Krakowski Instytut Prawa Karnego Fundacja

dr hab. Agnieszka Barczak-Oplustil

dr hab. Mikołaj Małecki

dr hab. Szymon Tarapata

dr Adam Behan

dr Witold Zontek

Katedra Prawa Karnego
Uniwersytet Jagielloński

Kraków, 15.02.2022 r.

Ekspertyza

Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasusa)

Wnioski

1. **Użycie systemów teleinformatycznych, których integralną częścią są programy komputerowe, pozwalające utrwalać, bez wiedzy i zgody użytkownika, prowadzone rozmowy telefoniczne oraz pobierać wiadomości SMS/MMS oraz wiadomości z komunikatorów używanych przez osobę poddaną kontroli operacyjnej, w tym wiadomości wysyłane i otrzymywane przed datą rozpoczęcia kontroli operacyjnej, jest zgodne z przepisami polskiego prawa, pod warunkiem wykorzystania do tego celu akredytowanych przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego programów komputerowych zapewniających bezpieczeństwo informacji niejawnych, których funkcjonalności nie umożliwiają ingerencji w treść danych zgromadzonych w urządzeniu ani udostępniania tych danych osobom trzecim, nieuprawnionym do dostępu do informacji niejawnych.**

2. **Użycie programów komputerowych pozwalających utrwalać treść rozmów i obraz w pomieszczeniach, w których znajduje się telefon/tablet/inne urządzenie, po przejęciu kontroli nad urządzeniem i uruchomieniu przez służby mikrofonu lub kamery, jest sprzeczne z przepisami polskiego prawa, które nie przewidują kompetencji służb do aktywnego wykorzystywania funkcjonalności systemu informatycznego lub urządzenia końcowego w celu agregowania danych nie znajdujących się w systemie informatycznym objętym kontrolą w wyniku**

aktywności użytkownika tego systemu bądź na skutek jego indywidualnej konfiguracji.

3. **Użycie programów komputerowych pobierających z telefonu/ tabletu/innego urządzenia osoby objętej kontrolą operacyjną dane dostępowe (hasła/klucze) pozwalające na logowanie się na serwerach z pocztą elektroniczną, bankowych, portalach społecznościowych jest zgodne z przepisami polskiego prawa, przy czym jest sprzeczne z przepisami polskiego prawa przeglądanie i pobieranie danych zgromadzonych w tych systemach informatycznych po odrębnym zalogowaniu się do nich przez służby za pomocą pobranych danych dostępowych (haseł/kluczy).**

4. **Użycie programów komputerowych pobierających z telefonu/ tabletu/innego urządzenia osoby objętej kontrolą operacyjną całą jego zawartość zgromadzoną w urządzeniu w trakcie trwania oraz przed rozpoczęciem kontroli operacyjnej budzi wątpliwości co do zgodności z przepisami polskiego prawa w kontekście spełnienia *in concreto* konstytucyjnej zasady proporcjonalności, a jest sprzeczne z przepisami polskiego prawa, gdy wykorzystane są do tego celu nieakredytowane przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego programy komputerowe nie zapewniające bezpieczeństwa informacji niejawnych, bądź których funkcjonalności umożliwiają ingerencję w treść danych zgromadzonych w urządzeniu, bądź których użycie wiąże się z udostępnianiem tych danych osobom trzecim nieuprawnionym do dostępu do informacji niejawnych.**

5. **Użycie w ramach kontroli operacyjnej programów komputerowych pozwalających na uzyskanie dostępu do całości lub części systemu informatycznego w telefonie/tablecie/innym urządzeniu osoby poddanej kontroli operacyjnej i dokonywanie zmian w ich zawartości (w tym dodawanie, edytowanie lub usuwanie plików) jest sprzeczne z przepisami polskiego prawa.**

6. **Nabycie i używanie programów komputerowych, których wykorzystywanie w ramach kontroli operacyjnej wiąże się z przekazywaniem pozyskiwanych danych do osób trzecich, nieuprawnionych do dostępu do informacji niejawnych, w szczególności administratorów lub służb wywiadowczych obcych państw, jest sprzeczne z przepisami polskiego prawa.**

7. **Wniosek o kontrolę operacyjną kierowany do sądu powinien określać cele, zakres i sposób kontroli, w tym wykorzystywane programy komputerowe wraz ze wskazaniem ich funkcjonalności w kontekście rodzaju, źródeł i liczby pozyskiwanych informacji, a także zakres czasowy gromadzenia danych.**

8. **Osoba kontrolowana, w świetle standardu konstytucyjnego, powinna mieć prawo do powiadomienia o zakończonej wobec niej kontroli operacyjnej i złożenia zażalenia do niezależnego organu kontroli na podjęte wobec niej czynności operacyjne.**

Analiza

1.

Rozważania dotyczące używania w ramach kontroli operacyjnej określonego typu programów komputerowych, które pozwalają operatorom na uzyskanie informacji znacznie przekraczających wyobrażenia, jakie przyświecały ustawodawcy przy kształtowaniu regulacji prawnych definiujących kontrolę operacyjną, poprzedzić należy skrótowym przybliżeniem modelu, w jakim działają wskazane programy, ich możliwości i ograniczeń, co będzie punktem wyjścia dla sprecyzowania ram prawnych ich funkcjonowania.

Każdy program komputerowy jest w istocie zbiorem instrukcji (kodu źródłowego) napisanego w jakimś języku programowania, których liczba linii kodu częstokroć przekracza miliony. Programami komputerowymi są zarówno programy użytkowe – np. elementy pakietu Office czy komunikatory jak Messanger czy WhatsUp, ale także całe systemy operacyjne Windows, Android czy iOS. Z oczywistych powodów w kodzie tym mogą znaleźć się błędy bądź luki, które w wyniku różnych operacji dokonanych przez atakującego mogą doprowadzić do tożsamego skutku: błędy te czy wykorzystane luki mogą sprawiać, że system działa niestabilnie lub niepoprawnie, w szczególności błąd może skutkować tym, że osoba nieuprawniona uzyska uprawnienia dostępu do systemu bądź nadania sobie uprawnień administratora systemu.

W kontekście omijania bądź przełamywania zabezpieczeń oferowanych przez producentów oprogramowania należy zwrócić uwagę na linię czasu kluczową z punktu widzenia zrozumienia istoty programu Pegasus.

Producent oprogramowania, dowiadując się o luce bądź błędzie w swoim programie, umożliwiającym nieuprawnione działanie, może rozpocząć proces poprawy kodu, którego efektem będzie „aktualizacja" systemu. Aktualizacje mają przede wszystkim na celu eliminację tych niedoskonałości kodu, które zostały zidentyfikowane przez producenta oprogramowania. Producent może dowiedzieć się o tych błędach na wiele sposobów; jest jednakowoż grupa błędów/luk, które nie zostają wykryte ani zgłoszone producentowi, lecz są sprzedawane na czarnym rynku, bezpośrednio do grup przestępczych bądź do serwisów skupujących takie luki (zob. np. *https://zerodium.com/program.html*). Jako iż wartość najcenniejszych luk „zero clik" – które umożliwiają iniekcję złośliwego kodu bez jakiejkolwiek aktywności ofiary (nie wymagają nawet np. kliknięcia w przesłany w SMS/mailu link) – kosztują na czarnym rynku nawet około 2 mln. dolarów, wynajdujący te luki i następnie z nich korzystający dbają, aby nie dowiedział się o nich producent (wówczas zostałyby one naprawione). Luki te – zwane „lukami dnia zerowego" (ang. *0-day*) – są typem luk, o których nie wie sam producent, który nie może zabezpieczyć systemu przed zagrożeniami, jakie mogą one powodować.

Przykładowo, w 2019 r. WhatsApp ujawnił, że oprogramowanie NSO było wykorzystywane do wysyłania złośliwego oprogramowania do ponad 1400 telefonów, wykorzystując lukę zero-day. Wystarczającym dla iniekcji złośliwego kodu było nawiązanie połączenia przez WhatsApp z docelowym urządzeniem, aby złośliwy kod Pegasusa mógł zostać zainstalowany na telefonie, nawet jeśli cel nigdy nie odebrał połączenia.

Najniebezpieczniejsze i kluczowe z perspektywy analizowanego zagadnienia są zatem takie luki 0-day, które poza faktem bycia nieodkrytymi przez producenta umożliwiają wykonanie złośliwego kodu,

który pozwoli następnie uczynić z atakującego administratora systemu bądź przyznać atakującemu tożsame jak administratorowi uprawnienia. Umożliwi to atakującemu wykonywanie dowolnych operacji w danym środowisku informatycznym, w tym szereg aktywności budzących poważne wątpliwości prawne.

Egzemplifikacją narzędzia wykorzystującego wskazane luki jest program Izraelskiej firmy NSO – Pegasus – oprogramowanie typu *spyware* (od połącznia słów *spy* (szpiegować) i *software* (oprogramowanie), którego istotą i celem jest wykradanie informacji przechowywanych w systemach informatycznych. Pegasus to w największym uproszczeniu zespół zagregowanych luk 0-day połączony z interfejsem umożliwiającym infekowanie urządzenia i następcze wykonywanie komend z poziomu administratora systemu wraz z możliwością wysyłania danych z urządzeń ofiary, oraz katalogowania i opracowywania pobranych danych. Jako że system przeznaczony jest do infekowania urządzeń mobilnych, posiada wyłącznie zdolność atakowania urządzeń wyposażonych w „mobilne" systemy operacyjne tj. Android, iOS, Blackberry OS czy Symbian.

Administrator systemu – używając jednej z dostępnych dla danej wersji systemu operacyjnego metod – dokonuje przesłania kodu programu klienckiego Pegasus nazywanego „agentem" na atakowane urządzenie końcowe (telefon/tablet atakowanego). Jego uruchomienie na atakowanym urządzeniu otwiera kanał komunikacyjny z centralą danego operatora, umożliwiając odbieranie poleceń i komend, które agent, posiadając pełne uprawnienia administracyjne, wykonywać może na urządzeniu bez wiedzy użytkownika.

Jednocześnie **agent, a za jego pośrednictwem administrator, ma pełny dostęp do zasobów programowych i sprzętowych**

oferowanych przez dany model urządzenia, z których wskazać m.in. należy: dostęp do kamery i mikrofonu, dostęp do wiadomości e-mail, SMS i komunikatorów internetowych, śledzenie lokalizacji urządzenia, dostęp do ustawień urządzenia, zgromadzonych plików (dokumentów, zdjęć, nagrań), danych wprowadzonych do kalendarza, wykazów kontaktów, połączeń telefonicznych, historii wyszukiwania w przeglądarkach internetowych oraz social mediów i aplikacji zainstalowanych na urządzeniu.

