Konstytucyjne prawa i wolności w obliczu nowych systemów inwigilacji

Kamila Brylak-Hudyma[1]

Wszechobecny rozwój technologiczny oraz masowa komputeryzacja nieodzownie wpływają nie tylko na codzienne życie obywateli, ale również na dostępność nowych technik inwigilacji. Dynamiczny rozwój tych nowych technologii powoduje, że ustawodawstwo państw wydaje się nie nadążać z wprowadzeniem odpowiednich uregulowań prawnych, które chroniłyby podstawowe prawa i wolności obywatela przed niedozwoloną kontrolą. Według medialnych doniesień jeden z systemów inwigilacji – Pegasus miał zostać zakupiony przez Centralne Biuro Antykorupcyjne (CBA). Oprogramowanie to jest wyjątkowo trudne do wykrycia przez użytkownika, którego sprzęt został zainfekowany. Ponadto w przypadku znalezienia Pegasusa na urządzeniu przy użyciu innych programów dochodzi do jego samozniszczenia i zatarcia wszelkich śladów obecności. Oznacza to, że obywatel może być kontrolowany i o tym nie wiedzieć. Pojawiły się więc wątpliwości co do ewentualnych podstaw prawnych do używania przez władze państwa systemów szpiegujących. Niniejszy artykuł dokonuje analizy obowiązujących przepisów w kontekście hipotetycznego uprawnienia władz do kontroli obywateli przy użyciu systemów takich jak Pegasus oraz wskazuje zagrożenia, które może spowodować jego używanie. Autorka próbuje wartościować i porównać zagwarantowane w Konstytucji oraz w aktach prawa międzynarodowego prawa i wolności obywatelskie z interesem i bezpieczeństwem państwa, który miałby stanowić podstawę do przeprowadzenia tego typu kontroli.

Uwagi wstępne

Wszechobecna cyfryzacja i rozwój technologiczny odciska swoje piętno w niemal każdej dziedzinie życia ludzkiego. Gdziekolwiek się nie poruszamy, zawsze towarzyszą nam urządzenia elektroniczne z dostępem do Internetu. Nie można się oprzeć wrażeniu, że część życia jest prowadzona w tej wirtualnej przestrzeni, a rozwój technologiczny nieodzownie oddziałuje na każdą sferę funkcjonowania człowieka. Trudno wyobrazić sobie dzisiejszy świat bez ułatwień, które przyniosła ludzkości komputeryzacja oraz dostęp do Internetu. Jednakże oprócz wymieniania wszystkich ich zalet nie można nie wspomnieć o równie licznych zagrożeniach, które niesie za sobą nieustanny rozwój cyfryzacji. Przede wszystkim aby móc korzystać z niektórych dobrodziejstw Internetu czy urządzeń elektronicznych, należy w pierwszej kolejności założyć profil (konto) i podać dane osobowe. Ponadto, prowadząc portal społecznościowy czy blog, użytkownicy często udostępniają swój wizerunek oraz informacje na temat codziennych aktywności, tworząc przy tym elektroniczną bazę danych o sobie. Niektóre z aplikacji otrzymują również dostęp do aktualnej lokalizacji swoich użytkowników. Nie zawsze wiadomo, w jakich celach dane te mogą zostać użyte[2]. Pytanie, które mogłoby się w tym miejscu pojawić, to na ile świadomie użytkownicy podają o sobie informacje i czy są świadomi konsekwencji ich upublicznienia.

O ile oczywiste jest, że wszelkie ataki hakerskie, crackerskie są nielegalne i powinny zostać potępione, o tyle warto zastanowić się nad ewentualną możliwością stosowania szpiegowskich oprogramowań przez władze państwowe w celu kontroli obywateli i gromadzenia informacji o nich. Takie działania mogłyby być uzasadnione interesem i bezpieczeństwem państwa oraz wspomóc walkę z przestępczością. Jednym z takich programów, dającym szerokie spektrum inwigilacji, jest oprogramowanie Pegasus. Według medialnych doniesień z 2019 r. CBA miało je zakupić od izraelskiej firmy *NSO Group*, zajmującej się cyberbezpieczeństwem[3]. Jednakże zgodnie z oświadczeniem CBA z 4.9.2019 r. zamieszczonym na oficjalnej stronie CBA żaden: „system masowej inwigilacji Polaków" nie został zakupiony, a wszelkie spekulacje w tym temacie nie znajdują faktycznych podstaw[4]. Komunikat jest sformułowany ogólnie i nie jest w nim podana wprost informacja, że to Pegasus nie został zakupiony, co jest istotne, ponieważ program ten nie jest przeznaczony do masowej inwigilacji (kontrolowane mają być pojedyncze jednostki). Niemniej można założyć, że przy obecnej dynamice rozwoju technologicznego w przyszłości mogą powstać kolejne aplikacje czy programy szpiegujące, które będą pozwalały na tajne i masowe monitorowanie sprzętu elektronicznego jednostek.

[1] Absolwentka Prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[2] *A. Mednis*, Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość, Legalis/el. 2016. Niemniej należy mieć na względzie, że zgodnie z art. 13 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [Dz.Urz. UE L Nr 119, s. 1] administrator podczas pozyskiwania danych osobowych musi poinformować osobę, od której uzyskuje dane, o celach przetwarzania danych osobowych oraz wskazać podstawę prawną przetwarzania.

[3] Zob. https://businessinsider.com.pl/technologie/nowe-technologie/pegasus-opracowala-firma-nso-group-jak-wyglada-branza-w-izraelu/61b5ygx (dostęp z 10.4.2020 r.).

[4] Zob. https://cba.gov.pl/pl/aktualnosci/4207,Oswiadczenie-CBA.html (dostęp z 10.4.2020 r.).

