KANCELARIA
SENATU

BIURO ANALIZ,
DOKUMENTACJI
I KORESPONDENCJI

Ocena legalności i skutków prawnych działań podejmowanych przy użyciu systemu Pegasus

Opinie
i ekspertyzy

OE–426

WARSZAWA 2022

Biuro Analiz, Dokumentacji i Korespondencji

Dyrektor – Agata Karwowska-Sokołowska
tel. 22 694 94 32, fax 22 694 94 28,
e-mail: Agata.Karwowska-Sokolowska@senat.gov.pl

Wicedyrektor – Danuta Antoszkiewicz
tel. 22 694 93 21,
e-mail: Danuta.Antoszkiewicz@senat.gov.pl

Dział Analiz i Opracowań Tematycznych
tel. 22 694 95 33, fax 22 694 94 28
Redaktor prowadzący – Urszula Luboińska

Opracowanie graficzno-techniczne
Centrum Informacyjne Senatu
Dział Wydawniczy

Kancelaria Senatu
wrzesień 2022

r.pr. dr hab. Mariusz Bidziński, prof. Uniwersytetu SWPS
SWPS Uniwersytet Humanistycznospołeczny w Warszawie

Ocena legalności i skutków prawnych działań podejmowanych przy użyciu systemu Pegasus

I. Źródła prawa

1. Konstytucja Rzeczypospolitej Polskiej z dn. 2 kwietnia 1997 r. (Dz. U. z 1997 r., nr 78, poz. 483 z późn. zm.);
2. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności, sporządzona w Rzymie dn. 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r., nr 61, poz. 284 z późn. zm.);
3. Ustawa z dn. 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2022 r., poz. 1360 t.j.);
4. Ustawa z dn. 6 kwietnia 1990 r. o Policji (Dz. U. z 2021 r., poz. 1882 z późn. zm.);
5. Ustawa z dn. 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2022 r., poz. 1138 z późn. zm.);
6. Ustawa z dn. 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2022 r., poz. 1375 t.j.);
7. Ustawa z dn. 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz. U. z 2021 r., poz. 289 z późn. zm.);
8. Ustawa z dn. 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2022 r., poz. 1900 z późn. zm.);
9. Ustawa z dn. 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2022 r., poz. 1634 z późn. zm.);
10. Ustawa z dn. 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2021 r., poz. 2234 z późn. zm.);
11. Uchwała Senatu Rzeczypospolitej Polskiej z dn. 12 stycznia 2022 r. w sprawie powołania Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych;

12. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 z późn. zm.);
13. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2022 r., poz. 557 z późn. zm.);
14. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2022 r., poz. 502 z późn. zm.);
15. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r., nr 159, poz. 948).

II. Skróty i akronimy

1. „CBA”	– Centralne Biuro Antykorupcyjne.
2. „EKPC”	– Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności.
3. „ETPC”	– Europejski Trybunał Praw Człowieka.
4. „k.c.”	– Ustawa z dn. 23 kwietnia 1964 r. Kodeks cywilny.
5. „k.k.”	– Ustawa z dn. 6 czerwca 1997 r. Kodeks karny.
6. „Konstytucja RP”	Konstytucja Rzeczypospolitej Polskiej z dn. 2 kwietnia 1997 r.
7. „k.p.k.”	– Ustawa z dn. 6 czerwca 1997 r. Kodeks postępowania karnego.
8. „Ustawa o CBA”	– Ustawa z dn. 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym.
9. u.o.i.n.	– ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
10. Ustawa o ABW	– Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.
11. Ustawa o SKW	– Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

III. Stan faktyczny

Pegasus to nazwa oprogramowania szpiegującego, możliwego do zainstalowania na urządzeniach elektronicznych korzystających z systemów iOS i Android (w tym zwłaszcza na telefonach komórkowych),

produkowanego przez izraelską spółkę NSO Group Technologies Ltd. Zainstalowanie oprogramowania na urządzeniu odbywa się zdalnie, bez świadomości użytkownika i otwiera podmiotowi infekującemu praktycznie nieograniczony dostęp do urządzenia, umożliwiając m.in.: dostęp do wiadomości e-mail oraz SMS-ów; śledzenie pozycji urządzenia (GPS); modyfikowanie ustawień technicznych urządzenia (w tym dostępu do sieci); dostęp do historii przeglądania stron internetowych, zapisanych kontaktów, sieci społecznościowych; wykonywanie połączeń telefonicznych; dokonywanie i przeglądanie wpisów w kalendarzu; pozyskiwanie plików z urządzenia (w tym usuniętych); instalowanie własnych oraz modyfikacja istniejących plików na urządzeniu; wysyłanie wiadomości; dostęp do aparatu i galerii urządzenia (w tym możliwość wykonywania zdjęć, filmów i zrzutów ekranu); nagrywanie dźwięku itp[1]. Innymi słowy, zainfekowanie urządzenia Pegasusem daje infekującemu praktycznie całkowitą kontrolę nad urządzeniem, z jego bieżącym używaniem oraz modyfikacją zapisanych w urządzeniu treści włącznie. Stosowanie Pegasusa jest niezależne od wiedzy i zgody operatorów telekomunikacyjnych czy internetowych[2].

Jednocześnie wskazuje się, że kontrolę nad oprogramowaniem posiada licencjodawca, tj. NSO Group Technologies Ltd. z siedzibą w Herclijji (Izrael), co wiąże się z dostępem tego podmiotu do danych gromadzonych i przetwarzanych przez oprogramowanie[3]. Dystrybucja licencji na Pegasusa jest reglamentowana przez Ministerstwo Obrony Izraela; licencja jest udzielana jedynie podmiotom państwowym[4]. Z uwagi na ofensywny charakter narzędzia (możliwość ingerencji w funkcjonowanie i zawartość zainfekowanego urządzenia), jest ono nazywane „bronią antyterrorystyczną".

