówić ciut wolniej, bo dźwięk za szybko do nas dochodzi, tak że bardzo proszę o troszeczkę wolniejsze tempo odpowiedzi.

Świadek nr 1:

Dobrze.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo proszę.

Świadek nr 1:

Akredytacją bezpieczeństwa jest kompleksowa ocena bezpieczeństwa systemów teleinformatycznych. Należy jednakże pamiętać, że zgodnie z ustawową definicją systemem teleinformatycznym jest zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania. Tutaj należałoby zadać sobie pytanie, czy potoczne rozumienie określenia systemu Pegasus jest zbieżne z jego ustawową definicją tak naprawdę, dlatego że z doniesień medialnych wynika bardziej, że tutaj posłużono się pewną usługą lub oprogramowaniem zakupionym od strony trzeciej, a nie systemem teleinformatycznym w ustawowym rozumieniu, czyli nie czymś, co jest przedmiotem akredytacji bezpieczeństwa teleinformatycznego.

Kontynuując, każda akredytacja tak naprawdę prowadzona jest na wniosek podmiotu, czyli jednostki organizacyjnej, która taki system tworzy zgodnie z dokumentacją bezpieczeństwa analizowaną czy to w ABW, czy w SKW, i wynikami audytu. Wydawane jest ewentualne świadectwo w przypadku zarówno pozytywnej oceny dokumentacji, jak i pozytywnych wyników audytu bezpieczeństwa systemu.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czy w takim razie dysponent tego systemu zwrócił się do Agencji Bezpieczeństwa Wewnętrznego o przeprowadzenie sprawdzeń?

Świadek nr 1:

Proszę pamiętać, że większość dokumentacji bezpieczeństwa... są opatrzone klauzulami, szczególnie dokumentacji przeznaczonych do systemów, które mają służyć pracy operacyjnej. Jeżeli chodzi o część jawną, mogę powiedzieć, że zgodnie z moją wiedzą w Agencji Bezpieczeństwa Wewnętrznego nigdy nie zostało wydane świadectwo dla systemu pod nazwą Pegasus, dla CBA oczywiście, bo nie chcę tu mówić o tym, że jakaś jednostka nazwała sobie tak system.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Proszę w takim razie powiedzieć, w jakim celu w ogóle udziela się takiej akredytacji.

Świadek nr 1:

Akredytacji bezpieczeństwa teleinformatycznego... Znaczący... W jakim celu? Zgodnie z art. 48 ust. 1 ustawy o ochronie informacji niejawnych systemy teleinformatyczne przeznaczone do przetwarzania informacji niejawnych podlegają akredytacji. Ustawowo jest to wymóg. Niemniej jednak należy pamiętać o zapisach art. 51, który stanowi pewne wyłączenia z obowiązku akredytacji. W obecnym brzmieniu tego artykułu z obowiązku akredytacji, o którym mowa w art. 48 ust. 1, nie podlegają systemy teleinformatyczne, których elementy znajdują się poza strefami ochronnymi oraz służące bezpośrednio do pozyskiwania i przekazywania w sposób niejawny informacji, która z utrwalania dowodów w trakcie realizacji czynności operacyjno-rozpoznawczych lub procesowych przez uprawnione do tego podmioty... Wyłączenie obowiązku akredytacji nie obejmuje interfejsów, o których mowa w art. 179 – prawo telekomunikacyjne. Obowiązkowi akredytacji również nie podlegają systemy teleinformatyczne, a obowiązkowi certyfikacji urządzenia i narzędzia kryptograficzne wykorzystywane przez ABW, SKW, AW lub SWW do pozyskiwania lub przetwarzania informacji niejawnych podczas wykonywania czynności operacyjno-rozpoznawczych. Jest to brzmienie art. 51, zmienione w 2022 r. zapisami ustawy o obronie Ojczyzny.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Proszę powiedzieć w takim razie... 2017 r., w momencie, kiedy system Pegasus rozpoczyna działanie na terytorium RP, przepisy wyglądały inaczej?

Świadek nr 1:

Tak, były wprowadzone... w 2022 r. były wprowadzone drobne, ale bardzo znaczące zmiany, jeżeli chodzi o treść tego art. 51 stanowiącego wyłączenia z obowiązku akredytacji, dlatego że w oryginalnym brzmieniu, które obowiązywało przez 11 lat tak naprawdę, jak ustawa... od wejścia w życie ustawy do 2022 r., nie znajdowało się sformułowanie „systemy, których elementy znajdują się”, tylko „systemy znajdujące się poza strefami ochronnymi”, co stanowi nie... (*niezrozumiałe*) jeżeli chodzi o treść, natomiast bardzo znaczącą merytorycznie zmianę ustawową.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

A w przypadku takiego systemu jak Pegasus, którego elementy znajdowały się w tej strefie ochronnej, ale część elementów znajdowała się poza, czy w takim razie system Pegasus miał... powinien zostać akredytowany?

Świadek nr 1:

Szczerze mówiąc, nie mam wiedzy, czy wszystkie elementy systemu Pegasus między rozpoczęciem jego użytkowania przez CBA a 2022 r. znajdowały się w strefach czy poza nimi. Natomiast jeżeli jakkolwiek element systemu znajdował się w strefach ochronnych i w takim systemie były przetwarzane informacje niejawne, a całość spełnia wymogi systemu teleinformatycznego jako takiego, to obowiązkiem kierownika jednostki organizacyjnej było przedłożenie dokumentacji i rozpoczęcie procesu akredytacji takiego systemu.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Podczas jednej z konferencji pana Wąsika i Kamińskiego mieliśmy możliwość dowiedzenia się, że właśnie w strefie tej ochronnej znajdowały się komputery i operatorzy, którzy korzystali z systemu Pegasus. Czy w takim razie można uznać, że jeden element tego systemu znajdował się w strefie bezpieczeństwa?

Świadek nr 1:

Jeżeli... Można tak uznać, natomiast jeszcze jest troszeczkę głębsze pytanie tak naprawdę, o to, czy nawet jeżeli ci operatorzy znajdowali się w strefach ochronnych, to czy informacje, które były przetwarzane na takich elementach systemu, wpisywały się w definicję informacji niejawnych.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

My wiemy, że wpisywały się w tę definicję informacji niejawnych.

Dobrze, na tym etapie dziękuję.

Bardzo proszę, oddaję głos teraz panu wiceprzewodniczącemu Marcinowi Bosackiemu. Bardzo proszę.

Poseł Marcin Bosacki (KO):

Dziękuję bardzo, pani przewodnicząca.

Proszę świadka, najpierw pytanie troszkę ogólne. Czy według wiedzy świadka możliwe jest udzielenie akredytacji bezpieczeństwa albo wtedy było, czyli w 2017 r., wtedy kiedy elementy tego systemu, na przykład sieć anonimizująca – myślę, że doskonale pan wie, jest zapoznany z takim pojęciem – nie znajdują się pod kontrolą agencji, która tego systemu używa? Czy byłoby możliwe udzielenie takiego... takiej akredytacji?

Świadek nr 1:

Trudno jest odpowiedzieć tak naprawdę na takie pytanie, dlatego że trzeba pamiętać o tym, że każdy system teleinformatyczny ma jakieś wyznaczone granice. I tutaj to, co chciałem podkreślić, odpowiadając na pierwsze pytania... Ogólne pojęcie systemu, którym posługujemy się na co dzień, nieco odbiega od definicji systemu teleinformatycznego. Niekoniecznie należałoby stwierdzić, że ta sieć anonimizująca byłaby częścią takiego, nawet akredytowanego systemu. To jest jedna rzecz.

Druga rzecz to to, czy w takiej sieci rzeczywiście byłyby przetwarzane informacje w taki czy inny sposób, które stanowiłyby informację rzeczywiście niejawną, natomiast w przypadku gdybyśmy mówili ogólnie, całkowicie odrębnie od systemu Pegasus, to gdyby informacje niejawne miałyby być przetwarzane w częściach systemu, które są poza kontrolą drugiego organizatora czy też jednostki organizacyjnej, która odpowiada za taki system, trudno by mi było sobie wyobrazić, żeby kierownik jednostki zaakceptował ryzyko z tym związane. A sam proces szacowania ryzyka jest tak naprawdę podstawą wyznaczenia poziomu bezpieczeństwa każdego systemu teleinformatycznego. W tym momencie już nie mówimy tak naprawdę tylko o systemach niejawnych, dlatego że procesy zarządzania ryzykiem i zarządzania bezpieczeństwem informacji oparte o szacowanie ryzyka dotyczą zarówno systemów jawnych, jak i niejawnych.

Poseł Marcin Bosacki (KO):

Przez chwilę zaakceptuję tę świadka wątpliwość czy też odnoszenie się do sytuacji hipotetycznej, a nie systemu Pegasus. Mam w związku z tym pytanie takie. Czy jeśli pan mówi „kierownik jednostki”, to pan ma na myśli kierownik jednostki, która może albo powinna zgłosić się do państwa, czyli do ABW, z prośbą o uzyskanie akredytacji? O tym mówimy, tak, o tym kierowniku jednostki?

Świadek nr 1:

Tak, dokładnie. Jeżeli chodzi o jakąkolwiek służbę w Polsce, jest to szef tej służby. Praktykowane jest również, że taką dokumentację zgłasza dyrektor pionu technicznego ewentualnie.

Poseł Marcin Bosacki (KO):

Czyli z pana wiedzy, jak rozumiem, szerokiej i długiej trudno by było sobie wyobrazić – bo to pan przed chwilą powiedział, ale ja chcę trochę uprościć i jaśniejszym językiem powiedzieć – że można byłoby w polskich służbach specjalnych używać systemu, którego elementy mogą być nie tylko nie pod kontrolą tej służby, ale wręcz poza granicami naszego kraju.

Świadek nr 1:

Jeżeli byłyby to kluczowe elementy, w których przetwarzane byłyby informacje niejawne, to tak. Byłoby to bardzo trudne do akredytacji.

Poseł Marcin Bosacki (KO):

Powtórzę słowa pani przewodniczącej, że według naszej wiedzy, także z przesłuchań świadków, wynika, że oczywiście w systemie Pegasus były przetwarzane dane podległe klauzuli niejawności.

Mam do pana kolejne pytanie, bo pan zeznał już, że Agencja Bezpieczeństwa Wewnętrznego nie wydała akredytacji na prośbę CBA dla systemu, który nazywałby się Pegasus. Czy wydała bądź odmówiła wydania, czy w ogóle uzyskiwała prośbę na inny system czy inaczej nazywający się system, na przykład – wiemy o tej nazwie z przekazów medialnych – nazywający się Jarvis? To jest ten sam system, tylko używano w służbach tego... tej nazwy.

Świadek nr 1:

Taka nazwa na żadnym świadectwie akredytacji również się nie pojawiła.

Poseł Marcin Bosacki (KO):

Dziękuję. Jeszcze jedno pytanie. Czy według pana opinii i zgodnie z pana, ze świadka ugruntowaną wiedzą, czy dowody pozyskane przez służby za pomocą systemu teleinformatycznego, który nie został poddany procedurze akredytacji bezpieczeństwa i który, co już wiemy, częściowo był nie pod kontrolą polskich służb, mogą być czy mogłyby być wykorzystane skutecznie w postępowaniu karnym?

Świadek nr 1:

Przykro mi, nie jestem prawnikiem i nie jestem w stanie odpowiedzieć na to pytanie.

Poseł Marcin Bosacki (KO):

Proszę w takim razie jeszcze odpowiedzieć na jedno pytanie. Czy możliwe jest, aby system teleinformatyczny... Pan miał wątpliwość, czy to jest system informatyczny, ale nadal poruszamy się w tej sferze jakby nie odnoszącej się tylko do Pegasusa, tylko pytanie jest ogólne. Czy możliwe jest, aby system teleinformatyczny był legalnie stosowany przez polskie służby, mimo że nie przeprowadzono procedury akredytacji? Czy są jakieś wyjątki od zasady, że systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, muszą być akredytowane przez jedną z dwóch właściwych do tego agencji?

Świadek nr 1:

Tak jak wspominałem wcześniej, rzeczony art. 51 ustawy o ochronie informacji niejawnych wyłączający z obowiązku akredytacji systemy – już mówiąc w skrócie – przeznaczone do czynności operacyjno-rozpoznawczych lub dochodzeniowo-śledczych, pod pewnymi dodatkowymi warunkami oczywiście... W obecnym brzmieniu ustawy systemy, których elementy znajdują się...

Poseł Marcin Bosacki (KO):

Nie...

Świadek nr 1:

...poza strefami ochronnymi...

Poseł Marcin Bosacki (KO):

...absolutnie... Chodzi mi o stan prawny z 2017 r.

Świadek nr 1:

Czyli byłyby to systemy, które w całości znajdowałyby się poza strefami ochronnymi.

Poseł Marcin Bosacki (KO):

Jak wiemy, również z konferencji prasowych panów Kamińskiego i Wąsika, z całą pewnością system Pegasus był obsługiwany w strefach ochronnych.

Dziękuję, na razie nie mam więcej pytań. Będę miał jeszcze w drugiej turze. Dziękuję.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Bardzo proszę, Witold Zembaczyński zadaje pytanie.

Poseł Witold Zembaczyński (KO):

Wielce szanowna pani przewodnicząca, Wysoka Komisjo, szanowni państwo doradcy, proszę świadka, proszę zatem powiedzieć, ale opierajmy się na roku 2017, wtedy kiedy mamy to okienko, w którym Pegasus zostaje przez CBA nabyty... Proszę powiedzieć, czy w tamtym czasie CBA powinno zwrócić się do Agencji Bezpieczeństwa Wewnętrznego o udzielenie akredytacji bezpieczeństwa teleinformatycznego przed zakupem Pegasus, czy po jego nabyciu.

Świadek nr 1:

To znaczy, trudno byłoby zwrócić się o jakąkolwiek akredytację, nie mając tak naprawdę systemu... *(niezrozumiale)*

Poseł Witold Zembaczyński (KO):

Rozumiem. Chodzi o rekomendację. Chodzi o rekomendację agencji na przykład w zakresie bezpieczeństwa, dotychczasową wiedzę. No przecież to nie jest jedyne oprogramowanie o podobnych parametrach.

Świadek nr 1:

Nie ma takiego ustawowego obowiązku. Tu należałoby podejść do tego typu zakupów zdroworozsądkowo. Wiadomo, że jeżeli próbujemy zakupić coś, co może nie jest standardowym oprogramowaniem czy standardowym systemem, to taka odpowiedź na pewno byłaby do CBA udzielona, gdyby się do nas o nią zwrócili.

Poseł Witold Zembaczyński (KO):

Takiego zapytania o opinię na temat użycia Pegasus w polskiej rzeczywistości prawnej i służb specjalnych nie było?

Świadek nr 1:

Nie mam wiedzy na ten temat.

Poseł Witold Zembaczyński (KO):

Proszę powiedzieć, ile czasu zajmuje taka akredytacja systemu kontroli operacyjnej, kiedy wszystkie przepisy są spełnione – chodzi o stan prawny 2017 r.

Świadek nr 1:

Jeżeli chodzi o systemy do kontroli operacyjnej czy jakiegokolwiek systemy teleinformatyczne, tutaj ustawodawca nałożył maksymalny termin 6 miesięcy. Przy dużym skomplikowaniu możliwe jest rozszerzenie o kolejne 6 miesięcy takiego okresu, czyli mówimy o czasie do roku od złożenia kompletnej dokumentacji.

Poseł Witold Zembaczyński (KO):

Rozumiem. I zazwyczaj to jest tak, że jest system nabyty, złożony jest wniosek o akredytację, potem do roku trwa proces, tak?

Świadek nr 1:

Mhm.

Poseł Witold Zembaczyński (KO):

Dziękuję. Proszę... Tak? Coś chce świadek dodać?

Świadek nr 1:

Nie chciałbym się odnosić odnośnie nabycia systemu czy też przedłużenia jakiegokolwiek tego typu formy, natomiast proces ustawowo może trwać do 12 miesięcy.

Poseł Witold Zembaczyński (KO):

Proszę powiedzieć w nawiązaniu do dotychczasowych odpowiedzi, czy CBA przekazywało ABW jakiegokolwiek materiały dotyczące systemu Pegasus. Czy sondowano możliwość tej akredytacji? Może chciano wiedzieć, ile wcześniej powinni przekazać materiały

dotyczące bezpieczeństwa systemu, tak aby Pegasus był stosowany zgodnie z prawem i bez dostępu osób nieuprawnionych?

Świadek nr 1:

Nie mam niestety żadnej wiedzy na ten temat.