Niniejszy artykuł ma na celu analizę przepisów prawnych w kontekście hipotetycznego uprawnienia władz do kontroli obywateli przy użyciu systemów pokroju Pegasusa oraz wskazanie zagrożenia, które może za sobą nieść tego typu aktywność poprzez potencjalne naruszenie prawa do prywatności, prawa do ochrony tajemnicy korespondencji, prawa do ochrony danych osobowych. Temat ten jest ważny, ponieważ nieustannie powstają nowe systemy inwigilacyjne, a obywatel wydaje się bezbronny w stosunku do nich. Świadomość, że państwo jest we władaniu Pegasusa czy innego szpiegującego oprogramowania, mogłaby rewolucyjnie wpłynąć na sposób użytkowania sprzętu elektronicznego i Internetu przez jednostki. Zwłaszcza biorąc pod uwagę, że niemal każdy jest posiadaczem sprzętu elektronicznego (zarówno prywatnego, jak i służbowego). Zgodnie z raportem Głównego Urzędu Statystycznego z 2019 r. pt. Polska w liczbach 2019, w 2018 r., dominującym urządzeniem, przez które Polacy łączą się z Internetem był smartfon[5].

Pegasus

Oprogramowanie Pegasus jest rozbudowanym narzędziem umożliwiającym dostęp do zainfekowanego urządzenia i zawartych w nich danych, które może bez trudu prześledzić i przechwycić. Do zainstalowania oprogramowania na telefonie komórkowym dochodzi poprzez kliknięcie w przesłany link (np. w SMS-ie). Za jego pośrednictwem dochodzi do tzw. *remote jailbreak*, który wykorzystuje istniejące luki w zabezpieczeniach urządzenia elektronicznego i powoduje osadzenie w nim Pegasusa. Użytkownik oprogramowania może od tej chwili inwigilować właściciela urządzenia, bez jego zgody i wiedzy[6]. Problematyczne jest to, że posiada on funkcję autodestrukcji, która aktywowana jest w sytuacji, gdy użytkownik szpiegowskiego oprogramowania nie komunikował się z nim dłuższy czas albo gdy prawdopodobne stało się jego wykrycie na zainfekowanym urządzeniu. Okazuje się więc, że w wielu przypadkach osoba, która była kontrolowana, nigdy nie posiądzie wiedzy na temat tego, że jej sprzęt i jego zawartość była przedmiotem inwigilacji. Twórcy Pegasusa podnoszą, że oprogramowanie tego typu są przeznaczone wyłącznie dla służb państwowych i mają służyć w walce z przestępczością oraz terroryzmem. Służby państw mają kierować działanie Pegasusa na konkretne osoby (wobec których istnieją dowody na to, że mogą być zaangażowane w działania przestępcze)[7].

Prawo do prywatności

W systemie prawa nie ma przepisu definiującego pojęcie „prywatności" czy „życie prywatne", dlatego też bliższego zrozumienia ich znaczenia należy szukać w doktrynie przedmiotu. Przedstawia ona prywatność jako pewną sferę działalności jednostki, która nie jest poddana zewnętrznej kontroli, i wskazuje, że „życie prywatne to przymioty, wewnętrzne przeżycia osobiste (jednostkowe) człowieka i ich oceny, refleksje dotyczące wydarzeń zewnętrznych i jego wrażenia zmysłowe, a także stan zdrowia oraz sytuacja majątkowa"[8]. Ze swojej istoty nie są one dedykowane na publiczne rozpowszechnienie i każdy powinien mieć zagwarantowaną możliwość dokonania dobrowolnego wyboru, czy chce, w jaki sposób, w jakim zakresie i komu udostępnić fragmenty swojej egzystencji[9]. W każdym środowisku społeczno-kulturowym obszar prywatności będzie inaczej rozumiany i gwarantowany w zależności od przystosowania osób w nim mieszkających do większej lub mniejszej potrzeby izolacji, stopnia dystansu, potrzeb nawiązywania czy też utrzymywania relacji towarzyskich[10]. Potrzeba zagwarantowania prawa do prywatności uzasadniona jest tym, że każdej osobie powinno przysługiwać prawo do „wyłącznej kontroli tej sfery życia, która nie dotyczy innych, a w której wolność od ciekawości innych jest swoistą *conditio sine qua* non swobodnego rozwoju jednostki"[11]. Prawo to jest gwarantowane w art. 47 Konstytucji RP i zgodnie z jego brzmieniem „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". W przepisie tym zostały zakodowane dwa rodzaje praw: pierwsze – prawo do ochrony prywatności, życia rodzinnego, czci, dobrego imienia, oraz drugie – prawo do samostanowienia[12]. Ustanowiona w art. 47 Konstytucji RP norma stanowi wskazówkę do interpretacji pozostałych praw i gwarancji konstytucyjnych, a ponadto jeśli prawo do prywatności i jego ochrona nie będzie w pełni gwarantowana przez pozostałe źródła prawa, to możliwe zawsze jest odwołanie się do gwarancji konstytucyjnej.

---

[5] Z raportu wynika również, że 96,2% przedsiębiorstw zaopatrzone jest w komputery stacjonarne lub przenośne, a 95,6% posiada dostęp do Internetu. Ponadto 66,8% z nich posiada własną stronę internetową, a 30,3% przedsiębiorców do prowadzenia działalności gospodarczej wykorzystuje także media społecznościowe, https://stat.gov.pl/obszary-tematyczne/inne-opracowania/inne-opracowania-zbiorcze/polska-w-liczbach-2019,14,12.html (dostęp z 10.4.2020 r.).

[6] Zob. https://www.komputerswiat.pl/artykuly/redakcyjne/pegasus-moze-podsluchac-kazdego-nawet-szefa-amazona-jak-dziala-system-inwigilacji/e4rkez2 (dostęp z 11.4.2020 r.).

[7] Zob. https://www.komputerswiat.pl/artykuly/redakcyjne/pegasus-moze-podsluchac-kazdego-nawet-szefa-amazona-jak-dziala-system-inwigilacji/e4rkez2; https://plblog.kaspersky.com/pegasus-spyware/6551/ (dostęp z 11.4.2020 r.).

[8] *B. Banaszak*, Konstytucja Rzeczypospolitej Polskiej. Komentarz, Legalis/el. 2012, art. 47 Nb 4, [za:] wyrok TK z 19.5.1998 r., U 5/97, OTK 1998, Nr 4, poz. 46.