Ulokowanie „agenta" daje zatem możliwość niczym nieograniczonej ingerencji w urządzenie i przechowywane na nim dane, znacznie przekraczając nawet możliwości prawowitego użytkownika systemu, który może wykonywać wyłącznie operacje dozwolone przez system operacyjny i współdziałające z nim oprogramowanie.

(https://ia801005.us.archive.org/1/items/nso-pegasus/NSO-Pegasus.pdf)

Wskazane funkcjonalności dotyczą wersji systemu z 2016 r., gdyż z tego roku pochodzi ostatni, dostępny w przestrzeni publicznej dokument firmy NSO. Zawiera on szereg szczegółowych informacji przedstawiających możliwości systemu i wydaje się, że w ciągu 6 lat mógł zostać on zostać wzbogacony o nowe funkcjonalności.

2.

Materiały NSO wskazują na trzy modele wykorzystywania programu Pegasus, co będzie miało fundamentalne znaczenie dla określenia zakresu dopuszczalności stosowania tego rodzaju narzędzia na gruncie obowiązującego w Polsce prawa:

1) ekstrakcja początkowa/wstępna;
2) pasywne przechwytywanie;
3) aktywne zbieranie danych.

Pierwszy model działania umożliwia pobranie szeregu informacji przechowywanych na urządzeniu końcowym, wśród których wymienić należy bazę wiadomości SMS/MMS, listę kontaktów, historię połączeń, dane kalendarza, e-maile, dane z komunikatorów, historię przeglądania. Co istotne, sam producent zaznaczył, że „wstępna ekstrakcja danych jest opcją, a nie koniecznością”. Jeśli korzystającej z oprogramowania organizacji nie wolno – w świetle obowiązującego prawa – uzyskiwać dostępu do danych historycznych, zgromadzonych przed okresem kontroli operacyjnej, opcję tę można wyłączyć, wskutek czego monitoringowi będą poddane tylko dane nowe/spływające do urządzenia w czasie kontroli operacyjnej.

Podstawowe znaczenie w pracy operacyjnej ma drugi i trzeci model. Model „pasywnego przechwytywania” pozwala na uzyskiwanie zakresu informacji w zasadzie tożsamego z pierwszym, pozwalając

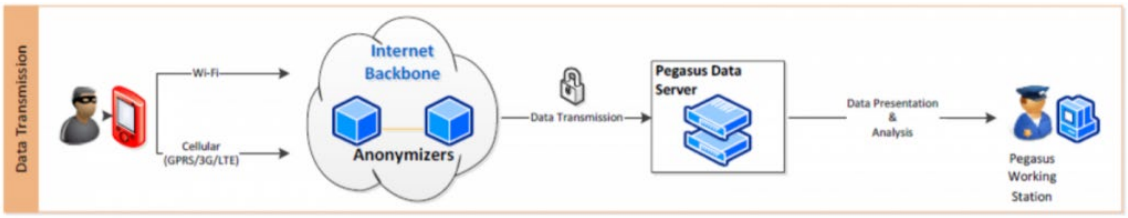
jedynie na uzyskiwanie nieco większej ilości danych np. BTSów, do których podłączony jest dany telefon. **Model „aktywnego zbierania danych" umożliwia zaś aktywne pozyskiwanie danych poprzez utrwalanie rozmów, pobieranie plików znajdujących się na urządzeniu, uruchamianie bez wiedzy użytkownika mikrofonu i kamery celem przechwytywania dźwięku/obrazu z wykorzystaniem mikrofonów/kamery znajdujących się w danym urządzeniu czy lokalizacji na podstawie danych pobieranych z modułu GPS. Możliwe jest także przechwytywanie ekranu czy monitorowanie wprowadzanych za pomocą klawiatury znaków, dopełniając pełną cyfrową inwigilację podmiotu objętego opisywanym nadzorem.**

Należy zaznaczyć, że specyfika możliwości omawianego rodzaju oprogramowania nie jest zarezerwowana wyłącznie dla jednego, konkretnego programu (Pegasus). W zakresie swych ogromnych możliwości inwigilacyjnych Pegasus niczym nie różniłby się od innego oprogramowania, które – wykorzystując systemowe czy programowe luki 0-day – umożliwiałoby uzyskanie przez nieuprawnioną osobę praw administratora urządzenia, a tym samym stosowania opisanych wcześniej metod inwigilacji. Z perspektywy prawnej każde tego typu oprogramowanie, operujące tożsamymi funkcjonalnościami, powinno być traktowane jednolicie w perspektywie zgodności lub sprzeczności z prawem jego pozyskania i użytkowania przez służby państwowe.

3.

Przystępując do prawnej oceny omawianych programów szpiegujących należy przede wszystkim wziąć pod uwagę **bezpieczeństwo informacji uzyskanych za ich pośrednictwem**. Opracowanie NSO wskazuje, że dla zapewnienia bezpieczeństwa

informacji pozyskiwane dane przesyłane są z atakowanego urządzenia na serwer operatora (np. CBA) za pośrednictwem zanonimizowanej sieci transmisji (ang. *Pegasus Anonymizing Transmission Network*, PATN), zasadzającej się na tworzeniu rozsianych po świecie, dedykowanych wirtualnych serwerów, przez które transmitowany jest ruch sieciowy, zanim trafi on do operatora.



Jakkolwiek sam model znacznie ewoluował, głównie na skutek publikowania przez Amnesty International raportów tyczących działania Pegasusa (zob. *https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/*), to nie zmienia się sposób transferu zasadzający się na wykorzystywaniu **rozproszonej geograficznie sieci połączeń** transferujących dane od atakowanego urządzenia do miejsca lokalizacji serwera danej instancji (np. siedziby CBA), także poza obszar Rzeczypospolitej.

Innymi słowy, jeśli zaatakowane urządzenie końcowe znajduje się w Szczecinie, a serwer CBA w Warszawie, to całość danych z telefonu przekazana zostanie np. do Londynu, potem np. do San Francisco, następnie do np. Kairu i dopiero z powrotem do Warszawy. Dodać należy, że będące w gestii NSO zewnętrzne serwery można wyposażyć w oprogramowanie, które transmitowane dane przesyłałoby również do siedziby samego NSO.

Pozyskane w toku kontroli operacyjnej dane pozostają pod szczególną ochroną określoną w ustawie o ochronie informacji niejawnych (ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz. U. z 2019 r. poz. 742, dalej: uoin.) **i jako takie nie mogą być bez określonej w prawie kompetencji przekazywane osobom trzecim, nieuprawnionym do dostępu czy przetwarzania informacji objętych klauzulą tajności.** Należy także zauważyć, że procedura nadania informacjom pozyskiwanym w ramach kontroli operacyjnej klauzuli tajności (oklauzulowanie informacji) ma służyć zapewnieniu obywatelowi ochrony jego wolności i praw, tak aby dane wrażliwe i liczne informacje o życiu prywatnym jednostki nie były dostępne dla nieokreślonego grona osób, a także aby zapewnić bezpieczeństwo ich przetwarzania oraz umożliwić ich skuteczne zniszczenie zgodnie z przewidzianą procedurą. Z perspektywy konstytucyjnej – o której będzie jeszcze mowa później – **niedopuszczalne jest pozyskiwanie tak głęboko ingerujących w prawo do prywatności informacji w ramach kontroli operacyjnej, którym nie zostanie nadana stosowna klauzula poufności i będą one w konsekwencji, w sposób niekontrolowany, dostępne dla osób postronnych zwłaszcza, jeśli ich pozyskiwanie odbywać się będzie przez nieakredytowane systemy teleinformatyczne.**

Transfer danych za pośrednictwem kanałów, których z powodów czysto technicznych niepodobna nadzorować, jak również w sytuacji, gdy nie jest możliwe monitorowanie poziomu ich bezpieczeństwa (zachowania poufności) w oczywisty sposób narusza zasady postępowania z pozyskiwanymi danymi oraz informacjami niejawnymi, określone w ustawie merytorycznej.

Systemy informatyczne służące do kontroli operacyjnej, z uwagi na fakt przetwarzania danych niejawnych, muszą spełniać rygorystyczne wymogi bezpieczeństwa teleinformatycznego nakładane przez ustawę o informacjach niejawnych i wydane na jej mocy rozporządzenie w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 159, poz. 948). W szczególności, **system taki gwarantować powinien poufność**, przez którą należy rozumieć taką jego właściwość, że informacja nie jest ujawniana (obejmuje to także możliwość swobodnego dostępu do danych) podmiotom do tego nieuprawnionym, co w przypadku braku pełnej kontroli nad infrastrukturą służącą do transmisji danych nie może być skutecznie zagwarantowane z powodów czysto technicznych. Opisany powyżej model transmisji przesyłanych w ramach polskiej instancji Pegasusa – zakładający od strony technicznej brak możliwości realnej weryfikacji bezpieczeństwa tego systemu przed nieuprawnionym dostępem służb państwa obcego czy NSO, możliwość istnienia w systemie licznych podatności umieszczonych tamże przez jego producenta – uniemożliwia spełnienie warunku poufności, a tym samym **nie mógł i nie może uzyskać świadectwa akredytacji bezpieczeństwa informatycznego.**

Warto także zwrócić uwagę, iż potencjalnie podatności systemu rzutować też będą na brak możliwości zagwarantowania **integralności**, rozumianej jako właściwość określająca, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony. Rozważać ją trzeba w dwóch aspektach – operatora i figuranta.

W pierwszym aspekcie chodzi o niemożność zagwarantowania, iż system dostarczy dane, które zostały pobrane z urządzenia objętego kontrolą operacyjną w niezmodyfikowany sposób. Brak kodów źródłowych aplikacji, brak kontroli węzłów pośredniczących CBA

(użytkownik Pegasusa) oznacza **brak gwarancji, że pobierane dane nie są w żaden sposób modyfikowane w czasie transmisji**.

W drugim aspekcie zwrócić należy uwagę, że poprzez aktywne modyfikowanie danych w systemie operacyjnym urządzenia infekowanego agentem oraz możliwością wysyłania nań danych bez wiedzy użytkownika, brak jest możliwości wskazania – bądź byłoby to bardzo utrudnione – które z danych znalazły się na urządzeniu na skutek działania operatora systemu Pegasus, a które na skutek działania samego użytkownika urządzenia poddanego inwigilacji.