Poseł Witold Zembaczyński (KO):

Na jakim etapie powinien rozpocząć się proces konsultacji z ABW w celu sprawdzenia, czy system do kontroli operacyjnej może być bezpiecznie stosowany? Czy powinno to się rozpocząć na etapie właśnie planu zakupowego, czy też na etapie już wdrożenia jakiegoś testowego użycia? Czy użycie systemu jest możliwe dopiero po pełnym procesie akredytacji?

Świadek nr 1:

To znaczy tak, użycie systemu, i tu mówimy o stanie na rok 2017...

Poseł Witold Zembaczyński (KO):

Tak.

Świadek nr 1:

Użycie systemu, który znajdowałby się w strefach ochronnych, wykorzystanie go produkcyjnie wymaga posiadania przez taki system akredytacji... wymaga posiadania przez taki system posiadania akredytacji bezpieczeństwa teleinformatycznego, czyli posiadania wydanego świadectwa akredytacji. Krótko.

Poseł Witold Zembaczyński (KO):

Dziękuję.

Proszę powiedzieć, czy zdarzyły się jakiegokolwiek przypadki, że którykolwiek z systemów, nad którymi pracowaliśmy, po prostu nie spełniał tych wymagań bezpieczeństwa do przetwarzania i obróbki informacji niejawnych.

Świadek nr 1:

Czy... Przepraszam, proszę o doprecyzowanie pytania. Czy chodzi o systemy, które używały akredytację, czy o...

Poseł Witold Zembaczyński (KO):

O odmowę. Chodzi mi o odmowę, proszę świadka, gdyż my badamy jako Komisja Śledcza nie tylko wyłącznie samego Pegasusa, ale również inne systemy, które służą pracy operacyjnej. Proszę zatem odpowiedzieć. Czy zdarzały się przypadki odmowy, to znaczy takie, w których ta akredytacja nie mogła być udzielona?

Świadek nr 1:

Szczerze mówiąc, nie przypominam sobie przypadków odmowy jako odmowy, natomiast standardowe tak naprawdę w procesie akredytacji są zmiany w systemie. Dokumentacja jest przygotowana już na etapie projektowania i może być wtedy konsultowana. Bardzo często zdarzają się zmiany w takim systemie. Bardzo często zdarzają się zmiany w dokumentacji. Zdarzają się również... Zdarza się również konieczność przeprowadzenia ponownego audytu, gdyż system nie spełnia wymagań pomimo tego, że one są opisane w dokumentacji. I z mojej praktyki wynika to, że raczej jako służba staramy się doprowadzić do tego, żeby system, który został zaprojektowany, który jest wdrażany w jakiejś jednostce organizacyjnej, uzyskał tę akredytację. Staramy się prowadzić ten proces w taki sposób, żeby również poinstruować tego organizatora systemu, osoby odpowiedzialne za to, tak aby można było spełnić wymagania funkcjonalne jednostek, które użytkują systemy przetwarzające informacje niejawne, ale w sposób bezpieczny.

Poseł Witold Zembaczyński (KO):

Bardzo dziękuję za tę odpowiedź. Proszę świadka, zgodnie z art. 49 ustawy o ochronie informacji niejawnych to szef Centralnego Biura Antykorupcyjnego, gdzie funkcjonował Pegasus, odpowiada za opracowanie i przekazanie ABW lub SKW dokumentacji bezpieczeństwa systemu do kontroli operacyjnej. Czy to się zgadza?

Świadek nr 1:

Tak naprawdę każdego systemu teleinformatycznego.

Poseł Witold Zembaczyński (KO):

Jaka zatem odpowiedzialność grozi szefowi CBA, jeżeli użytkował Pegasusa bez przekazania takiej dokumentacji do ABW lub SKW?

Świadek nr 1:

Nie jestem prawnikiem. Powstrzymam się od odpowiedzi.

Poseł Witold Zembaczyński (KO):

Rozumiem. Czy szef CBA, czy też dyrektor biura techniki operacyjnej odpowiada za bezpieczeństwo stosowania systemu kontroli operacyjnej typu Pegasus? Kto z nich?

Świadek nr 1:

Proszę pamiętać, że zgodnie z art. 14 ustawy o ochronie informacji niejawnych kierownik jednostki organizacyjnej, czyli w tym wypadku szef CBA, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony. Jest to wprost wynikająca odpowiedzialność z art. 14 ust. 1 ustawy o ochronie informacji niejawnych.

Poseł Witold Zembaczyński (KO):

Dziękuję.

Czy akredytacja systemu teleinformatycznego dokonywana przez Agencję Bezpieczeństwa Wewnętrznego jest procesem łącznym czy też oddzielnym od procesu certyfikacji poszczególnych narzędzi czy też urządzeń do realizacji zabezpieczenia teleinformatycznego przeznaczonego do ochrony informacji niejawnych, czyli system versus urządzenie?

Świadek nr 1:

Są to procesy rozłączne. Proces certyfikacji jest to tak naprawdę proces stricte badań i oceny pewnych urządzeń, narzędzi i środków służących do zapewnienia bezpieczeństwa informacjom niejawnym przetwarzanym w systemach. Natomiast w procesie akredytacji opieramy się tak naprawdę na wynikach procesów certyfikacji, w szczególności na wydanych certyfikatach. Bo tutaj należy też pamiętać, że akurat nie w przypadku, o którym mówimy, jeżeli chodzi o systemy typu Pegasus, natomiast w przypadkach przekazywania informacji niejawnych poza strefy ochronne rozporządzenie w sprawie bezpieczeństwa teleinformatycznego nakłada obowiązek stosowania urządzeń kryptograficznych, które są certyfikowane. I tutaj, jeżeli chodzi o proces certyfikacji, to są specjalistyczne laboratoria i zespoły osób, które są wysoce wykwalifikowane do tego, żeby taką ocenę konkretnego urządzenia, narzędzia lub środka przeprowadzić.

Poseł Witold Zembaczyński (KO):

Proszę świadka, na tym etapie prosiłbym świadka o takie podsumowanie dotychczas złożonych zeznań. Czy zatem Pegasus, który był, jak powszechnie nam wiadomo, używany przez CBA i wykorzystywany do pracy operacyjnej, podlegał w 2017 r. temu bezwzględnemu obowiązkowi akredytacji ABW, czy też nie podlegał? Proszę o odpowiedź „tak” lub „nie”.

Świadek nr 1:

Nie jestem w stanie odpowiedzieć, udzielić odpowiedzi „tak” lub „nie”, gdyż nie analizowałem całej konstrukcji systemu Pegasus w CBA. Nie są mi znane te dokumenty, więc odpowiedzi „tak” lub „nie” nie jestem w stanie niestety udzielić.

Poseł Witold Zembaczyński (KO):

Rozumiem. Czyli brak tej odpowiedzi wynika z braku dostępu do pewnej wiedzy odnośnie zasobów, jakimi dysponowało CBA, jeżeli chodzi o cały system Pegasusa, czyli urządzenia oraz oprogramowanie, tak?

Świadek nr 1:

Tak.

Poseł Witold Zembaczyński (KO):

Bardzo dziękuję.

Może zadam ostatnie pytanie w tej części. Proszę świadka, tu świadek bardzo dobrze orientuje się w przepisach ustawy o ochronie informacji niejawnych, więc ja tutaj posłuję

się art. 51 i zacytuję go. Mianowicie obowiązkowi akredytacji bezpieczeństwa teleinformatycznego, o którym mowa w art. 48 ust. 1 – o czym rozmawialiśmy – nie podlegają systemy teleinformatyczne, których elementy znajdują się poza strefami ochronnymi oraz służące bezpośrednio do pozyskiwania i przekazywania w sposób niejawną informacji i utrwalania dowodów w trakcie realizacji czynności operacyjno-rozpoznawczych lub procesowych przez uprawnione do tego podmioty.

Jakby mógł świadek Wysokiej Komisji, opinii publicznej wytłumaczyć, jak zatem w kontekście Pegasusu należy interpretować ten art. 51.

Świadek nr 1:

Pozwolę sobie jedynie zaznaczyć, że przytoczył pan zapis ustawy, który został wprowadzony w 2022 r.

Poseł Witold Zembaczyński (KO):

No więc właśnie, dlatego mamy tutaj stan prawny 2022 i 2017. Jakbym mógł uprzejmie prosić świadka o odniesienie się do tych obydwu stanów prawnych.

Świadek nr 1:

Jak najbardziej. Rok 2011, wejście w życie ustawy, czyli zapisy oryginalne ustawy, które w kontekście art. 51 merytorycznie nie zostały zmienione do roku 2022, mówiły o tym, że obowiązkowi akredytacji bezpieczeństwa teleinformatycznego nie podlegają systemy teleinformatyczne znajdujące się poza strefami ochronnymi i dalej służące do pozyskiwania i przekazywania w sposób niejawną informacji oraz utrwalania dowodów w trakcie realizacji czynności operacyjno-rozpoznawczych lub procesowych przez uprawnione do tego podmioty.

Na tym na razie zakończę przytoczenie artykułu. Mowa tu jest o systemach, które w całości znajdowały się poza strefami ochronnymi, służyły do prowadzenia czynności operacyjno-rozpoznawczych lub procesowych przez uprawnione do tego podmioty. Jeżeli system znajdował się w całości poza strefą i służył do wykonywania określonych czynności przez uprawnione do tego podmioty, można było wykorzystywać ten system bez uzyskania akredytacji bezpieczeństwa teleinformatycznego.

Poseł Witold Zembaczyński (KO):

Proszę świadka...

Świadek nr 1:

Wyłączenie nigdy nie obejmowało i w dalszym ciągu nie obejmuje interfejsów, o których mowa w prawie telekomunikacyjnym.

Poseł Witold Zembaczyński (KO):

Proszę świadka, ale proszę z uwagi na swoje doświadczenie powiedzieć nam, jak... skąd intencja zmiany tego przepisu w 2022 r. Czy to wynikało z prozy pracy służb? Czy to była jakaś wola ustawodawcy bliżej nieokreślona?

Świadek nr 1:

Nie mam wiedzy, skąd wynikała chęć zmiany i zmiana tego artykułu ustawy o obronie Ojczyzny, natomiast artykuł był jak najbardziej wykorzystywany od 2011 r. i takie systemy były, które korzystały z tego artykułu.

Poseł Witold Zembaczyński (KO):

I po 2022 r. stan prawny się zmienia, co również ma istotny wpływ na proces akredytacji systemów teleinformatycznych używanych przez służby specjalne.

Świadek nr 1:

I tak, i nie, dlatego że to, że coś nie podlega obowiązkowi akredytacji, a nie może być akredytowane, to są troszeczkę odrębne pojęcia. I tutaj zgodnie z moim doświadczeniem zbyt dużo się, jeżeli chodzi o podejście do tego typu systemów, się zbyt mocno nie zmieniło, dlatego że, proszę pamiętać, wydanie akredytacji potwierdza jednak bezpieczeństwo takiego systemu i potwierdza to, że w tym systemie można w bezpieczny sposób przetwarzać informacje niejawną. Artykuł, który w oryginalnym brzmieniu był wprowadzony w celu zapewnienia możliwości pracy funkcjonariuszom uprawnionych podmiotów poza

strefami ochronnymi i mimo to w razie konieczności przetwarzania informacji niejawnych w różnych sytuacjach...

Poseł Witold Zembaczyński (KO):

Bardzo dziękuję za te odpowiedzi.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Teraz pytania zadaje przewodniczący Tomasz Treła. Bardzo proszę.

Poseł Tomasz Treła (Lewica):

Dziękuję bardzo.

Ja mam pytanie do świadka w kontekście tego, o czym pan mówił, że ta akredytacja może w wyjątkowych sytuacjach być przedłużona do 12 miesięcy. Nie wchodząc w szczególności, proszę powiedzieć, jakie dokumenty państwo powinniście otrzymać celem takiego kompletnego rozpatrzenia wniosku o akredytację.

Świadek nr 1:

Tutaj mogę wejść w szczegóły. Tak naprawdę wszystkie dokumenty wymagane do przeprowadzenia procesu akredytacji są opisane zarówno w ustawie, jak i w rozporządzeniu dotyczącym bezpieczeństwa teleinformatycznego. Przede wszystkim są to dokumenty szczególnych wymagań bezpieczeństwa, czyli dokument, który opisuje zasady budowy, funkcjonalności, a także elementy ochrony zarówno organizacyjnej, fizycznej, jak i technicznej systemu teleinformatycznego. W tym dokumencie lub w dokumencie odrębnym znajdują się... znajduje się... znajdować się musi – przepraszam – raport z procesu szacowania ryzyka, czyli z określenia, jakie mamy ryzyko dla atrybutów bezpieczeństwa informacji niejawnej oraz w jaki sposób przeciwdziałamy, jakie mamy ryzyko szczątkowe. Bo proszę pamiętać, że ryzyko ujawnienia informacji czy nieuprawnionej zmiany, czy wręcz utraty nigdy nie jest zerowe, zawsze jest na pewnym określonym poziomie. To do kierownika jednostki organizacyjnej należy określenie tego poziomu i akceptacja ryzyk, które on akceptuje, akceptacja ryzyk szczątkowych pozostałych po procesie szacowania ryzyka.

Dodatkowym dokumentem są procedury bezpiecznej eksploatacji, czyli dokument mówiący o tym, w jaki sposób wykorzystuje się taki system, jak może... jakie są zadania i odpowiedzialność administratora tego systemu, inspektora bezpieczeństwa, jakie prawa i obowiązki ma użytkownik tego systemu. To jest tak naprawdę komplet dokumentacji bezpieczeństwa.

Poseł Tomasz Treła (Lewica):

A proszę powiedzieć, bo nie wiem, czy to pytanie padło – może mi umknęło – czy w pana praktyce, karierze, doświadczeniu były takie przypadki, że były wnioski o akredytację i te wnioski były uzupełniane, a finalnie akredytacja przez Agencję Bezpieczeństwa Wewnętrznego nie była udzielana.

Świadek nr 1:

Trudno jest na to odpowiedzieć z uwagi na mnogość systemów, natomiast... Nie jest w stanie w 100% odpowiedzieć. Mogły się zdarzyć, ale to raczej w wyniku... w wyniku tego, że jednostka organizacyjna rezygnowała z dalszej akredytacji tego systemu, czyli na jakimś etapie go po prostu zamykała, niż z chęci wydania odmowy akredytacji. Natomiast nie jestem w stanie w 100% powiedzieć, że nigdy taka odmowa nie miała miejsca.

Poseł Tomasz Treła (Lewica):

Ale rozumiem, że pana kierunek odpowiedzi jest taki, że najprawdopodobniej ci, którzy wnioskowali, mogli się z tego wycofać, a nie było to jednostronnie po stronie Agencji Bezpieczeństwa Wewnętrznego, że były jakieś nieprawidłowości, niejasności, niekompletne dokumenty i tym podobne rzeczy.

Świadek nr 1:

Nieprawidłowości, niejasności, niekompletne dokumenty to jest tak naprawdę niestety standard naszej pracy, jeżeli chodzi o akredytację. I tutaj staramy się raczej poprosić o uzupełnienie, wskazać obszary, które wymagają uszczegółowienia bądź zmiany, a nie wydawać decyzję odmowną.

Poseł Tomasz Treła (Lewica):

OK. Proszę mi powiedzieć – bo też pan był uprzejmy chyba o to zahaczyć podczas jednej z odpowiedzi – czy ja to dobrze zrozumiałem, że w takich normalnych, praktycznych, funkcjonalnych zasadach Centralne Biuro Antykorupcyjne chcąc zakupić tego typu oprogramowanie, na etapie przygotowawczym powinno zwrócić się do Agencji Bezpieczeństwa Wewnętrznego z pewnymi informacjami, planami, założeniami, jeżeli chodzi o posiadanie tak naprawdę jako państwo polskie tego typu oprogramowania.

Świadek nr 1:

Nigdy nie mieli takiego ustawowego obowiązku, natomiast trudno jest mi wyrokować, czy się zwrócili, czy nie. Nie mam takiej wiedzy, tylko że tu bardziej wypowiadałem się w temacie ogólnym. Osobiście, ja, budując niestandardowy system, który kosztował wielkie pieniądze, zwróciłbym się do podmiotu akredytującego z pytaniem, w jaki sposób przygotować się do takiej akredytacji już wcześniej, na etapie projektowania systemu.

Poseł Tomasz Treła (Lewica):

OK. Czyli tak na dobrą sprawę pana interpretacja i pana odpowiedź, doradztwo byłoby takie: jeżeli kupujemy niestandardowe oprogramowanie, to dobrze by było, żeby jednostka, która kupuje, z jednostką, która akredytuje, była w kooperacji, w porozumieniu, żeby nie popełnić żadnego błędu na etapie planowania, projektowania, kupowania tego systemu.

Świadek nr 1:

Może nie kupowania, dlatego że to jest odrębny proces, natomiast jeżeli chodzi o projektowanie jakichś rozbudowanych, niestandardowych systemów, zawsze były dopuszczalne... zawsze była dopuszczalna możliwość wcześniejszej konsultacji i konstrukcji takiego systemu.