[9] *Ibidem*.

[10] *J. Braciak*, Prawo do prywatności, [w:] *B. Banaszak*, *A. Preisner* (red.), Prawa i wolności obywatelskie w Konstytucji RP, Warszawa 2002, s. 278.

[11] *M. Pryciak*, Prawo do prywatności, www.bibliotekacyfrowa.pl/Content/37379/011.pdf (dostęp z 10.4.2020 r.), [za:] *M. Safjan*, Prawo do ochrony życia prywatnego, [w:] Szkoła Praw Człowieka, Helsińska Fundacja Praw Człowieka, Warszawa 2006, s. 211 i n.

[12] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP. Tom I. Komentarz do art. 1–86, Legalis/el. 2016, art. 47.

Na arenie prawa międzynarodowego i europejskiego prawo do prywatności gwarantowane jest również przez Międzynarodowy Pakt Obywatelskich i Politycznych z 19.12.1966 r.[13] oraz Kartę Praw Podstawowych UE z 26.10.2012 r.[14]. Fundamentalne znaczenie nad brzmieniem art. 47 Konstytucji RP miała regulacja zawarta w art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności z 4.11.1950 r.[15]. Przewiduje on, że każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji, a wszelka ingerencja władzy publicznej w korzystanie z prawa do prywatności i tajemnicy korespondencji jest niedopuszczalna. Wyjątek od tej regulacji stanowią przypadki przewidziane przez ustawę i konieczne w demokratycznym społeczeństwie z uwagi na m.in. bezpieczeństwo państwowe i publiczne, ochronę porządku, zapobieganie przestępstwom, ochronę praw i wolności innych osób.

Prawo do ochrony tajemnicy korespondencji

W art. 49 Konstytucji RP zapewniono wolność i ochronę tajemnicy komunikowania się, a ich ograniczenie może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony. Za komunikowanie uznaje się proces porozumiewania się, utrzymywanie relacji towarzyskich. W procesie tym muszą występować co najmniej dwie strony, które wzajemnie wymieniają się wiadomościami, z tym że dopuszcza się sytuację, w której tylko jedna z nich aktywnie przesyła komunikaty, a druga przyjmuje postawę bierną. Prawo do ochrony tajemnicy komunikowania przyznane jest wszystkim jednostkom, w tym także osobom prawnym. Sposób przekazywania informacji pozostaje w tym przypadku bez znaczenia, tzn. że osoby mogą się ze sobą komunikować osobiście albo za pomocą dostępnych środków przekazu[16]. Regulacja konstytucyjna chroni również dane osobowe osób uczestniczących w konwersacji, informacje o historii przeglądarki internetowej, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP czy numerze IMEI[17]. Autonomia informacyjna obejmuje również ochronę przed niejawnym monitorowaniem osób i przeprowadzanych przez nią konwersacji[18], a także zabezpiecza przed dostępem do billingów z prowadzonych przez jednostkę rozmów telefonicznych, które zawierają dane o datach, długości trwania rozmów telefonicznych, połączeniach przychodzących i wychodzących[19]. Dzięki art. 49 Konstytucji RP osobom komunikującym się zagwarantowana jest wolność w trakcie całego procesu wymiany wiadomości i żaden inny podmiot nie powinien mieć dostępu i zapoznawać się z korespondencją, która nie była do niego adresowana.

Gwarancja autonomii informacyjnej

Kolejna gwarancja konstytucyjna, ściśle związana z prawem do prywatności, jest uregulowana w art. 51 Konstytucji RP. Regulacja ta przewiduje, że nie można nikogo zobowiązać inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby, a władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Ponadto każdemu przysługuje prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych, a jakiekolwiek ograniczenia tego prawa mogą być przewidziane tylko przez ustawę. Każdy jest uprawniony do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą[20]. O ile postanowienia ustawy zasadniczej skierowane są w większości przypadków do organów państwa, o tyle należy rozumieć, że obowiązek przewidziany w art. 51 Konstytucji RP będzie odnosił się również do podmiotów niepublicznych. Ustawodawca przyjął zatem szeroki zakres podmiotów zobowiązanych do przestrzegania prawa zawartego w art. 51 Konstytucji RP. Warto zwrócić uwagę na redakcję przedmiotowego artykułu, użyte bowiem w ust. 1 słowo „nikt" należy interpretować jako „każdy", przez co, jak wskazuje się w doktrynie, mamy do czynienia z prawem człowieka[21]. Inaczej to wygląda w ust. 2 art. 51 Konstytucji RP. Przepis wzmiankuje już tylko o „obywatelach", co może prowadzić do konkluzji, jakoby władze publiczne mogły gromadzić, przetwarzać dane dotyczące pozostałych osób (nie obywateli) i – co ważne – informacje, które będą przetwarzane, nie muszą spełniać przesłanki niezbędności w demokratycznym państwie prawnym. Wiele trudności interpretacyjnych powoduje zawarte w ust. 2 omawianego artykułu sformułowanie: „informacje o obywatelach (...) niezbędne w demokratycznym państwie prawnym". Rozpoczynając od próby zdefiniowania zwrotu „informacja niezbędna", można przyjąć, że są to dane, które pozwolą na: „normalne funkcjonowanie jednostki w zorganizowanym w państwo społeczeństwie". Z perspektywy organów władzy publicznej niezbędne będą te dane, które są newralgiczne dla podjęcia, kontynuowania lub zakończenia podjętych działań i aktywności (pozostających oczywiście w zakresie uprawnień władzy). Doktryna nie zaprzecza możliwości istnienia i funkcjonowania baz danych czy też informatycznych systemów, które miałyby być dedykowane gromadzeniu infor-

