Komentarz KBN

Nr 4 (93) / 2022 21 lutego 2022 r.

Niniejsza publikacja ukazuje się na warunkach międzynarodowej licencji publicznej Creative Commons 4.0 – uznanie autorstwa – na tych samych warunkach – użycie niekomercyjne.
This work is licensed under a Creative Commons Attribution – NonCommercial – ShareAlike 4.0 International License.

# Mity o skrzydlatym koniu. Wokół debaty o Pegasusie i kontroli operacyjnej

Arkadiusz Nyzio

**Kontrowersje wokół spyware'owego oprogramowania Pegasus przyczyniły się do tego, że po raz pierwszy od sześciu lat w przestrzeni publicznej szerzej zaistniał temat kontroli operacyjnej. Także tym razem zagadnienie czynności operacyjno-rozpoznawczych sprawiło, że media i portale społecznościowe zapełniły się błędami merytorycznymi, uproszczeniami i teoriami spiskowymi. Warto pochylić się nad kilkunastoma najpowszechniejszymi mitami, które utrudniają zrozumienie zjawiska i wyciągniecie wniosków koniecznych do uszczelnienia procedury.**

**1. Kontrola operacyjna dotyczy garstki osób. To sprawa marginalna, której nadaje się zdecydowanie zbyt wielkie znaczenie.**

W latach 2010–2020 sama Policja wnioskowała o objęcie kontrolą operacyjną ponad 51 tys. ludzi. W sumie w tych latach zarządzono kontrolę operacyjną wobec około 60 tys. osób, czyli mniej więcej tylu, ilu mieszka w Zamościu czy Przemyślu. Ale na tym nie koniec.

To, że podsłuch zarządzono wobec osoby X, nie oznacza, że podsłuchiwana była tylko osoba X. Podsłuchiwane były jej rozmowy, a zatem także – pośrednio – jej rozmówcy, w tym ludzie, którzy nie mieli żadnego związku ze sprawą, którą interesowały się instytucje bezpieczeństwa. Jeśli podsłuchiwany jest X, z którym zdarza mi się rozmawiać przez telefon, to ja również jestem –

nawet nie mam pojęcia o tym, że mój znajomy X ma (lub może mieć) cokolwiek wspólnego z jakimkolwiek czynem zabronionym. A podsłuch może być prowadzony tygodniami, miesiącami czy nawet latami.

**2. Kontrolę operacyjną prowadzi tylko kilka wyspecjalizowanych służb. Nie ma powodu, aby obawiać się podsłuchu ABW lub SKW – przecież to „specjalne" instytucje, które nie zajmują się „zwykłymi ludźmi", tylko terrorystami czy członkami mafii.**

Prawo do prowadzenia kontroli operacyjnej posiada w Polsce 11 instytucji. Po pierwsze, jest to pięć służb specjalnych: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu i Centralne Biuro Antykorupcyjne (służby cywilne) oraz Służba Wywiadu Wojskowego i Służba Kontrwywiadu Wojskowego (służby wojskowe). Po drugie, uprawnienie to posiadają służby policyjne: Policja, Straż Graniczna, Żandarmeria Wojskowa i Służba Celno-Skarbowa. Po trzecie, uprawnienie to przysługuje także specyficznej instytucji zajmującej się ochroną najważniejszych osób i obiektów w państwie, czyli Służbie Ochrony Państwa. Po czwarte, kontrolę operacyjną może także prowadzić Biuro Nadzoru Wewnętrznego, czyli komórka organizacyjna Ministerstwa Spraw Wewnętrznych i Administracji. Często zapomina się o kontroli operacyjnej prowadzonej przez wywiady, trzeba więc zaznaczyć, że jest to możliwe, ale przy dwóch zastrzeżeniach: wyłącznie w związku z ich działalnością poza granicami państwa oraz wyłącznie za pośrednictwem kontrwywiadów.

Każda z instytucji prowadzi kontrolę operacyjną w granicach swoich właściwości przedmiotowych (czyli w zakresie tego, czym się zajmuje) i podmiotowych (czyli w zakresie tego, kim się zajmuje). Za zdecydowaną większość przypadków kontroli operacyjnej odpowiada Policja, a nie służby specjalne. To właśnie Policja posiada najszerszy katalog przedmiotowy i podmiotowy.