W opisanym stanie rzeczy sprowadzona jest do zera możliwość weryfikacji systemu Pegasus zgodnie z obowiązkiem ustawowym wynikającym z art. 48 uoin. Na mocy wskazanego przepisu systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego, którego dokonać winno ABW lub SKW. Wydanie rzeczonej akredytacji poprzedzić musi – zgodnie z art. 48 ust. 4 uoin. – kompletny dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego, który opracowywany być powinien już na etapie projektowania samej aplikacji, która będzie podstawą do stworzenia dokumentacji bezpieczeństwa systemu teleinformatycznego. Jako iż centralny serwer polskiej instancji systemu Pegasus znajdować się musi w wyznaczonej ku temu strefie ochronnej, nie stosuje się do niego wyłączenia z art. 51 uoin. Nie sposób także, ze względu na kwestie technologiczne, udzielić wymaganej prawem akredytacji bez przeprowadzenia miarodajnych testów programu i uzyskania dostępu do kodów źródłowych i infrastruktury całości ekosystemu.

Stwierdzić należy zatem, że system **Pegasus nie może być stosowany na gruncie polskiego prawa już to z uwagi na**

niemożność urzeczywistnienia określonej w ustawie, prawidłowej i skutecznej akredytacji i weryfikacji podstawowych wymagań bezpieczeństwa teleinformatycznego związanego z ochroną informacji niejawnych (zob. wydane na podstawie delegacji ustawowej wyrażonej w art. 49 ust. 9 uoin. rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz. U. Nr 159, poz. 948). **Polski system prawny nie dopuszcza stosowania programów, w ramach których pozyskiwane dane operacyjne poddane są transferowi w niekontrolowanych przez właściwe służby kanałach transmisji, co rodzi ryzyko naruszenia ich integralności oraz nie zapewnia im wymaganej prawem poufności.**

W związku z powyższym za niezgodne z przepisami polskiego prawa należy uznać wszelkie działania operacyjne z wykorzystaniem nieakredytowanych programów komputerowych, które nie zapewniają bezpieczeństwa informacji niejawnych, bądź których użycie wiąże się z udostępnianiem tych danych osobom trzecim nieuprawnionym do dostępu do informacji niejawnych.

4.

Rozważając dopuszczalność wykorzystywania oprogramowania przystosowanego do przejęcia kontroli nad urządzeniem końcowym, uzyskania dostępu do systemu informatycznego czy też pobierania i utrwalania szerokiego spektrum danych po przełamaniu zabezpieczeń urządzenia końcowego, o których była mowa wcześniej, należy zwrócić uwagę na zakres kompetencji przyznanych Agencji Bezpieczeństwa Wewnętrznego w ściśle określonym przypadku, wskazanym w art. 32a ust. 7 i 8 ustawy o ABW:

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.*

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.

Jak widać, po pierwsze: ABW posiada uprawnienie do korzystania z programów, których przykładem jest Pegasus w ściśle sprecyzowanym, wyłącznym celu „określenia podatności ocenianego systemu na możliwość popełnienia przestępstw" wskazanych w przytoczonym przepisie. Program ten nie może być wytwarzany, pozyskiwany ani używany przez wskazaną służbę w jakimkolwiek innym celu. Po drugie, brak jest jednocześnie analogicznych postanowień względem dopuszczalności wykorzystania takiego oprogramowania w ramach prowadzenia czynności operacyjnych w przypadku jakiejkolwiek ze służb, których zadaniem jest kontrola operacyjna.

Z powyższego wynika, że **wytworzenie, pozyskanie lub używanie programu Pegasus z wykorzystaniem jego funkcjonalności „aktywnego zbierania danych" oraz łamania lub omijania zabezpieczeń systemów informatycznych jest**

w polskim porządku prawnym dozwolone w ściśle sprecyzowanej sytuacji, w ramach działalności ABW, a w tym zakresie wyłącznie w wąskim celu badania podatności systemów informatycznych na przestępne ataki.

W pozostałym zakresie, w jakim przepisy obowiązującego prawa nie przewidują szczegółowej kompetencji do operowania omawianego rodzaju oprogramowaniem, **pozyskanie (np. w drodze zakupu) lub udostępnienie kolejnym osobom programu typu Pegasus, który przystosowany jest do aktywnego atakowania telefonu/tabletu/innego urządzenia, wyczerpuje znamiona czynu zabronionego opisanego w art. 269b § 1 Kodeksu karnego** (z zastrzeżeniem §1a oraz art. 269c k.k., które jednak nie znajdują zastosowania w analizowanym kontekście).

5.

Przepisy regulujące prowadzenie inwigilacji były kilkukrotnie przedmiotem analizy Trybunału Konstytucyjnego pod kątem **standardów i granic ingerencji władzy publicznej w prawa i wolności obywatelskie.** Inwigilacja prowadzić może bowiem do naruszenia podstawowych praw konstytucyjnych, takich jak np.: prawo jednostki do prywatności (art. 47 Konstytucji; prawo to nie ulega na mocy art. 233 ust. 1 Konstytucji ograniczeniu w stanie wojennym lub wyjątkowym), konstytucyjnej wolności komunikowania i związanej z tym ochrony tajemnicy komunikacji (art. 49 Konstytucji) i ochrony autonomii informacyjnej (art. 51 Konstytucji). Przy czym autonomia informacyjna stanowi istotny element prawa do prywatności polegający na „samodzielnym decydowaniu o ujawnianiu innym podmiotom informacji dotyczących własnej osoby, a także na sprawowaniu kontroli nad tymi

informacjami, nawet jeżeli znajdują się w posiadaniu innych osób" (wyrok TK z 30 lipca 2014 r., K 23/11. nb 250 i powołane tam orzecznictwo).

W konsekwencji zbyt głębokiej, nieproporcjonalnej ingerencji w te prawa może dojść także do naruszenia zasady godności człowieka (zob. wyrok TK z 23 czerwca 2009 r., K 54/07 nb 239, wyrok TK z 30 lipca 2014 r., K 23/11, nb 249). Jak stwierdził TK w wyroku z 12 grudnia 2005 (K 32/04, nb 67):

> *„Zachowanie przez człowieka godności wymaga bowiem poszanowania jego sfery czysto osobistej, gdzie nie jest narażony na konieczność „bycia z innymi" czy „dzielenia się z innymi" swoimi przeżyciami czy doznaniami o intymnym charakterze. Dlatego sfera prywatna jest zbudowana z różnych kręgów w mniejszym lub większym stopniu otwartych (prawnie) na oddziaływanie zewnętrzne, gdzie konstytucyjna aprobata dla władczego wkroczenia przez władzę nie jest jednakowa".*

Szczególną uwagę Trybunał zwracał na rangę uprawnienia wynikającego z art. 51 ust. 4 Konstytucji, który to przepis statuuje prawo każdego do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych oraz zebranych w sposób sprzeczny z ustawą (prawo do przedstawiania i kształtowania swojego publicznego wizerunku). Prawo to obejmuje także informacje zebrane w drodze działalności operacyjnej, jakkolwiek ze względu na fakt, że nie są one ujawniane wobec zainteresowanego w czasie trwania kontroli, jest ono faktycznie ograniczone (wyrok TK z dnia 12 grudnia 2005, K 32/04, nb 73). Podkreślenia jednak wymaga, że art. 51 ust. 4 Konstytucji nie przewiduje – w przeciwieństwie do praw wynikających z art. 51

ust. 1 i 2 w zw. z art. 51 ust. 5 czy z art. 51 ust. 3 Konstytucji – współdziałania ustawodawcy zwykłego w uregulowaniu wynikającego z niego prawa. Uzasadnione ochroną innych praw i wolności konstytucyjnych wkroczenie w prawo gwarantowane art. 51 ust. 4 Konstytucji nie jest jednak zabronione, ale ocena proporcjonalności wkroczenia musi się odbywać wg surowszych kryteriów niż w przypadku praw, które dookreśla ustawodawca zwykły (wyrok TK z dnia 12 grudnia 2005, K 32/04, nb 75, wyrok TK z dnia 23 czerwca 2009 r., K 54/07, nb 254).

Trybunał Konstytucyjny nie kwestionuje dopuszczalności prowadzenia szeroko rozumianej kontroli operacyjnej uzasadnianej ochroną bezpieczeństwa publicznego, wskazując jednak, że ze względu na jej niejawny charakter jest ona podatna na nadużycia i może prowadzić do zniszczenia instytucji demokratycznych, a także redukcji praw obywatelskich. Z tego względu **konieczne jest wprowadzenie szeregu mechanizmów gwarantujących, że wkroczenie w prawa i wolności obywatelskie będzie proporcjonalne. Te gwarancje powinny mieć charakter zarówno materialnoprawny, jak i proceduralny.**

Na płaszczyźnie materialnoprawnej istotne znaczenie ma sposób unormowania kontroli operacyjnej, tj. wprowadzenie przepisów określających sposób wkraczania w prawa i wolności jednostki, precyzujących między innymi, **kiedy i na jakich zasadach, wobec kogo, jak długo może być stosowana kontrola operacyjna.**

Na płaszczyźnie proceduralnej natomiast podkreśla się konieczność zapewnienia wszelkiego rodzaju **gwarancji, służących kontroli przez organ niezależny od rządu sposobu realizacji przesłanek materialnoprawnych; kontrola ta nie może mieć**

charakteru fasadowego. Nawet w przypadku wąsko ujętego zakresu przypadków, w których dopuszczalna będzie kontrola operacyjna, jeżeli brak jest efektywnych mechanizmów kontroli na płaszczyźnie proceduralnej (związanych chociażby z weryfikacją zasadności zastosowania kontroli operacyjnej w konkretnej sprawie), przyjąć należy, że ma miejsce niedopuszczalne naruszenie praw i wolności konstytucyjnych obywatela. Trybunał dopuszcza zatem nawet głębokie wkraczanie w sferę prywatności, pod warunkiem opatrzenia owej ingerencji należytymi gwarancjami proceduralnymi.