[13] Dz.U. z 1977 r. Nr 38, poz. 167.
[14] Dz.Urz. UE C Nr 326, s. 391.
[15] Dz.U. 1993 r. Nr 61, poz. 284.
[16] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 47.
[17] Zob. wyrok TK z 30.7.2014 r., K 23/11, OTK-A 2014, Nr 7, poz. 80.
[18] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 49.
[19] M. Wild [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 49, [za:] wyrok TK z 30.7.2014 r., K 23/11, OTK-A 2014, Nr 7, poz. 80.
[20] Art. 51 ust. 1–4 Konstytucji RP.
[21] *B. Banaszak*, Konstytucja..., art. 51, Nb 4.

macji. Jednakże władza publiczna nie może posiłkować się tego typu programami tylko dla swojej wygody, ponieważ najprawdopodobniej dochodziłoby do nadużyć z jej strony[22]. Trybunał Konstytucyjny przedstawił pogląd, że co do zasady gromadzenie danych o jednostkach, nawet bez informowania ich o tym procesie, nie jest zakazane, pod warunkiem że spełnia przesłankę konieczności zgodnej ze standardami obowiązującymi w demokratycznym państwie prawnym. Chodzi więc o gromadzenie danych o jednostkach w celu ochrony wartości panujących w demokratycznym państwie prawnym, jeżeli cel ten nie może zostać osiągnięty przy użyciu innych instrumentów[23]. Przedstawione stanowisko jest niezwykle istotne w perspektywie dalszych rozważań na temat możliwości zastosowania oprogramowania Pegasus do inwigilacji społeczeństwa.

Ograniczenia praw i wolności

Przedstawione powyżej i gwarantowane przez Konstytucję RP (oraz akty międzynarodowe i europejskie) prawa nie mają charakteru absolutnego i po wystąpieniu przesłanek i spełnieniu odpowiednich warunków mogą zostać ograniczone. Wprowadzenie obostrzeń powinno spełniać konstytucyjne kryteria, tj. ograniczenie jednych praw i wolności musi być uzasadnione potrzebą zapewnienia bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób[24]. Przy wprowadzaniu jakichkolwiek ograniczeń należy kierować się zasadą proporcjonalności i dokonać porównania – wolności, która ma zostać niejako „poświęcona", oraz prawa, które ma być chronione[25]. Zgodnie z treścią zasady proporcjonalności regulacja ograniczająca wolności obywatelskie może być wprowadzona, jeżeli:

1) jest w stanie doprowadzić do zamierzonych przez nią skutków;
2) jest niezbędna do zapewnienia interesowi publicznemu, z którym jest powiązana, ochrony;
3) efekt wprowadzonych ograniczeń pozostanie w odpowiedniej relacji (proporcji) do nałożonych na jednostkę ciężarów.

Przewidziana w art. 31 ust. 3 Konstytucji RP zasada jest w inherentnym związku z zakazem nadmiernej ingerencji w sferę praw i wolności konstytucyjnych obywateli[26]. Dokonanie oceny, czy podjęta ingerencja była konieczna i proporcjonalna, jest uzależnione od analizy specyfiki poszczególnych uprawnień i wolności konstytucyjnych (np. standardy dotyczące wolności i praw ekonomicznych i socjalnych nie będą tak surowe jak te dotyczące praw osobistych i politycznych)[27]. Ograniczenie obywatelskich praw musi być wprowadzone przez ustawę.

Jedną z regulacji bezpośrednio ingerującą w sferę przedstawionych powyżej praw i wolności są przepisy dotyczące możliwości zastosowania kontroli operacyjnej. Kontrola ta jest prowadzona niejawnie i polega na monitorowaniu treści korespondencji, zawartości przesyłek oraz na stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych. Oprócz treści rozmów można uzyskać jeszcze inne informacje przesyłane za pomocą sieci telekomunikacyjnych[28]. Rola przedsiębiorcy telekomunikacyjnego jest w tym kontekście bardzo ważna, ponieważ jest on zobligowany do zapewnienia, na własny koszt, warunków dostępu i utrwalania w zakresie wszystkich świadczonych usług telekomunikacyjnych[29]. Uprawnionym organem do przeprowadzenia kontroli operacyjnej jest m.in. Policja, CBA, ABW[30]. Zgodnie z art. 19 przewidziany przez ustawę z 6.4.1990 r. o Policji[31] przy wykonywaniu czynności operacyjno-rozpoznawczych, podejmowanych przez Policję w celu zapobieżenia, wykrycia, ustalenia sprawców, a także uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego, umyślnych przestępstw wymienionych w nim enumeratywnie, gdy inne środki okazały się bezskuteczne albo będą nieprzydatne, sąd okręgowy może, w drodze postanowienia, zarządzić kontrolę operacyjną. Wniosek o zarządzenie kontroli składa Komendant Główny Policji, komendant wojewódzki Policji albo Komendant CBŚP po uzyskaniu zgody odpowiedniego prokuratora. Jednakże w sytuacji niecierpiącej zwłoki, która mogłaby spowodować utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa, komendant może zarządzić kontrolę operacyjną, zwracając się jednocześnie do właściwego sądu z wnioskiem o wydanie postanowienia w tej sprawie. Jeżeli sąd w terminie pięciu dni od dnia zarządzenia kontroli nie wyrazi na nią zgody, to kontrola jest wstrzymywana i dokonuje się protokolarnego, komisyjnego zniszczenia materiałów zgromadzonych podczas jej stosowania[32]. Kontrola może trwać nie dłużej niż trzy miesiące, z tym że może zostać jednorazowo przedłużona o kolejne trzy miesiące[33]. Oczywiście może dojść do sytuacji, w której podczas kontroli uzyskano dowód popełnienia przestępstwa (wymienionego przez jeden z punktów