**3. Kontrola operacyjna w Polsce objęta jest uprzednią kontrolą sądową, co oznacza, że za każdym razem to sąd decyduje o rozpoczęciu i przedłużeniu podsłuchu.**

Tak, ale nie do końca. Kontrola uprzednia rzeczywiście jest regułą, ale są od niej wyjątki.

Po pierwsze, w przypadkach „niecierpiących zwłoki", jeżeli mogłoby to spowodować „utratę informacji lub zatarcie albo zniszczenie dowodów przestępstwa", uprawnione instytucje same zarządzają kontrolę operacyjną, jednocześnie zwracając się do właściwego sądu z wnioskiem o wydanie postanowienia w tej sprawie. Sądy mają pięć dni, aby rozpatrzyć wniosek. Jeśli rozpatrzą go negatywnie, służba ma obowiązek wstrzymać kontrolę operacyjną, a następnie protokolarnie i komisyjnie zniszczyć materiały zgromadzone podczas jej stosowania. W 2020 r. około 17% wszystkich policyjnych wniosków złożono w trybie przypadków „niecierpiących zwłoki".

Po drugie, szef ABW może zarządzić podsłuchiwanie osoby niebędącej obywatelem RP w celu „rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym". Zarządzenie (wraz z uzasadnieniem) szef ABW musi „niezwłocznie" przekazać prokuratorowi generalnemu i ministrowi koordynatorowi służb specjalnych (jeżeli został powołany). Prokurator generalny może nakazać zaprzestanie czynności inwigilacyjnych. Udział sądu w tej procedurze

w ogóle nie jest przewidziany. Nie dysponujemy też jakimikolwiek danymi dotyczącymi tego, jak często ABW sięga po to uprawnienie. Należy dodać, że jest to rozwiązanie w sposób jaskrawy niezgodne z polską konstytucją. Wkrótce minie sześć lat jego obowiązywania.

**4. Kontrola uprzednia realizowana przez sądy zapobiega patologiom związanym z podsłuchami. Niewielka liczba odrzucanych wniosków potwierdza jej rygorystyczny charakter.**

W sensie formalnym kontrola operacyjna poprzedzona jest rozbudowaną procedurą wstępną. W praktyce sądowa kontrola uprzednia ma jednak w dużej mierze wadliwy lub wręcz fasadowy charakter.

Wniosek o zarządzenie kontroli operacyjnej właściwa instytucja bezpieczeństwa przedstawia wraz z „materiałami uzasadniającymi potrzebę zastosowania kontroli operacyjnej". Ustawodawca nie stworzył zamkniętego katalogu informacji, które muszą znaleźć się we wniosku, wskazał jednak, że muszą być to „w szczególności": 1. „Numer sprawy i jej kryptonim, jeżeli został jej nadany"; 2. „Opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej"; 3. „Okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków"; 4. „Dane osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania"; 5. „Cel, czas i rodzaj prowadzonej kontroli operacyjnej".

W związku ze sprawą oprogramowania Pegasus w przestrzeni publicznej pojawiło się wiele wątpliwości dotyczących tego, czy sędziowie są informowani o tym, jakie narzędzie techniczne będzie stosowane w realizacji kontroli operacyjnej. Warto zatem przypomnieć, że pojęcie „kontrola operacyjna" obejmuje katalog rozwiązań wykraczających poza telefoniczny podsłuch (podsłuch telefonii komórkowej, PTK), z którym to jest najczęściej kojarzone. W instytucji kontroli operacyjnej chodzi o niejawne pozyskiwanie danych stanowiących treść komunikacji pomiędzy ludźmi. Obejmuje ona także przegląd korespondencji (w tym elektronicznej) i przesyłek, zapis rozmowy na czacie, treść SMS-ów i MMS-ów, zapis wideokonferencji czy uzyskiwanie i utrwalanie obrazu lub dźwięku z pomieszczeń, środków transportu lub miejsc „innych niż miejsca publiczne". Podsłuch nie musi więc mieć związku z komunikacją teleinformatyczną, ale może np. polegać na zainstalowaniu ukrytej kamery lub pluskwy podsłuchowej (tzw. podsłuch pokojowy) w mieszkaniu czy samochodzie. We wniosku o zarządzenie kontroli właściwa instytucja bezpieczeństwa powinna umieścić informację o – jak wspomniano powyżej – rodzaju kontroli operacyjnej, czyli narzędziu, przy pomocy którego będzie ona prowadzona. Rodzaje kontroli operacyjnej określone są jednobrzmiąco we wszystkich ustawach kompetencyjnych właściwych instytucji[1].