Poseł Tomasz Treła (Lewica):

Proszę powiedzieć, czy pan ma wiedzę, czy w Agencji Bezpieczeństwa Wewnętrznego była jakakolwiek informacja przekazywana, czy mówiło się o tym, że Centralne Biuro Antykorupcyjne od 2017 r. jest w posiadaniu systemu, który ma weryfikować, sprawdzać numery telefonów, pozyskiwać informacje. Mówię o 2017, 2018, 2019, 2020. Czy to była wiedza, która gdzieś towarzyszyła Agencji Bezpieczeństwa Wewnętrznego, że inna służba taki sprzęt posiada?

Świadek nr 1:

Nie mam wiedzy na ten temat.

Poseł Tomasz Treła (Lewica):

Nie ma pan wiedzy na ten temat?

Świadek nr 1:

Nie.

Poseł Tomasz Treła (Lewica):

Dziękuję.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Teraz pytanie zadaje pan przewodniczący Paweł Śliz.

Poseł Paweł Śliz (Polska2050-TD):

Proszę świadka, jak świadek mógłby wyjaśnić w takich słowach bez żargonu, zrozumiałych, nieprofesjonalnych, jaki jest cel takiej akredytacji? Po co ją ABW przeprowadza i czemu ona jest istotna?

Świadek nr 1:

Celem akredytacji jest potwierdzenie, że system teleinformatyczny, czyli po prostu, mówiąc już bardzo nieprofesjonalnie, komputer, na którym ktoś chce przetwarzać informacje niejawne, jest zabezpieczony w sposób wystarczający, żeby te informacje nie trafiły do osób nieuprawnionych.

Poseł Paweł Śliz (Polska2050-TD):

Czyli chodzi o to, żeby informacje, jakieś zakluzulowane, chociażby tajne czy ściśle tajne, nie... w sposób niezgodny z prawem nie wyciekły do jakichś innych organów niżli te, które prowadzą czynności operacyjne, były dostępne. Tak to mam rozumieć, tak?

Świadek nr 1:

Nie do końca. Proszę pamiętać, że informacje niejawne to nie zawsze są informacje dotyczące czynności operacyjnych.

Poseł Paweł Śliz (Polska2050-TD):

Ale w tym przypadku mówimy o takim oprogramowaniu, które służy do podsłuchiwania, mówiąc wprost. Czyli akceptacja ma zabezpieczyć, żeby te informacje nie wyciekły gdzieś na zewnątrz, tak?

Świadek nr 1:

Akredytacja ma potwierdzić, że został osiągnięty odpowiedni poziom bezpieczeństwa, bo sama akredytacja sama w sobie nie zabezpiecza informacji. Proces akredytacji służy potwierdzeniu bezpieczeństwa.

Poseł Paweł Śliz (Polska2050-TD):

Że ten program jest bezpieczny, tak jest?

Świadek nr 1:

System.

Poseł Paweł Śliz (Polska2050-TD):

System jest bezpieczny. Tak jest.

Jakby pan mógł wyjaśnić, w jaki sposób wygląda ta akredytacja, ponieważ mówił pan, że – wiem to też z rozporządzenia prezesa Rady Ministrów z 2011 r. – że proces ten rozpoczyna się na etapie planowania, zaprojektowania takiego systemu, czyli jeszcze tak przed projektowaniem i wdrażaniem. Potem dopiero ma ten etap planowania i szacowania ryzyka. Innymi słowy, czy zanim program zostanie stworzony... Czy to jest tak, że idziemy do sklepu, kupujemy sobie ten program z półki i potem dokonujemy tej akredytacji? I jak w takim kontekście według pana ma się fakt zakupu Pegasusu i niecały miesiąc później rozpoczęcia jego użytkowania?

Świadek nr 1:

Nie bardzo rozumiem pytanie. Prosiłbym o jego doprecyzowanie.

Poseł Paweł Śliz (Polska2050-TD):

To znaczy, kiedy rozpoczyna się akredytacja takiego oprogramowania? Czy może jeszcze inaczej: Czy możemy zakupić po prostu taki system, zwrócić się do ABW o akredytację, czy to musi być na etapie planowania, na etapie projektowania takiego systemu?

Świadek nr 1:

Zgodnie z ustawą, którą pan przytoczył, dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania, a w razie potrzeby konsultuje z ABW albo SKW bieżąco na etapie wdrażania i modyfikuje na etapie eksploatacji. Czyli tak naprawdę etap projektowania, który przechodzi płynnie w etap wdrażania, to jest ten moment, w którym ta dokumentacja tak naprawdę powinna trafić do Agencji Bezpieczeństwa Wewnętrznego lub Służby Kontrwywiadu Wojskowego w zależności od podległości ustawowej, kiedy system powinien... kiedy proces akredytacji systemu powinien zostać rozpoczęty.

Poseł Paweł Śliz (Polska2050-TD):

Proszę pana, wiemy także, że Pegasus był wielokrotnie aktualizowany. Jakby mógł pan powiedzieć, czy są jakieś przepisy, rozporządzenia, które mówią coś na temat tych testów bezpieczeństwa i konieczności uaktualniania dokumentacji po każdej aktualizacji. Czy jest to konieczne?

Świadek nr 1:

Tak, jest to... jest to jeden z wymogów. O ile same testy bezpieczeństwa są wskazane jako po prostu element, który ma być wykonywany w systemach teleinformatycznych, aktualizacja... dokumentacja bezpieczeństwa tak naprawdę całościowo powinna odzwierciedlać stan faktyczny na każdym etapie życia systemu. Proszę pamiętać, że podstawą zmian nie są tak naprawdę ani testy bezpieczeństwa, ani też zmiany w dokumentacji, tylko podstawą dokonywania zmian w systemie jest szacowanie ryzyka i to zawsze jest punkt odniesienia.

Jeżeli zaś chodzi o aktualizacje, to w każdym systemie teleinformatycznym my wymagamy tego, żeby podstawowe elementy tego systemu były aktualizowane. Czy mówimy o systemie operacyjnym, czy o oprogramowaniu antywirusowym, czy o... może urządzeniach sieciowych, zawsze wymagane jest utrzymywanie aktualnych rozwiązań z uwagi na chociażby poprawę lub bezpieczeństwo, ale tu już mówimy w oderwaniu od systemu Pegasus.

Poseł Paweł Śliz (Polska2050-TD):

Z technicznego punktu widzenia czy mogło być tak, że jeżeli CBA wprowadziło jakąś aktualizację do tego systemu, to... czy ten podmiot mógł wprowadzić jakieś dane, jakieś funkcje, o których CBA nie miało żadnej wiedzy, na przykład możliwość wyciągania tych informacji, które system gromadził?

Świadek nr 1:

Nie posiadam takiej wiedzy na temat sposobu aktualizacji tego systemu w CBA. Natomiast biorąc pod uwagę ogólne doniesienia medialne, bo jedynie na tym mogę opierać swoją odpowiedź, nie na informacjach gdzieś tam... strictly z mojej działki, czyli z akredytacji, z bezpieczeństwa informacji niejawnych, trudno byłoby sobie wyobrazić, żeby było to niemożliwe. Proszę pamiętać, że jest to wysoko zaawansowane oprogramowanie stworzone przez, można powiedzieć, specjalistów w swoich działkach i nie mam wiedzy, czy jakiegokolwiek aktualizacje były w 100% bezpieczne, czy były niebezpieczne. Trudno jest wyrokować.

Poseł Paweł Śliz (Polska2050-TD):

I ostatnia taka kwestia. Jakby pan mógł dokonać oceny. Kupujemy system, który nie posiada weryfikacji, który działa na dostarczonym przez wykonawcę sprzęcie. Czy jest na przykład możliwe, że serwery, które zostały zainstalowane, mogły mieć modyfikowane kości pamięci czy inne, jakieś dodatkowe elementy, które umożliwiałyby osobom zewnętrznym dostęp do danych z tego systemu?

Świadek nr 1:

Trudno jest się wypowiedzieć na tak zadane pytanie. Nie mam wiedzy co do tego. Tak jak wspominałem już, nie mam wiedzy co do samej konstrukcji tego systemu ani w jaki sposób jakie elementy były zakupywane, gdzie i przez kogo, i dostarczane przez kogo, natomiast nie wydaje mi się, żeby w tak organizowanym systemie modyfikacja kości pamięci była konieczna do tego, żeby ewentualnie jakieś szkodliwe działania prowadzić.

Poseł Paweł Śliz (Polska2050-TD):

A co byłoby... To w takim razie nie jest potrzebna aż modyfikacja, czyli są jakieś możliwości, żeby prowadzić jakieś szkodliwe działania, żeby wyciągać te informacje z tego systemu?

Świadek nr 1:

Nie mam wiedzy na temat konstrukcji tego systemu. Mówię tu o najwykleszych w świecie działaniach hackerskich, czyli czymś, co spotyka tak naprawdę ludzi na całym świecie codziennie, jeżeli tylko są podłączeni do sieci Internet. Biorąc pod uwagę, że system przeznaczony do inwigilacji urządzeń mobilnych również musiał mieć jakieś wyjście na świat, mówiąc kolokwialnie, nie jestem w stanie w 100% powiedzieć, że w drugą stronę nie działało się nic niebezpiecznego.

Poseł Paweł Śliz (Polska2050-TD):

Proszę pana, jeżeli CBA kupuje już gotowy system, czy jest możliwe przeprowadzenie akredytacji? Ile czasu w takim wypadku taka akredytacja by trwała?

Świadek nr 1:

Na pewno nie dłużej, niż przewidział ustawodawca. Tutaj pytanie rodzi się takie: Kto byłby... Jakie dokumenty potwierdzałyby spełnienie wymagań bezpieczeństwa takiego gotowego systemu i w jaki sposób miałyby się odbywać zarządzanie takim systemem? To jest naprawdę szereg pytań, na które trzeba byłoby indywidualnie odpowiadać w każdym przypadku wykorzystania jakiegokolwiek systemu przeznaczonego do ochrony informacji niejawnych, do przetwarzania informacji niejawnych.

Poseł Paweł Śliz (Polska2050-TD):

Czy z pana wiedzy ABW przeprowadzała akredytacje już zakupionych i gotowych systemów?

Świadek nr 1:

Tak.

Poseł Paweł Śliz (Polska2050-TD):

Czy one się kończyły również negatywną opinią ABW?

Świadek nr 1:

Nie jestem w stanie przywołać w tym momencie takich przypadków.

Poseł Paweł Śliz (Polska2050-TD):

I ostatnie pytanie. Proszę pana, czy program, który nie posiada akredytacji na sprzęcie, który nie posiada certyfikacji, w którym aktualizacje nie są w żaden sposób nadzorowane... czy taki system jest systemem w pełni bezpiecznym?

Świadek nr 1:

To znaczy, tak naprawdę to odpowiedź na to pytanie... to pan już... pan na nie odpowiedział, zadając pytanie. Jeżeli nie mam kontroli nad systemem, to nie mogę powiedzieć, że system jest bezpieczny.

Poseł Paweł Śliz (Polska2050-TD):

Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Teraz pytanie zadaje pani Joanna Kluzik-Rostkowska. Bardzo proszę.

Poseł Joanna Kluzik-Rostkowska (KO):

Witam serdecznie. Proszę świadka, ja chciałam kilka rzeczy uporządkować, bo tu już rozmawiamy godzinę. Z tych informacji, które mamy, z dokumentów, które mamy, m.in. z udostępnionej specyfikacji urządzeń, dla nas to jest czymś oczywistym, że to jest system teleinformatyczny. To jest jakby kwestia pierwsza.

Kwestia druga. Z wiedzy, którą jako Komisja uzyskaliśmy, urządzenia znajdowały się w strefach ochronnych. To jest drugie nasze ustalenie.

Trzecia kwestia, która wyniknęła nam z przesłuchania biegłego Krzysztofa Dyki, to jest kwestia taka, że serwery anonimizujące miały być pod kontrolą CBA. To tak dla uporządkowania tej kwestii.

W związku z tym mam dwa pytania. Tutaj też taka moja prośba. Prosił o to Paweł Śliz, żebyśmy mogli operować w miarę potocznym językiem, żeby również ci, którzy nas słuchają, byli w stanie zrozumieć, jak wygląda ten proces.

Czy pan może bardzo prosto w kilku punktach powiedzieć, jak zgodnie z prawem taka certyfikacja powinna wyglądać, czyli w którym momencie wchodzi ABW i jakie czynności powinny być podjęte, żeby do tej certyfikacji, o której już wiemy, że jej nie było, żeby ona była możliwa?

I pytanie drugie: Kto w sensie personalnym w momencie, kiedy okazuje się, że mamy taki system i on nie zapewnia nam bezpieczeństwa, o czym pan przed chwilą mówił – „nam” w sensie służb, które na tych urządzeniach czy w tym programie będą pracowały – to kto powinien się czuć tą sytuacją zaniepokojony? Czy jest taka przestrzeń do tego, żeby ktoś, kto ponosi odpowiedzialność w momencie, kiedy widzi, że służby pracują na programie bez akredytacji, powinien się poczuć odpowiedzialny za to i ewentualnie przekazać tę wiedzę dalej?

Świadek nr 1:

Pozwolę sobie zacząć odpowiedź od drugiego pytania. Proszę pamiętać, że za ochronę informacji niejawnych w jednostce organizacyjnej, w tym wypadku w CBA czy w jakiegokolwiek innej służbie, odpowiada kierownik jednostki organizacyjnej, czyli w przypadku CBA jest to szef CBA i to on ma ustawowy obowiązek zapewnienia ochrony, w szczególności zorganizowania i zapewnienia funkcjonowania tej ochrony. Jest to wprost wpisane w art. 14 ustawy o ochronie informacji niejawnych.

Jeżeli chodzi o sam proces akredytacji, bo rozumiem, że o to pani pytała, to w momencie, kiedy system jest na etapie projektowania, czyli ktoś sobie wymyślił, że potrzebuje systemu do przetwarzania informacji niejawnych, który będzie miał określone funkcjonalności, ale nie na... nie jest to etap: „zaplanowałem, że chcę zbudować system”, tylko już go projektuję, mam wybrane pomieszczenia, dobrany odpowiedni sprzęt, wszystkie wymogi już zaczynają być pomału spełniane, wiem, jakie zabezpieczenia powinienem wdrożyć, jestem w stanie opisać to dokumentacyjnie, w tym momencie po skompletowaniu takiej dokumentacji, przeprowadzeniu procesu szacowania ryzyka, dokumentacja taka zostaje skierowana do ABW albo SKW w przypadku systemów przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej zostaje to skierowane do odpowiedniej służby celem oceny dokumentacji. I w tym momencie rozpoczyna się proces akredytacji, od oceny, czy rzeczywiście opisane środki bezpieczeństwa są wystarczające, żeby zapewnić ochronę informacjom niejawnym.

Chciałbym tu zwrócić uwagę na jeszcze jedną rzecz à propos tego, czy ten system był bezpiecznie wykorzystywany w CBA, czy nie. Tutaj ja odpowiadałem na pytania dotyczące systemu, który znajduje się całkowicie poza kontrolą służby, czyli jest w jakiś sposób aktualizowany i organizator tego systemu nie ma żadnego wpływu na aktualizacje. I taki system nie będzie bezpieczny. Natomiast w momencie gdyby służby miały możliwość panowania nad aktualizacjami, to tutaj już tak jednoznacznego stwierdzenia wydać bym nie mógł.

Poseł Joanna Kluzik-Rostkowska (KO):

Dziękuję.

Czyli zaczynając od mojego pytania nr 2, nie ma żadnej wątpliwości, że to szef CBA wziął na siebie pełną odpowiedzialność za to, że pracowano na systemie bez akredytacji. My... Bo tutaj pan mówił o systemie, który jest budowany wewnątrz, ale w momencie kiedy jest system, który my kupujemy, to po pierwsze, ten zakup jest poprzedzony konsultacjami, a poza tym... które są niezbędne do tego, żeby wyłonić ostateczny system. Ale z tego, co mówił nasz biegły, Krzysztof Dyki, wynika, że tego typu zaawansowane oprogramowanie rzadko jest budowane w jednym państwie, więc my wiemy, że to był system zakupiony od firmy NSO po uzyskaniu zgody rządu Izraela. Natomiast Krzysztof Dyki mówił o tym, że przy tak skomplikowanych pracach korzysta się z doświadczeń globalnych. I wydaje się, że to jest sytuacja, która jakby potęguje jeszcze ryzyko, że przy takim zebraniu z międzynarodowego rynku poszczególnych części jakby brak szczelności akredytacji może być większy. Więc czy takie rzeczy przy akredytowaniu się bada? To znaczy, jakie czynniki uczestniczyły w przygotowywaniu tego programu? Tutaj mieliśmy do czynienia z sytuacją jednak wyjątkową – z tego, co mówią eksperci – to znaczy, że był tutaj użyty pośrednik. W związku z tym jest pytanie, czy to jest również w zainteresowaniu ABW, wtedy kiedy przyszłoby państwu taki system certyfikować.

