Komentarz KBN

Nr 12 (84) / 2021 5 listopada 2021 r.

Pegasus - oprogramowanie inwigilacyjne w Polsce i na świecie

Jakub Stelmach[1]

Oprogramowanie szpiegujące *Pegasus* już od co najmniej 5 lat znane jest światowej opinii publicznej jako narzędzie inwigilacji wymierzone najczęściej w dziennikarzy, aktywistów, a tym samym podstawy funkcjonowania społeczeństwa obywatelskiego. Na przełomie 2018 i 2019 roku za sprawą ustaleń Najwyższej Izby Kontroli i śledztwa dziennikarskiego padło podejrzenie o zakup przez Centralne Biuro Antykorupcyjne rzeczonego oprogramowania. Wydarzenie to po raz kolejny rozpoczęło w Polsce publiczną debatę nad uprawnieniami służb specjalnych oraz skutecznością mechanizmów kontroli i nadzoru nad nimi. W ciągu następnych lat temat wykorzystywania oprogramowania do naruszania praw i wolności kilkukrotnie powracał, zarówno w Polsce, jak i na świecie.

W lipcu 2021 r. doniesienia o wykorzystaniu oprogramowania zyskały nowy charakter, kiedy okazało się, że potencjalną jego ofiarą mógł być jeden z głównych europejskich polityków, prezydent Francji Emmanuel Macron. Temat *Pegasusa* i jego wpływu na politykę międzynarodową, jak i sytuację wewnętrzną w wielu państwach ponownie znalazł się w zainteresowaniu mediów.

[1] Student I roku studiów II stopnia na kierunku „bezpieczeństwo narodowe", w roku akademickim 2020/2021 przygotował pracę licencjacką pt. „Kontrola obywatelska nad cywilnymi służbami specjalnymi w Polsce", której promotorem był dr Mateusz Kolaszyński.

Skupiając się jednak na samych aspektach technicznych oprogramowania oraz konsekwencjach jego wykorzystania łatwo pominąć aspekt związany z uprawnieniami służb specjalnych, kontrolą nad ich działalnością oraz nowymi technologiami, które coraz częściej wymykają się dotychczasowym próbom ich regulacji.

Specyfika pegaza

Mitologicznego pegaza, dzikiego, uskrzydlonego konia można odczytywać jako symbol nieskrępowania i absolutnej swobody. Jedynie heros Bellerofont oraz sam Zeus byli w stanie zapanować nad mitycznym wierzchowcem. Patrząc na oprogramowanie *Pegasus* można z łatwością zauważyć trafność nadanej nazwy. To, co stanowi o charakterze oprogramowania to sposób jego rozprzestrzeniania. Z trzech podstawowych metod zainfekowania telefonu tylko jedna wymaga jakiejkolwiek interakcji ze strony użytkownika. Instalacja oprogramowania może odbyć się poprzez otworzenie odpowiedniego linku, samo jego wyświetlenie (w przypadku wysłania za pośrednictwem komunikatora tworzącego automatycznie podgląd strony) lub przesłanie sygnału rozpoczynającego instalacje oprogramowania (do czego nie jest konieczny udział operatora sieci). Dotychczas panowało przeświadczenie, że urządzenia Apple od czasu aktualizacji 9.3.5 systemu operacyjnego iOS są odporne na zainfekowanie. Najnowsze doniesienia informują jednak o wykorzystywaniu nowszych, świeżo powstałych luk w zabezpieczeniach. Pytaniem bez odpowiedzi pozostaje kwestia odporności na zainfekowanie urządzeń funkcjonujących na mniej popularnych systemach, takich jak np. często wskazywany przez użytkowników za najbezpieczniejszy Ubuntu. Z jednej strony można założyć, że ich niszowość mogła skutkować niedostosowaniem przez producenta oprogramowania do funkcjonowania w środowisku innym niż Android i iOS. Z drugiej strony należy pamiętać, że przez wiele lat również wspomniany iOS był wskazywany jako odporny na zainfekowanie. W przypadku zainfekowania oprogramowanie zyskuje dostęp do wszystkich funkcji telefonów. Począwszy od danych zapisanych w pamięci podręcznej, ustalenia lokalizacji, uzyskania informacji zawartych w zainstalowanych aplikacjach (w tym komunikatorach) po możliwość zdalnego rejestrowania i nagrywania dźwięku oraz obrazu – *de facto* służąc jako aktywny podsłuch.