Dopuszczalność naruszenia praw i wolności konstytucyjnych warunkowana jest stwierdzeniem, że zostały spełnione przesłanki opisane w art. 31 ust 3 Konstytucji, z których najwięcej uwagi poświęca się przesłance **proporcjonalności**. Z ugruntowanego orzecznictwa TK wynika, że dla oceny, czy ograniczenie praw było proporcjonalne, konieczne jest uzyskanie pozytywnej odpowiedzi na trzy pytania:

1) czy wprowadzona regulacja jest w stanie doprowadzić do zamierzonych przez nią skutków,
2) czy regulacja ta jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana,
3) czy efekty wprowadzonej regulacji pozostają w proporcji do ciężarów nakładanych przez nią na obywatela.

6.

Trybunał Konstytucyjny wielokrotnie podkreślał, że niedopuszczalna jest zarówno praktycznie nieograniczona inwigilacja w ramach czynności operacyjnych, jak też możliwość arbitralnego rozpowszechnia zgromadzonych w ten sposób informacji. Zastosowanie środków kontroli operacyjnej nie może bowiem

– w ocenie Trybunału Konstytucyjnego – prowadzić do erozji fundamentów tego państwa, do których należy zaliczyć godność ludzką z jednej strony i unikanie arbitralności w działaniu władz z drugiej. Zbytnie rozszerzenie zakresu uprawnień w zakresie przeprowadzanej kontroli operacyjnej prowadzić może do przekształcenia państwa demokratycznego w państwo policyjne.

Analiza orzecznictwa TK prowadzi do wniosku, że u podstaw dopuszczalności stosowania inwigilacji leży założenie, iż informacje zgromadzone w ramach prowadzonej inwigilacji znajdują się w bezpiecznym i wyłącznym posiadaniu/dyspozycji stosownych służb. Trybunał Konstytucyjny wskazywał także na konieczność bezwzględnego wyeliminowania „dostępu osób nieuprawnionych do przechowywanych materiałów zgromadzonych w ramach czynności operacyjno-rozpoznawczych, których rezultaty muszą być objęte tajemnicą dopóty, dopóki nie zostaną udostępnione jako materiał dowodowy w procesie karnym, na zasadach stosowanych w postępowaniu karnym” (wyrok z dnia 12 grudnia 2005 r., K 32/04, nb 66). W przeciwnym razie dojść może do naruszenia ochrony zaufania obywatela do państwa.

Należy zauważyć, że Trybunał Konstytucyjny w wyroku z dnia z dnia 23 czerwca 2009 r., K 54/07 stwierdził sprzeczność z art. 47 i art. 51 w związku z art. 31 ust. 3 i art. 30 Konstytucji regulacji zawartej w art. 22 ust. 4-7 ustawy o CBA z tego m.in. względu, że umożliwiała ona CBA gromadzenie i przetwarzanie danych wrażliwych w zakresie, w którym nie jest to niezbędne dla celów ścigania korupcji, jak też przyjmowała nadmiernie wydłużony okres obowiązkowej weryfikacji danych zgromadzonych w zbiorach CBA oraz brak dostatecznej ich ochrony przed niepowołanym dostępem lub ich wykorzystaniem w celach

niezgodnych z prawem i celem ich pozyskania (podobna argumentacja leży u podstaw uznania za niekonstytucyjny art. 40 ustawy o CBA).

A minori ad maius, jeżeli użyty w toku kontroli operacyjnej środek ze swojej istoty (np. z uwagi na techniczny sposób działania programu komputerowego) zakłada, że **uzyskane przy jego użyciu informacje trafią nie tylko do uprawnionego podmiotu prowadzącego czynności operacyjne, ale także najpewniej do osób trzecich („na zewnątrz", jak to ma miejsce w przypadku wykorzystania pełnych funkcjonalności Pegasusa), to użycie określonego środka jest niedopuszczalne w świetle konstytucyjnych standardów ochrony konstytucyjnych praw i wolności.** Nawet przyjmując, że bardzo poważne zagrożenie bezpieczeństwa państwa na skutek zmiany sytuacji geopolitycznej, w tym konieczność zwalczania terroryzmu bezpośrednio zagrażającego bezpieczeństwu państwa, w pewnym momencie wymusi na państwie zastosowanie takich narzędzi (będzie to wtedy swoistego rodzaju stan wyższej konieczności), to dla przyjęcia spełnienia przesłanki proporcjonalności konieczne będzie wprowadzenie **wyjątkowo rygorystycznej procedury,** gwarantującej zachowanie standardów tak agresywnej inwigilacji.

W tym kontekście trzeba zauważyć, że **Europejski Trybunał Praw Człowieka wypracował minimalne wymogi, które powinny być określone w prawie krajowym w celu uniknięcia nadużyć w zakresie czynności operacyjnych. Zastrzegł, że system prawny musi przewidywać** (1) charakter przestępstw, które mogą skutkować wydaniem nakazu przechwytywania; (2) definicję kategorii osób narażonych na przechwycenie ich komunikacji; (3) ograniczenie czasu przechwytywania; (4) procedurę, której należy przestrzegać przy badaniu, wykorzystywaniu i przechowywaniu uzyskanych danych; (5) środki

ostrożności, jakie należy podjąć podczas przekazywania danych innym stronom; oraz (6) okoliczności, w których przechwycone dane mogą lub muszą zostać usunięte lub zniszczone. Jak wskazał Trybunał,

> *„(…) ma to szczególne znaczenie w przypadku tzw.* ***hurtowego przechwytywania danych (bulk interception), gdzie służby gromadzą ogromne ilości nieprzefiltrowanych danych elektronicznych dotyczących aktywności określonej osoby lub grup osób****. Każdy etap procesu masowego przechwytywania – w tym wstępna autoryzacja i wszelkie późniejsze przedłużenia, wybór nośników, wybór i zastosowanie kryteriów i poszczególnych zapytań oraz wykorzystanie, przechowywanie, dalsze przesyłanie i usuwanie materiału przechwytywania – również powinien podlegać nadzorowi niezależnego organu, a nadzór ten powinien być wystarczająco solidny, aby utrzymać „ingerencję" w to, co jest „niezbędne w demokratycznym społeczeństwie"* (tak w wyroku Wielkiej Izby z dnia 25 maja 2021 r. Centrum För Rättvisa przeciwko Szwecji, skarga nr 35252/08 § 246 i n.).

Brak szczególnych procedur zwiększonej i efektywnej kontroli nad pozyskiwaniem hurtowych ilości danych w ramach czynności operacyjnych jest niezgodne z art. 8 Europejskiej Konwencji Praw Człowieka.

Zarysowany **standard konstytucyjny i konwencyjny potwierdza, że stosowanie programu typu Pegasus jest sprzeczne z przepisami polskiego prawa** już to w zakresie wymogu akredytacji konkretnego programu, zagwarantowania bezpieczeństwa transferu danych w ramach kontroli operacyjnej oraz ochrony informacji niejawnych przed ich

przejęciem przez osoby nieuprawnione, jako naruszenie konstytucyjnego standardu ochrony tajemnicy korespondencji, ochrony autonomii informacyjnej oraz prawa do prywatności, i to niezależnie od oceny zastosowania omawianego programu w kontekście zasady proporcjonalności *in genere* (w aspekcie konstytucyjności obowiązujących uregulowań ustawowych) oraz *in concreto* (w aspekcie zastosowania przepisów w konkretnym przypadku operacyjnym), o czym z kolei będzie mowa niżej.

7.

Należy podkreślić, że narzędzia, których działanie opiera się na wykorzystaniu omówionych luk w systemach informatycznych posiada większość państw prowadzących działalność wywiadowczą w zakresie cyber-wywiadu. To zrozumiałe w kontekście konieczności zapewnienia państwu zewnętrznego i wewnętrznego bezpieczeństwa. Programy umożliwiające zaawansowaną inwigilację obywateli są jednak z istoty rzeczy **stworzone do pracy wywiadowczej oraz aktywności skoncentrowanej na ochronie państwa przed wysoce groźną przestępczością,** której zapobieganie i zwalczanie w kontekście konstytucyjnej zasady proporcjonalności musi być uzasadnione w demokratycznym państwie prawnym.

W tej perspektywie stosowanie programów typu Pegasus jawi się jako niedopuszczalne w ramach kontroli operacyjnej, zaś niezależnie od tego użycie oprogramowania pozwalającego na głęboką inwigilację obywatela musi budzić zastrzeżenia w świetle ogólnych standardów konieczności i proporcjonalności wyznaczonych przez polskie prawo.

Standardy kontroli operacyjnej zawarte zostały w przepisach, które regulują działalność poszczególnych służb. Przesłanki jej stosowania opisano w art. 19 ustawy z 6 kwietnia 1990 r. o Policji (Dz.U.2021.1882 t.j.), art. 27 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U.2020.27 t.j. – dalej: „ustawa o ABW"), art. 17 ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U.2021.1671 t.j. – dalej: „ustawa o CBA"), art. 31 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz.U.2019.687 t.j. – dalej: „ustawa o SKW"), art. 118 ustawy z 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz.U.2021.422 t.j.), art. 9e ustawy z 12 października 1990 r. o Straży Granicznej (Dz.U.2021.1486 t.j. – dalej: „ustawa o SG"), art. 42 ustawy z 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz.U.2021.575 t.j. – dalej: „ustawa o SOP"). **Regulacje te zawierają katalog przestępstw, w przypadku których może być stosowana kontrola operacyjna. Jest on zróżnicowany w zależności od konkretnej ustawy.**

Stosowanie kontroli operacyjnej nie jest uzależnione od tego, czy konkretne przestępstwo zostało już popełnione. Ustawy stanowią, że może ona zostać wdrożona nie tylko w celu wykrycia, ustalenia sprawców, uzyskania i utrwalenia dowodów, ale również zapobieżenia, ściganych z oskarżenia publicznego, czynów przestępnych wymienionych w katalogu. Można po nią więc sięgnąć np. wówczas, gdy służby mają wiarygodną informację o przygotowywanym przestępstwie. Dziać się tak będzie nawet jeśli przygotowanie konkretnego czynu przestępnego nie jest karalne. Kontrolę operacyjną stosuje się więc także na głębokim przedpolu popełnienia przestępstwa. Poszczególne ustawy mogą przewidywać jeszcze inne cele stosowania kontroli operacyjnej.

Przykładowo art. 27 ust. 1 ustawy o ABW czy też art. 17 ust. 1 ustawy o CBA stanowią, że można ją wdrożyć w celu ujawnienia mienia zagrożonego przepadkiem.