Świadek nr 1:

To znaczy, trudno mi jest się do tego ustosunkować, ale z zupełnie innych powodów. Proszę pamiętać, że w dobie dzisiejszej informatyki większość złożonego oprogramowania – ja nie mówię tutaj o oprogramowaniu służącym do realizacji czynności operacyjno-rozpoznawczych czy o jakiegokolwiek inwigilacji – większość oprogramowania, mówię tutaj chociażby o systemie... systemach operacyjnych czy systemach antywirusowych, to już nie jest oprogramowanie, które jest szczelnie zamknięte w jednym biurcu. W bardzo wielu przypadkach kod i oprogramowanie są tworzone na całym świecie tak naprawdę, bo można tu już w tym momencie tak powiedzieć. Proszę pamiętać, że biura wsparcia największych firm nie znajdują się w miejscach, gdzie te firmy

urzędują tak naprawdę, tylko jest szukany inny rynek, więc to są też osoby, które mają jakąś tam wiedzę o funkcjonowaniu czy systemów, czy oprogramowania.

Natomiast jeżeli chodzi o badanie łańcucha dostaw, bo o tym pani tak naprawdę mówiła w momencie, kiedy wspominała pani o tym, że oprogramowanie było tworzone w wielu państwach, był pośrednik, to jest coś określane mianem łańcucha dostaw... bezpieczeństwa łańcucha dostaw i na obecnym etapie w procesie akredytacji nie jest to w 100% badane.

Poseł Joanna Kluzik-Rostkowska (KO):

OK. Czy w takim razie... Proszę mi powiedzieć tak. Czy z punktu widzenia bezpieczeństwa, minimalizowania ryzyka wycieku danych system Pegasus powinien być podlegać akredytacji? Czy poszczególne jego części powinny być przez państwa certyfikowane, tak już patrząc na to historycznie, biorąc pod uwagę te wszystkie ryzyka, o których dzisiaj już wiemy? Bo też z przesłuchania pana Krzysztofa Dyki mamy taką wiedzę, że żeby CBA mogło zainstalować Pegasus na smartfonie osoby, którą się zajmują... że ten system... że to musiało przechodzić przez serwery NSO, w związku z tym to jest taki moment, w którym te dane mogły wyciec, i to w dodatku nie tylko gdzieś tu, wewnątrz Polski, ale tak naprawdę za granicę. Jak pan to ocenia dzisiaj?

Świadek nr 1:

Nie jestem w stanie odnieść się bezpośrednio do systemu Pegasus z uwagi chociażby na to, że pomimo tego, że pewne dane mogłyby lub nie mogły dostać się do podmiotów zagranicznych... Pytanie naprawdę tu jest bardzo kluczowe moim zdaniem: Czy były to dane, które mogłyby stanowić informację niejawną? W jakim zakresie tak naprawdę dało się powiązać z tymi danymi osobę, która była inwigilowana, i służbę, która taką inwigilację zlecała?

Jeżeli chodzi o badanie bezpieczeństwa, czyli certyfikację tak naprawdę poszczególnych elementów – czy oprogramowania, czy poszczególnych urządzeń – to tutaj nie mamy takiego wprost zapisu ustawowego, że te elementy muszą podlegać certyfikacji, żeby można było przetwarzać informacje niejawne. Tutaj jako przykład podam system operacyjny Windows. Nigdy nie był przedmiotem certyfikacji w ABW, a jest wykorzystywany do przetwarzania informacji niejawnych. Czy stanowi to zagrożenie dla bezpieczeństwa informacji?

Poseł Joanna Kluzik-Rostkowska (KO):

Biorąc pod uwagę, że CBA zajmowało się osobami, co do których miało pewne przypuszczenia, podejrzenia, można sobie dosyć łatwo wyobrazić, że wśród wielu informacji pozyskiwanych były też takie, które są wrażliwe, już nie mówiąc o tym, że sam fakt, że interesujemy się tymi osobami, a nie innymi, jest pewnym pokazaniem miękkiego podbrzusza pracy naszych służb. W związku z tym my uważamy, że to ryzyko było bardzo duże.

Z tego, co pan mówi, wynika też jeszcze jedna rzecz, że z punktu widzenia bezpieczeństwa większe bezpieczeństwo zapewniają nam te systemy, które budujemy sami czy które możemy budować sami, bo wtedy ten etap akredytacji się zaczyna wcześniej i jakby jest czymś bardziej oczywistym, a tu już sam zakup od obcego podmiotu przez pośrednika na wejściu powodował większe ryzyko, któremu nie przeciwdziałano chociażby w taki sposób, że nie przeprowadzono tego procesu akredytacji. To moje ostatnie pytanie. Dziękuję.

Świadek nr 1:

Czy mogłaby pani – przepraszam – doprecyzować, jaka jest tak naprawdę treść pytania, dlatego że... Zgadza się z częścią stwierdzeń, które tutaj pani wygłosiła. Natomiast jakiej odpowiedzi by pani oczekiwała ode mnie?

Poseł Joanna Kluzik-Rostkowska (KO):

Czy uważa pan, że w momencie, w którym służby budują system porównywalny czy podobny do Pegasus wewnątrz, to ta szansa, że on będzie bezpieczny, jest większa, ponieważ to podlega akredytacji, czy tam już przyglądamy się temu systemowi w momencie, w którym on jest... w momencie, w którym on jest budowany, a wtedy kiedy kupujemy na zewnątrz, to jakby już na samym wejściu ryzyko, że ten system nie będzie bezpieczny, jest większe? Czy to jest prawda i czy w związku z tym warto tym bardziej zadbać o akredytację?

Świadek nr 1:

To znaczy, powiedziałbym to w ten sposób. Im wcześniej podmiot organizujący system zwróci się do służb z prośbą o konsultacje danych rozwiązań technicznych i danego pomysłu – tak naprawdę swojego – na organizację, przygotowanie systemu teleinformatycznego, tym szanse na to, że system uzyska akredytację w takiej formie, w jakiej został uzgodniony, są wyższe. Tutaj w momencie, gdyby ktoś zakupił system gotowy, skonfigurowany, zostało mu dostarczone pełne gotowe środowisko, to mówimy o zwiększeniu ryzyka, ale nie dla bezpieczeństwa informacji, tylko w momencie zgłoszenia do akredytacji jest większe ryzyko, że będzie szereg uwag czy to do dokumentacji, czy później, w trakcie audytu, które będą powodowały konieczność modyfikacji takiego systemu często już na poziomie jego funkcjonalności.

Posel Joanna Kluzik-Rostkowska (KO):

Dziękuję bardzo za tę odpowiedź.

Ja rozumiem, że panu może nie wypadać o tym powiedzieć, ale tak naprawdę mój wniosek jest taki, że ponieważ to ryzyko było podwyższone, to ktoś uznał, że w ogóle nie warto iść w tę stronę. Dedykuję to szefowi instytucji, który był odpowiedzialny za wprowadzenie do polskiego systemu. Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję, pani posel.

Teraz pytanie zadaje pan poseł Patryk Jaskulski.

Posel Patryk Jaskulski (KO):

Dziękuję bardzo.

Pani przewodnicząca, Wysoka Komisjo, drodzy doradcy, szanowna opinio publiczna, panie świadku, ciężko nie odnieść wrażenia, że zaczął pan trochę swoje zeznania jak u Hitchcocka, stwierdzeniem, że Pegasus nie jest systemem teleinformatycznym. Czy... I za tym idzie fakt, że nie podlegał obowiązkowi akredytacji. Czy jest jakikolwiek dokument oficjalny, wydany przez Agencję Bezpieczeństwa Wewnętrznego, który by potwierdzał taką interpretację prawną?

Świadek nr 1:

Nie mam wiedzy o takim dokumencie, natomiast chciałbym sprostować. Jeżeli zostało odebrane, że Pegasus nie był systemem teleinformatycznym i nie podlegał... i przez to nie podlegał akredytacji, to nie było to intencją mojej wypowiedzi. Tym, co chciałem podkreślić, był fakt, że pojęcie funkcjonujące w przestrzeni medialnej „system Pegasus” niekoniecznie pokrywa się w 100% z definicją ustawową systemu teleinformatycznego, wobec którego przeprowadzany jest proces akredytacji.

Posel Patryk Jaskulski (KO):

Dziękuję za to sprostowanie. Natomiast ciężko nie odnieść wrażenia, że jednak pan tym stwierdzeniem trochę ustawił dalsze losy dyskusji.

Proszę mi odpowiedzieć, kto weryfikuje, jaki system w takim razie musi mieć akredytację, kto ocenia, czy coś jest lub też nie jest takim systemem teleinformatycznym.

Świadek nr 1:

Tak jak powtarzałem to już kilkakrotnie w trakcie tego przesłuchania, kierownik jednostki organizacyjnej odpowiada za ochronę informacji niejawnych przetwarzanych w swojej jednostce, w szczególności za ich organizację i zapewnienie funkcjonowania.

Posel Patryk Jaskulski (KO):

Proszę odpowiedzieć mi na pytanie: Czy ktoś nadzoruje takiego kierownika jednostki konkretnej, inne służby w tym wypadku?

Świadek nr 1:

Jeżeli chodzi o nadzór nad ochroną informacji niejawnych, to proszę pamiętać, że to też jest wpisane i przypisane dwóm służbom – ABW i SKW – w określonym zakresie. Natomiast kierownik jednostki... Czy jest nadzorowany? No, trudno odpowiedzieć na takie pytanie.

Posel Patryk Jaskulski (KO):

Proszę powiedzieć, czy pojawił się formalny wniosek o akredytację systemu wyprodukowanego przez NSO, czyli Pegasusa. Czy CBA się zwróciło z takim pismem do ABW?

Świadek nr 1:

Odpowiem w troszeczkę inny sposób niż dotychczas, gdyż pytanie jest inaczej zadane. Jeżeli chodzi o funkcjonalność poszczególnych systemów, które były akredytowane w ABW, jest to informacja, która jest wpisana tak naprawdę w dokumentację bezpieczeństwa, a te dokumentacje są niejawne, więc niestety nie mogę wprost odpowiedzieć na takie pytanie. Mogę jedynie powtórzyć moją wcześniejszą wypowiedź, bo świadectwa akredytacji są dokumentami jawnymi – nie znam, sprawdzałem historycznie, nie znam przypadku, żeby dla Centralnego Biura Antykorupcyjnego zostało wydane świadectwo akredytacji dla systemu pod nazwą „Pegasus” lub „Jarvis”.

Posel Patryk Jaskulski (KO):

Mam takie pytanie, bo jakby funkcjonalność Pegasusa jest doskonale znana opinii publicznej, także panu. Czy znając tę funkcjonalność, możliwości tak naprawdę pełnej inwigilacji, zgrywania dokumentów z telefonów, pozyskiwania w ten sposób informacji... chciałbym zrozumieć, czy według takiej ogólnej wiedzy, jak działa Pegasus, czy system z taką funkcjonalnością powinien zostać poddany procesowi akredytacji?

Świadek nr 1:

Trudno jest odpowiedzieć na to pytanie z uwagi na pewną złożoność tego typu systemów, o których mówiłem. Oprócz tego, że system, który podlega akredytacji, musi być systemem teleinformatycznym, muszą być w nim przetwarzane informacje niejawne. Informacje niejawne są to informacje, które zostały wyszczególnione, pewne kategorie tych informacji zostały wyszczególnione w ustawie wprost. I tak naprawdę, jeżeli chodzi o tego typu informacje, o których tutaj mówimy, czyli pochodzące gdzieś tam z pracy operacyjnej, to zgodnie z ustawą informacjom niejawnym nadaje się klauzulę, jeżeli ich nieuprawnione ujawnienie utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa.

Pytanie, czy ujawnienie takich informacji, które z samej swojej natury... Przepraszam, może to, co powiem będzie dość dziwnym stwierdzeniem, ale informacja, która została wyciągnięta za pomocą tego typu oprogramowania, nie była w swej naturze informacją niejawną na początku. Mówimy tutaj o treści rozmów, czy poprzez komunikatory, czy rozmów telefonicznych. Sam fakt odbycia takiej rozmowy przez dwie osoby ze swojej natury jest informacją, zgodnie z ustawą, jawną. Ktoś może nie chcieć, żeby to wypłynęło, natomiast sama ta informacja, to, że jedna osoba dzwoniła do drugiej, czy komunikowali się za pomocą komunikatorów jawnych, internetowych, w myśl rozumienia ustawy, jest informacją jawną. Tak naprawdę wykorzystanie tego faktu, połączenie tego, że służba interesuje się takim, a nie innym obywatelem, to, że zbierane są informacje, że ta służba interesuje się w takiej, a nie innej sprawie i że w związku z tym zainteresowaniem zebrano taki, a nie inny materiał, dopiero może być uznane jako informacja niejawna. Natomiast sama treść wiadomości przesyłanych pomiędzy dwoma użytkownikami sieci komórkowej, jawnej, nie może z mocy prawa stanowić informacji niejawnej.

Posel Patryk Jaskulski (KO):

Rozumiem. Natomiast my doskonale wiemy, że za pomocą Pegasusa byli podsłuchiwanie chociażby posłowie, którzy też mają dostęp na przykład do informacji niejawnych, więc nie do końca rozumiem pana interpretację. Ale chciałbym jakby bardziej podpytać dalej o pana opinię. Czy znając jakby dzisiaj pełną wiedzę odnośnie Pegasusa, czy w pana opinii używanie Pegasusa przez Centralne Biuro Antykorupcyjne bez stosownej akredytacji było zgodne z prawem, praktyką?

Świadek nr 1:

Pozwolę sobie w takim razie najpierw uszczegółowić poprzednią wypowiedź. Nieważne, kto był podsłuchiwany i jakie poświadczenia miał – nie miał prawa na prywatnych urządzeniach przetwarzać informacji niejawnych. Od tego są systemy teleinformatyczne, które posiadają akredytację per zasa pozaustawowymi wyłączeniami. I teraz powtórzę

jeszcze raz: jeżeli w 2017 r. oprogramowanie było zainstalowane w systemie teleinformatycznym, którego elementy znajdowały się w strefach ochronnych CBA, w mojej opinii taki system powinien podlegać akredytacji bezpieczeństwa teleinformatycznego, jeżeli informacje w nim przetwarzane wypełniały ustawowe przesłanki do tego, żeby być określone jako „informacja niejawna”.

Posel Patryk Jaskulski (KO):

Dziękuję za odpowiedź na to pytanie.

Jeszcze dwa ostatnie pytania. Czy ABW obserwuje, jakich systemów używają inne służby i czy monitoruje ich bezpieczeństwo, już po tym, jak zaczęli używać Pegasusa, czy ABW zaczęło się tym tematem interesować w jakimkolwiek stopniu?

Pełnomocnik świadka Marcin Bryłka:

Przepraszam, Marcin Bryłka, pełnomocnik.

Miałbym prośbę do pani przewodniczącej o uchylenie tego pytania, bo to już dotyczy zadań ustawowych ABW, a bezpośrednio nie jest związane z przedmiotem przesłuchania.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Przychylam się do wniosku pełnomocnika.

Bardzo proszę o kolejne pytanie albo zmianę formy tego pytania.

Posel Patryk Jaskulski (KO):

Dobrze, to jakby przyjmuję prośbę pana świadka. Mam pytanie, czy inne służby, czyli czy też ABW stosowało i używało Pegasusa.

Świadek nr 1:

Nie mam wiedzy w tym temacie.

Posel Patryk Jaskulski (KO):

A czy ABW podejmowało jakiekolwiek działania, by zniwelować skutki wycieku informacji, które mogły mieć miejsce za pośrednictwem Pegasusa? Mam tu na myśli informacje, które publicznie...

Pełnomocnik świadka Marcin Bryłka:

Pani przewodnicząca, Marcin Bryłka, pełnomocnik.

Jeszcze raz zgłaszam wniosek o uchylenie tego pytania z tego samego powodu, o którym mówiłem wcześniej.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Tak, panie pośle, ja uchylam to pytanie.

Posel Patryk Jaskulski (KO):

Dobrze. Nie mam więcej pytań w takim razie.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Przechodzimy do kolejnej tury zadawania pytań.

Proszę powiedzieć, na jaki okres wydawana jest akredytacja, jeżeli ona jest wykonywana.