[1] Na początku 2016 r. ustawodawca ustanowił następujący katalog rodzajów: „Kontrola operacyjna prowadzona jest niejawnie i polega 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".

Zgodnie z prawem kontrola operacyjna w Polsce powinna być stosowana przy uwzględnieniu dwóch kryteriów prawnych: proporcjonalności i subsydiarności. Jest też kryterium będące ich przedłużeniem, a właściwie syntezą – dla potrzeb tego komentarza będę je nazywał „selektywnością".

Proporcjonalność oznacza, że kontrolę operacyjną można stosować tylko w odniesieniu do ściśle określonych czynów zabronionych, wymienionych we właściwych ustawach kompetencyjnych (tzw. przestępstwa katalogowe). Chodzi o to, aby tak dolegliwe środki były stosowane w związku z równie poważnymi przykładami naruszenia prawa. Samo sformułowanie „przestępstwa katalogowe" jasno wskazuje, że wykluczone jest stosowanie tej instytucji prawnej w związku z wykroczeniami, np. zakłóceniem spokoju lub porządku publicznego czy w związku z kąpielą w miejscu zabronionym. Ale również nie każdy typ przestępstwa może być przesłanką do zarządzenia kontroli. Przykładowo, Policja nie może wnioskować o założenie podsłuchu w związku z przestępstwem uporczywego nękania czy naruszenia intymności seksualnej. Jest to jednak możliwe w przypadku rozboju czy zabójstwa.

Należy dodać, że katalog przestępstw jest ciągle rozszerzany, czemu nie towarzyszy jakiekolwiek zainteresowanie opinii publicznej. Od 30 listopada 2020 r. policjanci mogą stosować kontrolę operacyjną w związku z wytwarzaniem, posiadaniem lub obrotem nowymi substancjami psychoaktywnymi (NSP), czyli tzw. dopalaczami. Wprowadzająca to rozwiązanie ustawa z 30 kwietnia 2020 r. została poparta przez niemal cały Sejm. O wiele szersza zmiana miała miejsce kilka tygodni temu, a przyniosła ją ustawa powołująca policyjne Centralne Biuro Zwalczania Cyberprzestępczości. Niejako „przy okazji", z dniem 12 stycznia br. policyjny katalog przestępstw powiększono o dziewięć pozycji[2]. Na początku listopada 2021 r. opublikowana została kolejna edycja „komentarza inwigilacyjnego" mojego autorstwa, przedstawiającego wszystkie dostępne w Polsce statystyki dotyczące czynności operacyjno-rozpoznawczych. Pisałem w nim, że Policja nie może prowadzić kontroli operacyjnej w związku z kradzieżą z włamaniem – i w tamtym momencie była to prawda. Dziesięć tygodni później art. 279 Kodeksu karnego (kk) dodano jednak do katalogu. Ale uwaga – nie chodzi o każdą kradzież z włamaniem, tylko, jak wskazali projektodawcy, o kradzież z włamaniem „w kontekście środków pieniężnych zapisanych na rachunkach bankowych". Ta intencja prawodawcy nie ma swojego literalnego odzwierciedlenia w przepisach ustawowych, co prowadzi do oczywistego pytania o to, jak sądy będą interpretowały wnioski o zarządzenie kontroli operacyjnej zawierające tę właśnie podstawę prawną[3]. O chaotyczności stanowienia polskiego prawa najlepiej świadczy fakt, że projektodawca postulował wpisanie

[2] Chodzi o przestępstwa: elektronicznej korupcji seksualnej małoletniego (art. 200a), propagowania pedofilii (art. 200b), wprowadzenia w błąd instytucji użyteczności publicznej co do zagrożenia, czyli fałszywego alarmu (art. 224a), bezprawnego uzyskania informacji, czyli hackingu komputerowego (art. 267), niszczenia danych informatycznych (art. 268a), zakłócania systemu komputerowego (art. 269a), wytwarzania programów komputerowych służących do zakłócania systemu komputerowego (art. 269b), kradzieży z włamaniem (art. 279) i oszustwa komputerowego (art. 287).