Pegasus umożliwia m.in. pozyskiwanie danych przez pobieranie plików znajdujących się na urządzeniu, utrwalanie rozmów, uruchamianie mikrofonu/kamery bez aktywności użytkownika urządzenia czy odzyskiwanie danych usuniętych z urządzenia. Za pomocą Pegasusa można

---

1 B. Marczak, J. Scott-Railton, S. McKune, B. Abdul Razzak, R. Deibert, HIDE AND SEEK. Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries, 18 września 2018 r, https://citizenlab.ca/, dostęp w dn. 13 stycznia 2022 r.

2 J. Trela, Czy Pegasus może być legalny?, „Rzeczpospolita", 11 stycznia 2022 r.

3 tak A. Zoll w wywiadzie z D. Wysocką-Schnepf, Prof. Zoll: Pegasus? To zbrodnia szpiegostwa. Kamiński, Wąsik, Ziobro, Kaczyński - postawiłbym im ten zarzut, 29 grudnia 2021 r., https://wyborcza.pl/, dostęp w dn. 13 stycznia 2022 r.

4 J.A. Gross, Amid fallout from NSO scandal, Israel imposes new restrictions on cyber exports, 6 grudnia 2021 r., https://www.timesofisrael.com/, dostęp w dn. 17 stycznia 2021 r.

również stworzyć tzw. „zdalny pulpit" i w czasie rzeczywistym nadzorować treści wprowadzane na urządzeniu przez jego użytkownika.

IV. Analiza prawna

Zasady prowadzenia kontroli operacyjnej (w tym podsłuchu operacyjnego) regulują ustawy szczególne, w tym zwłaszcza pragmatyki służbowe. Wskazać można w tym zakresie np. na art. 17 ustawy o CBA, art. 19 ustawy z dn. 6 kwietnia 1990 r. o Policji czy art. 9 ustawy z dn. 10 czerwca 2016 r. o działaniach antyterrorystycznych. Ustawodawca przewidział zasadniczo pięć rodzajów kontroli operacyjnej, która może polegać na:

1. uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
2. uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
3. uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
4. uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;
5. uzyskiwaniu dostępu i kontroli zawartości przesyłek.

Wskazuje się, że „Stosowanie środków technicznych umożliwia uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych"[5]. Ustawy nie przewidują natomiast dopuszczalności przejmowania kontroli nad urządzeniem czy modyfikacji zapisanych w jego pamięci treści[6].

Uwzględniając konstytucyjne granice ingerencji w prawa jednostek (w tym zwłaszcza prawo do prywatności i prawa z nią związane), ustawowe ramy dla inwigilacji z jednej strony oraz możliwości techniczne i sposób funkcjonowania Pegasusa z drugiej, dojść należy do wniosku, że jego stosowanie jest na gruncie prawa polskiego niedopuszczalne.

Po pierwsze, Pegasus jako ofensywne narzędzie totalnej inwigilacji, nie wpisuje się w ramy istniejących instytucji procesowych.

5 S. Hoc, P. Szustakiewicz, ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz, LEX/el. 2012, komentarz do art. 17 ustawy o CBA, pkt 5.

6 co do uzyskiwania i utrwalania danych zawartych na nośnikach danych por. szerzej M. Gabriel-Węglowski, Działania antyterrorystyczne. Komentarz, Warszawa 2018, komentarz do art. 9 ustawy o działaniach antyterrorystycznych, pkt. 22–29.

Zainfekowanie urządzenia takim oprogramowaniem skutkuje uzyskaniem przez infekującego nie tylko pełnego dostępu do wszystkich danych znajdujących się na urządzeniu, ale również możliwości kontroli urządzenia, w tym zmiany zawartości pamięci urządzenia. Przepisy ustaw (tj. art. 237 i 241 k.p.k. oraz przepisy ustaw szczególnych) zawierają katalogi dopuszczalnych czynności operacyjnych (kontrola i utrwalanie rozmów, uzyskiwanie i utrwalanie treści korespondencji itd.), natomiast nie wskazują na konkretne środki służące do realizacji tych czynności (np. poprzez wskazanie technicznej metody podsłuchu). Nie ulega przy tym wątpliwości, że wyrażenie przez właściwy organ zgody na daną czynność stanowi upoważnienie tylko i wyłącznie do realizowania jej przy pomocy środków adekwatnych. Dopuszczalne jest stosowanie tylko takich środków, które nie prowadzą do dalszej ingerencji w prawa jednostki, niż jest to niezbędne do osiągnięcia zamierzonego celu (reguła instrumentalnego nakazu). Ani przepisy k.p.k., ani ustaw szczególnych, nie dają organom państwa uprawnienia do ingerencji w zawartość urządzeń ani możliwości przejmowania nad nimi kontroli, albowiem celem inwigilacji procesowej jest uzyskanie określonych informacji (danych) – i to w formie możliwie nieinwazyjnej, a nie kreowanie, zmiana albo usuwanie danych. Z tego wszakże względu, Pegasus traktowany jest nie jako narzędzie operacyjne (do zbierania danych o przestępstwach), ale jako broń (narzędzie do wpływania na postępowanie przestępców i podmiotów wrogich). Fakt ten powoduje, że niezależnie od kwestii dopuszczalności stosowania Pegasusa w świetle konstytucji i EKPC (o czym dalej), nie ma prawnej możliwości realizowania przy jego pomocy ani kontroli przewidzianej w art. 237-242 k.p.k., ani kontroli operacyjnej przewidzianej w ustawach szczególnych (w tym zwłaszcza art. 17 ustawy o CBA).