Poszczególne ustawy zawierają szereg tożsamych przesłanek stosowania kontroli operacyjnej. Jej wdrożenia jest możliwe **dopiero w przypadku stwierdzenia, że inne środki okazały się bezskuteczne lub będą nieprzydatne.** Można ją zatem stosować jedynie wtedy, gdy realizacja celu w postaci zapobieżenia, wykrycia, ustalenia sprawców lub pozyskania bądź utrwalenia dowodów przestępstwa nie jest możliwa przy użyciu mniej inwazyjnych (co do technicznych cech oprogramowania czy *in concreto* wykorzystywanych funkcji) instrumentów inwigilacji. **W przepisach dotyczących kontroli operacyjnej wyrażono więc wprost przesłankę konieczności**.

Nawiązuje to do stanowiska Trybunału Konstytucyjnego, który wielokrotnie podkreślał, że nie jest wystarczającym usprawiedliwieniem dla stosowania czynności operacyjnych państwa fakt, że są one celowe, użyteczne czy też tanie, ani też to, że stosowane są one w innych państwach. **Zasadnicze znaczenie ma bowiem to, czy są one konieczne w demokratycznym państwie prawa** (K 32/04). Dostrzegając przy tym role nowych technologii w pozyskiwaniu wiedzy o działalności przestępczej, ustawodawca – zdaniem Trybunału Konstytucyjnego – „nie może ignorować specyfiki naruszeń prawa dokonywanych z ich wykorzystaniem ani skali zjawiska w polskich realiach” (wyrok TK z 30 lipca 2014 r., K 23/11, nb 263).

W przepisach dotyczących kontroli operacyjnej nie wysłowiono wprost zasady proporcjonalności. Nie powinno jednak budzić żadnych wątpliwości, że znajduje ona zastosowanie do tej instytucji prawnej. Kontrola operacyjna ingeruje bardzo głęboko przede wszystkim

w konstytucyjnie chronione prawo do prywatności, ochrony danych osobowych, w tajemnicę komunikowania się czy też godność człowieka. Przy jej stosowaniu niewątpliwie trzeba bezpośrednio stosować wynikający z art. 31 ust. 3 ustawy zasadniczej test proporcjonalności.

Użycie kontroli operacyjnej musi być więc adekwatne do celu, któremu ma ona służyć i brać pod uwagę charakter i stopień ingerencji w dobra prawne osoby, która ma być kontrolowana. Im poważniejsze przestępstwo, tym bardziej inwazyjny środek może być stosowany w konkretnej sytuacji.

W przypadku realnej groźby wystąpienia zamachów terrorystycznych służby powinny być uprawnione do używania najdalej idących form inwigilacji jednostki. Jednak w przypadku mniej poważnych przestępstw niedopuszczalne jest stosowanie środków sprowadzających się do najgłębszej ingerencji w dobra przynależne człowiekowi. Nie do pogodzenia z konstytucyjnym testem proporcjonalności byłaby przykładowo sytuacja, w której dana osoba ulegałaby permanentnej obserwacji i podsłuchiwaniu za pomocą kamery i mikrofonu wbudowanego w jej urządzenie mobilne w celu wykrycia sprawcy nieumyślnego zniszczenia zabytku z art. 108 ust. 2 ustawy z dnia 23.07.2003 r. o ochronie zabytków i opiece nad zabytkami (Dz.U.2021.710 t.j.). Możliwość stosowania kontroli operacyjnej w przypadku takiego przestępstwa jest przewidziana w art. 19 ust. 1 pkt 3a ustawy o Policji. **Nie oznacza to jednak, że sam „katalogowy" status danego czynu zabronionego usprawiedliwia w każdym przypadku, automatycznie stosowanie najintensywniejszych środków kontroli**, gdyż tak agresywna inwigilacja obywatela musi spełniać każdorazowo test proporcjonalności.

To, że kontrola operacyjna w ustroju państwa demokratycznego ma służyć realizacji konstytucyjnie dopuszczalnego celu oznacza, iż może być ona zastosowana wyłącznie do zapobiegania i wykrywania poważnych przestępstw. Można po nią sięgnąć, gdy istnieje realna obawa, że przestępstwo może zostać lub zostało już popełnione. Niedopuszczalne jest więc powołanie się jedynie na abstrakcyjną obawę popełnienia przestępstwa pod pretekstem realizacji pozaustawowych celów, w tym np. pozyskiwania całego spektrum informacji istotnych z punktu widzenia kampanii wyborczej czy też zbierania „haków" na przeciwników politycznych.

8.

Przepisy o kontroli operacyjnej wymieniają rodzaje kontroli operacyjnej, które mogą zostać wdrożone. Przykładowo art. 19 ust. 6 ustawy o Policji wskazuje, że może ona 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 (jak wynika z art. 19 ust. 6a ustawy o Policji – kontroli operacyjnej nie stanowią czynności polegające na uzyskiwaniu i utrwalaniu obrazu w pomieszczeniach przeznaczonych dla osób zatrzymanych lub doprowadzonych w celu wytrzeźwienia, policyjnych izb dziecka, pokoi przejściowych oraz tymczasowych pomieszczeń przejściowych; na tego rodzaju czynności nie jest wymagana zgoda ze strony sądu);

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

Taki sam katalog zawiera art. 19 ust. 6 ustawy o CBA, art. 17 ust. 5 ustawy o CBA, art. 31 ust. 4 ustawy o SKW, art. 118 ust. 3 ustawy o KAS, art. 9e ust. 7 ustawy o SG, art. 43 ustawy o SOP.

Przepisy ustaw nie precyzują, jakie dokładnie metody i środki techniczne mogą być użyte przy stosowaniu kontroli operacyjnej. W szczególności nie wymieniają one nazwy i nie zawierają specyfikacji oprogramowania, które może być użyte do inwigilacji. Taki stan rzeczy nie budzi jednak wątpliwości z punktu widzenia standardu konstytucyjnego.

W wyroku TK z 30 lipca 2014 r., K 23/11 wskazano, że nie jest konieczne sprecyzowanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie ich parametrów. Mając na uwadze ogromną liczbę środków stosowanych przez organy państwa przydatnych w pracy operacyjno-rozpoznawczej, ustawowy ich katalog musiałby być rozbudowany, a co za tym idzie norma prawna musiałaby być kazuistyczna. Rozwiązanie to mogłoby kolidować z wymogiem abstrakcyjności normy prawnej. Jak wielokrotnie wskazywał Trybunał, przestrzeganie wymogów wynikających z zasady dostatecznej określoności prawa nie może prowadzić do kazuistyki unormowania. TK dodał, że w dobie rozwoju technologicznego, wielości form popełniania przestępstw i kanałów komunikowania się przestępców

nie wydaje się realne stworzenie zamkniętego katalogu środków technicznych, które mogą być stosowane w celu uzasadnionego konstytucyjnie niejawnego pozyskiwania informacji, bez uszczerbku dla efektywnej walki z zagrożeniami czy dekonspiracji działalności operacyjnej.

Trybunał Konstytucyjny nadmienił jednak, że z punktu widzenia zasady określoności prawa **istotne jest sprecyzowanie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach.** Nie chodzi tu jednak o wskazanie skonkretyzowanych technicznych metod ich zdobywania, ale rodzajowych nazw poszczególnych środków i informacji możliwych do pozyskania za ich pomocą (np. „podsłuch rozmów telefonicznych", „podsłuch i podgląd pomieszczeń i osób", „podsłuch techniczny środków łączności przewodowej i radiowej", „nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu", „nadzór elektroniczny środków łączności przewodowej lub radiowej"). Trybunał podkreślił, że musi być to **zamknięty katalog rodzajów środków** służących do niejawnego pozyskiwania informacji i dowodów, co ogranicza arbitralność organów państwa, a ponadto umożliwia sprawowanie efektywnej kontroli nad niejawną działalnością operacyjno-rozpoznawczą w zakresie wykorzystywanych metod pozyskiwania informacji o osobach.

Z powyższego wynika, że przepisy określające **środki i metody działania operacyjnego muszą spełniać cechę dostatecznej określoności:** nie w zakresie parametrów technicznych narzędzi wykorzystywanych do ich uzyskiwania, lecz **ujętych opisowo sposobów działania, które pozwolą na jednoznaczne przyporządkowanie określonej metody stosowanej przez służby do ich ustawowej**

charakterystyki; muszą ponadto tworzyć katalog zamknięty, tak aby wyznaczyć wskazanej kontroli przewidziane prawem granice.

Należy także brać pod uwagę zmieniającą się wciąż rzeczywistość technologiczną i rozszerzanie możliwości technicznych ingerowania w prawa i wolności obywatelskie, wskutek czego zbyt ogólnie ujęte przepisy uchwalane w danym momencie czasowym rodzą ryzyko niekontrolowanego, samoczynnego rozszerzania się zakresu ich zastosowania, być może wbrew wyraźnej intencji ustawodawcy. Ma to istotne znaczenie z punktu widzenia zasady, że kompetencji do działania instytucji publicznych nie można domniemywać, organy władzy mają działać na podstawie i w granicach prawa, a w ich przypadku – odmiennie niż w zakresie praw i wolności obywateli – znajduje zastosowanie zasada: **„co nie jest wyraźnie dozwolone, jest zakazane”**.

9.

Jednym z rodzajów kontroli operacyjnej jest uzyskiwanie i utrwalanie treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych. Nie ulega aktualnie wątpliwości, iż czynność ta nie polega wyłącznie na nagrywaniu i podsłuchiwaniu klasycznych rozmów telefonicznych. Chodzi także o takie rozmowy, które prowadzone są za pomocą komunikatorów typu Signal czy Whatsapp. Trudno w realiach XXI w. zakwestionować dopuszczalność stosowania programu komputerowego pozwalającego na podsłuchiwanie rozmów prowadzonych za pomocą wspomnianych aplikacji. Trzeba jednak zastrzec, że również i ten rodzaj kontroli musi być realizowany analogicznie do klasycznego podsłuchu

telefonicznego, co oznacza, że służby mogą słuchać i rejestrować rozmowy prowadzone przez użytkownika urządzenia, lecz **nie są uprawnione do ich inicjowania.**

Analogiczne zasady prowadzenia kontroli operacyjnej dotyczą uzyskiwania i utrwalania obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne. Przepisy prawa nie precyzują, w jaki sposób należy dokonywać takich czynności. Regulacje te wyraźnie nie wykluczają też możliwości uzyskiwania i utrwalania obrazu lub dźwięku za pomocą aparatu/kamery i mikrofonu, w które wyposażony jest system informatyczny należący do figuranta. Jednak **kontrola operacyjna nie może *de lege lata* polegać na przejmowaniu kontroli nad systemem informatycznym użytkownika (telefonu/tabletu) i wykonywaniu przy jego pomocy takich aktywności, które nie są realizowane przez dysponenta urządzenia.**

Skoro stosowanie różnych rodzajów inwigilacji może odbywać się w ramach **kontroli operacyjnej**, to realizujące ją służby zobowiązane są to jej prowadzenia w sposób **pasywny** w tym sensie, iż nie mogą przejmować kontroli nad urządzeniem figuranta. Oczywiste jest, że w przypadku stosowania tradycyjnego podsłuchu telefonicznego funkcjonariusze nie są uprawnieni do inicjowania połączeń z telefonu podsłuchiwanego. Ich uprawnienie sprowadza się jedynie do sprawdzania tego, z kim i o czym rozmawia figurant. Inicjowanie określonych działań, w tym swoiste prowokowanie do zachowań pozwalających na wykrycie przestępstwa poprzedzone wiarygodnymi informacjami, że zostało ono popełnione, jest możliwe tylko w przypadku istnienia ku temu wyraźnych i precyzyjnych podstaw ustawowych.