[3] Na posiedzeniu sejmowej Komisji Administracji i Spraw Wewnętrznych w dniu 30 listopada 2021 r. wiceminister spraw wewnętrznych i administracji Maciej Wąsik mówił, że chodzi o „kradzież z włamaniem np. na konto". Poseł opozycji Konrad Frysztak zauważył: „Ale rozszerzacie ten przepis nie tylko na kradzież z włamaniem danych, ale również na kradzież z włamaniem do kiosku Ruchu… ". Wiceminister odparł niezrażony: „Każdorazowo sąd będzie oceniał, czy jest to metoda adekwatna. To nie jest tak, że policjant naciska guzik i ma kontrolę operacyjną. Pisze

do policyjnego katalogu przestępstwa, które… już w nim było. Chodzi o art. 269 kk (sabotaż komputerowy), który dopisano do katalogu ponad 20 lat temu.

Z kolei subsydiarność zawiera się w formule: „gdy inne środki okazały się bezskuteczne albo będą nieprzydatne". Tym samym kontrola operacyjna nie może być rozwiązaniem, po które sięga się „z automatu", domyślnie, ale dopiero po rozważeniu i wyczerpaniu innych możliwości. Ma to zabezpieczać jednostkę przed niepotrzebnym „pójściem na skróty" przez służby.

„Selektywność" jest pochodną i konsekwencją tych dwóch kryteriów. Kontrola operacyjna powinna być możliwie jak najmniej inwazyjna – zwłaszcza w odniesieniu do osób trzecich. Jak już bowiem wspomniano, inwigilowanie osoby X niechybnie wiąże się z inwigilowaniem jej otoczenia. Przede wszystkim osób jej bliskich, ale także – w niektórych przypadkach – osób postronnych. Kontrola operacyjna powinna być więc zorganizowana w taki sposób, aby do niejawnego pozyskania informacji doszło w jak najmniej dotkliwy dla osób trzecich sposób.

I właśnie te trzy kwestie rozważają sędziowie w ramach kontroli uprzedniej sprawowanej nad kontrolą operacyjną. Najpierw rozstrzygają, czy wnioskowana kontrola operacyjna posiada odpowiednią podstawę prawną. Przykładowo, jeśli Policja wnioskować będzie o kontrolę operacyjną w związku z kradzieżą, sąd ma obowiązek wydać postanowienie odmowne, wskazując w uzasadnieniu, że art. 278 kk nie jest wymieniony przez ustawodawcę jako właściwa przesłanka. Inaczej byłoby w związku z kradzieżą z włamaniem lub w związku z rozbojem, gdyż w odniesieniu do Policji są to „przestępstwa katalogowe". Następnie sąd rozważa, czy spełniono przesłankę subsydiarności. W swoim wniosku właściwa instytucja bezpieczeństwa musi uzasadnić, że „inne środki okazały się bezskuteczne" lub wyjaśnić, dlaczego są „nieprzydatne". W trzeciej kolejności sędzia upewnia się, czy i w jakim zakresie (technicznym, czasowym) proponowane przez wnioskodawców rozwiązania narażają na szwank prywatność osób z otoczenia figuranta.

Jest to sprawa bardziej skomplikowana niż mogłoby się wydawać. Przykładowo, w doktrynie podkreśla się, że kontroli operacyjnej nie można prowadzić wobec obrońcy chronionego przez tajemnicę obrończą (*explicite* stwierdził to w 2011 r. Sąd Najwyższy). Co jednak w sytuacji, w której podsłuch zarządzono wobec osoby X w związku ze sprawą Y, a ta sama osoba ma status oskarżonego w sprawie Z? Instytucja bezpieczeństwa mogłaby w ten sposób wejść w posiadanie informacji objętej zakazem dowodowym. Miałaby wówczas obowiązek zniszczyć wszelkie uzyskane materiały, ale funkcjonariusze, którzy się z nimi zapoznali, nie mogliby ich przecież „odsłyszeć" lub „odzobaczyć". Takie przykłady można mnożyć. Instytucja bezpieczeństwa mogłaby np. wnioskować o założenie podsłuchu w gabinecie lekarza podejrzanego o łapownictwo. Realizacja tego wniosku prowadziłaby do naruszenia prawa do prywatności pacjentów, a także do naruszenia tajemnicy lekarskiej. Wyraźnie inaczej wyglądałaby sytuacja, gdyby wnioskowano o założenie lekarzowi podsłuchu telefonicznego – byłoby to rozwiązanie nieporównywalnie bardziej „selektywne".