O ile uzyskiwanie zgód pierwotnych nadal regulują procedury zawarte w ustawach szczególnych (określające także katalog przestępstw, co do których taką zgodę można uzyskać), o tyle decyzję w przedmiocie wykorzystania materiałów nieobjętych zgodą pierwotną podejmuje z mocy art. 168b prokurator.

Sąd Apelacyjny w Katowicach stwierdził, że zważywszy na zawarty w art. 237 § 3 k.p.k. zamknięty katalog przestępstw, konsekwencje przyjęcia uregulowania przepisu art. 237a k.p.k. mogą polegać wyłącznie na tym, iż decyzja prokuratora, o której mowa w cytowanym przepisie, odnosi się do postępowania przygotowawczego i w żadnym razie nie wiąże sądu. W konsekwencji wniosek o przeprowadzenie dowodu z informacji uzyskanej poza granicami ustawowymi kontroli i utrwalania rozmów telefonicznych powinien być przez sąd oddalony, względnie dowody te

nie powinny stanowić podstawy wyrokowania, jako niemające cechy legalności. Jedyna, pozostająca w zgodzie z gwarancyjnym charakterem przepisu art. 237 § 3 k.p.k. oraz regułami rzetelnego procesu karnego, interpretacja normy wynikającej z art. 237a k.p.k. jest taka, że prokurator, uzyskując wymienione wyżej informacje, może podjąć decyzję o ich wykorzystaniu w celu poszukiwania innych, legalnych dowodów, potwierdzających posiadane informacje, a więc mogą one stanowić podstawę dalszych czynności dowodowych, a nie je zastępować (wyrok Sądu Apelacyjnego w Katowicach z dnia 4 listopada 2017 r. II AKa 263/17).

Dowodami uzyskanymi w wyniku kontroli operacyjnej zarządzonej postanowieniem sądu wydanym na podstawie art. 17 ust. 1 i 2 ustawy o CBA, które pozwalają na wszczęcie postępowania karnego lub mają znaczenie dla toczącego się postępowania karnego (art. 17 ust. 15 ustawy o CBA), są jedynie dowody dotyczące przestępstw określonych w jej art. 17 ust. 1, które zostały wskazane w postanowieniu o zastosowaniu kontroli operacyjnej lub w postanowieniu o udzieleniu tzw. zgody następczej, w tym wydanej także w toku kontroli operacyjnej (art. 17 ust. 3 ustawy o CBA), a popełnionych przez osobę, której dotyczyła zgoda pierwotna, i osobę, co do której wydano zgodę następczą (por. uchwała SN (7) z 23 marca 2011 r., I KZP 32/10).

Co więcej, obowiązujące przepisy prawa nie pozwalają żadnemu z organów państwowych na przełamywanie zabezpieczeń (*hacking*) i przechwytywanie oraz wykorzystywanie treści przekazów komunikacyjnych[7]. Potwierdza to fakt, że **na gruncie obecnie obowiązujących regulacji stosowania kontroli sądowej oraz operacyjnej, stosowanie Pegasusa nie może mieć miejsca.**

Należy jednocześnie podkreślić, że włamanie się do urządzenia przy użyciu Pegasusa wiąże się z ingerencją w strukturę danych urządzenia. W połączeniu z możliwością niekontrolowanej ingerencji w funkcjonowanie i pamięć urządzenia (a zatem możliwość zmiany treści utrwalonych na nim plików oraz wykonywania wszelkiego rodzaju czynności bez zgody i wiedzy użytkownika telefonu), wartość dowodowa danych pozyskanych przy pomocy Pegasusa jest znikoma, jeżeli nie zerowa. Nigdy bowiem nie ma pewności, że zawartość urządzenia nie została zmodyfikowana przez organ stosujący Pegasusa na niekorzyść podmiotu inwigilowanego. Również ten aspekt funkcjonowania systemu wyłącza dopuszczalność jego stosowania **– z uwagi na nieprzydatność na gruncie procesowym.**

7 tak Rzecznik Praw Obywatelskich w wystąpieniu z dn. 9 września 2019 r. o znaku VII.519.2.2019.AG, s. 4.

W kontekście powyższego należy ponadto zasygnalizować, że zgoda sądu na podjęcie określonych czynności operacyjnych **nie oznacza zgody** na wykorzystanie przez inwigilującego dowolnych środków technicznych, w tym Pegasusa, choćby nawet podmiot zamierzający go stosować poinformował o tym sąd. Jak zostało wyżej wskazane, sąd nie posiada kompetencji do legalizowania stosowania środków, których stosowanie w świetle prawa jest niedopuszczalne (czy to generalnie, czy też w indywidualnym przypadku). W konsekwencji, nawet wydanie przez sąd zgody na przeprowadzenie kontroli procesowej lub operacyjnej w określony sposób i przy wykorzystaniu określonych środków technicznych nie prowadzi do dekryminalizacji zastosowania Pegasusa.

W ocenie Eksperta, stosowanie Pegasusa jest nie do pogodzenia z wartościami wyrażonymi w art. 47, art. 49 i art. 51 ust. 2 Konstytucji RP oraz art. 8 EKPC, albowiem stanowi zbyt daleko idącą, rażąco nieproporcjonalną ingerencję w prawa jednostek. Jakkolwiek na gruncie Konstytucji RP jest dopuszczalne nawet daleko idące ograniczenie prawa do prywatności oraz tajemnicy komunikacji, to ingerencja ta nie może godzić w istotę tych praw. Zainfekowanie urządzenia Pegasusem sprawia, że służby uzyskują całkowitą kontrolę nad urządzeniem, co przy roli telefonów komórkowych oznacza praktycznie przejęcie kontroli nad życiem prywatnym (możliwość dostępu do wszystkich zalogowanych serwisów, dokonywania dyspozycji majątkowych, korespondowania z innymi ludźmi pod przykrywką użytkownika telefonu, podsłuchiwania i podglądania w każdym czasie i miejscu itd.; w istocie: kradzież tożsamości). Jest to nie tylko naruszenie prywatności w wymiarze powzięcia wiedzy o życiu prywatnym, ale również w wymiarze nieuświadomionej inwigilowanemu najgłębszej ingerencji w jego życie osobiste. Tak głęboka ingerencja w sferę prywatności (a nawet głębiej: intymności) człowieka narusza istotę prawa wyrażonego w art. 47 Konstytucji RP oraz narusza przyrodzoną godność człowieka (art. 30 Konstytucji RP), albowiem czyni człowieka jedynie instrumentem w urzeczywistnianiu celów organu władzy[8].