Świadek nr 1:

Akredytacja bezpieczeństwa zgodnie z ustawą wydawana jest na okres maksymalnie 5 lat.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. Mieliśmy tutaj pewną dyskusję na temat przetwarzania informacji niejawnych. Na czym polega w takim razie, jakby pan miał określić, przetwarzanie informacji niejawnych w systemach teleinformatycznych?

Świadek nr 1:

Zgodnie... Tak naprawdę znowu powołam się na definicję ustawową, gdzie przetwarzaniem informacji zostały określone tak naprawdę wszelkie czynności wykonywane na informacjach niejawnych.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli chodzi mi o to, żeby po prostu nasi słuchacze zrozumieli i mogli sobie sami odpowiedzieć na to pytanie, mając wiedzę, która dzisiaj jest powszechnie już dostępna. Czy system Pegasus według tej definicji przetwarzał informacje niejawne w systemie teleinformatycznym?

Świadek nr 1:

To znaczy tak. To, na co próbowałem zwrócić uwagę, odpowiadając na jedno z poprzednich pytań, to że zostały wyciągnięte informacje wrażliwe i sama treść tych informacji nie stanowi tak naprawdę informacji niejawnej, gdyż każda z tych osób, zgodnie z zasadami, zakładam, nigdy nie przetwarzały i nie przetwarzała na pewno informacji niejawnych za pomocą swoich prywatnych urządzeń elektronicznych. To, czy można było powiązać działania wobec konkretnej osoby ze służbą, w jakikolwiek sposób, to zaczyna stanowić informację niejawną.

Jeżeli chodzi o samo przetwarzanie informacji, to biorąc pod uwagę bardzo szeroką definicję ustawową, nie ma absolutnie wątpliwości, że wykorzystując oprogramowanie, usługę, czy też kolokwialnie mówiąc system typu Pegasus, mamy do czynienia z przetwarzaniem informacji.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

W takim razie mamy jedną przesłankę spełnioną – przetwarzanie informacji niejawnych. Druga przesłanka, która wymagana jest do przeprowadzenia akredytacji, to czy system znajduje się w sferze ochronnej, tak? Czy system Pegasus posiadając operatorów, którzy podejmują pierwsze działania infekujące, czy znajdujące się w danych pomieszczeniach komputery plus serwery znajdujące się w sferze ochronnej... czy to było również przesłanką, jedną z kolejnych przesłanek do tego, żeby taką akredytację wykonać?

Świadek nr 1:

To znaczy, tutaj przesłanki należałoby tak naprawdę, pani przewodnicząca, odwrócić. Jeżeli mamy do czynienia z systemem teleinformatycznym, w którym przetwarzane są informacje niejawne, ale z ustawowym systemem teleinformatycznym, informacje... przetwarzanie informacji niejawnych, również zgodnie z ustawową definicją, jeżeli to jest wypełnione, to taki system teleinformatyczny podlega akredytacji, chyba że służy – i tutaj dopiero wchodzi to „chyba że” – tak naprawdę dopiero jest art. 51. Więc tak naprawdę nie jest to tak, że jeżeli jest w strefie i przetwarza, i coś tam musi podlegać, tylko system teleinformatyczny, w którym przetwarzane są informacje niejawne, musi być akredytowany, chyba że zostaną wypełnione przesłanki z art. 51.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli...

Świadek nr 1:

Tutaj, jeżeli mówimy o tym o systemie, w którym... którego elementy miałyby znajdować się w strefie ochronnej, w którym byłyby przetwarzane informacje niejawne, to taki system, zgodnie z literą prawa obowiązującą w 2017 r. powinien podlegać akredytacji bezpieczeństwa teleinformatycznego.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli, jeżeli system Pegasus przetwarzał informacje niejawne i znajdował się w sferze ochronnej w 2017 r., podlegał akredytacji?

Świadek nr 1:

Jeżeli były... w systemie takim teleinformatycznym były przetwarzane informacje niejawne i znajdował się w strefach ochronnych, powinien podlegać akredytacji. Tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Rozumiem, że mamy już jasność co do odpowiedzialności. To znaczy, szef Centralnego Biura Antykorupcyjnego miał ustawowy obowiązek zadbać o ochronę informacji niejawnej.

Świadek nr 1:

Tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli to decyzja szefa CBA, która dopuściła do użytkowania system Pegasus... to on bierze na siebie odpowiedzialność niewykonania akredytacji czy niezwrócenia się do Agencji Bezpieczeństwa Wewnętrznego o wykonanie takiego sprawdzenia.

Świadek nr 1:

Nie zdam decyzji dopuszczającej taki system do działania, więc nie mogę tutaj tego przypisać w żaden sposób komukolwiek. Natomiast tutaj niekoniecznie decyduje o takim lub innym działaniu, bo to nie o tym mówimy, że to kierownik jednostki organizacyjnej oświadczyć musi za każdym razem wszystkie działania związane z przetwarzaniem informacji niejawnych podpisywać, tylko mówimy o jego niezbywalnej odpowiedzialności za...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

...ochronę tych informacji.

Świadek nr 1:

...ochronę tych informacji.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze. Czyli jeżeli w toku zgromadzonego przez nas materiału dowodowego, w toku prowadzonych dalej postępowań w przyszłości okaże się, że system Pegasus powinien posiadać akredytację, a jej nie powinien, to odpowiedzialność za to ponosi szef jednostki, która nabyła ten system, czyli szef Centralnego Biura Antykorupcyjnego, jeżeli chodzi o kwestie dotyczące ochrony informacji niejawnych.

Świadek nr 1:

Bezpośrednio, tak. To jest odpowiedzialność niezbywalna. Proszę tylko jeszcze pamiętać, że ustawa mówi też o pełnomocniku ochrony do spraw ochrony informacji... pełnomocnika ochrony informacji niejawnych zwanego pełnomocnikiem...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Oczywiście, ale bez...

Świadek nr 1:

...który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych w jednostce. To jest osoba podległa bezpośrednio szefowi CBA.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

OK, czyli podwładny niższego szczebla, pod szefem danej jednostki, czyli szefem CBA, to jeszcze pełnomocnik do spraw ochrony informacji niejawnych. Proszę powiedzieć w takim razie, czy wyłączenie z akredytacji bezpieczeństwa teleinformatycznego, określone w art. 51 ustawy o ochronie informacji niejawnych miało w pana... według pana wiedzy zastosowanie do Pegasusu?

Świadek nr 1:

Nie mam wiedzy na ten temat, tak jak mówię, nie mam potwierdzonych informacji, nie mam żadnych dokumentów na temat tego, w jaki sposób był zrobiony podział na informacje, które były przetwarzane w systemie.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobrze.

Świadek nr 1:

Proszę pamiętać, że cały czas mówimy o systemie, który w taki czy inny sposób miał styk z systemami jawnymi. Musiał mieć.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Musiał mieć i wiemy również, wszystko na to wskazuje, że był aktualizowany zdalnie, co znaczy, że była możliwość ingerencji w system, który znajdował się w sferach bezpieczeństwa, z zewnątrz, a nawet z zewnątrz naszego kraju.

Ale proszę powiedzieć, czy nowelizacja w 2022 r. art. 51 ustawy o ochronie informacji niejawnych w tym zakresie, że systemy wyłączone z obowiązku akredytacji opisano, zmieniając zapis, że dokładano tam... że te części systemu teleinformatycznego znajdują się poza strefami... Jak pan interpretuje te zmiany? Co ona miała... czy ona miała jakieś przełożenie na system Pegasus? Czy zmieniła się... zmieniłyby się obowiązki w stosunku do dysponenta tego systemu Pegasus – 2017 r. kontra 2022 r. po wprowadzeniu zmian w ustawie o obronie Ojczyzny?

Świadek nr 1:

Po wprowadzeniu zmian znacznie rozszerzył się katalog systemów, który mógł zostać wyłączony z obowiązku akredytacji. Bo tutaj tak naprawdę w oryginalnym brzmieniu tego przepisu mówimy o systemach, które w całości znajdowały się poza strefami ochronnymi, więc możemy sobie wyobrazić jakieś bardzo wyspecjalizowane systemy teleinformatyczne, czyli tak naprawdę jakieś tam narzędzia wykorzystywane do realizacji czynności operacyjno-rozpoznawczych lub procesowych, które mogły zahaczać lub w pełni wypełniać definicję ustawową systemu teleinformatycznego. Przepis był wykorzystywany po to, żeby funkcjonariusze, którzy z takich narzędzi korzystali, nie musieli się zastanawiać nad tym, czy działają zgodnie z literą prawa, czy to prawo przekraczają. Tutaj mówimy o systemach, które... których serwerownia mogłaby być zlokalizowana w służbie, w strefie ochronnej. Po czym... już naprawdę kuriozalny przypadek bym podał, po czym ściśle tajne informacje, o ile byłyby operacyjno-rozpoznawcze lub dochodzeniowo-śledcze, funkcjonariusz mógłby przetwarzać w salonie.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dobra. Czyli stosując taki prosty język, żeby też wszyscy nas zrozumieli. Czy jeżeli okaże się w toku naszego tutaj dochodzenia, śledztwa prowadzonego przez Komisję Śledczą, ale także dalszych postępowań, że system Pegasus musiał mieć akredytację, to czy błędem w takim razie, który jakby nakładał obowiązek w 2017 r., obowiązek akredytacji, było umieszczenie tego systemu w sferach... strefie tej ochronnej?

Świadek nr 1:

To znaczy, ciężko powiedzieć...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Jeżeli on znajdowałby się... Jeżeli taki system, który spełnia te wszystkie przesłanki, o których chwilę temu rozmawialiśmy, byłby poza strefami ochronnymi, czy on wtedy po prostu nie musiał być... podlegać akredytacji?

Świadek nr 1:

Wtedy najprawdopodobniej ta dyskusja mogłaby być zakończona bardzo szybko, jeżeli wiedzielibyśmy o tym, że żaden element nigdy nie znajdował się w strefie i cały art. 51 byłby wypełniony, wtedy oczywiście nie byłoby nawet o czym dyskutować. Natomiast stwierdzenie, że było błędem w kontekście możliwości wyłączenia z akredytacji, tak, w kontekście bezpieczeństwa informacji niejawnych, przetworzonych, jednak strefy ochronne zostały wprowadzone po to, aby zapewnić bezpieczeństwo fizyczne informacjom niejawnym.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Czyli rozumiem, że mówi pan, że jeżeli taki system znajdował się w sferze ochronnej, ten system Pegasus powinien mieć akredytację, wypełniając wszystkie przesłanki.

Świadek nr 1:

To, co powtarzałem od początku, jeżeli którakolwiek z przesłanek byłaby niewypełniona w 100%, jeżeli chodzi o art. 51, system przetwarzający informacje niejawne powinien być akredytowany.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję panu bardzo.

Czy CBA w takim razie mogło... Nie. Czy... Inne pytanie. Czy gdyby pan był szefem Centralnego Biura Antykorupcyjnego i z dzisiaj posiadanych informacji na temat tego systemu miałby pan możliwość... dysponowałby pan takim systemem, czy poddałby pan go akredytacji w roku 2017, w obecnym... w tamtym stanie prawnym?

Świadek nr 1:

Nie mam wystarczającej wiedzy, żeby jednoznacznie określić, czy powinien taki system podlegać, czy też nie, szczególnie pod kątem funkcjonalnym, to, co próbowałem wielokrotnie powiedzieć. Ja rozumiem, że kwestia wyciągania informacji, które każdy z nas chciałby zachować dla siebie, jest kwestią wrażliwą. Nie jestem w stanie w 100% powiedzieć, czy to była informacja niejawna i na jaki... w jaki sposób było prowadzone powiązanie służby, czy też operatora, czy konkretnego urządzenia, na którym pracowali funkcjonariusze CBA, z zapytaniem kierowanym do sieci anonimizującej.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję. Ja bym jednak mając dzisiejszą wiedzę, taką akredytację przeprowadziła. Bardzo dziękuję.

Kto... Na tę chwilę dziękuję. Tutaj pan przewodniczący Bosacki zgłasza się do kolejnych pytań. Bardzo proszę.

Poseł Marcin Bosacki (KO):

Dziękuję bardzo, pani przewodnicząca.

Ja bym chciał, żeby to bardzo mocno wybrzmiało, bo pan tę tezę wygłosił, odpowiadając na pytania kilkorga z nas. Moim zdaniem to jest najważniejszy wniosek, który już mamy po dzisiejszym przesłuchaniu funkcjonariusza ABW, czyli jeśli w 2017 r. mieliśmy do czynienia z systemem teleinformatycznym, który po drugie, przetwarzał informacje niejawne i, po trzecie, którego część funkcjonowała w strefie ochronnej, to potrzebna była akredytacja. Wiemy również z dzisiejszego przesłuchania, że ABW takiej akredytacji nie wydało. Również według wiedzy świadka nic nie wiadomo mu o tym, żeby CBA się o taką akredytację zwracało. Uważam, że to już samo w sobie jest absolutnie przełomowym odkryciem dzisiejszego przesłuchania i będziemy dalej badać tę sprawę, dlaczego ówczesne szefostwo CBA takich kroków nie podjęło, mimo że było do tego zobowiązane.

Natomiast do pana mam pytanie następujące: Czy na etapie wstępnym, w którym wiemy, że CBA pytało o inne służby, o udział w tym systemie, zanim jeszcze go kupiło, pytało również, czy pana wiedza tego dotyczy, ABW lub inne służby, co do bezpieczeństwa tego systemu... Ja mówię... Nie chodzi mi o pytanie o certyfikację, tylko na tym etapie wstępnym pozyskiwania systemu Pegasus w 2017 r., czy CBA zgłaszało się do ABW lub innych służb z oceną bezpieczeństwa tego systemu.

Świadek nr 1:

Nie mam wiedzy w tym zakresie.

Poseł Marcin Bosacki (KO):

A czy gdyby tak było, powinien pan mieć taką wiedzę?

Świadek nr 1:

Trudno mi się odnieść w ogóle do tak postawionego pytania. Naprawdę... Mówimy o sytuacji, która nie miała miejsca. Proszę pamiętać, że...

Poseł Marcin Bosacki (KO):

Nie, nie, to jest co innego.

Świadek nr 1:

Takie pytanie... Znaczy... nie mam wiedzy...

Poseł Marcin Bosacki (KO):

Czy pan opowiada, że pan nie ma wiedzy, czy też, że ta sytuacja nie miała miejsca? To są dwie różne odpowiedzi, przepraszam.

Świadek nr 1:

Mówimy... Zgodnie z moją... Ja nie mam wiedzy. Przepraszam, źle się wyraziłem. Nie mam wiedzy w tym zakresie. Mówimy tu z mojego punktu widzenia o hipotetycznej sytuacji – gdyby służba o coś zapytała, byłoby to zapytanie niejawne. I to tak naprawdę nie jest... nie byłoby moją decyzją, czy ja miałbym dostęp do takiej informacji, czy nie. Proszę pamiętać, że jedną z podstawowych zasad, jeżeli chodzi o przetwarzanie

informacji niejawnych, jest to, że pomimo poświadczeń bezpieczeństwa, dostęp do informacji uzyskuje się tylko w zakresie niezbędnym do wypełnienia swoich obowiązków.

Posel Marcin Bosacki (KO):

Jasne, zrozumiałem.

Chciałem pociągnąć te pytania zadane przez panią przewodniczącą o zmianę przepisów w 2022 r., ponieważ ona, myślę, że nie tylko dla mnie, wśród członków Komisji jest wysoce podejrzana i wygląda, jakby ktoś ex post chciał przynajmniej stwarzać pozory legalizacji tego, co zrobiono w roku 2017. W tych zmianach są dwie rzeczy dla oceny sytuacji, którą my badamy, czyli zakupu i użycia Pegasusa, absolutnie kluczowe. Jedna to jest ta, o której pan już wspomniał, czyli że akredytacji nie podlegają nie tylko systemy, których całość jest poza systemem, tylko systemy, których nawet część jest poza systemem, co zwiększa pulę tych systemów, które nie muszą uzyskać akredytacji.

Drugą zmianą było to, że w tej... że do tej ustawy dodano nazwy czterech służb, które teoretycznie... których systemy teoretycznie nie muszą być... nie muszą uzyskać... nie muszą być przez państwa, czyli przez ABW badane i nie muszą uzyskać certyfikacji ABW. I tam wymieniono tylko kontrwywiad i wywiad cywilny i wojskowy, czyli ABW, AW, SKW i SWW. Czy panu jest wiadome, dlaczego w tym zbiorze nie zawarto innych służb, które mogą prowadzić działania operacyjne potocznie nazywane inwigilacją, w tym CBA?