---

wniosek, który musi zaakceptować prokurator i musi zaakceptować sąd okręgowy. Panie pośle, ta metoda jest pod nadzwyczajną kontrolą organów sądowych".

Sąd nie rozstrzyga zatem jedynie o tym, czy kontrola operacyjna może mieć miejsce, ale rozważa całość zagadnienia: jej cel, czas i rodzaj czynności. Każdorazowo dokonuje ważenia treści wniosku z konstytucyjnymi zasadami ochrony życia prywatnego (np. art. 47) i wolności komunikowania się (np. art. 49), w związku z art. 31 ust. 3 konstytucji, który określa dopuszczalne ograniczenia w korzystaniu z konstytucyjnych wolności i praw[4]. Drugim punktem odniesienia jest Konwencja o ochronie praw człowieka i podstawowych wolności, którą Polska ratyfikowała trzydzieści lat temu.

Aby odrzucić wniosek o kontrolę operacyjną, sędzia musi dysponować jakimś argumentem. Musi też swoją decyzję uzasadnić. Jeżeli we wniosku podana jest poprawna podstawa prawna i jeżeli znajdzie się w nim przekonujące uzasadnienie wraz z formułką o spełnieniu warunku subsydiarności, to wniosek nie może, tylko musi zostać zaakceptowany. Jeśli sędzia wykryje wadę prawną (np. wnioskodawca zamierza stosować podsłuch w związku z przestępstwem spoza swojego katalogu lub wnioskuje o przyjęcia środka niepotrzebnie inwazyjnego – np. zainstalowania ukrytej kamery w pokoju nauczycielskim, tylko dlatego, że jeden z nauczycieli jest podejrzewany o obrót środkami odurzającymi), ma obowiązek zwrócić na to uwagę i wydać postanowienie odmowne. Przysługuje na nie oczywiście zażalenie, zgodnie z procedurami Kodeksu postępowania karnego (kpk). Służba może też poprawić wniosek i złożyć go ponownie.

W 2020 r. instytucje bezpieczeństwa złożyły wnioski dotyczące 6440 osób, a sądy odrzuciły wnioski dotyczące 29[5]. Sądy nie decydują się na zarządzenie kontroli operacyjnej średnio w przypadku 0,5% osób rocznie (na podstawie danych z lat 2010–2020). Nie wiemy, co jest głównym powodem odrzucania wniosków, ale twierdzenie, że tak niski wskaźnik wynika ze szczelności procedury, świadczy o jej nierozumieniu. W skrócie polega ona bowiem na tym, że wszystkie wnioski pozbawione ewidentnych wad formalnych są akceptowane.

**5. Sędziowie są leniwi. Wydanie postanowienia o zarządzeniu kontroli operacyjnej nie wymaga pisemnego uzasadnienia, ale wydanie postanowienia odmownego – już tak. Sędziowie idą więc na łatwiznę i „taśmowo" podpisują wnioski, bo tak jest po prostu wygodniej.**

Problem ma charakter systemowy, a nie personalny. Sędziowie działają na podstawie prawa i w granicach prawa. Ustawodawca nie wyposażył ich w instrumenty umożliwiające weryfikację wniosków składanych przez służby. Muszą przyjmować ich argumentację za dobrą monetę. Aby napisać postanowienie odmowne, trzeba mieć ku temu podstawy prawne. Sędzia nie może kierować się swoim „widzimisię" lub intuicją. Nie może brać pod uwagę pozamerytorycznych przesłanek, takich jak brak zaufania lub sympatii wobec instytucji-wnioskodawcy czy tego, że w da-

[4] Art. 31 ust. 1 ustawy zasadniczej stanowi, że: „Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw".