Wobec wykorzystywania omawianego oprogramowania bez podstawy prawnej nie da się prawidłowo przeprowadzić testu proporcjonalności. Przyjmując nawet założenie, że potencjalnym uzasadnieniem dla inwigilacji może być chęć zagwarantowania zewnętrznego lub wewnętrznego bezpieczeństwa państwa oraz zapobieżenia przestępstwom, to ochrona tych wartości ma przecież swoje granice. Totalna inwigilacja,

8 por. wyrok Trybunału Konstytucyjnego z dn. 9 lipca 2009 r., sygn. SK 48/05, OTK-ZU 2009 r., seria „A", nr 7, poz. 108.

połączona z możliwością niejawnego wpływania na życie inwigilowanego (sterowania nim), charakteryzuje państwa totalitarne i nie może być stosowana w państwach demokratycznych. Takie działanie nie służy bowiem ochronie obywateli oraz ich godności, która stanowi źródło innych praw podmiotowych, ale służy ochronie aparatu państwowego przed samymi obywatelami.

Kontrola operacyjna, w toku której używany jest program komputerowy niedopuszczalny z punktu widzenia polskiego ustawodawstwa, nie może prowadzić do zdobycia materiałów mogących stanowić dowód w sprawie. Dowód uzyskany przez funkcjonariusza publicznego z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego jest dowodem niedopuszczalnym i jako taki nie może zostać wykorzystany w procesie karnym. Charakter, właściwości i możliwości Pegasusa, które pozwalają na większą ingerencję w urządzenie niż posiada jego aktualny użytkownik uniemożliwiają zdobycie wiarygodnych dowodów. Dlatego też, materiały zdobyte przy użyciu Pegasusa nie powinny być dopuszczalne na gruncie polskiego prawa jako dowody. Gromadzenie materiału dowodowego nie może polegać na zbieraniu wszelkich informacji dotyczących zjawisk i zdarzeń, a jedynie tych, które winny być przedmiotem postępowania, czyli mają prawne znaczenie dla rozstrzygnięcia, a w konsekwencji udowodnienia zajścia przesłanek wskazanych w normie prawnej będącej jego podstawą prawną.

Jak zostało wyżej wskazane, Pegasus nie jest uznawany za narzędzie kontroli operacyjnej, ale jako broń cybernetyczna w walce z zagrożeniami dla bezpieczeństwa kraju. Uzyskane przy użyciu Pegasusa dane chronione są na mocy ustawy o ochronie informacji niejawnych – u.o.i-.n. Dane te nie mogą być bez podstawy prawnej przekazywane osobom trzecim, podmiotom nieuprawnionym do dostępu czy przetwarzania informacji do których zastosowanie znajdzie klauzula tajności. Czynności operacyjno-rozpoznawcze i powzięte w ich wyniku informacje są informacjami niejawnymi w rozumieniu u.o.i.n. Ma to stanowić gwarancję dla obywatela by dane jego dotyczące, nierzadko będące danymi wrażliwymi, dot. intymnej sfery jego życia prywatnego, nie były dostępne dla szerokiego grona podmiotów.

Oprogramowanie służące do wykonywania czynności operacyjno-rozpoznawczych i sprawowania kontroli operacyjnej powinny spełniać wymogi bezpieczeństwa informatycznego, tak, by zagwarantować poufność zdobywanych w ten sposób informacji. Artykuł 48 u.o.i.n. stanowi, że systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne podlegają akredytacji bezpieczeństwa teleinformatycznego. Akredytacja bezpieczeństwa informatycznego to dopuszczenie

danego systemu do przetwarzania informacji niejawnych. Certyfikacja zaś to proces potwierdzenia zdolności danego urządzenia lub innego środka do ochrony informacji niejawnych. Akredytacji i certyfikacji udziela ABW albo SKW. By legalnie udzielić akredytacji bezpieczeństwa ABW bądź SKW musi dysponować kompletną dokumentacją bezpieczeństwa systemu teleinformatycznego.

Na podstawie delegacji ustawowej zawartej w art. 49 ust. 9 u.o.i.n. Prezes Rady Ministrów wydał rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego. Rozporządzenie to określa i definiuje integralność informacji niejawnych jako właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony.

System służący do kontroli operacyjnej powinien gwarantować, że informacje uzyskane przy jego pomocy nie będą udostępniane podmiotom nieuprawnionym. Ponadto, powinien zapewniać integralność pozyskanych danych, by mieć pewność, że nie zostały one w jakikolwiek sposób zmodyfikowane.

Z uwagi na właściwości i możliwości Pegasusa brak jest gwarancji, że pobrane dane nie zostały zmodyfikowane. Co więcej, sposób transmisji danych wskazuje na używanie niekontrolowanych, bądź z istoty niemożliwych do skontrolowania, kanałów transmisji danych co godzi w zasady poufności i integralności danych. Z tych przyczyn, Pegasus nie może legalnie uzyskać świadectwa akredytacji i certyfikacji bezpieczeństwa informatycznego. Nie zapewnia bowiem podstawowych wymagań bezpieczeństwa teleinformatycznego związanego z ochroną informacji niejawnych. Za niezgodne z polskimi przepisami należy zatem uznać stosowanie programów niekontrolowanych przez polskie służby. Czynności operacyjno-rozpoznawcze podejmowane przy udziale systemów, które nie zapewniają bezpieczeństwa, poufności i integralności informacji niejawnych są niedopuszczalne.