[22] *Ibidem*, art. 51, Nb 5–6.
[23] Zob. orzeczenie TK z 23.6.2009 r., K 54/07, OTK 2009, Nr 6A, poz. 86.
[24] Art. 31 ust. 3 Konstytucji RP.
[25] *B. Banaszak*, Konstytucja..., art. 47 Nb 8 [za:] wyrok TK z 21.10.1998 r., K 24/98, OTK Nr 6/1998, poz. 97.
[26] Orzeczenie TK z 23.6.2009 r., K 54/07, Legalis.
[27] *Ibidem*.
[28] *B. Opaliński*, *M. Rogalski, P. Szustakiewicz* (red.), Ustawa o Policji. Komentarz, wyd. 1, Legalis/e. 2015, art. 19, Nb 9, [za:] *J. Korycki*, Kontrola operacyjna, Prok. i Pr. Nr 7–8/2006, s. 150.
[29] Art. 179 ust. 3a ustawy z 16.7.2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2019 r. poz. 2460 ze zm.).
[30] Z uwagi na ramy niniejszego artykułu omówiona zostanie kontrola operacyjna przeprowadzana przez Policję oraz CBA.
[31] T.j. Dz.U. z 2020 r. poz. 360 ze zm.; dalej jako: PolU.
[32] Art. 19 ust. 3 PolU.
[33] Art. 19 ust. 8 PolU.

art. 19 PolU) i popełnionego przez osobę, wobec której była stosowana kontrola operacyjna, ale innego niż to przestępstwo, które było przedmiotem kontroli operacyjnej wobec tej osoby. Wówczas o zgodzie na wykorzystanie takiego dowodu w postępowaniu karnym będzie decydował sąd, który zarządził kontrolę operacyjną[34]. Kontrowersyjne jest jednak to, że osoba, wobec której takie działania były prowadzone, nie ma wglądu do materiałów zgromadzonych podczas ich trwania i nie może ich zweryfikować. Zgromadzone podczas kontroli materiały, które nie zawierają dowodów pozwalających na wszczęcie postępowania karnego lub dowodów mających znaczenie dla toczącego się postępowania karnego podlegają niezwłocznemu, protokolarnemu i komisyjnemu zniszczeniu[35].

Kolejną regulacją, ingerującą w sferę praw i wolności obywatelskich, jest art. 20 PolU. Zgodnie z nim Policja, z zachowaniem ograniczeń wynikających z art. 19, może uzyskiwać (niejawnie) informacje, a następnie je gromadzić, sprawdzać oraz przetwarzać. Informacjami, do których może mieć dostęp Policja, są dane osobowe, o których mowa w art. 14 ust. 1[36] ustawy z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[37]. Policja ponadto może uzyskać odciski linii papilarnych, zdjęcia, szkice i opisy wizerunku, cechy i znaki szczególne, pseudonimy oraz informacje o miejscu zamieszkania lub pobytu, wykształceniu, zawodzie, miejscu i stanowisku pracy oraz sytuacji materialnej i stanie majątku, dokumentach i przedmiotach, którymi sprawca się posługuje, sposobie działania sprawcy, jego środowisku i kontaktach[38]. Podobnie jak w przypadku prowadzenia kontroli operacyjnej, zgodę na gromadzenie i wykorzystanie danych musi wyrazić sąd. Zgromadzone dane podlegają ochronie przewidzianej w przepisach o ochronie informacji niejawnych i mogą być udostępniane jedynie policjantom prowadzącym czynności w danej sprawie i ich przełożonym. Akta zawierające te informacje i dane udostępnia się ponadto wyłącznie sądom i prokuratorom, jeżeli następuje to w celu ścigania karnego[39]. Zebrane dane osobowe przechowuje się przez okres niezbędny do realizacji ustawowych zadań Policji. Po zakończeniu sprawy (nie rzadziej niż co 10 lat od dnia uzyskania informacji) organy Policji dokonują ich weryfikacji i usuwają te dane, które okazały się zbędne[40].

Podobne uprawnienia przysługują CBA. W granicach swoich zadań[41] funkcjonariusze CBA wykonują czynności operacyjno-rozpoznawcze, czynności kontrolne czynności operacyjno-rozpoznawcze i analityczno-informacyjne, które uogólniając, mają służyć zapobieganiu popełniania przestępstw, ich wykrywaniu oraz zwalczaniu korupcji. Podczas przeprowadzania tych czynności funkcjonariusze mają obowiązek poszanowania godności ludzkiej oraz przestrzegania i ochrony praw człowieka niezależnie od jego narodowości, pochodzenia, sytuacji społecznej, przekonań politycznych lub religijnych albo światopoglądowych[42]. Przy wykonywaniu czynności operacyjno-rozpoznawczych, które CBA podejmuje w celu wykrywania przestępstw i utrwalania dowodów ich popełnienia, może zostać zarządzona kontrola operacyjna. Wniosek o jej przeprowadzenie składa do sądu Szef CBA po uzyskaniu pisemnej zgody Prokuratora Generalnego. Kontrola operacyjna jest niejawna i może być zastosowana, jeżeli inne środki okazały się bezskuteczne albo nieprzydatne do osiągnięcia ustawowych zadań i celów CBA. Zgromadzone podczas stosowania kontroli materiały, które nie stanowią informacji potwierdzających zaistnienie przestępstwa, podlegają niezwłocznemu zniszczeniu[43]. Centralne Biuro Antykorupcyjne do realizacji ustawowych celów również może uzyskiwać niezbędne dane określone w art. 18 CenBiurAnU, a następnie je przetwarzać bez wiedzy i zgody osoby, której dotyczą. Szef CBA prowadzi rejestr wystąpień o uzyskanie danych telekomunikacyjnych, pocztowych i internetowych zawierający informacje identyfikujące jednostkę organizacyjną CBA i funkcjonariusza CBA uzyskującego te dane, ich rodzaj, cel uzyskania oraz czas, w którym zostały uzyskane. Kontrolę nad uzyskiwaniem przez CBA tego typu danych sprawuje Sąd Okręgowy w Warszawie[44]. Artykuł 22 CenBiurAnU daje CBA ogólne uprawnienie do tego, by w zakresie swojej właściwości uzyskiwało, gromadziło, sprawdzało i przetwarzało (w tym także niejawnie) informacje. Przepis ten był badany przez TK w przywoływanym już w niniejszym artykule wyroku z 23.6.2009 r.[45]. Trybunał stwierdził, że artykuł ten w ust. 1–3 w zakresie, w jakim dopuszcza uzyskiwanie (w tym także – niejawnie), gromadzenie, sprawdzanie i przetwarzanie informacji niezbędnych do zwalczania przestępstw, w obszarze należącym do ustawowo określonych zadań CBA jest zgodny z art. 47 w zw. z art. 31 ust. 3, art. 51 w zw. z art. 31 ust. 3 i art. 30 Konstytucji RP. Takie rozstrzygnięcie zostało uzasadnione faktem, że zwalczanie korupcji jest obowiązkiem państwa i dlatego też pod warunkiem utrzymania działań CBA ściśle w ramach ustawowo wyznaczonych – brak jest wystarczających podstaw do stwierdzenia, że postanowienia art. 22 ust. 1–3 CenBiurAnU są niezgodne z prawem do