Przykładem takiej regulacji jest art. 19a ustawy o Policji, który daje służbom możliwość przeprowadzenia tzw. „zakupu kontrolowanego". Ustawodawca nie stworzył podobnego przepisu dotyczącego podejmowana działań/aktywności w stosunku do urządzenia elektronicznego figuranta.

Artykuł 19 ust. 6 ustawy o Policji przewiduje w pkt. 4 kompetencję do prowadzenia kontroli operacyjnej polegającej na „uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych". Już samo językowe ujęcie przepisu nie pozostawia wątpliwości, że chodzić może jedynie o pozyskanie danych zagregowanych w danym systemie z uwagi na jego natywne funkcjonalności zaakceptowane przez administratora (np. użytkownika smartfonu).

Zgodnie ze Słownikiem Języka Polskiego (*sjp.pwn.pl*) „uzyskać" znaczy tyle co „osiągnąć, otrzymać, zdobyć", a „utrwalać" znaczy „zarejestrować dźwięki, obrazy na taśmach, płytach, w pamięci komputera itp. w celu ich późniejszego odtworzenia; też: zapisać tekst". Obie te czynności nie są zawieszone w próżni, lecz wyraźnie odnoszą się funkcjonalnie do danych zawartych w określonym systemie. Zaś zwrot „zawarty" znaczy tyle, co „będący składnikiem czegoś lub znajdujący się w czymś". Oznacza to, że na gruncie interpretacji językowej omawianego przepisu, w zarysowanym wcześniej kontekście konstytucyjnym, jako klarowny jawi się wniosek, iż **utrwalanie i uzyskiwanie dotyczyć może jedynie takich danych, które temporalnie znalazły się już w danym systemie przed podjęciem kontroli operacyjnej.**

Tytułem przykładu, jeśli system samodzielnie nie ściąga poczty elektronicznej lub plików z chmury, nie nasłuchuje dźwięków i nie rejestruje dźwięku lub obrazu, to uruchomienie tych funkcjonalności wykracza poza kompetencje przydane służbom na gruncie omawianych regulacji. **Funkcjonariusze nie mogą też sterować urządzeniem figuranta w taki sposób, by dokonać na nim takich operacji, których w czasie rzeczywistym nie podejmuje sam figurant. Nie są więc uprawnieni do całkowitego panowania nad cudzym telefonem, tabletem, komputerem** itp., które przekształcałoby je w swoisty „hub" do aktywnego pobierania informacji z zewnętrznych systemów zintegrowanych z danym urządzeniem.

Wykonywanie tego rodzaju czynności pozwalałoby na totalną inwigilację jednostki. Jej stosowanie jest materią niezwykle wrażliwą z punktu widzenia praw i wolności obywatelskich, stanowi bowiem najdalej idącą ingerencję w jej prywatność. Taki sposób wykonywania kontroli operacyjnej pozwalałby na obserwację człowieka nawet w najbardziej osobistych i intymnych dla niego sytuacjach, i pozyskiwanie najwrażliwszych danych. Tego rodzaju środki chętnie stosowane są w państwach totalitarnych w celu uzyskania całkowitej kontroli nad obywatelami. Państwa te kierują się bowiem przekonaniem, że jeżeli władza będzie wiedziała o obywatelu wszystko, to wykorzystując zdobyte w ten sposób informacje będzie mogła realnie wpływać na zachowania takiego obywatela, dla realizacji określonych celów politycznych. **Sytuacja taka nie może zostać zaakceptowana w warunkach demokratycznego państwa prawnego, pod rządami aktualnej Konstytucji Rzeczypospolitej.**

Zakaz podejmowania omawianych czynności nie może mieć jednak charakteru bezwzględnego. Pojawienie się istotnych zagrożeń

bezpieczeństwa publicznego może uzasadniać totalną inwigilację osób będących źródłem zagrożenia. Jak wynika to z przeprowadzonych rozważań natury konstytucyjnej i konwencyjnej, od regulacji tego typu wymagać trzeba precyzji. Powinny dotyczyć one bardzo wąskiej grupy przypadków. Stosowna norma kompetencyjna, zezwalająca na totalną inwigilację, musi dotyczyć wyłącznie najpoważniejszych przestępstw, czyli czynów o charakterze terrorystycznym lub godzących w najistotniejsze dobra prawne, w tym w szczególności życie lub zdrowie innych osób.

De lege lata obecne regulacje wymagań tych nie spełniają. **Przepis kompetencyjny rangi ustawowej, zezwalający na generalne uzyskiwanie i utrwalanie obrazu lub dźwięku razi swą ogólnością, winien więc być interpretowany zawężająco, przy przyjęciu ustrojowego założenia istnienia w Polsce państwa demokratycznego.**

Nie jest oczywiście wykluczone wprowadzenie przez ustawodawcę wyraźnej i precyzyjnej podstawy prawnej dla utrwalania obrazu lub dźwięku również poprzez włączenie kamerki lub mikrofonu urządzenia elektronicznego przez służby bez zgody lub wiedzy jego użytkownika. Kompetencja ta powinna jednak, jak już wspomniano, dotyczyć tylko najpoważniejszych przestępstw (winna więc zawierać ich autonomiczny katalog), a także określać szereg dodatkowych, restrykcyjnych warunków materialnoprawnych (wymóg określoności i taksatywności form kontroli) oraz wymogów proceduralnych, które muszą zostać spełnione w szczególności przed wdrożeniem kontroli wobec konkretnej osoby.

Przeprowadzone rozważania oznaczają, że nie stoi w sprzeczności z obowiązującymi przepisami uzyskiwanie i utrwalanie obrazu i dźwięku,

rejestrowanego przez jego dysponenta za pomocą funkcjonalności samego urządzenia. Dozwolone jest zatem pobranie zdjęcia/ filmu/nagrania audio, które wykonał sam użytkownik.

Nie jest natomiast dopuszczalne użycie programów komputerowych bądź ich funkcji, które umożliwią – poprzez uzyskanie właściwych uprawnień systemowych – sterowanie sprzętowymi zasobami systemu informatycznego celem uruchomienia tego samego aparatu/mikrofonu, i następnie uzyskanie w ten sposób zainicjowanej sekwencji zapisu danych. Nie jest dozwolone samodzielne uruchamianie przez służby, w ramach kontroli operacyjnej, mikrofonu/aparatu w urządzeniu osoby poddawanej kontroli celem zapisu nagrania dźwiękowego/obrazu i uzyskiwania w ten sposób określonych danych.

10.

Podobne wnioski dotyczą kolejnych rodzajów kontroli operacyjnej w postaci uzyskiwania i utrwalania treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej oraz uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych.

Jak już wspomniano, w obecnym stanie prawnym inwigilujący nie może uzyskać kontroli nad cudzym urządzeniem elektronicznym ani robić z pamięcią urządzenie nic więcej ponad to, co czyni sam użytkownik (nie może inicjować zdarzeń systemowych ani interakcji z innymi systemami/programami). Sprawia to, że **funkcjonariusz może w zgodzie z prawem pozyskiwać i utrwalać jedynie te dane,**

które już znajdują się w pamięci urządzenia i są wynikiem aktywności samego użytkownika. Nie jest on zaś uprawniony do pozyskiwania dodatkowych danych, które nie znajdują się w systemie informatycznym i nie znalazły się tam na skutek działania użytkownika.

Dotyczy to wszystkich danych, w tym pochodzących z poczty elektronicznej. **Inwigilujący może więc jedynie pozyskiwać i utrwalać wiadomości, które zostały zapisane w pamięci urządzenia, nie ma natomiast uprawnienia samodzielnie logować się na zewnętrzne serwery**, czy nawet korzystając ze zintegrowanych na tymże urządzeniu zewnętrznych systemów informatycznych inicjować komunikatów/komend, których efektem byłoby pobranie dodatkowych danych na kontrolowane urządzenie, co rzekomo miałoby mieścić się w przesłance „pozyskiwania" oraz „utrwalania" danych. Zatem, przykładowo, nawet w przypadku skonfigurowanego programu pocztowego, który przechowuje na danym urządzeniu maile z ostatnich 30 dni, nie jest dopuszczalna zmiana ustawień programu, aby na dane urządzenie pobrane zostały wiadomości z 90 dni, ani też pobieranie danych/plików z zewnętrznych, nawet skonfigurowanych usług chmurowych, jeśli sam użytkownik takiej czynności nie wykonał samodzielnie. Analogicznie, niemożność inicjalizacji modułów sprzętowych wyklucza możliwość samodzielnego włączenia nadajnika GPS czy żyroskopu. W zakresie uprawnień służb mieści się natomiast monitorowanie tego, co użytkownik robi na swym urządzeniu i pozyskiwanie (pobieranie) tych danych (informacji), które zostały na niego ściągnięte przez użytkownika inwigilowanego systemu informatycznego.