Przechodząc do oceny, czy stosowanie Pegasusa może być objęte kontratypem ustawowym, należy zwrócić uwagę na kilka okoliczności. Zachowanie realizujące znamiona typu czynu zabronionego podjęte w sytuacji kontratypowej oznacza typowe, z punktu widzenia celu ustanowienia danej normy, naruszenie nakazu lub zakazu wynikającego z tej normy, prowadzące do naruszenia lub narażenia chronionego tą normą dobra prawnego. Jednak takie zachowanie nie może zostać uznane za bezprawne z uwagi na charakterystyczne dla sytuacji kontratypowej usprawiedliwienie dla naruszenia tej normy. Kontratyp jest okolicznością legalizują działanie bezprawne.

Zgodnie z art. 32a ust. 7-9 Ustawy o ABW:

7. ABW może wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b Kodeksu karnego, oraz ich używać w celu określenia podatności ocenianego systemu na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a Kodeksu karnego.

8. Używając urządzeń lub programów komputerowych, o których mowa w ust. 7, ABW może uzyskać dostęp do informacji dla niej nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, lub może uzyskać dostęp do całości lub części systemu teleinformatycznego.

9. Informacje uzyskane przez ABW w wyniku przeprowadzania oceny bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych ABW oraz podlegają one niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

Powyższe uregulowania pozwalałyby ABW na korzystanie z programu Pegasus, ale tylko i wyłączenie dla „określenia podatności ocenianego systemu na możliwość popełnienia przestępstw". Warto dodać, że ocenie tej podlegają jedynie systemy teleinformatyczne organów administracji publicznej i infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Przepisy te nie pozwalają na używanie programu Pegasus w jakimkolwiek innym zakresie. ABW może korzystać z Pegasusa w tej jednej, ściśle prawem określonej sytuacji, tylko po to, by ocenić podatność i bezpieczeństwo systemów informatycznych na ataki z zewnątrz stanowiące przestępstwa. Używanie programu Pegasus do łamania/omijania zabezpieczeń systemów informatycznych innych niż należących do administracji publicznej czy infrastruktury krytycznej nie jest legalne.

Kontrola operacyjna, podobnie jak podsłuch procesowy, wymaga uzyskania postanowienia sądu o zarządzeniu kontroli (albo zarządzenia następczego, zatwierdzającego kontrolę przeprowadzoną w warunkach niecierpiących zwłoki) i może być prowadzona przez daną służbę jedynie w związku z określonymi w danej ustawie przestępstwami. Kontrola ma zawsze charakter subsydiarny, co oznacza, że może być zarządzona tylko wtedy, gdy inne środki okazały się bezskuteczne lub są nieprzydatne (M. Rogalski, *Podsłuch procesowy i pozaprocesowy. Kontrola i utrwalanie rozmów na podstawie kpk oraz ustaw szczególnych*, Warszawa 2019, LEX/el., rozdział III, pkt 2).

Trybunał Konstytucyjny w wyroku z dn. 30 lipca 2014 r. o sygn. K 23/11 (OTK-ZU 2014 r., seria „A", nr 7, poz. 80) wskazał, że przy stosowaniu środków kontroli operacyjnej, niezbędna jest ich indywidualizacja,

albowiem organy mogą stosować jedynie te środki, które są prawnie dopuszczalne. W kontekście tej wypowiedzi Trybunału należy zauważyć, że o ile sądy powinny kontrolować środki techniczne, które zamierzają wykorzystywać służby, to ustawy nie przyznają im kompetencji do legalizowania stosowania środków technicznych, których stosowanie jest generalnie albo w danych warunkach niedopuszczalne.

Wniosek o zastosowanie kontroli operacyjnej powinien zawierać wskazanie miejsca, sposobu i rodzaju przeprowadzanej kontroli. Należy w nim zawrzeć dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana jest kontrola operacyjna (art. 9 ust. 7 Ustawy o Policji). Należy zatem stwierdzić, że wniosek o zastosowanie kontroli operacyjnej powinien zawierać wskazanie sposobu stosowania konkretnego rodzaju, czy też konkretnych rodzajów kontroli. Co z kolei implikuje obowiązek wskazania środków technicznych służących przeprowadzaniu kontroli operacyjnej (art. 17 ust. 5 Ustawy o CBA). Sąd decydujący o zarządzeniu kontroli operacyjnej musi mieć możliwość weryfikacji czy urządzenia techniczne temu celowi służące są w ogóle dopuszczalne. W przeciwnym wypadku zgoda na kontrolę operacyjną jest blankietowa, jest jedynie formalnością. Przy czym środki kontroli operacyjnej powinny być określone przepisami i powinny zostać konkretnie wskazane we wniosku o kontrolę operacyjną. I najważniejsze, wniosek ten powinien zawierać takie informacje co do środka kontroli, które umożliwią sądowi rzeczywistą weryfikację, czy środek ten jest dopuszczalny na gruncie polskiego prawa i czy spełnia wymogi celowości, konieczności i proporcjonalności wkroczenia w prawa i wolności obywatelskie.