[5] W 2020 r. wnioski Policji dotyczyły 5364 osób (prokurator nie wyraził zgody na kontrolę operacyjną odnośnie do 109 osób, a sądy wydały postanowienia odmowne względem 16 osób, dalej analogicznie); Straż Graniczna – 328 (3, 0); CBA – 298 (1, 2); ABW – 214 (0, 7); SKW – 133 (4, 2); Żandarmeria Wojskowa – 87 (1, 2); Służba Celno-Skarbowa w ramach Krajowej Administracji Skarbowej – 16 (0, 0).

nym kwartale „wyrobił już" normę postanowień pozytywnych. Każdy wniosek musi być rozpatrywany indywidualnie. Widząc poprawnie uzupełniony formularz sędzia ma obowiązek wydać postanowienie o zarządzeniu kontroli operacyjnej.

Sędzia otrzymuje na swoje biurko krótki formularz zawierający podstawowe informacje (tak wygląda policyjny wzór wniosku i wzór postanowienia sądu). Postanowienia nie wydaje skład orzekający – z oczywistych powodów (czyli konieczności ochrony informacji niejawnych) sędziowie nie mają możliwości konsultowania sprawy między sobą. Nie mogą korzystać z rady znajomych funkcjonariuszy czy posiłkować się wsparciem merytorycznym zewnętrznych ekspertów. Każde tego rodzaju działanie wiązałoby się z odpowiedzialnością karną i dyscyplinarną.

Decyzja jest podejmowana jednoosobowo. Jedynym instrumentem, jakim dysponuje mający wątpliwości sędzia, jest zarządzenie posiedzenia z udziałem przedstawiciela instytucji-wnioskodawcy i właściwego prokuratora. Ten ostatni również uczestniczy w procedurze kontroli operacyjnej. Zanim wniosek trafi do sądu, przechodzi przez jego ręce. Już na tym etapie może więc trafić „do kosza".

Dodajmy, że nie ma w Polsce sędziów „etatowo" zajmujących się kontrolą operacyjną. Wnioski Policji i Straży Granicznej trafiają do właściwych terytorialnie sądów okręgowych, wnioski Żandarmerii Wojskowej – do właściwych terytorialnie wojskowych sądów okręgowych, wnioski SKW – do wojskowego sądu okręgowego w Warszawie, a wnioski wszystkich pozostałych instytucji – do sądu okręgowego w Warszawie. Sama tylko Policja w 2020 r. złożyła ponad 10 tys. wniosków (czyli składała jeden co 52 minuty) dotyczących ponad 5,3 tys. osób. Tymczasem w tym samym roku wakaty w sądownictwie wynosiły około 10%. Zarzucone ogromem wniosków sądy, zwłaszcza warszawski, mogą więc wprawdzie zażądać od wnioskodawców dodatkowych materiałów i wyjaśnień, ale nie tylko nie mają czasu, aby uczynić z tego regularną praktykę, ale przede wszystkim nie mają ku temu podstaw – przecież od strony formalnej zazwyczaj wszystko się zgadza.

**6. Sędzia może przecież domagać się od właściwej instytucji bezpieczeństwa udostępnienia materiałów śledztwa i na tej podstawie podjąć decyzję, czy kontrola operacyjna jest zasadna. Dlaczego sędziowie nie czytają akt śledztwa?**

Dlatego, że nie ma (jeszcze) żadnego śledztwa.

Najprościej rzecz ujmując, instytucje prawnokarne stosuje się w dwóch trybach: kodeksowym (procesowym) i pozakodeksowym (pozaprocesowym). Tryb kodeksowy jest uregulowany w kpk, a pozakodeksowy – w ustawach kompetencyjnych, czyli aktach prawnych opisujących funkcjonowanie poszczególnych instytucji bezpieczeństwa (np. ustawa o Policji, ustawa o Straży Granicznej, ustawa o CBA itd.).

Niektóre rozwiązania prawnokarne są ściśle związane z postępowaniem karnym[6] i mogą być prowadzone tylko na gruncie przepisów kpk. Inne występują wyłącznie w trybie pozakodeksowym. Są też i takie, które realizowane są w obu trybach, posiadają jednak wówczas odmienne uregulowanie i procedurę. Ich podręcznikowym przykładem jest instytucja zatrzymania osoby, która występuje w sumie w czterech wersjach – procesowej i trzech pozaprocesowych.