Świadek nr 1:

To znaczy, chciałbym rozbić tę odpowiedź na dwie części. Nie mam wiedzy, dlaczego zostały wprowadzane jakiekolwiek zmiany, jeżeli chodzi o ustawę o ochronie informacji niejawnych w 2022 r., ustawę o obronie Ojczyzny. Natomiast pragnę zwrócić uwagę na to, że jeżeli chodzi o art. 51 ust. 2, o którym pan wspomina, to nie zostały tam dodane cztery służby, a dwie. Oryginalne brzmienie ust. 2 tego artykułu dotyczyło wywiadu cywilnego i wywiadu wojskowego dla systemów poza granicami Rzeczypospolitej oraz wydzielonych stanowisk służących do odbioru takich informacji. Tak że tutaj dwie służby wywiadowcze zostały rozszerzone o dwie służby kontrwywiadowcze.

Posel Marcin Bosacki (KO):

Rozumiem. Moje pytania zmierzają do pytania, na które bardzo proszę, żeby pan zgodnie ze swoją wiedzą precyzyjnie odpowiedział. Czy po zmianie ustawy z 2011 r. w roku 2022 system – ja nie chcę mówić system Pegasus, bo pan nie chce oceniać systemu Pegasus, bo nie ma pan na jego temat wiedzy – ale czy system, który potrzebowałby akredytacji w roku 2017, po zmianach w roku 2022 można interpretować, że już tej akredytacji by nie potrzebował?

Świadek nr 1:

Hipotetycznie zakładając, że mamy system, którego elementy, powiedzmy, nazwijmy to serwery plus część operatorska systemu stoi... znajduje się w strefie ochronnej danego podmiotu...

Posel Marcin Bosacki (KO):

Tak.

Świadek nr 1:

...w 2017 r. niezależnie od jego wykorzystania, od jego przeznaczenia i tego, kto go organizował, taki system musi podlegać akredytacji. Nie mówimy tutaj o systemach wywiadowczych, czyli art. 51 ust. 2.

Posel Marcin Bosacki (KO):

Tak.

Świadek nr 1:

To zostawiamy gdzieś tam obok, bo to są stacje... to były stacje służące do odbioru informacji z zagranicy, one nie podlegały akredytacji. Mówimy o systemach używanych przez inne podmioty niż wywiad wojskowy, wywiad cywilny, czyli art. 51 ust. 1, który został zmieniony. Mam stanowisko w strefie ochronnej, system podlega akredytacji. To nie ulega wątpliwości, nie ulega dyskusji. Jeżeli są przetwarzane informacje niejawne, jeżeli

pozostałe przesłanki systemu są spełnione, to zwolnienia z obowiązku akredytacji... tutaj zwolnienie nie ma miejsca. W 2022 roku...

Poseł Marcin Bosacki (KO):

W 2017 r., tak? W 2017 r., bo chcę, żeby to zabrzmiało. Pan mówi... opisuje sytuację na rok 2017.

Świadek nr 1:

Na rok 2017. W tym momencie mamy zmianę w ustawie rok 2022. Mam taki sam system, którego elementy znajdują się w moich strefach ochronnych, ale części tego systemu są wyniesione poza te strefy – taki system już nie musi podlegać akredytacji, o ile jest wykorzystywany przez uprawnione podmioty bezpośrednio do pozyskiwania i przekazywania informacji, czyli wypełnienie pozostałej części tego artykułu. Oczywiście nie jest to interfejs u operatora, o którym mowa w prawie telekomunikacyjnym.

Poseł Marcin Bosacki (KO):

Bardzo panu dziękuję.

System, który pan opisuje abstrakcyjnie, my możemy przypisać absolutnie systemowi Pegasus i możemy stwierdzić, że system Pegasus, który z całą pewnością w 2017 r., ponieważ był systemem teleinformatycznym, ponieważ przetwarzał informacje niejawne i ponieważ jego część znajdowała się w strefach ochronnych, musiał podlegać akredytacji. Natomiast po zmianach z 2022 r., co perwersyjne w mojej ocenie, dokonanych w ustawie o obronie Ojczyzny, którą, jak wszyscy pamiętamy, jednogłośnie przyjmowaliśmy zaraz po agresji pełnoskalowej Rosji na Ukrainę, już takiej akredytacji nie musiał podlegać.

Ostatnie zdanie, pani przewodnicząca.

Panowie Wąsik i Kamiński na swoich konferencjach prasowych bronili się, twierdząc, że system Pegasus był zakupiony i funkcjonował legalnie, dlatego że funkcjonował w strefach ochronnych. Jest dokładnie odwrotnie. Funkcjonował on w strefach ochronnych nielegalnie, bo w 2017 r. aż do 2022 r., każdy system, który funkcjonował w strefach ochronnych, musiał podlegać akredytacji. Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Szanowni państwo, tutaj widzimy, że doszło do próby zatuszowania tak naprawdę tego braku akredytacji i niewykonania go w 2017 r.

Bardzo proszę, Witold Zembaczyński teraz zadaje pytania.

Poseł Witold Zembaczyński (KO):

Wielce szanowna pani przewodnicząca, Wysoka Komisjo, szanowni państwo doradcy, proszę świadka, proszę powiedzieć, z jakich etapów w warunkach stanu prawnego 2017 r. składał się proces akredytacji, konkretnie z systemu kontroli operacyjnej.

Świadek nr 1:

Niezależnie od przeznaczenia systemu, etapy akredytacji są nieodmiennie te same – ocena dokumentacji bezpieczeństwa i w zależności od wyniku wydanie świadectwa lub odmowa wydania świadectwa.

Poseł Witold Zembaczyński (KO):

Rozumiem. Tutaj słowem klucz jest słowo „bezpieczeństwo”. W opinii Komisji tego bezpieczeństwa użytkowania systemu brakowało, dlatego dochodzimy do coraz bardziej istotnych szczegółów. Zatem jakie są warunki otrzymania świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego, służącego do kontroli systemu operacyjnego, konkretnie systemu Pegasus, którego część znajduje się po stronie CBA, w tej przestrzeni zamkniętej, a pozostałe odnogi tego systemu znajdują się poza granicami kraju?

Świadek nr 1:

Nie jestem w stanie odpowiedzieć na to pytanie. Tak jak mówiłem, nie mam wiedzy, pełnej wiedzy odnośnie zarówno konstrukcji, jak i zasad wykorzystywania systemu teleinformatycznego, w którym... którego elementem lub częścią składową miałby być

Pegasus lub samego systemu pod nazwą „Pegasus”, bo to są też, proszę zwrócić uwagę, dwie różne rzeczy.

Poseł Witold Zembaczyński (KO):

Proszę świadka, czy to jest normalne, że największa, najbardziej okrzepła, najbardziej zdolna i doświadczona służba specjalna – polski kontrwywiad cywilny – nie ma wiedzy o tym, że CBA dysponuje systemem do kontroli operacyjnej, pozyskując mniej lub bardziej wątpliwe i wiarygodne materiały w procesie karnym, materiały dowodowe przez ten system? Czy to jest normalna konstrukcja państwa?

Świadek nr 1:

Pani przewodnicząca, wnoszę o uchylenie tego pytania, bo ono dotyczy oceny, a nie faktów.

Poseł Witold Zembaczyński (KO):

Dobrze, to ja zmodyfikuję to pytanie, proszę świadka. Czy zatem Agencja Bezpieczeństwa Wewnętrznego jest instytucją powołaną do posiadania wiedzy o użytkowaniu systemów operacyjnych przez cywilne służby specjalne?

Świadek nr 1:

Pani przewodnicząca, również wnoszę o uchylenie tego pytania, bo to jest poza zakresem wiedzy świadka i poza okolicznościami, na które tu zostałem wezwany.

Poseł Witold Zembaczyński (KO):

Ja powtórzę pytanie. Czy Agencja Bezpieczeństwa Wewnętrznego jest powołana do tego, żeby posiadać wiedzę na temat użytkowanych systemów kontroli operacyjnych przez inne cywilne służby specjalne?

Świadek nr 1:

Odpowiadając na to pytanie, odesłałbym do... niestety, ale do art. 5 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, którego nie jestem w stanie przytoczyć w tym momencie z pamięci. Zostały tam opisane wszystkie zadania, zarówno ABW, jak i AW. Art. 5 to jest ABW, art. 6 to jest AW.

Poseł Witold Zembaczyński (KO):

Proszę powiedzieć, jaką klauzulę mają systemy do przetwarzania informacji niejawnych stosowane do kontroli operacyjnej.

Świadek nr 1:

Pani przewodnicząca, również wnoszę o uchylenie tego pytania, bo już tutaj dotykamy kwestii informacji niejawnych...

Poseł Witold Zembaczyński (KO):

Ale czy to jest klauzula...

Świadek nr 1:

...i ewentualnie o tych okolicznościach moglibyśmy porozmawiać na posiedzeniu niejawnym.

Poseł Witold Zembaczyński (KO):

Ja zmodyfikuję to pytanie.

Przewodniczący poseł Marcin Bosacki (KO):

Ja w tej chwili... Przepraszam, ja w tej chwili prowadzę pod nieobecność chwilową pani przewodniczącej i zgadzam się tym razem ze świadkiem – uchylam to pytanie. Proszę sformułować je inaczej.

Poseł Witold Zembaczyński (KO):

Proszę, panie przewodniczący, powiedzieć, co pan uchyla z tego pytania, żeby mógł zmodyfikować pytanie.

Przewodniczący poseł Marcin Bosacki (KO):

Uchylam pytanie w całości dotyczące tego, w jaki sposób świadek ma ocenić, co certyfikuje, a co nie certyfikuje ABW.

Poseł Witold Zembaczyński (KO):

To ja może powtórzę pytanie. Jaką klauzulę posiadają systemy do przetwarzania informacji niejawnych stosowane do kontroli operacyjnej? Czy to jest klauzula „tajne”, „ściśle tajne”, „poufne” czy „zastrzeżone”?

Świadek nr 1:

Proszę mi wybaczyć, ale nie jest to informacja jawna. Jeżeli chodzi o to, w jaki sposób są chronione, jakie informacje są przetwarzane, to już w tym momencie tak naprawdę niestety zaczynamy wkraczać...

Poseł Witold Zembaczyński (KO):

Chodzi mi o...

Świadek nr 1:

...na bardzo niebezpieczny grunt art. 35 i 39 bodajże ustawy o ABW i AW, czyli rzeczy, o których niezależnie od formy przesłuchania nie mógłbym się wypowiadać.

Poseł Witold Zembaczyński (KO):

Proszę świadka, czy to...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Przepraszam.

Poseł Witold Zembaczyński (KO):

Bardzo proszę, pani przewodnicząca.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Przepraszam, chciałabym powiedzieć, że od godziny 15.00 mamy zarezerwowane pomieszczenia do dalszego prowadzenia Komisji w trybie niejawnym. Tak że bardzo proszę, zadamy to pytanie w trybie niejawnym.

Poseł Witold Zembaczyński (KO):

Precyzując...

Dziękuję, pani przewodnicząca.

Precyzując to pytanie, proszę zatem powiedzieć, czy systemy do przetwarzania informacji niejawnych stosowane w kontroli operacyjnej są jawne.

Świadek nr 1:

Pani przewodnicząca, również proszę o uchylenie tego pytania.

Poseł Witold Zembaczyński (KO):

Dobrze, przejdźmy dalej. Jest tutaj świadek niechętny do tego, żeby odpowiedzieć, w związku z tym będziemy kontynuowali.

Proszę powiedzieć, jakie podstawowe wymagania bezpieczeństwa powinien spełnić Pegasus, aby mógł być legalnie i bezpiecznie wykorzystywany w Polsce. Podstawowe wymagania bezpieczeństwa – jakie one są?

Świadek nr 1:

Nie znam konstrukcji tego systemu, nie jestem w stanie się wypowiedzieć, w jaki sposób miałyby być zabezpieczone.

Poseł Witold Zembaczyński (KO):

Czy zatem...

Świadek nr 1:

Poza tym, jeżeli, nie mogę... Przepraszam, dokończę tylko wypowiedź.

Poseł Witold Zembaczyński (KO):

Proszę.

Świadek nr 1:

Nie mogę również wypowiadać się per analogia z uwagi na to, że jakkolwiek opis systemów teleinformatycznych przetwarzających informacje niejawne, w zakresie zarówno funkcjonalności, jak i wdrożonych zabezpieczeń, sam w sobie stanowi

informację niejawną, tak że tak jak pani przewodnicząca zaznaczyła, na godzinę 15.00 jest wyznaczona godzina posiedzenia niejawnego. Wtedy mógłbym troszeczkę szerzej się wypowiedzieć.

Poseł Witold Zembaczyński (KO):

Dobrze, proszę świadka. Rozumiem, w porządku.

Proszę zatem powiedzieć, czy według świadka wiedzy CBA lub inne służby przedstawiały lub konsultowały z ABW procedury bezpiecznej eksploatacji Pegasusa już w trakcie samego użytkowania.

Świadek nr 1:

Nic mi na ten temat nie wiadomo, żeby taka sytuacja miała miejsce.

Poseł Witold Zembaczyński (KO):

Dziękuję za odpowiedź.

Czy CBA prosiło ABW o sprawdzenie elektromagnetycznej emisji ujawniającej, która pochodzi z elementów systemu przetwarzającego niejawne informacje, jakim był Pegasus?

Świadek nr 1:

Nie mam wiedzy w tym temacie.

Poseł Witold Zembaczyński (KO):

Rozporządzenie prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego mówi o konieczności ustalania zasad tworzenia i przechowywania kopii zapasowych. Czy system Pegasus według świadka wiedzy tworzył takie kopie i gdzie one mogły być standardowo przechowywane?

Świadek nr 1:

Naprawdę zwracam się z prośbą o uchylenie tego pytania. Tutaj wkraczamy naprawdę na grunt informacji, które same w sobie są niejawne.

Poseł Witold Zembaczyński (KO):

Dobrze, to ja rozwinę...

Świadek nr 1:

Nie chciałbym się wypowiadać, nie mam wiedzy na temat konstrukcji samego systemu, co podkreślałem nieraz.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Świadek nr 1:

Natomiast jeżeli chodzi o wypowiedzenie się ogólnie, gdzie takie coś mogłoby lub nie mogłoby być przechowywane, jest to informacja niejawna dedykowana konkretnym systemom.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Ja oczywiście uchylam to pytanie.

Panie pośle, bardzo proszę o zadawanie pytań, które możemy zadać podczas jawnego posiedzenia. O godzinie 15.00 przejdziemy w tryb niejawny, wtedy będzie pan miał możliwość zadawania pytań wkraczających w sferę informacji niejawnych.

Poseł Witold Zembaczyński (KO):

Dobrze, to może pani pozwoli... Ja absolutnie w tę sferę nie wkraczam, natomiast chcę rozwinąć to pytanie. Chodzi mi konkretnie o fakt pęknięcia płyty z zapisem podsłuchów Krzysztofa Brejzy. Czy świadkowi jest cokolwiek wiadomo na temat tego wydarzenia?

Świadek nr 1:

Nie mam wiedzy w tym temacie, poza doniesieniami medialnymi.

Poseł Witold Zembaczyński (KO):

Czy często zdarzają się takie przypadki? Jaka powinna być reakcja służb w takim zdarzeniu?

Świadek nr 1:

Nie mam wiedzy w tym temacie. Poza tym, przepraszam, ale wykracza to poza samą akredytację, bo tu już mówimy tak naprawdę o jakimś niewłaściwym...

Poseł Witold Zembaczyński (KO):

Nie, to...

Świadek nr 1:

...o incydentach związanych z niewłaściwą obsługą nośnika danych. Z całym szacunkiem...

Poseł Witold Zembaczyński (KO):

Proszę świadka, z uwagi na to, że trudno jest świadkowi nawet określić, kto był de facto administratorem systemu Pegasus, musimy zadać pytania, które przyczynią się do tego, żeby wszystkie wątpliwości wokół jego użycia Komisja rozwiązała.

Dlatego proszę jeszcze odpowiedzieć, czy i kiedy ABW zostało poinformowane przez CBA o zaprzestaniu eksploatacji systemu Pegasus.

Świadek nr 1:

Nie mam wiedzy w tym zakresie.

Poseł Witold Zembaczyński (KO):

A kto powinien posiadać dokumentację bezpieczeństwa teleinformatycznego Pegasus w swoim archiwum – czy to jest CBA, czy to jest ABW?

Świadek nr 1:

Tak jak wielokrotnie zaznaczałem, nie mam wiedzy, aby system pod nazwą Pegasus był akredytowany w ABW czy też dokumentacja takiego systemu pod taką nazwą, bo to... Świadcstwo nie zostało takie wydane nigdy. To mogę powiedzieć na posiedzeniu jawnym. Czy funkcjonalności odnośnie samych procesów akredytacji systemów wprowadzonych na rzecz różnych służb nie są informacją jawną, nie mogę się tutaj wypowiadać. Wypowiem się po godzinie 15.00. Z przyjemnością odpowiem na to pytanie.