Powyższy opis pozwala na zauważenie nieokiełznanego charakteru nowoczesnego oprogramowania służącego inwigilacji. Połączenie łatwości i szybkości rozprzestrzeniania praktycznie pozostawia potencjalny cel bez szansy na przeciwdziałanie zainfekowaniu urządzenia. Dodatkowo możliwość całkowitego przejęcia kontroli nad urządzeniem oraz cyfryzacja wielu aspektów życia sprawia, że nazywanie *Pegasusa* oraz innych, podobnych mu programów mianem „narzędzi totalnej inwigilacji" wydaje się bardzo trafne. Komisja Wenecka już w 2015 r. w dokumencie *Report on the Democratic Oversight of Signals Intelligence Agencies* ostrzegała, że dynamicznemu rozwojowi nowych technologii wykorzystywanych w działalności wywiadowczej muszą towarzyszyć równie dynamiczne zmiany w porządku prawnym. Bez tego nowe technologie i możliwości jakie oferują mogą znaleźć się poza prawnymi granicami regulującymi działalność wywiadowczą. Stworzenie takich przypisów jest ważnym, ale i niezwykle trudnym zadaniem. Od ustawodawcy wymaga się fachowej wiedzy o technologiach, które ma uregulować oraz pogodzenia gwarancji praw i wolności jednostki z uprawnieniami służb, tak by te dalej mogły skutecznie realizować swoje ustawowe zadania. Na gruncie polskim jednym z przykładów przepisu, który mógłby być

bardziej szczegółowy, jest art. 6 ust. 8 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu stwierdzający lakonicznie, że do zadań AW należy „prowadzenie wywiadu elektronicznego".

Pegaz na świecie

Charakter *Pegasusa* i łatwość, z jaką może zostać użyty, przełożyły się bezpośrednio na jego wykorzystanie na całym globie. Już od momentu powstania program był wykorzystywany jako narzędzie wymierzone głównie w dziennikarzy i aktywistów społecznych. Po raz pierwszy oprogramowanie zostało wykryte przez Ahmeda Mansoora, aktywistę działającego w Zjednoczonych Emiratach Arabskich, którego zaintrygował specyficzny link mający zawierać informacje o osobach przetrzymywanych na terytorium ZEA. Śledztwo podjęte przez organizację Citizen Lab wykazało, że wejście w link zainfekowałoby telefon Mansoora oprogramowaniem szpiegującym. Dalsze śledztwo pozwoliło wskazać izraelską firmę NSO Group jako producenta.

Jednym z najtragiczniejszych epizodów z użyciem *Pegasusa* było zabójstwo Dżamala Chaszukdżiego (Jamala Ahmada Khashoggiego), saudyjskiego dziennikarza zabitego w konsulacie w Stambule. Jak wyznał Edward Snowden, Chaszukdżi był inwigilowany i namierzony przed śmiercią dzięki uzyskaniu kontroli nad jego osobistym telefonem. Najnowszy wyciek informacji potwierdza utrzymanie się dotychczasowego trendu. Lista 50000 numerów telefonów zainfekowanych lub będących potencjalnymi celami dla oprogramowania w znacznej większości zawiera dane dziennikarzy i aktywistów. Należy przy tym zaznaczyć, że pełna wersja listy nie została publicznie udostępniona. Jednak udostępniono ją dziennikarzom czołowych brytyjskich, francuskich, amerykańskich i indyjskich mediów. Samo przedostanie się listy do przedstawicieli czwartej władzy było najprawdopodobniej wynikiem działania wewnętrznego sygnalisty z NSO Group. Jako państwa przodujące w wykorzystaniu *Pegasusa* wskazuje się Arabię Saudyjską, Azerbejdżan, Bahrajn, Kazachstan, Meksyk, Maroko, Rwandę, Indie, Węgry i Zjednoczone Emiraty Arabskie. Poważne kontrowersje wzbudziło znalezienie wśród potencjalnie zainfekowanych numerów telefonów tych należących do prezydenta Francji Emmanuela Macrona, byłego premiera Édouarda Philippe'a i 14 ministrów. Oskarżenie o podsłuchiwanie padło na Maroko, które oficjalnie zaprzeczyło wykorzystywaniu *Pegasusa.* W atmosferze potencjalnego skandalu politycznego doszło do spotkania ministrów obrony Francji i Izraela, podczas którego strona izraelska zobowiązała się do podjęcia działań kontrolnych wobec NSO Group.