[34] Zob. art. 19 ust. 15c PolU.
[35] Art. 19 ust. 16–17 PolU.
[36] M.in. dane osobowe ujawniające pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych.
[37] Dz.U. z 2019 r. poz. 125.
[38] Art. 20 ust. 2b PolU.
[39] Art. 20 ust. 4 PolU.
[40] Art. 17–17b PolU.
[41] Art. 2 ustawy z 9.6.2006 r. o Centralnym Biurze Antykorupcyjnym, t.j. Dz.U. z 2019 r. poz. 1921 ze zm.; dalej jako: CenBiurAnU.
[42] Art. 13 CenBiurAnU.
[43] Art. 17 CenBiurAnU.
[44] Art. 18a CenBiurAnU.
[45] K 54/07, Legalis. Obecnie w art. 22 pozostał ust. 1, a pozostałe zostały uchylone.

prywatności oraz z prawem do autonomii informacyjnej. Niemniej jednak powyższe uprawnienia CBA mogą zostać użyte tylko w celu zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania działalności godzącej w interesy ekonomiczne państwa. Sama możliwość kontrolowania obywateli poprzez wprowadzenie zapisów o kontroli operacyjnej budziła i wciąż budzi wiele kontrowersji. W trakcie jej trwania również można pozyskać wiele prywatnych i intymnych informacji, co oznacza, że służby państwa są już autoryzowane przez ustawodawstwo do wykorzystania mechanizmów inwigilacji względem obywateli. Niemniej następuje to tylko w przypadku enumeratywnie wymienionych przez ustawy przestępstw i jest poprzedzone ściśle określoną procedurą. Co ważne, Policja, by przejrzeć wiadomości, billing połączeń musi skontaktować się z przedsiębiorcą telekomunikacyjnym, operatorem pocztowym oraz usługodawca świadczący usługi drogą elektroniczną, czyli „zostawia po sobie ślad". Gdyby organy ścigania były we władaniu Pegasusa, nie byłyby zmuszone kontaktować się z kimkolwiek, by uzyskać potrzebne informacje. Pytanie również, czy udostępniane byłyby dane o liczbie przeprowadzonych kontroli, tak jak jest to chociażby w przypadku ustawy z 28.1.2016 r. – Prawo o prokuraturze[46]. Zgodnie z art. 11 ust. 1 PrProkU, Prokurator Generalny przedstawia Sejmowi i Senatowi roczną informację o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej. Z ostatniej przedłożonej informacji za 2018 r. wynika, że wszystkie uprawnione organy skierowały łącznie wobec 6088 osób wnioski o zarządzenie kontroli i utrwalanie rozmów lub wnioski o zarządzenie kontroli operacyjnej, przy czym: sąd zarządził kontrolę i utrwalanie rozmów lub kontrolę operacyjną wobec 5915 osób. Sąd odmówił zarządzenia kontroli i utrwalania rozmów lub kontroli operacyjnej wobec 25 osób, a wobec 148 osób wnioski o kontrolę operacyjną nie uzyskały zgody prokuratora[47]. Z przedstawionych danych wynika, że sądy w zdecydowanej większości wyrażają zgodę na przeprowadzenie kontroli operacyjnej, która powinna być traktowana jako ostateczność. Hipotetycznie więc, gdyby władze były w posiadaniu Pegasusa, to w jakiej relacji pozostawałoby jego użycie do kontroli operacyjnej? Czy w tym przypadku za ostateczność należałoby już traktować nie zastosowanie kontroli operacyjnej, a szpiegowskiego oprogramowania, czy też Pegasus byłby zastrzeżony tylko dla konkretnej służby do konkretnych działań zapewniających ochronę państwa. Niemniej w obecnym stanie: „Żaden bowiem przepis prawa nie pozwala żadnemu organowi państwowemu na przełamywanie zabezpieczeń i przechwytywanie, a także wykorzystywanie, w ten sposób treści przekazów komunikacyjnych oraz uzyskiwanie dostępu do wszelkich informacji i danych z urządzenia mobilnego"[48].

Bezpieczeństwo i interes państwa

Przedstawione uprawnienia Policji i CBA, ukierunkowane na zwalczanie przestępczości, mają za zadanie zapewnić bezpieczeństwo w państwie, które stanowi fundamentalny warunek jego rozwoju oraz społeczeństwa w nim funkcjonującego. Powszechnie przyjmowane jest, że nie jest możliwe ustanowienie stałych standardów bezpieczeństwa, ponieważ jest to proces, który zmienia się i powinien być dostosowany do zachodzących w społeczeństwie i w świecie zależności i zjawisk[49]. Dlatego ciężko jest wskazać jedną definicję bezpieczeństwa narodowego[50], co jest związane z dynamiką zmian warunków otoczenia, rozwojem cywilizacyjnym i technologicznym oraz sferą nowych potrzeb poszczególnych podmiotów. Ważne jest, by pojmować bezpieczeństwo w stosunkach narodowych jak dynamiczny proces o zmiennej intensywności[51]. W literaturze wskazuje się, że można wyróżnić cztery podstawowe wartości wchodzące w skład bezpieczeństwa narodowego – tj. przetrwanie, integralność terytorialna, niezależność polityczna, jakość życia (w wielu aspektach, np. kulturowym, rozwojowym, edukacyjnym, ekonomicznym)[52], a zagrożenie którejkolwiek z nich może stanowić niebezpieczeństwo dla szeroko pojętego interesu państwa i skutkować osłabieniem bezpieczeństwa narodowego. Zadaniem władzy jest więc troska i dbałość o zapewnienie obywatelom realnego bezpieczeństwa i ochrony, ale również powstrzymanie się od ingerowania w prywatną sferę ich życia. Wymagane jest wprowadzenie do porządku prawnego odpowiednich regulacji zapewniających instrumenty, które upoważnią władze do podejmowania adekwatnych działań pozwalających na utrzymanie porządku i bezpieczeństwa w państwie. Nieuniknione są sytuacje, w których w celu ochrony jednych wartości należy ograniczyć drugie. Wprowadzając jakiekolwiek ograniczenie wolności i praw obywatelskich, ustawodawca powinien kierować się opisaną