Zgodnie z art. 6 ust. 1 ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze (dalej: p.o.a.) adwokat zobowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej. Ustawa określająca ramy ustrojowe adwokatury, w tym statuująca kardynalne zasady jej funkcjonowania, formułuje bezwzględny nakaz dochowania tajemnicy zawodowej. Przepis ten ustanawia bezpośrednią i bezwzględną ochronę tajemnicy adwokackiej. Identycznie brzmiące postanowienia co do tajemnicy radcowskiej i jej ochrony zawiera ustawa z dnia 6 lipca 1982 r. o radcach prawnych.

Zgodnie z § 19 ust. 2 i ust. 3 Kodeksu Etyki Adwokackiej tajemnicą adwokacką objęte są materiały znajdujące się w aktach adwokackich, a ponadto wszystkie wiadomości, notatki i dokumenty dotyczące sprawy uzyskane od klienta oraz innych osób, niezależnie od miejsca, w którym się znajdują. Podobne uregulowania znajdują się w Kodeksie Etyki Radcy Prawnego, gdzie wskazuje się wprost, że tajemnica zawodowa stanowi

podstawę zaufania klienta i jest gwarancją praw i wolności. Tajemnice te są nieograniczone w czasie i obowiązują nawet po zaprzestaniu wykonywania zawodu adwokata czy radcy prawnego.

Zgodnie z przepisem art. 180 § 2 k.p.k. osoby zobowiązane do zachowania tajemnicy adwokackiej mogą być przesłuchane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. W postępowaniu przygotowawczym w przedmiocie przesłuchania lub zezwolenia na przesłuchanie stosowną decyzję wydaje sąd, na posiedzeniu bez udziału stron, w terminie nie dłuższym niż 7 dni od daty doręczenia wniosku prokuratora. Na postanowienie to służy zażalenie. Zakaz przesłuchania adwokata na okoliczności objęte tajemnicą zawodową ma więc w świetle przepisów Kodeksu postępowania karnego charakter względny, gdyż możliwe jest zwolnienie z obowiązku zachowania tego rodzaju tajemnicy przy kumulatywnym spełnieniu ww. przesłanek.

Szczególnym rodzajem tajemnicy zawodowej jest tajemnica obrończa. W postępowaniu karnym podlega ona pełnej ochronie, a jej zakres obejmuje wszelkie informacje istotne dla obrony oskarżonego, uzyskane przez adwokata/radcę prawnego działającego w charakterze obrońcy. Wiedza obrońcy dotycząca sprawy jest tajemnicą dla organów prowadzących postępowanie karne. Dysponuje nią sam obrońca, w porozumieniu z oskarżonym i na jego korzyść. Tajemnica obrończa równa jest tajemnicy spowiedzi (art. 178 k.p.k.).

Organy procesowe nie są uprawnione do uzyskiwania tej wiedzy od obrońcy środkami przewidzianymi w procedurze karnej. Wyraża się to w obowiązywaniu bezwzględnego zakazu przesłuchiwania jako świadków obrońcy lub adwokata/radcy prawnego działającego na podstawie art. 245 § 1 k.p.k., co do faktów, o których dowiedział się on udzielając porady prawnej lub prowadząc sprawę (art. 178 pkt 1 k.p.k.). Obrońca jest też poza kręgiem osób, wobec których dopuszcza się kontrolę i utrwalanie rozmów (art. 237 § 4 k.p.k.). Z tych samych względów w toku przeszukania nie wolno zatrzymać pism lub innych dokumentów obejmujących okoliczności związane z wykonywaniem funkcji obrońcy, niezależnie od tego czy wykonuje on tę funkcję w sprawie, której dotyczy przeszukanie, czy w innej, przy czym samo oświadczenie obrońcy o takim charakterze dokumentów jest wiążące dla organu dokonującego przeszukania.

Z samej natury tajemnicy obrończej wynika, że jako taka nie podlega weryfikacji przez organ prowadzący postępowanie, bądź wykonujący zleconą mu czynność procesową. Żadne środki procesowe nie mogą wyłączać ani ograniczać gwarancji ścisłej ochrony tajemnicy obrończej.

Dla zawodu zaufania publicznego – adwokata czy radcy prawnego – ale także i przede wszystkim dla obywateli, których osoby wykonujące te zawód reprezentują, tajemnica adwokacka/radcowska i obrończa jest fundamentalna. Zapewnia ona obywatelom, klientom ochronę ich praw, poszanowanie do prywatności i realne prawo do sądu oraz stanowi podstawę dla zapewnienia rzetelnego procesu i prawa do obrony. Próby inwigilacji pełnomocników czy obrońców godzą w podstawowe zasady państwa prawa, podważają wiarygodność wymiaru sprawiedliwości i skutkują erozją zaufania obywateli do państwa. Tajemnica obrończa, adwokacka czy radcowska nie istnieją dla potrzeb adwokata czy radcy prawnego. Tajemnice te powstały w interesie klientów, zapewniają obywatelem gwarancję, że nie dojdzie do naruszenia ich praw i wolności zapewnionych w Konstytucji.

Oczywiste jest przy tym, że z uwagi na postęp techniki, adwokaci i radcowie prawni szeroko korzystają z urządzeń teleinformatycznych, telefonów i komputerów z dostępem do Internetu. Nie budzi wątpliwości, że na tych nośnikach znajdują się również dane dotyczące obywateli, których reprezentują, które to dane objęte są tajemnicami zawodowymi adwokata lub radcy prawnego bądź też tajemnicą obrończą. Pozyskiwanie tych danych – nawet bez użycia Pegasusa – jest bezwzględnie niedopuszczalne w demokratycznym państwie prawa. Z punktu widzenia kodeksu postępowania karnego jest nielegalne i narusza szereg praw i wolności konstytucyjnych: art. 47 Konstytucji (prawo do poszanowania prywatności), art. 49 Konstytucji (prawo do tajemnicy korespondencji), art. 51 Konstytucji (prawo do ochrony danych osobowych), art. 42 Konstytucji (prawo do obrony), art. 45 ust. 1 Konstytucji (prawo do sprawiedliwego procesu).