Co się tyczy programów komputerowych pobierających z telefonu/tabletu/innego urządzenia osoby objętej kontrolą operacyjną dane dostępowe (hasła/klucze) pozwalających na logowanie się na serwerach z pocztą elektroniczną, bankowych czy portalach społecznościowych należy stwierdzić, że ich użycie jest zgodne z przepisami polskiego prawa. Jednakże pobranie wspomnianych danych jest dopuszczalne jedynie wtedy, gdy inwigilujący pozyska je z pamięci urządzenia. Natomiast **sprzeczne z przepisami polskiego prawa jest samodzielne przeglądanie i pobieranie danych zgromadzonych w tych serwerach i portalach po odrębnym zalogowaniu się do nich za pomocą pobranych danych dostępowych (haseł/kluczy) przez funkcjonariusza prowadzącego inwigilację.** Czynność taka polega bowiem na zakazanych, dodatkowych aktywnościach ze strony funkcjonariusza, nie ograniczających się do monitorowania tego, co jest przeglądane na urządzeniu przez jego użytkownika lub uzyskiwaniu już zapisanych danych.

11.

Brak podstaw, by wykluczyć dopuszczalność pozyskiwania danych z pamięci urządzenia, które zostały wytworzone przed datą postanowienia sądowego o udzieleniu zgody na stosowanie kontroli operacyjnej. Trzeba jednak zaznaczyć, że jeżeli informacje takie nie dadzą podstaw do wszczęcia postępowania karnego lub ujawnienia ich w toku takiego postępowania, wówczas ich zapis powinien zostać protokolarnie zniszczony.

Wątpliwości musi zaś budzić pozyskiwanie z urządzenia tych danych, które pochodzą sprzed czasu popełnienia przestępstwa, jeżeli z góry wiadomo, że nie mogą one mieć

znaczenia dla jego wykrycia lub ujawnienia dowodów jego popełnienia. Pozyskiwanie takich danych nie spełnia wymogu konieczności, jawi się także jako niecelowe i nieproporcjonalne w świetle standardu konstytucyjnego.

12.

Stosowanie kontroli operacyjnej wymaga zgody sądu okręgowego, wyjątkiem jest art. 9 ustawy z 10 czerwca 2016 r. o działaniach terrorystycznych (Dz.U.2021.2234 t.j., na podstawie którego szef ABW może zarządzić inwigilację wobec cudzoziemca. Przepis ten musi budzić zasadnicze wątpliwości konstytucyjne. Nie przewiduje on bowiem przede wszystkim możliwości poddania zarządzenia szefa ABW – chociażby następczej – kontroli sądowej. Wydaje się z tego powodu, że stosując bezpośrednio przepisy Konstytucji, winno się uznać, że niedopuszczalne jest sięganie przez służby po tę procedurę (taka praktyka została wykluczona przez ETPCz w sprawie EKIMDZHIEV i inni przeciwko Bułgarii, wyrok z dnia 11 stycznia 2022 r., skarga nr 70078/12). Oznacza to, że jeśli ABW chce stosować takie środki inwigilacji, jakie są przewidziane w omawianym przepisie, winna sięgnąć po ogólne regulacje dotyczące kontroli operacyjnej.

W przypadku niektórych służb właściwy do udzielenia zgody będzie Sąd Okręgowy w Warszawie (m. in. ABW, SKW i CBA). Pisemny wniosek o jej wdrożenie składa szef właściwej służby po uzyskaniu pisemnej zgody Prokuratora Generalnego (w niektórych przypadkach wystarczająca będzie zgoda prokuratora okręgowego, co nastąpi wówczas, gdy wniosek o stosowanie kontroli operacyjnej pochodzi od komendanta wojewódzkiego Policji). Przepisy ustaw przewidują przypadki, kiedy rozpoczęcie kontroli operacyjnej nastąpi bez uprzedniej

zgody sądu. Może to nastąpić w przypadkach nie cierpiących zwłoki, jeżeli mogłoby to spowodować utratę informacji, zatarcie albo zniszczenie dowodów przestępstwa. Wówczas kontrolę operacyjną zarządza szef właściwej służby po uzyskaniu pisemnej zgody Prokuratora Generalnego (niekiedy prokuratora okręgowego). W takich sytuacjach stosujący kontrolę musi się jednocześnie zwrócić do właściwego sądu okręgowego o jej zatwierdzenie. Jeżeli sąd w ciągu 5 dni od dnia zarządzenia kontroli nie wyda zgody następczej, wówczas kontrola winna ulec przerwaniu, zaś materiały zgromadzone w jej toku trzeba protokolarnie zniszczyć.

Do wniosku o kontrolę operacyjną powinien zostać dołączony materiał, który uzasadnia jej stosowanie. **Nic nie stoi na przeszkodzie, by sąd okręgowy zwrócił się do wnioskodawcy o jego uzupełnienie. Wnioskujący powinien również, poza spełnieniem szeregu wymogów formalnych, wykazać w swym wniosku, że spełniona została przesłanka subsydiarności. Od wnioskodawcy powinno się również wymagać wykazania, że zastosowanie określonych środków kontroli jest celowe, konieczne i proporcjonalne. W ramach tej powinności mieści się też oczekiwanie udowodnienia, że sięgnięcie po określone rodzaje kontroli operacyjnej jest proporcjonalne, a więc nie jest zbyt dolegliwe dla jednostki w porównaniu do celu, którego osiągnięciu ma służyć inwigilacja.**

Wniosek o zastosowanie kontroli operacyjnej musi zawierać wskazanie miejsca oraz sposobu jej stosowania oraz rodzaj przeprowadzonej kontroli. Trzeba w nim też ująć dane osoby lub inne dane, pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana jest kontrola operacyjna (zob. np. art. 19 ust. 7 pkt. 4 i 5 ustawy o Policji). Należy więc stwierdzić, że wniosek musi zawierać wskazanie sposobu stosowania konkretnych rodzajów kontroli,

o których mowa w art. 19 ust. 6 ustawy o Policji, 19 ust. 6 ustawy o CBA, art. 17 ust. 5 ustawy o CBA, art. 31 ust. 4 ustawy o SKW, art. 118 ust. 3 ustawy o KAS, art. 9e ust. 7 ustawy o SG lub art. 43 ustawy o SOP. **Wnioskodawca musi więc czytelnie oznaczyć środki techniczne, mające służyć do przeprowadzenia kontroli operacyjnej.**

Taki standard został wskazany w wyroku Trybunału Konstytucyjnego, K 23/11, w którym podkreślono, że z punktu widzenia ochrony konstytucyjnych wolności i praw niezbędne jest zobowiązanie organów wnoszących o zarządzenie kontroli do wskazania określonego w prawie środka pozyskiwania informacji i dowodów w konkretnej sprawie oraz nałożenie na organy zarządzające takie czynności obowiązku wyrażenia zgody na konkretny rodzaj środka, służącego pozyskiwaniu informacji. Z orzeczenia trybunalskiego wynikają trzy główne wnioski. **Po pierwsze – używany przez służby środek musi być określony w prawie. Po drugie – winien on zostać wprost wskazany we wniosku o kontrolę operacyjną. Po trzecie – przekazane sądowi informacje na temat środka służącego do stosowania kontroli muszą być wystarczające do zbadania, czy stosowanie w konkretnej sprawie takiego instrumentu jest zgodne z przepisami polskiego prawa** ze względu na wagę przestępstwa, jakiemu ma zapobiec stosowanie tego środka, jak też charakter praw i wolności konstytucyjnych, które mogą zostać naruszone na skutek jego zastosowania, innymi słowy czy spełniony został wymóg proporcjonalności.

Informacje te muszą więc być na tyle pełne, by sędzia był w stanie zweryfikować, czy w toku kontroli operacyjnej nie będą używane takie programy lub takie ich funkcjonalności, których użycie jest niezgodne z polskim prawem lub będzie

to *in concreto* nieproporcjonalne. Sąd musi zatem wejść w posiadanie wszelkich informacji pozwalających miarodajnie ustalić, jak działa instrument, na użycie którego ma wyrazić zgodę. Jeśli informacji takie nie zostaną zawarte we wniosku, sąd winien zwrócić się do wnioskodawcy o jego uzupełnienie. W razie braku uzupełnienia wskazanych informacji, sąd powinien nie uwzględnić wniosku o zastosowanie kontroli operacyjnej.

Bezpodstawne jest przy tym stanowisko, że opisane informacje nie muszą być przekazane sądowi z powodu konieczności ochrony przez służby informacji o używanych przez nie środkach technicznych i metodach ich pracy operacyjnej. Stanowisko to jest bezpodstawne, ponieważ dostateczną ochronę wskazanych informacji zapewnia „oklauzulowanie" wniosku o zastosowanie kontroli operacyjnej, zaś samo postępowanie w przedmiocie jego rozpoznania toczy się z wyłączeniem jawności, przy zachowaniu rygorów przewidzianych dla przetwarzania informacji niejawnych. Co więcej, jeśli materiał zgromadzony w toku kontroli zostanie procesowo wykorzystany w postępowaniu karnym, wówczas i tak będzie możliwe ustalenie formy przeprowadzenia konkretnych czynności operacyjno-rozpoznawczych.

13.

W świetle powyższych regulacji oraz instruktywnych uwag Trybunału Konstytucyjnego należy uznać, że co do zasady nie ma przeszkód, by używać programów komputerowych, które służyłyby do wykonywania czynności wskazanych w art. 19 ust. 6 ustawy o Policji, art. 19 ust. 6 ustawy o CBA, art. 17 ust. 5 ustawy o CBA, art. 31 ust. 4 ustawy o SKW, art. 118 ust. 3 ustawy o KAS, art. 9e ust. 7 ustawy o SG, art. 43 ustawy o SOP. Możliwość użycia tych programów ma jednak

granice; **ich aplikacja musi się mieści w ustawowych ramach.** Nie chodzi przy tym jedynie o samą możliwość posiadania przez służby konkretnego programu, ale dopuszczalność jego użycia do kontroli operacyjnej, o czym była mowa wcześniej. Przykładowo, art. 32a ustawy o ABW daje tej służbie uprawnienia do posiadania programu „szpiegowskiego" działającego w tożsamym dla Pegasusa modelu atakowania podatności programowych i atakowania systemów informatycznych. Niemniej jednak przepis ten dotyczy wyłącznie działań polegających na ocenie bezpieczeństwa systemów informatycznych, nie zaś prowadzenia kontroli operacyjnej.