[46] T.j. Dz.U. z 2019 r. poz. 740 ze zm.; dalej jako: PrProkU.

[47] Jawna, roczna informacja Prokuratora Generalnego z 6.6.2019 r. o łącznej liczbie osób, wobec których został skierowany wniosek o zarządzenie kontroli i utrwalania rozmów lub wniosek o zarządzenie kontroli operacyjnej (druk senacki Nr 1209).

[48] Wystąpienie Rzecznika Praw Obywatelskich z 9.9.2019 r. skierowane do Prezesa Rady Ministrów w sprawie potencjalnego użycia systemu Pegasus, VII.519.2.2019.AG, s. 4, https://www.rpo.gov.pl/sites/default/files/Wystapienie_do_Premiera_ws_systemu_Pegasus_09.09.2019.pdf (dostęp z 20.4.2020 r.).

[49] *K. Olak*, *A. Olak*, Współczesne rozumienie bezpieczeństwa narodowego, ISSN 2300-1739, s. 470, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-750af56a-6af8-46ef-b41d-3a67e69d1217/c/Wspolczesne_rozumienie_467-480.pdf (dostęp 19.4.2020 r.).

[50] Pojęcie bezpieczeństwo państwa i bezpieczeństwo są ze sobą tożsame, *J. Czaputowicz*, Kryteria bezpieczeństwa międzynarodowego państwa – aspekty teoretyczne, [w:] *S. Dębski*, *B. Górki-Winter* (red.), Kryteria bezpieczeństwa międzynarodowego państwa, Warszawa 2003, s. 13.

[51] *J. Stańczyk*, Współczesne pojmowanie bezpieczeństwa, Warszawa 1996, s. 18–19.

[52] *J. Kukułka*, Bezpieczeństwo a współpraca europejska: współzależności i sprzeczności interesów, Sprawy Międzynarodowe 1982, Nr 7, s. 18.

powyżej zasadą proporcjonalności. Orzecznictwo podkreśla, że „im bardziej drastyczne (co do przedmiotu, zakresu, sposobu czy skutków) jest wkroczenie władzy w materię konstytucyjnie chronionych praw podstawowych, tym bardziej rygorystycznym przesłankom powinna podlegać procedura, stanowiąca gwarancję tego wkroczenia”[53]. Samo istnienie przepisów zezwalających na arbitralną inwigilację obywateli jest rozumiane jako naruszenie art. 8 EKPC i daje podstawę do wniesienia skargi do ETPC[54]. Nie można więc gromadzić danych o jednostkach w celu ich potencjalnego wykorzystania w przyszłości[55]. Pegasus nie mógłby więc z pewnością być używany w celach gromadzenia informacji o obywatelach, które mogłyby być w przyszłości użyte. Pomimo że prześledzenie działań obywatela z perspektywy kilku lat – gdzie był, jakie nawiązywał znajomości, czym się interesował, pozwoliłoby szybciej zweryfikować zgromadzone dowody oraz zrozumieć sposób jego działań, to takie gromadzenie danych za pomocą szpiegowskiego oprogramowania powinno zostać uznane za nielegalne. Rozwój technologiczny stanowi duże wyzwanie dla ustawodawcy, ponieważ prawo nieustannie musi być dostosowywane do pojawiających się na rynku innowacji technologicznych. Podkreśla to dynamikę zmienności pojęcia i znaczenia bezpieczeństwa państwa. Niestety, ale nie zawsze odpowiednie regulacje są wprowadzane na czas bądź nie są wystarczająco precyzyjne. Orzecznictwo podkreśla, że choć Konstytucja nie wzmiankuje o funkcjonowaniu obywateli w Internecie, to nie znaczy, że jej wolności i prawa nie będą się odnosiły analogicznie do tej wirtualnej przestrzeni i sposobu korzystania z niej. Informacje, które są przekazywane: „(...) za pomocą Internetu nie mogą być postrzegane jako funkcjonujące niejako obok, czy na marginesie konstytucyjnie chronionych form aktywności człowieka”[56].