Z uwagi na wskazaną wyżej generalną niedopuszczalność stosowania systemu Pegasus na gruncie prawa polskiego, posługiwanie się nim nawet dla realizacji celów prawnie dozwolonych (kontroli operacyjnej) jest niedopuszczalne. Jak zostało bowiem wyjaśnione, realizacja celów prawnie dozwolonych może następować jedynie przy wykorzystaniu legalnych środków. W konsekwencji, każde stosowanie systemu Pegasus dla celów określonych w k.p.k. i ustawach szczególnych stanowić będzie działanie penalizowane.

Artykuł 267 k.k. stanowi:

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej

zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Zgodnie z § 4 omawianego artykułu, karze podlega również ten, kto ujawnia informację uzyskaną w warunkach §§ 1-3 innej osobie. Z uwagi na sposób funkcjonowania systemu Pegasus, który wymaga zaangażowania podmiotu trzeciego (dostawcy systemu – NSO Group Technologies Ltd. albo podmiotów przez niego upoważnionych), z wysokim prawdopodobieństwem można przyjąć, że informacje pozyskiwane w drodze stosowania Pegasusa są przynajmniej częściowo przetwarzane przez osoby trzecie, w tym zwłaszcza zagraniczną spółkę prawa handlowego. Takie działanie kwalifikować należy jako ujawnienie pozyskanej nielegalnie informacji innej osobie, co wypełnia znamiona czynu opisanego w omawianym przepisie.

Stosownie do treści art. 130 § 2 k.k., *„Kto, biorąc udział w obcym wywiadzie albo działając na jego rzecz, udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 3”*. Jak zostało wyżej wskazane, ze stosowaniem oprogramowania Pegasus immanentnie wiąże się zautomatyzowane przetwarzanie przynajmniej części pozyskiwanych za pomocą oprogramowania danych przez podmiot zewnętrzny, tj. NSO Group Technologies Ltd., przy czym kontrolę nad udzielaniem licencji podmiotom zagranicznym posiada Ministerstwo Obrony Izraela. W takiej sytuacji, z wysokim prawdopodobieństwem można przyjąć, że dostęp do przetwarzanych informacji posiadają również służby specjalne państwa Izrael. Korzystanie z Pegasusa prowadzić musi zatem do automatycznego udzielania obcemu wywiadowi informacji, pośród których mogą być dane, których przekazanie może – choćby teoretycznie – wyrządzić szkodę Rzeczypospolitej Polskiej. Będzie tak np. w sytuacji, gdy obcy wywiad uzyska dostęp do informacji niejawnych, do których dostęp posiada poseł (senator), adwokat czy prokurator, w szczególności wiążących się z prowadzoną

kampanią wyborczą czy postępowaniami (karnymi, administracyjnymi, a nawet – cywilnymi) z udziałem osób piastujących funkcje w organach władzy publicznej. Wykorzystanie takich informacji przez obcy wywiad ze szkodą dla Rzeczypospolitej Polskiej jest nie tylko oczywiście możliwe, alerównież wysoce prawdopodobne. Jednocześnie, osoby wykorzystujące Pegasusa muszą mieć świadomość mechanizmu działania narzędzia oraz co najmniej wysokiego prawdopodobieństwa posiadania dostępu do pozyskiwanych danych przez służby specjalne obcego państwa, przez co korzystanie z Pegasusa kwalifikować należy jako „działanie na rzecz" obcego wywiadu w rozumieniu przywołanego przepisu. W konsekwencji, nie można obecnie wykluczyć, że osoby dokonujące kontroli operacyjnej przy pomocy oprogramowania Pegasus dopuścić się mogły zbrodni szpiegostwa. W obecnie obowiązującym stanie prawnym, żaden organ nie ma prawa włamywać się, przechwytywać, tworzyć, modyfikować i legalnie wykorzystywać treści w ten sposób zdobytych, nawet w ramach kontroli operacyjnej.

V. Konkluzje

1. Zgodnie z orzecznictwem Trybunału Konstytucyjnego, ograniczenie praw i wolności jednostki w drodze kontroli operacyjnej może nastąpić tylko w przypadku, gdy istnieje ku temu precyzyjna podstawa ustawowa, ingerencja jest konieczna w demokratycznym państwie prawnym, zaś cel ingerencji stanowi istotną wartość konstytucyjną.
2. Oprogramowanie Pegasus umożliwia inwigilującemu pełny (totalny) dostęp do urządzenia elektronicznego (telefonu) osoby inwigilowanej, w tym m. in. na podsłuchiwanie rozmów, ingerencję w wiadomości, modyfikowanie, usuwanie i dodawanie plików w pamięci urządzenia, zmianę ustawień technicznych itp.
3. Stosowanie Pegasusa jest na gruncie prawa polskiego niedopuszczalne z racji, iż umożliwia niekontrolowany dostęp do sfery intymnej człowieka, przyznając inwigilującemu możliwość niejawnego wpływania na tok życia inwigilowanego, w tym kradzież jego tożsamości.
4. Agencja Bezpieczeństwa Wewnętrznego może skorzystać z pegasusa (zakładając jego uprzednie legalne pozyskanie) tylko i wyłączenie dla „określenia podatności ocenianego systemu na możliwość popełnienia przestępstw". Ocenie tej podlegają jedynie systemy teleinformatyczne organów administracji publicznej i infrastruktury krytycznej (art. 32a ust. 7-9 Ustawy o ABW).