Do tego grona należy również podsłuch czy kontrola korespondencji. Można po nie sięgać w związku z toczącym się postępowaniem, na podstawie przepisów kpk. Tę instytucję prawną określa się jako kontrolę procesową. Nie ma ona związku z tematem omawianym obecnie w przestrzeni publicznej.

Będąca przedmiotem kontrowersji kontrola operacyjna jest rozwiązaniem pozaprocesowym (pozakodeksowym), stosowanym „na przedpolu" postępowania karnego. Zgromadzone w jej toku informacje mogą przyczynić się do wszczęcia śledztwa lub dochodzenia oraz uzyskania i utrwalenia dowodów przestępstwa, ale nie muszą.

**7. Narzekanie na podsłuchy w Polsce to użalanie się nad przestępcami.**

Przestępcą jest osoba prawomocnie skazana. W kontrowersjach wokół kontroli operacyjnej nie chodzi o osoby skazane. Więcej nawet – nie chodzi o osoby oskarżone czy chociażby o osoby, którym postawiono zarzuty. Jak wspomniano, chodzi o czynności prawne realizowane „na przedpolu" postępowania karnego. Mowa więc o sytuacji, w której nie toczy się jeszcze postępowanie przygotowawcze, będące pierwszym etapem postępowania karnego.

Kontrola operacyjna może dotyczyć każdego. Osoba X może być podsłuchiwana np. przez trzy miesiące, ponieważ Policja weszła w posiadanie informacji, że dopuściła się kradzieży z włamaniem. A sąd kontrolę zarządził, bo nie miał żadnych przesłanek, aby jej nie zarządzić. I nie w tym rzecz, że Policja (lub inna instytucja-wnioskodawca) postąpiła w złej wierze, celowo wprowadzając w błąd sąd lub prokuratora, ale że uzyskane przez nią informacje uzasadniające prowadzenie kontroli operacyjnej po prostu mogły być nieprecyzyjne lub nieprawdziwe. Przedmiotem zainteresowania instytucji bezpieczeństwa może być osoba krystalicznie uczciwa.

Trzeba też pamiętać, że kontrola operacyjna jest stosowana nie tylko w celu wykrycia i ustalenia sprawców przestępstwa, ale także w celu zapobiegania przestępstwu. A zatem można być podsłuchiwanym w związku z przestępstwem, do którego jeszcze nie doszło.

**8. Afera wokół inwigilacji ma charakter ściśle polityczny, a jej celem jest uderzenie w obecny obóz władzy. Gdzie byli naukowcy i eksperci, gdzie był Rzecznik Praw Obywatelskich, gdzie był Trybunał Konstytucyjny? Dlaczego nikt nie zwracał uwagi na wadliwość polskiego sprawa, a teraz nagle wszyscy sobie o tym przypomnieli?**

[6] Wykonywanie czynności procesowych jest możliwe po wydaniu przez prokuratora postanowienia o wszczęciu postępowania przygotowawczego (w postaci śledztwa lub dochodzenia). Wyjątkiem jest tzw. postępowanie w niezbędnym zakresie, czyli czynności procesowe prowadzone w wypadkach niecierpiących zwłoki, jeszcze przed wydaniem postanowienia o wszczęciu śledztwa lub dochodzenia (np. oględziny czy przeszukanie).

Sprawie kontroli operacyjnej poświęcono niezliczoną liczbę opracowań naukowych i analitycznych, wielokrotnie interweniowali w niej również Rzecznik Praw Obywatelskich (RPO) i Trybunał Konstytucyjny (TK). Debata na ten temat trwa nie od dzisiaj i nie od dekady, a od zarania III RP. To właśnie dzięki naciskom ekspertów, RPO i TK 20 lat temu wprowadzono do polskiego porządku prawnego instytucję uprzedniej kontroli sądowej nad kontrolą operacyjną – w latach 90. sąd w ogóle nie uczestniczył w tej procedurze.