Natomiast proszę pamiętać, że zawsze jako zasadę należy traktować to, że jeżeli dokumentacja, jakakolwiek, dotycząca eksploatacji systemu jawnego czy niejawnego jest wytwarzana, to osoba, która... znaczy osoba, instytucja, która użytkuje taki system, powinna mieć w swoich zasobach taką dokumentację. Czy w archiwalnych? Nie wiem. Nie mam wiedzy merytorycznej, żeby się na to wypowiedzieć.

Poseł Witold Zembaczyński (KO):

Bardzo dziękuję za tę odpowiedź.

Proszę powiedzieć zatem, czy badania akredytujące obejmują sprawdzenie integralności danych, tj. zabezpieczenie przed możliwością modyfikacji danych pozyskanych przez dany system na urządzeniu końcowym użytkownika.

Świadek nr 1:

Nie jest to elementem składowym procesu akredytacji... (*niezrozumiale*) Natomiast proszę pamiętać, że proces dostosowywany jest do konkretnych funkcjonalności konkretnego systemu, czy to badań i oceny bezpieczeństwa w ramach certyfikacji, czy też akredytacji bezpieczeństwa teleinformatycznego.

Poseł Witold Zembaczyński (KO):

Rozumiem. Proszę powiedzieć... Czyli elementem akredytacji nie jest zupełnie kwestia waloru dowodowego pozyskanych materiałów, tylko funkcjonalność systemu.

Świadek nr 1:

Nie do końca w ten sposób, dlatego że... nie, jeżeli chodzi o samo pytanie dotyczące później waloru dowodowego, nie, nie jest to przedmiotem akredytacji. Jeżeli zaś chodzi o samą funkcjonalność, to też nie mogę się niestety z tym stwierdzeniem zgodzić w 100%. Przedmiotem akredytacji jest ocena bezpieczeństwa systemu teleinformatycznego, czyli na ile informacje niejawne przetwarzane w systemie są bezpieczne. Tutaj mówimy również o zachowaniu... zarówno o zachowaniu poufności, integralności i dostępności.

Są to trzy podstawowe atrybuty, które każdy system teleinformatyczny musi zapewniać. Jeżeli nawiązuje pan do tego, czy w trakcie akredytacji była badana możliwość, czy materiał można zmodyfikować, to teraz należałoby zadać pytanie, czy miałyby być to jedna z funkcjonalności systemu.

Posel Witold Zembaczyński (KO):

Rozumiem. Czyli nie jest wykluczone, że system może mieć funkcjonalność służącą modyfikacji pozyskanych treści z elektronicznych urządzeń końcowych, czego w tym wypadku świadek nie jest w stanie rozstrzygnąć z uwagi na brak akredytacji tego konkretnego systemu. Czy tak mam to rozumieć?

Świadek nr 1:

Nie jestem w stanie tego rozstrzygnąć z uwagi na brak szczegółowej wiedzy dotyczącej zarówno strony technicznej, jak i proceduralnej wykorzystania tego typu rozwiązań w innych służbach.

Posel Witold Zembaczyński (KO):

Proszę świadka, proszę zatem powiedzieć, gdzie Wysoka Komisja może znaleźć odpowiedzi na te wszystkie pytania, na które świadek nie ma wiedzy bądź tej wiedzy nie posiada Agencja Bezpieczeństwa Wewnętrznego.

Świadek nr 1:

Zwróciłbym się na pewno na miejscu szanownej Komisji do organizatora, czyli do jednostki, która wykorzystywała takie oprogramowanie czy też, kolokwialnie mówiąc, system, czyli do funkcjonariuszy CBA, którzy byli bezpośrednio zaangażowani w obsługę tego.

Posel Witold Zembaczyński (KO):

Bardzo dziękuję świadkowi.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Teraz pytanie zadaje poseł Paweł Śliz. Bardzo proszę, panie przewodniczący.

Posel Paweł Śliz (Polska2050-TD):

Ja bym chciał wrócić do tej odpowiedzialności kierownika, o której pan mówił, jednostki. Na pytania pani przewodniczącej mówił pan, że tam zgodnie również z rozporządzeniem odpowiedzialnym jest także pełnomocnik do spraw informacji niejawnych. A czy na tych poszczególnych etapach nie ma też inspektora bezpieczeństwa teleinformatycznego?

Świadek nr 1:

Powiem to w ten sposób. Art. 14 ustawy mówi wprost: kierownik jednostki organizacyjnej odpowiada za ochronę, w szczególności za organizowanie i zapewnienie funkcjonowania ochrony, ust. 2 art. 14: kierownikowi jednostki organizacyjnej bezpośrednio podlega przez niego... zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych. I tu mówimy całościowo o ochronie informacji niejawnych przetwarzanych w instytucji, w jednostce organizacyjnej, czyli w jakiejś instytucji, w firmie, gdziekolwiek.

Natomiast nawiązując do inspektora czy, idąc dalej, administratora systemu teleinformatycznego, są to osoby wyznaczone do konkretnych systemów teleinformatycznych przetwarzających informacje niejawne – systemów, które podlegają co do zasady akredytacji. Więc czy tutaj można byłoby przypisywać... znaczy nie posługujemy się takim pojęciem jak inspektor bezpieczeństwa teleinformatycznego w jednostce organizacyjnej, tylko jest to inspektor bezpieczeństwa teleinformatycznego wyznaczony do konkretnego systemu.

Posel Paweł Śliz (Polska2050-TD):

I jaka byłaby odpowiedzialność w wypadku CBA takiego wyznaczonego inspektora?

Świadek nr 1:

Nie mam wiedzy, czy taki wyznaczony inspektor w tym przypadku w ogóle był, czy nie.

Posel Paweł Śliz (Polska2050-TD):

A jeżeli był?

Świadek nr 1:

Inspektor odpowiada tak naprawdę za wykorzystywanie akredytowanego systemu, podkreślam, akredytowanego systemu, zgodnie z jego dokumentacją. Czyli odpowiada za przestrzeganie przepisów jak najbardziej. Odpowiada za funkcjonalność, przestrzeganie zasad i wymagań bezpieczeństwa. Ale tu mówimy o systemie, który ma dokumentację, do której można się odnieść. Mówimy o systemie, który ma tutaj akredytację. Ja nie posiadam wiedzy na temat taki, żeby system, o który państwo pytają, taką akredytację posiadał.

Poseł Paweł Śliz (Polska2050-TD):

Wiemy, że nie. Dobrze.

Ja bym wrócił jeszcze do jednej kwestii, o którą pytałem w pierwszej turze. Jakby pan mógł odpowiedzieć, czy dla takiego gotowego systemu możliwe jest dokonanie jego analizy i potem dokonania akredytacji bez dostępu do kodów źródłowych tego oprogramowania i jakiejś kompletnej dokumentacji.

Świadek nr 1:

W wielu przypadkach, jeżeli chodzi o akredytację, nie mamy dostępu do kodów źródłowych aplikacji wykorzystywanych w konkretnych systemach teleinformatycznych. Mimo to takie systemy podlegają akredytacji. Proszę mi szczerze wierzyć, ja bardzo spłaszczę tutaj i podam przykład kompletnie niezwiązany ze sprawą, ale do kodów źródłowych pakietu Microsoft Office również nie miałem nigdy dostępu, a mimo to akredytowane są systemy, które wykorzystują pakiet Microsoft Office.

Poseł Paweł Śliz (Polska2050-TD):

Rozumiem.

Jeszcze jakby pan mógł opisać program... proces wycofywania takiego systemu z użycia. Jak wygląda taka procedura, tak krok po kroku, który uzyskał akredytację...

Świadek nr 1:

Procedura wycofania jest uzależniona od konkretnego systemu. Nie ma generycznej procedury wycofania, bo jest bardzo wiele różnych scenariuszy. Wszystko można sprowadzić tak naprawdę do bezpiecznego wycofania urządzeń z obiegu, w tym ich w pewnym momencie zniszczeniu w sposób bezpieczny. Jeżeli chodzi o dane wytworzone w takim systemie, to tak naprawdę w zależności od tego, jakie jest przeznaczenie takiego systemu teleinformatycznego, jakie są zasady ochrony czy wymogi na dostępność takich informacji, które były w nim przetwarzane... Bo tu mówimy często o zasobach archiwalnych, bo możemy porównać z jednej strony maszynę do pisania z bardzo skomplikowanym systemem bazodanowym. Będą zupełnie różne przypadki i sposób wycofania. Przepraszam za kolokwializm. Przez maszynę do pisania rozumiem oczywiście system teleinformatyczny, który służy wyłącznie do wytworzenia dokumentu w pakiecie biurowym i wydrukowania go na drukarce.

Poseł Paweł Śliz (Polska2050-TD):

Ja dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję.

Teraz pytanie zadaje pani poseł Joanna Kluzik-Rostkowska. Ma pytania jeszcze?

Poseł Joanna Kluzik-Rostkowska (KO):

Tak.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Proszę.

Poseł Joanna Kluzik-Rostkowska (KO):

Jeśli mogę jeszcze krótko. Bo tak, jedną kwestią jest akredytacja, bo ustawa mówi również o badaniu i certyfikacji urządzeń i aplikacji. Czy w związku z tym CBA powinno było się zwrócić do państwa o to, żeby certyfikować poszczególne urządzenia czy aplikacje?

Świadek nr 1:

To znaczy tak, z jednej strony, jeżeli mówimy o certyfikacji ochrony elektromagnetycznej, tak jak mówiłem, nie mam wiedzy, gdzie znajdowały się te elementy, ewentualnie takiego systemu czy elementy systemu, w którym byłoby wykorzystywane takie oprogramowanie, bo tak jak podkreślam, dla mnie to są dwie różne kwestie. W zależności od wyznaczonej sprzętowej strefy ochrony elektromagnetycznej w najlepszym możliwym przypadku można byłoby wykorzystywać sprzęt, który nie podlegał sam w sobie badaniom. Proszę pamiętać, że na tym etapie nawet gdybyśmy jako ABW przebadali urządzenia, które później byłyby wykorzystywane w takim systemie, niekoniecznie pod kątem ulotu elektromagnetycznego, niekoniecznie mielibyśmy 100% wiedzy, dlatego że potrzebujemy urządzeń, które będą skonfigurowane w sposób docelowy, ale nie wywołujemy na nich docelowego oprogramowania, jeżeli jest jakieś specyficzne, tylko sprawdzamy, czy takie urządzenie nie powoduje emisji ujawniającej, której poziom przekraczałby określone normy. Te normy również są informacją wysoko klauzulowaną, więc nie chciałbym dalej w to wchodzić.

Jeżeli zaś chodzi o ust. 3 art. 50, mówiącego o certyfikacji, czyli certyfikacji urządzenia lub narzędzia służącego do realizacji zabezpieczenia teleinformatycznego, to prowadzona taka certyfikacja jest na wniosek zainteresowanego podmiotu, co jest wprost w ustawie wpisane jako jedyny przypadek. Nie jest mi znany powód, dlaczego tylko w tym przypadku, bo tak naprawdę dobór środków, urządzeń i narzędzi jest tak naprawdę odpowiedzialnością jednostki organizującej system i tutaj my nie jesteśmy w stanie wymusić pewnych rzeczy. Oczywiście mamy w pewien sposób gdzieś tam skodyfikowany dobór środków ochrony elektromagnetycznej, w sensie strefa i urządzenie, tak żeby nie dało się wyczytać nic z emisji ujawniającej poza strefami kontrolowanymi przez jednostki organizacyjne. Urządzenia kryptograficzne zgodnie z rozporządzeniem muszą być certyfikowane, jeżeli służą do zapewnienia poufności informacji niejawnych przekazywanych w formie transmisji poza strefy ochronne.

Natomiast jeżeli chodzi o środki realizujące zabezpieczenie teleinformatyczne, to tutaj nigdzie w aktach wykonawczych czy w dalszej części ustawy nie ma bezpośredniego wskazania, że taki środek musiałby być certyfikowany. Jeżeli, tak jak mówię, chodzi o same komputery, czyli niekoniecznie nawet z oprogramowaniem, na dobrą sprawę, docelowym, bo to nie jest nigdzie ujęte w certyfikacie, jeżeli ma być system operacyjny zainstalowany na dysku twardym, to to jest minimalne wymaganie, żeby taki system się uruchamiał w celu zbadania komputera jako takiego na ulot elektromagnetyczny i wydanie mu certyfikatu. Natomiast to nie świadczy o funkcjonalności takiego sprzętu w żaden sposób.

Jeżeli chodzi o kryptografię, to tutaj ciężko, znając o tyle, o ile z doniesień medialnych funkcjonalności systemu... może inaczej, funkcjonalności Pegasusa, bo nie chciałbym nazywać tego systemem z uwagi na bliskość językową pojęć pomiędzy systemem teleinformatycznym, tym ustawowym pojęciem, a tym funkcjonującym w przestrzeni medialnym pojęciem „system Pegasus”, to tutaj nie znam takiego aspektu, który wymagałby użycia certyfikowanej kryptografii.

Natomiast jeżeli chodzi o bezpieczeństwo teleinformatyczne, tak jak mówiłem, nie ma jednoznacznego wskazania, że musiałoby być to badane.

Posel Joanna Kluzik-Rostkowska (KO):

Dziękuję bardzo.

Ja mam taką prośbę, gdyby pan mógł troszeczkę wolniej mówić, bo tu się rozpędzamy trochę w tym wszystkim.

Ale rozumiem, że żeby finalnie uzyskać akredytację, to te urządzenia powinny być certyfikowane, tak? Jednak była transmisja danych, informacji poza te strefy ochronne, więc to, rozumiem... jakby akredytację powinna poprzedzić certyfikacja.

Chciałam zapytać o to również, czy jakiegolwiek obowiązki są nakładane na właściciela systemu, czyli na NSO, albo na pośrednika, czyli na firmę Matic. Czy któryś z tych dwóch podmiotów miał obowiązek, powinien był również się do państwa zgłosić, żeby uzyskać potwierdzenie bezpieczeństwa korzystania z tego oprogramowania?

Świadek nr 1:

Obowiązek dotyczy jedynie tak naprawdę jednostki organizującej system, wykorzystującej jakiekolwiek narzędzia. Tutaj, jeżeli chodzi o... (*niezrozumiałe*) mojej, może przydługiej, wypowiedzi dotyczącej certyfikacji, nie do końca mogę się zgodzić ze stwierdzeniem, że skoro informacje były transmitowane poza strefę, to musiała być stosowana certyfikowana kryptografia, ale to nie... dalsze uzasadnienie niestety nie może paść tutaj na posiedzeniu jawnym.

Poseł Joanna Kluzik-Rostkowska (KO):

Dobrze, wrócimy do tego, jeśli można.

Jeszcze dwa krótkie pytania. Rozmawiamy tutaj o zagrożeniach, które istnieją same w sobie, a są potęgowane wtedy, kiedy tej akredytacji nie ma. Skupialiśmy się na tym, że informacje pozyskiwane dzięki temu oprogramowaniu mogą wyciekać i dostawać się w niepowołane ręce. Ale czy istnieją jeszcze inne zagrożenia? W momencie, kiedy możemy zakładać, że Pegasus mógł ingerować w treści, w dane, czy taki system... czy jakby pozyskiwane tą drogą informacje mogą być uznawane jako prawdziwe i pewne?

Świadek nr 1:

Nie jestem niestety biegłym, abym mógł się wypowiadać na temat możliwości dalszego wykorzystania, bo rozumiem, że tak naprawdę to jest clou tego pytania, dalszego wykorzystania informacji zebranych z wykorzystaniem tego typu narzędzi, tego narzędzia czy jakiegokolwiek innego analogicznego gdzieś tam w postępowaniach przed sądem czy jakichkolwiek innych.

Poseł Joanna Kluzik-Rostkowska (KO):

Dziękuję. Tutaj uprzedził pan moje pytanie ostatnie, czyli czym innym, rozumiem, jest wykorzystanie pozyskanych informacji jako takiej wiedzy operacyjnej, a później ewentualnie możliwość wykorzystania tej wiedzy w sensie procesowym, natomiast... I tutaj dziękuję.

Natomiast moje wcześniejsze pytanie dotyczyło tego, że ponieważ skupiamy się tutaj głównie na wycieku ewentualnych danych i dotarciu tych danych do podmiotów, do osób niepożądanych, to jakie jeszcze inne zagrożenia może mieć system, który nie podlega akredytacji? Ja tutaj zasugerowałam, że możliwość ingerencji w treści czy możliwość zainfekowania tych smartfonów może być takim niebezpieczeństwem. Czy jeszcze jakieś inne są?