5. Używanie Pegasus do łamania/omijania zabezpieczeń systemów informatycznych innych niż należących do administracji publicznej czy infrastruktury krytycznej nie jest legalne.
6. Pozyskanie materiałów dowodowych na skutek bezprawnej i nielegalnej kontroli operacyjnej wyklucza użycie ich za dowód w postępowaniu sądowym.
7. Legalnie prowadzona kontrola operacyjna może jedynie utrwalać i pozyskiwać dane znajdujące się w systemie informatycznych przed podjęciem kontroli operacyjnej.
8. Wniosek o kontrolę operacyjną musi zawierać takie informacje co do środka kontroli, które umożliwią sądowi rzeczywistą weryfikację czy środek ten jest dopuszczalny na gruncie polskiego prawa i czy spełnia wymogi celowości, konieczności i proporcjonalności wkroczenia w prawa i wolności obywatelskie.
9. Materiały pozyskane systemem Pegasus nie mogą stanowić dowodu w postępowaniu karnym ze względu na szeroką możliwość ingerencji przy użyciu Pegasusa w treść tychże dowodów oraz brak legalności stosowania tego oprogramowania na gruncie polskiego systemu prawnego.
10. Brak możliwości ustalenia czy dowody zgromadzone przy użyciu Pegasusa zostały zmodyfikowane w jakikolwiek sposób uniemożliwia wykorzystywanie ich w sprawiedliwym procesie.
11. Wykorzystywanie dowodów pozyskanych przy użyciu Pegasusa stanowi naruszenie art. 45 Konstytucji jak i art. 6 ust. 1 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Pozyskane w ten sposób materiały nie mogą stanowić dowodu, pozwalającego na poczynienie prawdziwych ustaleń faktycznych niezbędnych do wydania sprawiedliwego wyroku.
12. Pozyskiwanie w ramach kontroli operacyjnych danych z urządzenia utrwalonych przed czasem popełnienia przestępstwa (na skutek którego zarządzono kontrolę operacyjną) jest niedopuszczalne i wykracza poza granice obowiązujących norm prawnych.
13. Wykorzystywanie systemu Pegasus w zakresie inwigilacji i zbierania dowodów jest niedopuszczalne i stanowi wprost naruszenie praw i wolności obywatelskich określonych w Konstytucji.
14. Wyrażenie przez sąd zgody na zastosowanie kontroli operacyjnej przy użyciu Pegasusa (w braku świadomości sądu co do sposobów i narzędzi służących do kontroli operacyjnej) nie może prowadzić do zalegalizowania używania Pegasusa.

15. Dowody zdobyte w sposób sprzeczny z procedurami i w sposób naruszający tajemnicę adwokacką/radcowską i obrończą skutkują niemożliwością ich legalnego użycia.
16. Kontrola operacyjna realizowana przy pomocy Pegasusa polegająca na przejęciu kontroli nad urządzeniem teleinformatycznym i umożliwiająca m.in. sterowanie sprzętem informatycznym, uruchomienie aplikacji, mikrofonu czy aparatu jak i ingerowanie w treść zgromadzonych w urządzeniu danych jest nielegalna.
17. W systemie prawnym Rzeczpospolitej Polskiej stosowanie Pegasusa nie jest dopuszczalne. Brak jest jakichkolwiek ram ustawowych, które pozwalałyby służbom na prowadzenie działań operacyjnych połączonych z przełamywaniem zabezpieczeń i uzyskiwaniem kontroli nad urządzeniem elektronicznym.
18. Uregulowana w k.p.k. instytucja podsłuchu sądowego oraz warianty uregulowanej w ustawach szczególnych kontroli operacyjnej pozwalają jedynie na kontrolowanie i rejestrowanie – od chwili uzyskania sądowej zgody – rozmów i korespondencji inwigilowanych oraz kopiowanie zawartości nośników danych. Zakres ingerencji systemu Pegasus wykracza poza jakiekolwiek znane w polskim systemie prawnym normy.
19. Wobec braku ram ustawowych dla legalnego stosowania Pegasusa, każde jego wykorzystanie przez funkcjonariuszy organów państwa klasyfikować należy jako przekroczenie uprawnień ze szkodą dla interesu publicznego i prywatnego, co stanowi czyn opisany w art. 231 § 1 k.k.
20. Stosowanie Pegasusa wypełnia znamiona przestępstw opisanych w art. 267 §§ 1-3 k.k. (nieuprawnione uzyskiwanie dostępu do informacji, systemu informatycznego oraz posługiwanie się urządzeniem podsłuchowym).
21. Z uwagi na fakt, że wykorzystywanie Pegasusa związane jest z przetwarzaniem przynajmniej części pozyskiwanych danych przez podmiot zewnętrzny (administratora systemu i licencjodawcę – NSO Group Technologies Ltd.), stanowi to czyn opisany w art. 267 § 4 k.k.
22. Eksport licencji na Pegasusa podlega kontroli Ministerstwa Obrony Izraela, co wskazuje na bardzo wysokie prawdopodobieństwo, że dostęp do pozyskiwanych przez użytkowników oprogramowania danych posiadają służby specjalne tego państwa. Fakt ten może wypełniać znamiona zbrodni szpiegostwa (art. 130 § 2 k.k.), poprzez działanie na rzecz obcego wywiadu, polegające na zbieraniu i przekazywaniu danych istotnych z punktu widzenia bezpieczeństwa Rzeczypospolitej Polskiej.

23. Pegasus nie może legalnie uzyskać świadectwa akredytacji i certyfikacji bezpieczeństwa informatycznego. Nie zapewnia podstawowych wymagań bezpieczeństwa teleinformatycznego związanych z ochroną informacji niejawnych.
24. Za niezgodne z polskimi przepisami należy uznać stosowanie programów niekontrolowanych przez polskie służby. Czynności operacyjno-rozpoznawcze podejmowane przy udziale systemów, które nie zapewniają bezpieczeństwa, poufności i integralności informacji niejawnych są niedopuszczalne.