Podsumowanie

Próbując odpowiedzieć na pytanie, czy istnieje bezpośrednia podstawa prawna pozwalająca na użycie przez władze państwowe oprogramowania typu Pegasus (tj. programu, który bez wiedzy i zgody obywatela mógłby zostać zainstalowany na jego urządzenie elektronicznym i pozyskiwał, gromadził z niego dane), należy odpowiedzieć przecząco. Nie oznacza to jednak, że oprogramowanie to nie byłoby pod pewnymi warunkami ułatwieniem dla władz państwowych w kontekście zapewnienia państwu i obywatelom bezpieczeństwa. Jednakże obywatele powinni wiedzieć, że tego typu oprogramowanie jest we władaniu władz i w przypadku uzasadnionego podejrzenia bądź współpracy przy popełnieniu przestępstwa władze mogą inwigilować ich sprzęt. Informacja, że organy ścigania są w posiadaniu takich środków, mogłaby działać prewencyjnie i zniechęcać do podejmowania działań niezgodnych z prawem. Z drugiej jednak strony przestępcy, wiedząc, że państwo dysponuje szpiegowskimi oprogramowaniami, nie pozostawialiby na swoich urządzeniach żadnych śladów, a co więcej, przy ich użyciu manipulowaliby śledztwem (fabrykowali dowody, zrzucali podejrzenia na inną osobę). Mając na uwadze, ile danych wrażliwych znajduje się w smartfonach, tego typu kontrola powinna być zastrzeżona dla najcięższych przestępstw i stanowić ostateczność – tj. zgodnie z zasadą proporcjonalności być stosowaną tylko w przypadku niemożliwości osiągnięcia celu prowadzonego postępowania przy użyciu innych dostępnych i legalnych środków. Inwigilacja przy użyciu Pegasusa pozwoliłaby, a bynajmniej mogłaby zwiększyć wiarygodność zebranych zeznań, dowodów. Procedura potencjalnego użycia systemu pokroju Pegasusa powinna zostać bardzo szczegółowo uregulowana w ustawie oraz wymieniać enumeratywnie przestępstwa i sytuacje, w których może on zostać użyty (a nawet ograniczyć się do zwalczania terroryzmu i korupcji wśród urzędników). Ustawa nie mogłaby zawierać żadnych klauzul generalnych, nie tworząc tym samym pola na rozbieżności interpretacyjne i wnioskowania prawnicze. Ponadto taki akt musiałby jasno wskazywać, czy inwigilować można całe urządzenie i jego wszystkie aplikacje, programy, galerie oraz kto miałby być odpowiedzialny za monitoring. Z pewnością taka osoba nie powinna być w żaden sposób powiązana z obywatelem, który miałby być inwigilowany oraz musiałaby zobowiązać się do zachowania w tajemnicy wszelkich informacji, które poweźmie w trakcie przeprowadzania kontroli. Ustawodawca musiałby również określić czas prowadzenia kontroli i ewentualną możliwość jej przedłużenia. Podobnie jak to jest w przywołanych powyżej regulacjach ustawy o Policji czy CBA, przepisy o ewentualnym stosowaniu programu pokroju Pegasusa musiałby wskazywać sposób niszczenia zgromadzonych danych, gdyby okazało się, że nie są one przydatne do śledztwa, oraz okres, po którym podlegałyby one usunięciu. Kolejną kwestią jest ewentualne prowadzenie rejestru gromadzącego informacje o tym, kto, kiedy, jak długo, przez kogo, w jakim celu był kontrolowany, a także na jakim urządzeniu, czy dane zostały usunięte oraz czy były przydatne i czy podlegają po upływie określonego czasu weryfikacji i usunięciu. Problematyczne jest również zajęcie stanowiska co do tego, czy kontrolowanemu obywatelowi powinno zostać wskazane, że jego prawo do prywatności zostało naruszone, do których informacji uzyskano dostęp oraz jaka była podstawa użycia szpiegowskiego oprogra-

[53] Zob. wyrok TK z 13.3.2007 r., K 8/07, Legalis.
[54] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 47, Nb 1 [za:] wyrok Europejskiego Trybunału Praw Człowieka z 4.12.2015 r. w spr. *Zakharov* przeciwko Rosji, skarga Nr 47143/06, HUDOC).
[55] *M. Wild*, [w:] *M. Safjan*, *L. Bosek* (red.), Konstytucja RP..., art. 47, Nb 1.
[56] Zob. wyrok TK z 30.7.2014 r., K 23/11, OTK-A 2014, Nr 7, poz. 80.

mowania. Jednakże taka informacja mogłaby zaszkodzić prowadzonemu postępowaniu. Pozostaje również temat nadzoru nad przeprowadzaniem inwigilacji przy użyciu Pegasusa – kto byłby za niego odpowiedzialny i jak miałby on w praktyce wyglądać. Mając na względzie dynamikę rozwoju cyberprzestępczości, z pewnością w najbliższym czasie uda się opracować odpowiednie aplikacje czy programy blokujące szpiegowskie oprogramowania bądź pozwalające na ich natychmiastowe usunięcie. Tyle że równolegle mogą powstawać kolejne programy pozwalające pozyskiwać dane z telefonów komórkowych obywateli, co doprowadziłoby do tzw. błędnego koła.

Podsumowując, organy państwa nie mogą za pomocą szpiegowskich oprogramowań gromadzić danych w celu ich potencjalnego użycia w przyszłości. Ponadto, biorąc pod uwagę już istniejące sposoby pozyskiwania i gromadzenia danych oraz kontroli obywateli (jak np. opisana powyżej kontrola operacyjna), wydaje się, że użycie szpiegowskich oprogramowań byłoby zbyt daleko ingerującym w konstytucyjne prawa i wolności obywatelskie środkiem. Niemniej temat ten wydaje się interesujący do dalszej dyskusji nad hipotetycznym użyciem systemów szpiegowskich w celu ochrony interesu i bezpieczeństwa państwa.

Słowa kluczowe: Pegasus, bezpieczeństwo państwa, prawo do prywatności, inwigilacja, cyberbezpieczeństwo.

Constitutional rights and freedoms in the face of new surveillance systems

Ubiquitous technological development and mass computerization necessarily affect not only the dailiness of the citizens but also the availability of new surveillance techniques. The dynamic development of these new technologies makes the legislation of countries seem to be lagging behind the introduction of appropriate legal regulations that would protect the fundamental rights and freedoms of citizens against unauthorized control. According to media reports, one of the surveillance systems – Pegasus was purchased by the Central Anticorruption Bureau. This software is extremely hard to detect by the user whose hardware has been infected. In addition, if Pegasus is found on the device, it is self-destructed and any traces of its presence are deleted. This means that the citizen may be controlled and does not know about it. Therefore, some doubts have arisen regarding the possible legal basis for the use of spying systems by the state authorities. The present article analyses the applicable legislation in the context of the hypothetical power of the authorities to control citizens by using systems such as Pegasus and indicates the risks that the use of Pegasus may cause. The author tries to value and compare the civil rights and freedoms guaranteed by the Constitution and international law with the interest and security of the state, which would be the basis for such control.

Keywords: Pegasus, national security, right to privacy, surveillance, cybersecurity.