Przypadek Maroka ukazuje, jak potencjalnie niebezpiecznym wobec innych uczestników stosunków międzynarodowych może być oprogramowanie tego typu w sytuacji, gdy posiada je państwo niedemokratyczne, w którym nie funkcjonują sprawne mechanizmy kontroli i nadzoru zarówno nad służbami specjalnymi, jak i władzą polityczną.

Pegaz w Polsce

Pierwsze informacje dotyczące możliwości wystąpienia oprogramowania w Polsce pochodzą z raportu Citizen Lab z 2018 r. Raport wskazywał na operatora o pseudonimie ORZELBIALY, podejrzanego o wykorzystywanie sieci operatorów Polkomtel, FIBERLINK, Orange Polska, T-Mobile

Polska, PROSAT, Vectra i Netia do rozprzestrzeniania *Pegasusa.* Kolejną poszlakę mogącą wskazywać na obecność oprogramowania odkryła Najwyższa Izba Kontroli. NIK wykazał, że 25 mln złotych zostało przekazanych CBA ze środków Funduszu Pomocy Pokrzywdzonych Ministerstwa Sprawiedliwości. W 2019 r. w dziennikarskim śledztwie powiązano otrzymane przez CBA środki z zakupem za pośrednictwem jednej z firm informatycznych oprogramowania *Pegasus*. W krótkich komunikatach sekretarz Kolegium ds. Służb Specjalnych oraz samo CBA zaprzeczyli zakupowi takiego oprogramowania. W 2020 r. dziennikarze podejrzewali CBA o wykorzystywanie *Pegasusa* do inwigilowania byłego ministra transportu, budownictwa i gospodarki wodnej, będącego wówczas członkiem sztabu wyborczego opozycyjnego kandydata na urząd Prezydenta RP. Padło podejrzenie, że jego podsłuch miał służyć do inwigilacji całego sztabu wyborczego opozycji, czemu zaprzeczył minister koordynator służb specjalnych. Wyciek informacji o wykorzystaniu oprogramowania z lipca 2021 r. nie pozwala na potwierdzenie wszystkich podejrzeń. Dane udostępnione na GitHubie wśród listy 1406 stron internetowych potencjalnie wykorzystywanych do rozprzestrzeniania oprogramowania wskazują tylko na jedną polską domenę.

Jak osiodłać pegaza?

W reakcji na doniesienia z 2019 r. zespół ekspertów pracujący na zaproszenie Rzecznika Praw Obywatelskich opublikował raport „Osiodłać Pegaza" wskazujący na mankamenty obecnej, gwarantowanej przez państwo kontroli i nadzoru nad służbami specjalnymi oraz wskazujący na konieczne zmiany w porządku prawnym i postulujący utworzenie nowej, niezależnej instytucji kontrolnej. Publikacja raportu na pewien czas rozpowszechniła w dyskursie publicznym dyskusję nad uprawnieniami służb specjalnych, ich działalnością oraz kontrolą nad nimi (zob. np. M. Kolaszyński, „Osiodłać Pegaza" – założenia reformy kontroli nad służbami specjalnymi). Oprócz zwrócenia uwagi na formalno-prawne niedoskonałości obecnego państwowego systemu kontroli i nadzoru, raport podkreśla również jego archaiczność, zwłaszcza biorąc pod uwagę możliwości wykorzystywania nowych technologii przez służby specjalne. Problemem okazało się jednak utrzymanie stałego zainteresowania opinii publicznej.

W 2021 r. Fundacja Panoptykon podjęła próbę przywrócenia zainteresowania mediów tematem inwigilacji i konieczności ulepszenia mechanizmów kontroli nad służbami rozpoczynając własną kampanię medialną „Podsłuch jak się patrzy". W jej ramach ponownie udało się na pewien czas odzyskać zainteresowanie mediów oraz przedłożono prezydentowi, premierowi i marszałkom Sejmu i Senatu petycję postulującą utworzenie nowego, niezależnego organu kontroli. Zapytano również kluby i partie polityczne: Polska 2050, Koalicja Polska, Koalicja Obywatelska, Lewica, Konfederacja oraz Koło Parlamentarne Prawa i Sprawiedliwości o ich ocenę bieżącej sytuacji, pomysły i postulaty dotyczące usprawnień kontroli nadzoru. Niemal wszyscy zapytani zgodzili się co do konieczności stworzenia lepszych mechanizmów kontroli nad służbami. Odpowiedzi nie udzieliło Koło Parlamentarne Prawa i Sprawiedliwości. Sama możliwość posiadania przez polskie służby oprogramowania *Pegasus* stworzyła niebezpieczną sytuację społeczną. Rozpoczęta dyskusja skłania do refleksji nad niedoskonałościami państwowego systemu kontroli nad służbami specjalnymi. Wydawane przez organy państwa oświadczenia w sprawie *Pegasusa* często zostawały uznane za niewystarczające bądź wymijające. W momencie uwidocznienia niedostatków systemów nadzoru i kontroli część opinii publicznej i środowisk eksperckich nie jest w stanie