Świadek nr 1:

To znaczy, teraz chciałabym się odnieść jak najlepiej do tego pytania i... Może w ten sposób. Jeżeli mówi pani o ingerencji w urządzenia końcowe, mobilne urządzenia końcowe, czyli popularnie smartfony, z wykorzystaniem tego systemu i zmianę treści tam się znajdujących, to należałoby sobie odpowiedzieć na pytanie, czy taki miałby być cel i docelowa zakładana funkcjonalność, którą operator miałby mieć dostępną, tego czy jakiegokolwiek innego systemu, nie przypinając się do tej konkretnej sprawy. Możemy sobie wyobrazić, że służba potrzebowałaby takiego narzędzia. Czy wtedy byłoby ono niebezpieczne dla służby? Czy byłoby może zbyt szeroko idące i nie do wykorzystania zgodnie z polskim prawodawstwem? To są dwie różne kwestie.

Natomiast proszę pamiętać, że każda informacja, jeżeli mówimy w informatyce o bezpieczeństwie informacji, to mówimy o kilku atrybutach. Mówimy o poufności, czyli tak jak jest ustawowa definicja, bo proszę zwrócić uwagę, że dla każdej z klauzul ustawowa definicja informacji niejawnych rozpoczyna się tak naprawdę od stwierdzenia, że informacjom niejawnym nadaje się klauzulę „tajne”, „ściśle tajne”, „poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje... i tutaj w zależności od tego, jak wysoką szkodę. Ale cały czas mówimy o nieuprawnionym ujawnieniu i dlatego cała tutaj dyskusja skupia się na atrybucie poufności, czyli pewności tego, że dostęp do informacji będą miały wyłącznie osoby uprawnione.

W informatyce szeroko rozumianej mówimy dodatkowo o atrybucie dostępności, czyli o tym, że osoba uprawniona ma mieć możliwość dostępu do informacji na żądanie w określonym czasie. Nie musi być dostęp natychmiastowy, natomiast jest zawsze jakiś zakładany czas takiego dostępu i ten czas musi być zrealizowany. Wtedy mówimy o spełnieniu bezpieczeństwa pod kątem dostępności.

Dalej mamy integralność, to znaczy, że żadna informacja nie zostanie zmodyfikowana w sposób niekontrolowany przez uprawnioną do tego osobę. Bo jeżeli ja wytworzę informację niejawną w systemie teleinformatycznym, po czym będę musiał ją zmodyfikować, bo po prostu taka jest potrzeba – nie mówię, że zmienić opis całkowicie, natomiast może dodać coś do tej informacji, jestem osobą uprawnioną do jej modyfikacji – to mam do tego prawo. Ale nie powinno być sytuacji takiej, że ja dzisiaj wytworzę informację niejawną, odnoszę się do niej jutro, a tam są inne informacje, niż ja wpisałem, prawda?

Dodatkowo mamy jeszcze niezaprzeczalność i uwierzytelnienie, jeżeli chodzi o informacje, czyli tak naprawdę już potwierdzenie personalnie osoby wytworzającej to, że ja się nie mogę wyprzeć tego, że taki dany dokument wytworzyłem. To jest niezaprzeczalność. Uwierzytelnienie to tak naprawdę potwierdzenie moich praw dostępu do pewnych zasobów systemu.

Posel Joanna Kluzik-Rostkowska (KO):

Dziękuję bardzo. Właśnie mi chodziło o taką... Nie chodziło mi o sytuację, w której służby świadomie chcą zmienić coś na urządzeniu końcowym, bo rozumiem, że od tego są procedury i przepisy, ale właśnie o taką sytuację, że biorąc pod uwagę, że żeby CBA mogło korzystać z dostępu do smartfona konkretnej osoby, to to musiało przechodzić przez urządzenia NSO. I zakładając złą wolę właściciela systemu, tam się mogły znaleźć na samym końcu informacje, które wcale nie były w intencji... czy też zapisy, tak, które wcale nie były intencją pracownika służb, nad którym, jak rozumiem, przy takim procesie jest po prostu kontrola jakaś. Tak że o to mi chodziło. Dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję, pani posel.

W tej chwili pytanie zada poseł Patryk Jaskulski. Bardzo proszę.

Posel Patryk Jaskulski (KO):

Dziękuję bardzo, pani przewodnicząca, Wysoka Komisjo.

Panie świadku, przytoczył pan art. 5 ustawy o Agencji Bezpieczeństwa Wewnętrznego. Jeden z pierwszych ustępów mówi o tym, że do zadań ABW należy rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny. Pegasus ma status cyberbroni i eksperci, którzy znają się doskonale na tym oprogramowaniu, wielokrotnie alarmowali o tym, że część informacji może być elementem przecieku, może dostać się w ręce obcych służb specjalnych. Ciężko nie odnieść wrażenia, mam takie wrażenie, że ABW trochę jak takie przysłowiowe trzy mądre małpki się zachowuje w przypadku stosowania i używania Pegasusa przez CBA. Uduje, że nic nie widzi, udaje, że nic nie słyszy i niewiele chce też na tą okoliczność powiedzieć.

Chciałbym wrócić w swoich pytaniach do wątku użytkowania systemu bez akredytacji i ewentualnych procedur na taką okoliczność. Może mi powiedzieć, panie świadku, co dzieje się z systemem, który jest używany bez wymaganej akredytacji, pomijając jakby odpowiedzialność kierownika jednostki. Czy tak po prostu można go dalej sobie stosować, jeżeli państwo wiedzą, że jest jakiś system, który nie ma akredytacji, a jest stosowany przez jakąś ze służb, czy po prostu ta służba może dalej to użytkować? Czy mają państwo jakieś procedury na taką okoliczność?

Świadek nr 1:

Ale to... Proszę o doprecyzowanie pytania. Ja rozumiem, że tutaj nie chodzi o systemy wykorzystywane zgodnie z obowiązującym na chwilę projektowania, wdrażania czy eksploatacji stanem prawnym, jeżeli mówimy o art. 51, czy... tylko o systemy, które są wykorzystane niezgodnie z ustawą i zostaną przedstawione... i służba konkretna będzie posiadała dowody na wykorzystanie i przetwarzanie informacji niejawnych w takim systemie.

Posel Patryk Jaskulski (KO):

Jeszcze raz powtórzę w takim razie pytanie. Jeżeli państwo wiedzą, jeżeli Agencja Bezpieczeństwa Wewnętrznego wie o tym, że jakaś służba korzysta z systemu, który nie ma akredytacji, a może być źródłem jakby przecieku, zagrożenia dla państwa, czy są jakieś procedury na taką okoliczność?

Świadek nr 1:

Czy służba korzysta z tego systemu zgodnie czy niezgodnie z literą prawa?

Poseł Patryk Jaskulski (KO):

Jeżeli służba korzysta bez akredytacji, czyli, jak rozumiem, niezgodnie z literą prawa.

Świadek nr 1:

Mówiliśmy tutaj dzisiaj o tym, że dopuszcza się wykorzystanie systemów, które nie posiadają akredytacji i są w nich przetwarzane informacje niejawne, wyłączenie z trybu art. 51. Rozumiem, że nie chodzi zupełnie o te systemy. Mówimy o systemie niezgodnym z prawem, po prostu mówiąc kolokwialnie, złapaliśmy za rękę urzędnika, który na laptopie internetowym wytwarza informacje o klauzuli ściśle tajne.

Poseł Patryk Jaskulski (KO):

Dokładnie o taką sytuację... ma miejsce, a w zasadzie to cały czas wracamy do interpretacji tego, czy Pegasus powinien podlegać akredytacji, ale rozumiem, że tutaj jest rozbieżność, jeżeli chodzi o podejście.

Proszę mi powiedzieć, co się dzieje, jeżeli kierownik źle oceni, czy coś jest... czy nie jest podlegający akredytacji, to... czy jeżeli okaże się, że ten system jest stosowany bez takiej akredytacji, to czy tylko kierownik ponosi odpowiedzialność za to i czy dalej ten system może być użytkowany, czy państwo jakoś zabezpieczają...

Świadek nr 1:

Co do zasady taki system, jeżeli... To są przypadki zbyt indywidualne, żebym mógł jakąś generyczną zasadę podać. Jeżeli w trakcie kontroli, które są prowadzone zgodnie... są prowadzone w ciągu roku, jeżeli chodzi o ochronę informacji niejawnych, wychodzą jakiegokolwiek nieprawidłowości, to zawsze wygląda to tak, że informacje o tych nieprawidłowościach są gdzieś tam zbierane, są przedstawiane itd. Natomiast ciężko mi jest się wypowiadać, co tak naprawdę od strony przepisów już spoza ustawy o ochronie informacji niejawnych, bo tu mówimy o kodeksach, nie jestem w stanie wskazać przepisów, które taki kierownik jednostki musiałby... mógłby podpadać.

Poseł Patryk Jaskulski (KO):

Dobrze, dziękuję bardzo.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

Czy jeszcze ktoś z członków Komisji ma pytanie do świadka? Nie widzę. Czy świadek chciałby jeszcze zabrać głos i dodać coś w tej części jawnej dzisiejszego przesłuchania?

Świadek nr 1:

Nie, dziękuję.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Dziękuję.

W takim razie po sporządzeniu protokołu przesłuchania poinformujemy pana o terminie, w którym będzie pan mógł go podpisać. Dziękuję świadkowi za przybycie na tę część jawną. Informuję, że część niejawna przesłuchania odbędzie się o godzinie 15.00 w wyznaczonym pomieszczeniu. Bardzo świadkowi dziękuję.

My teraz przystępujemy do rozpatrzenia punktu drugiego dzisiejszego porządku dziennego, to znaczy przyjęcie wniosków dowodowych. Pozwólcie państwo, że w tej chwili przedstawię dwa kolejne wnioski dowodowe.

Pierwszy wniosek dowodowy zostanie skierowany do komendanta głównego Policji, do pana nadinspektora Marka Boronia i działając z upoważnienia Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celno-skarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od dnia 16 listopada 2015 r. do dnia 20 listopada 2023 r., w związku z treścią pisma komendanta z 18 lipca 2024 r. wnoszę o wyrażenie zgody przez komendanta na przedstawienie

odpisów wszystkich dokumentów, zarówno jawnych, poświadczonych za zgodność z oryginalnymi... z oryginałami, jak i niejawnymi, a także udzielenie pisemnych wyjaśnień w zakresie wskazanym w treści wniosku tutejszej Komisji z dnia 20 lutego 2024 r. Tutaj w załączeniu przedstawiamy wniosek, który składany był do ministra administracji i spraw wewnętrznych, a zakres kompetencji i możliwość udzielenia odpowiedzi spoczywa na komendancie głównym Policji.

Czy ktoś... Kto jest za przedstawionym przeze mnie wnioskiem? Kto jest przeciw? Kto się wstrzymał? Dziękuję.

Sekretarz Komisji Mariusz Pawełczyk:

5 głosów za.

Posel Tomasz Treła (Lewica):

Ja zagłosowałem.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Nie, tu jest 6 członków...

Posel Joanna Kluzik-Rostkowska (KO):

Ja nie wiem, mi się wydaje, że ja...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Coś mamy, rozumiem, z urzędzeniem.

Rozumiem, pani poseł, jest pani...

Posel Joanna Kluzik-Rostkowska (KO):

Tak, ja nawet spełniałam obowiązek. Wcisnęłam, co trzeba. Ale nie wiem, czy to zostało...

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Ale czy jest pani za, rozumiem?

Posel Joanna Kluzik-Rostkowska (KO):

Tak. Oczywiście.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Tak? Dobrze. Dziękuję. 6 głosów za, 0 wstrzymujących się, 0 przeciw.

Kolejny wniosek, który jako Komisja będziemy składać w związku z kolejnymi informacjami dotyczącymi systemu Hermes, a niepełną odpowiedzią z Ministerstwa Sprawiedliwości, do której również skierowaliśmy pismo o potraktowanie w pełni naszego wniosku składanego i prezentowanego przez pana posła Witolda Zembaczyńskiego. Składamy również wniosek do prokuratora Jaromira Rybczaka, prokuratora regionalnego w Rzeszowie. Komisja sejmowa zgodnie z uchwałą z dnia 19 lutego 2024 r. wystąpiła do Prokuratury Krajowej o przekazanie w trybie art. 14 ust. 1 ustawy z dnia 21 stycznia 1999 r. o sejmowej komisji śledczej pisemnych wyjaśnień w zakresie zakupu w 2021 r. za kwotę ok. 15 mln zł oprogramowania analitycznego Hermes. 21 maja 2024 r. kierownik zespołu śledczego nr 3 poinformował Komisję Śledczą, że w Prokuraturze Regionalnej w Rzeszowie za sygnaturą akt 2008-3.Ds.6.2024 prowadzone jest śledztwo w sprawie trybu dokonania zakupu przez Prokuraturę Krajową, zasadności nabycia, a także naruszenia zasad użytkowania systemu automatyzacji procesu gromadzenia informacji z otwartych źródeł OSINT, to jest o czyn z art. 231 § 1 Kodeksu karnego i art. 296 § 1 Kodeksu karnego i art. 296 § 3 Kodeksu karnego w związku z art. 11 § 2 Kodeksu karnego. Wobec powyższego na podstawie załączonej uchwały Komisji wnoszę o przesłanie w zdigitalizowanej formie całości materiału, w tym niejawnego, z prowadzonego śledztwa. Dokumenty, o które się zwracamy, mają istotne znaczenie dla realizacji przez Komisję zadania postawionego jej przez Sejm Rzeczypospolitej Polskiej, a określonego w uchwale Sejmu powołującej Komisję.

Bardzo proszę. Kto jest za zaprezentowanym przeze mnie wnioskiem? Bardzo proszę o podpisy. Kto jest przeciw? Kto się wstrzymał? Dziękuję.

6 głosów za, 0 głosów przeciwnych, 0 wstrzymujących się. Tym samym wniosek uzyskał większość.

Dobrze, szanowni państwo, tutaj się zgłasza pan przewodniczący Bosacki. Bardzo proszę, panie pośle.

Posel Marcin Bosacki (KO):

Pani przewodnicząca, szanowni... szanowne koleżanki i koledzy, wydaje mi się, że dzisiaj powinniśmy również zastanowić się, po tym w mojej ocenie absolutnie wstrząsającym zeznaniu funkcjonariusza ABW, nad rozpoczęciem prac nad skierowaniem wniosku o możliwości popełnienia przestępstwa przez ówczesnego, czyli w 2017 r., szefa Centralnego Biura Antykorupcyjnego, pana Ernesta Bejdy. Przynajmniej z art. 231 Kodeksu karnego, czyli niedopełnienia obowiązków przez niego, poprzez zaniechanie zainicjowania procesu akredytacji systemu Pegasus, a następnie akceptowanie korzystania z niego bez akredytacji, ale być może również z art. 265 – naruszenie tajemnicy państwowej poprzez wykorzystywanie systemu niegwarantującego bezpieczeństwa danych... Ja nie chcę, żebyśmy dzisiaj podejmowali jakąkolwiek uchwałę w tej sprawie, tylko chciałbym, żebyśmy wewnętrznie w Komisji podjęli decyzję o rozpoczęciu tego typu prac, które by sprawdziły, czy mamy już wystarczające dowody na tego typu zawiadomienie.

Przewodnicząca poseł Magdalena Sroka (PSL-TD):

Bardzo dziękuję, panie przewodniczący. Niewątpliwie po dzisiejszym posiedzeniu Komisji w mojej ocenie możemy stwierdzić, że system Pegasus, który był dopuszczony do użytkowania przez polskie służby, powinien posiadać akredytację. Był systemem, który w 2017 r. znajdował się w strefie ochronnej, był systemem teleinformatycznym, który przetwarzał informacje niejawne, a są to przesłanki, z których jasno wynikało, że w 2017 r., podejmując decyzję o jego zakupie, należało wykonać akredytację. Później w 2022 r. oczywiście próbowano rozmydlić ten temat, tak żeby już nie można było mówić, że systemy takie jak Pegasus jest w stosunku do nich wymagana akredytacja przez to, że jedna z części systemów znajduje się poza strefami ochronnymi. Szanowni państwo, próbowano w mojej ocenie zatuszować w 2022 r. błąd, który popełniono w 2017 r. I tutaj niewątpliwie można wysunąć wnioski, że mogło dojść do popełnienia przestępstwa przez ówczesnego szefa Centralnego Biura Antykorupcyjnego. Ja tutaj się przychylam absolutnie, panie pośle, że kończąc badanie kwestii akredytacji, ale myślę, że powinniśmy również poczekać na przesłuchanie pana Bejdy, bo to będzie również kluczowy dowód, który posłuży nam już niedługo, mam nadzieję, do sporządzenia takiego zawiadomienia o popełnieniu przestępstwa...

Szanowni państwo, wobec wyczerpania porządku dziennego dzisiejszego posiedzenia Komisji zamykam posiedzenie Komisji. Dziękuję państwu bardzo.