Trzeba zarazem pamiętać, że zadaniem czynności z art. 19 ust. 6 ustawy o CBA, art. 17 ust. 5 ustawy o CBA, art. 31 ust. 4 ustawy o SKW, art. 118 ust. 3 ustawy o KAS, art. 9e ust. 7 ustawy o SG, art. 43 ustawy o SOP jest **kontrola, a więc pozyskiwanie określonych informacji w celach weryfikacyjnych** pozwalających zapobiec przestępstwu katalogowemu lub umożliwiających pozyskanie dowodów na potrzeby procesu karnego. Nie można więc stosować ich do prowokacji, fabrykowania danych czy też „podrzucania" figurantowi materiału dowodowego w celu skierowania wobec niego postępowania karnego.

W tym kontekście ważne jest, że szereg czynności operacyjno-rozpoznawczych, w tych składających się na kontrolę operacyjną, realizuje znamiona opisanych w ustawie karnej czynów zabronionych. Ich legalizacja jest możliwa dopiero wtedy, gdy funkcjonariusze publiczni podejmują je w granicach przyznanych im uprawnień. Uprawnienia te powinny być przy tym precyzyjnie określone. **Funkcjonariusz publiczny musi dysponować wyraźną podstawą prawną, by podjąć w jej granicach konkretne zachowanie nie narażając się**

przy tym na zarzut odpowiedzialności karnej co najmniej za przekroczenie uprawnień. Brak właściwej podstawy kompetencyjnej lub działanie poza jej granicami oznacza popełnienie przez funkcjonariusza czynu przestępnego.

14.

Użycie w toku kontroli operacyjnej programu komputerowego, którego stosowanie jest niedozwolone w przepisach polskiego prawa, wywołuje szereg negatywnych konsekwencji zarówno na płaszczyźnie prawa materialnego, jak i procesowego. **Dowód uzyskany za pomocą takiego programu nie będzie mógł zostać wykorzystany w procesie karnym** w szczególności w kontekście art. 168a k.p.k., który stanowi: „Dowodu nie można uznać za niedopuszczalny wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego, chyba że dowód został uzyskany w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności".

Przepis ten jest w literaturze i orzecznictwie zasadnie wykładany w taki sposób, iż należy uznać za niedopuszczalny dowód, jeżeli został on uzyskany przez funkcjonariusza publicznego w związku z pełnieniem przez niego obowiązków służbowych z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego w rozumieniu art. 1 § 1 k.k. (zob. np. K. Lipiński, Glosa do wyroku Sądu Apelacyjnego we Wrocławiu z 27 kwietnia 2017 r., II AKa 213/16, Palestra 2017, nr 10, s. 83-88; postanowienie SN z 26 czerwca 2019 r., IV KK 328/18; wyrok SA we Wrocławiu z 22 listopada 2017 r., II AKa 224/17).

Charakter oprogramowania Pegasus i jego możliwość zasadzające się na nieskrępowanej edycji danych zawartych w urządzeniu sprawiają, iż na etapie prowadzonego postępowania, w przypadku przedłożenia przez oskarżyciela materiałów uzyskanych za pomocą tego oprogramowania, bądź w przypadku zabezpieczenia urządzenia końcowego (telefonu/tabletu), które poddane zostałoby ocenie przez biegłego, **sądy powinny uznawać te dowody za niedopuszczalne na gruncie obowiązującego prawa.** Niepodobna bowiem stwierdzić, czy dane nie były w jakikolwiek sposób modyfikowane, czy operator Pegasusa nie inicjował połączeń czy wysyłki wiadomości bez wiedzy ofiary, czy wręcz nie przesłał na urządzenie dodatkowych plików o charakterze przestępnym, których odkrycie przez biegłego, na etapie postępowania sądowego, miałoby świadczyć o winie zaatakowanego.

Do wyobrażenia jest sytuacja, w której w ramach czynności operacyjnych z wykorzystaniem analizowanego systemu, przy braku jakiegokolwiek nadzoru ze strony sądu, w telefonie użytkownika umieszczone zostaną np. materiały pedofilskie. „Anonim” wysłany przez te same służby doprowadzi do zatrzymania w świetle kamer posiadacza telefonu, a następnie zatrzymania tegoż telefonu, na którym biegły odkryje dodane tam materiały. Możliwości obrony przed opisanym atakiem są w zasadzie iluzoryczne; brak będzie w wielu przypadkach realnej możliwości przestawienia przeciwdowodu, że konkretny plik został tam umieszczony zdalnie za pomocą systemu inwigilującego. Narzędzia służące do weryfikacji urządzenia mogą nie wykrywać najnowszych wersji oprogramowania Pegasus, co negatywnie oddziałuje na szereg postępowań karnych również w sprawach osób

rzeczywiście dopuszczających się czynów o charakterze przestępnym (*https://github.com/mvt-project/mvt).*

Co do zasady w przypadku zabezpieczania nośnika danych, wykonywana jest wpierw – po wcześniejszym podłączeniu stosownego blokera zapisu (celem uniemożliwienia nadpisania i modyfikacji zabezpieczonych danych) – kopia binarna, z której obliczana jest suma kontrolna mająca zagwarantować, że dane poddane analizie przez biegłego będą tożsame z danymi znajdującymi się na zabezpieczonym nośniku i nie dojdzie do jakiejkolwiek zmiany danych na skutek wdrożonej analizy.

Przypadek, w którym na określonym urządzeniu instalowany jest program (agent Pegasusa), mający uprawnienia administracyjne do swobodnego manipulowania zgromadzonymi tam danymi sprawia, że tak czy inaczej **nie jest możliwe przydanie takim dowodom waloru jakiejkolwiek procesowej wiarygodności.** Nie świadczy to negatywnie o samym oprogramowaniu szpiegowskim, lecz o jego wykorzystaniu niezgodnie z przeznaczeniem: nie był on stworzony dla wyłącznie pasywnego zbierania informacji, ale do aktywnej pracy wywiadowczej, w której procesowe wykorzystywanie zgromadzonych danych ma zdecydowanie wtórne znaczenie w stosunku do celów wywiadowczych, np. zapobiegnięcia zamachowi terrorystycznemu.

Może się także zdarzyć, że zgoda na wdrożenie kontroli operacyjnej za pomocą nielegalnego programu komputerowego zostanie wydana przez sąd wskutek wprowadzenia sędziego w błąd przez wnioskodawcę. W takich sytuacjach wyrażenie zgody na kontrolę operacyjną z użyciem takiego programu nie może być skuteczne, zaś pozyskane za jego pomocą materiały nie mogą zostać użyte w procesie karnym. Oznacza to, że **wyrażona formalnie zgoda sądu**

na prowadzenie kontroli operacyjnej nie może legalizować użycia programu, którego stosowanie jest niedopuszczalne na gruncie polskiego prawa.

15.

Obecne regulacje dotyczące kontroli operacyjnej nie nakładają na organy władzy publicznej obowiązku poinformowania figuranta o tym, że był poddawany kontroli operacyjnej. Nadto obywatelowi, wobec którego wdrożona została kontrola, nie przysługuje środek zaskarżenia na postanowienie o poddaniu go tak inwazyjnym czynnościom operacyjno-rozpoznawczych. **Taki stan rzeczy rażąco narusza wynikające z art. 45 ust. 1 Konstytucji prawo do sądu w kontekście wynikającej z art. 78 i 176 ust. 1 Konstytucji zasady dwuinstancyjności postępowania.**

W demokratycznym państwie prawnym nie można tolerować sytuacji, w której jednostka nie może domagać się zbadania zasadności i zgodności z prawem podejmowanych wobec niej czynności przez organy władzy publicznej, które w sposób najbardziej drastyczny ingerują w jej prywatność lub życie rodzinne. Z tego powodu **ustawodawca powinien wprowadzić stosowne rozwiązania prawne, które nałożą na organy obowiązek poinformowania jednostki, po zakończeniu kontroli operacyjnej, o jej stosowaniu oraz będą przewidywać możliwość złożenia zażalenia na postanowienie o udzielenie zgody na stosowanie kontroli operacyjnej.**

Twierdzenie takie koresponduje z wyrokiem Trybunału Konstytucyjnego, K 23/11, w którym wskazano:

„Niejawne pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych. Przede wszystkim ma istnieć ***obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat, i to bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne****, które przypadkowo stały się obiektem kontroli. Powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji, co oczywiste, narażałoby je na nieskuteczność. Dlatego ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie. Tego wymagania nie uchyla wprowadzenie innych, zastępczych rozwiązań, jak choćby pełnomocnika osoby kontrolowanej. Na konieczność ustanowienia takiego obowiązku informacyjnego zwracał już uwagę TK w postanowieniu z 25 stycznia 2006 r., sygn. S 2/06. Zapewnienie informacji jest przesłanką skorzystania przez jednostki z wynikającego z art. 51 ust. 3 Konstytucji prawa dostępu do urzędowych dokumentów i zbiorów danych. Co do zasady, wszystkie zgromadzone i przetwarzane przez władze publiczne dane o jednostce - chociażby nawet nie tworzyły jednego zorganizowanego zbioru - powinny być udostępniane tej osobie, jeżeli wystąpi ze stosownym żądaniem. Warunkiem (i to podstawowym) skorzystania z prawa unormowanego w art. 51 ust. 3 Konstytucji jest wiedza o zgromadzeniu określonych danych i istnieniu ich zbioru.* ***Zaniechanie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji.***

Skoro jednostka nie wie o zebraniu na jej temat określonych informacji - ponieważ dokonało się to w sposób niejawny, bez jej wiedzy i zgody - nie dysponuje możliwością uzyskania dostępu do nich i nie może żądać ich sprostowania lub usunięcia na warunkach określonych w art. 51 ust. 4 Konstytucji. Obowiązek informacyjny w powyższym zakresie ma eliminować ryzyko niekontrolowanego tworzenia oraz utrzymywania zbiorów danych nieprzydatnych dla postępowań prowadzonych przez organy państwa, lecz potencjalnie wartościowych z punktu widzenia przyszłych, bliżej nieokreślonych czynności (…)".

Trybunał Konstytucyjny jednocześnie podkreślił, że w pewnych wypadkach można odstąpić od ustanowienia obowiązku informacyjnego. Dodał jednak, iż może to nastąpić szczególnie w takich sytuacjach, gdy dane zostały pozyskane wyłącznie przypadkowo i nie podlegają dalszej analizie, czy też gdy pozyskano dane dostępne w publicznych rejestrach.

Nie ulega wątpliwości, że **od obowiązku tego nie można odstąpić w razie drastycznego wkroczenia w prawo do prywatności, jak to ma miejsce w przypadkach wykorzystania programów o funkcjonalnościach Pegasusa.**