uwierzyć z zapewnienia organów, których realne kompetencje kontrolne są uznawane za iluzoryczne.

Jednym z możliwych rozwiązań jest utworzenie (wzorem większości państw UE) nowego, niezależnego organu kontroli. Dzięki apolityczności, wyspecjalizowaniu i wykorzystaniu bogatego zaplecza eksperckiego jego działalność mogłaby przyczynić się do odbudowy zaufania oraz pozwolić na uniknięcie podobnych sytuacji w przyszłości. Warto jednak zauważyć, że rozwiązanie bazujące na stworzeniu sprawnego systemu kontroli nad służbami mogłoby ograniczyć możliwości wykorzystania oprogramowania tego typu przez służby państwa, jednak nie miałoby przełożenia na zapewnienie bezpieczeństwa przed działaniami podjętymi przez służby zagraniczne. W przypadku Pegasusa kwestia ta zyskuje tym bardziej na znaczeniu z racji, że oprogramowanie to najczęściej wykorzystywane jest w państwach niedemokratycznych lub tych gdzie system demokratyczny działa wadliwie.

Podsumowanie

Najnowsza sprawa wykorzystania oprogramowania *Pegasus* skłania do refleksji nad wieloma implikacjami wynikającymi z wykorzystania najnowszych technologii przez służby specjalne. Pierwszą z nich jest kwestia niekontrolowanego wykorzystania nowych technologii w działalności wywiadowczej. Możliwości techniczne w zakresie pozyskiwania informacji oferowane przez najnowsze osiągnięcia techniki często wymykają się prawnym regulacjom pozyskiwania danych. Łatwość rozprzestrzeniania oprogramowania oraz problematyczność jego wykrycia i usunięcia stwarza ryzyko pominięcia w przeprowadzeniu kontroli operacyjnej zewnętrznych organów odpowiedzialnych za wyrażanie zgody na jej zarządzenie. Inną kwestią pozostaje fakt, że regulacje dotyczące pozyskiwania danych najczęściej skupiają się na danych stanowiących treść. Współcześnie jednak z racji na postępującą cyfryzację i internetyzację odpowiednio przetworzone dane niebędące treścią również mogą stać się bogatym źródłem prywatnych informacji.

Kolejna implikacja związana jest z prywatyzacją działalności wywiadowczej, w tym wypadku udziału podmiotów prywatnych jako producentów i dystrybutorów technologii. Przypadek NSO Group obrazuje, jak oprogramowanie dające olbrzymie możliwości inwigilacyjne było (według oficjalnych doniesień) dystrybuowane praktycznie bez wiedzy władz Izraela. Udostępnienie listy numerów telefonów, które mogły być zainfekowane *Pegasusem* nie wynikło z przeprowadzonych kontroli i audytów a jako informacja udostępniona mediom przez sygnalistę. Dodatkowo na uwagę zasługuję fakt, że sygnalista nie zdecydował się na przekazanie informacji odpowiednim organom państwa odpowiedzialnym za kontrolę, lecz światowej opinii publicznej.

Zastanawiający jest natomiast aspekt wpływu *Pegasusa* na opinię publiczną, zwłaszcza gdy porównamy lipcowy skandal z podsłuchiwaniem Emmanuela Macrona z tzw. aferą Snowdena z 2013 r. W obu przypadkach celem inwigilacji byli jedni z najważniejszych europejskich polityków (wówczas jedną z ofiar inwigilacji była kanclerz Niemiec Angela Merkel) oraz tysiące innych osób. Lipcowe doniesienia zdobyły zainteresowanie mediów na nieporównywalnie krótszy czas. Być może jako społeczeństwo oswoiliśmy się z inwigilacją i już ją zaakceptowaliśmy?