SENAT
RZECZYPOSPOLITEJ
POLSKIEJ

KOMISJA NADZWYCZAJNA DO SPRAW WYJAŚNIENIA
PRZYPADKÓW NIELEGALNEJ INWIGILACJI, ICH WPŁYWU
NA PROCES WYBORCZY W RZECZYPOSPOLITEJ POLSKIEJ
ORAZ REFORMY SŁUŻB SPECJALNYCH

Warszawa, 18 maja 2023 r.

BPS.DKS. KNI. 0331.3.2023

Pan
Mateusz Morawiecki
Prezes Rady Ministrów

Szanowny Panie Premierze,

pod koniec kwietnia br. Stały Komitet Rady Ministrów przyjął projekt ustawy zmieniającej m.in. ustawę o krajowym systemie cyberbezpieczeństwa. Nowelizacja ta dotyczy wielu kwestii, poddaje m. in. regulacji zmiany w zakresie obowiązków przedsiębiorców komunikacji elektronicznej, przepisów dotyczących krajowego systemu certyfikacji cyberbezpieczeństwa, uznania dostawcy za dostawcę wysokiego ryzyka czy też wprowadza przepisy dotyczące operatora strategicznej sieci bezpieczeństwa (OSSB) oraz rozdysponowania częstotliwości w paśmie 700 MHz.

Rządowe prace nad wskazanym projektem ustawy trwają już blisko 3 lata. Budzi on wiele wątpliwości, szczególnie w zakresie przepisów umożliwiających uznanie poszczególnych dostawców oprogramowania za tzw. dostawców wysokiego ryzyka i tym samym uniemożliwienie wykorzystania produkowanego przez nich sprzętu czy oprogramowania do budowy polskiej infrastruktury telekomunikacyjnej czy też ich używania przez instytucje i służby państwowe.

Innymi słowy, według proponowanych rozwiązań, sprzęt i oprogramowanie dostawcy uznanego za dostawcę wysokiego ryzyka nie będą mogły być używane w Polsce. Jako jedno z istotnych kryteriów uznania dostawcy za dostawcę wysokiego ryzyka, projekt wskazuje pochodzenie z kraju spoza Unii Europejskiej czy Sojuszu Północnoatlantyckiego, mając na uwadze stosowanie w danym kraju ochrony danych osobowych a także porozumień w zakresie ochrony tych danych stosowanych w relacjach z Unią Europejską.

W stanowisku, złożonym przez Ministra – Koordynatora Służb Specjalnych Mariusza Kamińskiego, do projektu podkreślono między innymi, że „nie przewiduje *on* rozwiązania w sytuacji, gdy ocena określająca wysokie ryzyko obejmie specyficzne urządzenia czy

oprogramowanie, które jest unikatowe, a na rynku brak jest alternatywnych rozwiązań technicznych umożliwiających jego zastąpienie". Zastrzeżenia te, zapewne wynikały z groźby utraty możliwości korzystania, przez polskie służby, w razie wejścia w życie proponowanych przepisów ustawy, z części oprogramowania szpiegowskiego produkowanego przez podmioty z państw nienależących do Unii Europejskiej czy Sojuszu Północnoatlantyckiego.

Obecnie obowiązujące polskie prawo nie przewiduje używania tak inwazyjnych narzędzi jakim jest Pegasus, a że jest używany przyznał Pan na konferencji prasowej w dniu 9 maja br.

Działania operacyjne Centralnego Biura Antykorupcyjnego wobec m. in. polityków opozycji: szefa sztabu wyborczego PO Krzysztofa Brejzy, posła RP Grzegorza Napieralskiego, poseł RP Magdaleny Łośko czy też prokurator Ewy Wrzosek, mecenasa Romana Giertycha, prezydenta miasta Inowrocławia Ryszarda Brejzy, przedsiębiorcy Andrzeja Długosza, przewodniczącego AgroUnii Michała Kołodziejczaka, prezydenta Pracodawców RP Andrzeja Malinowskiego, prezydenta miasta Sopotu Jacka Karnowskiego, były prowadzone z użyciem broni cybernetycznej.

Pegasus nie jest jedynym oprogramowaniem służącym do inwigilacji z jakiego korzystają polskie służby. Na początku bieżącego roku media poinformowały, że polska Policja odnowiła licencje na używanie oprogramowania służącego do pobierania danych z telefonów firmy Cellebrite. Rozwiązanie to wykorzystywane było m. in. do szpiegowania współpracowników Aleksieja Nawalnego czy też członków społeczności LGBT w Rosji.

Mając na względzie powyżej przedstawione argumenty, a także fakt, że z zgodnie z rozwiązaniami przyjętymi we wskazanym projekcie ustawy minister właściwy do spraw informatyzacji, będzie organem właściwym do wszczęcia, także z urzędu, postępowania w sprawie uznania danego dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, proszę o udzielenie odpowiedzi na poniższe pytania:

1. Czy przepisy zawarte w przygotowywanym projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UD 68) (wersja z dnia 05.05.2023 r. zamieszczona pod https://legislacja.gov.pl/docs//2/12337950/12716644/dokument620468.pdf) pozwolą na wszczęcie postępowania w sprawie uznania dostawców sprzętu czy oprogramowania, takiego jak Pegasus, za dostawców wysokiego ryzyka?

2. Czy w świetle proponowanych rozwiązań, dostawca Pegasusa spełnia kryteria pozwalające uznać go za dostawcę wysokiego ryzyka?

3. Czy inni dostawcy sprzętu lub oprogramowania służącego do inwigilacji, a produkowanego przez podmioty pochodzące z państw spoza Unii

Europejskiej bądź NATO, spełniają kryteria pozwalające uznać ich za dostawców wysokiego ryzyka? Jeśli tak, proszę o wskazanie tych podmiotów.

4. Czy powyższa kwestia była przedmiotem analizy w ramach prac nad ustawą? Czy w toku prac legislacyjnych to zagadnienie było przedmiotem roboczych konsultacji z udziałem Ministra – Koordynatora Służb Specjalnych, Ministerstwa Sprawiedliwości czy przedstawicieli samych służb? Jeśli tak, to proszę wskazać które to służby i czy celem tych konsultacji było takie skonstruowanie przepisów, które uniemożliwią uznanie producenta Pegasusa za dostawcę wysokiego ryzyka?

5. Czy po wejściu w życie przywołanego projektu ustawy, minister właściwy do spraw cyfryzacji zamierza wszcząć z urzędu postępowanie w sprawie uznania dostawcy Pegasusa lub innych podobnych narzędzi za dostawcę wysokiego ryzyka? A jeśli nie, to z jakich względów?

6. Czy jednym z powodów, tak długiego procedowania rzeczonego projektu ustawy oraz wprowadzania kolejnych licznych modyfikacji w treści przepisów zawartych w projekcie, była chęć takiego ich sformułowania, aby dostawcy takich narzędzi jak np. Pegasus, nie mieścili się w kryteriach proponowanych dla uznania za dostawcę wysokiego ryzyka?

7. Jakie będą konsekwencje ewentualnego uznania dostawcy Pegasusa za dostawcę wysokiego ryzyka? Czy w razie takiego uznania polskie służby utracą z mocy prawa możliwość wykorzystywania tego narzędzia? Czy informacje zdobyte za pośrednictwem tego narzędzia będą mogły być wykorzystywane w toku postępowań prowadzonych przez odpowiednie służby?

Odpowiedź na tak postawione pytania upewni nas czy działania bądź zamierzenia legislacyjne polskich władz nie służą zatarciu użycia nielegalnych środków operacyjnych.

Przewodniczący komisji
Marcin Bosacki