Pod koniec 2009 r., na fali kontrowersji związanych z inwigilowaniem dziennikarzy, ówczesny premier Donald Tusk przyznał, że podsłuchy zakłada się w Polsce „zbyt łatwo". Kilka miesięcy później do Sejmu trafił rządowy projekt nowelizacji kpk i niektórych innych ustaw (druk nr 2915 z 31 marca 2010 r.). Drogą tej ustawy, przyjętej zgodnie przez wszystkie siły parlamentarne, do polskiego prawa wprowadzono obowiązek przedstawiania przez prokuratora generalnego (wówczas organu odrębnego od ministra sprawiedliwości) parlamentowi jawnej rocznej informacji w zakresie kontroli operacyjnej i procesowej. Dzięki tej zmianie, przygotowanej naprędce w związku z sytuacją niewygodną dla rządzących, dysponujemy obecnie szczątkowymi danymi statystycznymi dotyczącymi kontroli operacyjnej. Na poziomie eksperckim debata na ten temat trwa nieprzerwanie, ale prawo nowelizowane jest doraźnie, w związku z aktualnymi kontrowersjami i pod presją czasu, czego przykładem są losy tzw. ustawy inwigilacyjnej czy implementacji tzw. dyrektywy policyjnej.

W 2014 r. Najwyższa Izba Kontroli przygotowała druzgocący raport dotyczący nadzoru i kontroli nad polskimi służbami specjalnymi. We wnioskach znalazło się następujące sformułowanie: „w wielu obszarach służby specjalne, pozbawione zewnętrznego cywilnego nadzoru, kontrolują same siebie".

Jeśli chodzi o TK, to wielokrotnie na przestrzeni lat pełnił on funkcję cywilizującą w zakresie uprawnień służb policyjnych i specjalnych. Liczba i znaczenie luk i wad prawnych „załatanych" jego orzeczeniami z jednej strony budzi uznanie, ale z drugiej świadczy o tym, jak niepokojąco niskie są standardy polskiego prawodawcy. Przykładem oddziaływania o doniosłym znaczeniu jest chociażby uchwała TK z 16 stycznia 1996 r. (sygn. W 12/94). Wyjaśniła ona, że wojskowe służby specjalne nie posiadają uprawnień do prowadzenia czynności dochodzeniowo-śledczych, czyli ścigania sprawców przestępstw. Ta kluczowa kwestia była bowiem nieuregulowana na poziomie ustawy, a przygotowanie i przyjęcie ustawy o Wojskowych Służbach Informacyjnych zajęło politykom dwanaście lat.

Jeśli chodzi o sprawy inwigilacyjne, to największe znaczenie mają dwa postanowienia TK: sygnalizacyjne z 25 stycznia 2006 r. (sygn. S 2/06) i wyrok z 30 lipca 2014 r. (sygn. K 23/11). Drugie z nich to jedno z najważniejszych orzeczeń w historii polskiego sądu konstytucyjnego. W tym obszernym wyroku TK przekonywał, że prawo dotyczące czynności operacyjno-rozpoznawczych wymagało kompleksowej zmiany, obejmującej zarówno kwestie formalne, jak i materialne i proceduralne. Nie miało to nic wspólnego z Pegasusem, a rządząca obecnie opcja polityczna była wówczas w opozycji. U sterów władzy była koalicja Platformy Obywatelskiej (PO) i Polskiego Stron-

nictwa Ludowego (PSL). Zaskarżone przez TK przepisy inwigilacyjne miały utracić moc obowiązującą z upływem 18 miesięcy od dnia ogłoszenia wyroku. Koalicja PO i PSL miała więc 14 miesięcy, aby do wyborów 2015 r. doprowadzić do zmiany prawa, ale postanowiła pozostawić tę sprawę „w spadku" swoim następcom. W efekcie powstała wspomniana „ustawa inwigilacyjna", która nie rozwiązała wszystkich starych problemów, za to dodała kilka nowych (zob. poniżej).

Także RPO interweniował w tej sprawie wielokrotnie, niezależnie od tego, kto sprawował tę funkcję i kto był wówczas u władzy. Ombudsman nie tylko wnosił o stwierdzenie niezgodności niektórych pozakodeksowych przepisów inwigilacyjnych z konstytucją (np. w 2011 r.), ale także patronował pracom eksperckim zmierzającym do wypracowania propozycji dotyczących tego, jak mogłaby wyglądać reforma nadzoru i kontroli nad służbami (raport z 2019 r.).

**9. Dlaczego sądy nic z tym prawem nie robią, skoro jest takie złe? Dlaczego sędziowie orzekają na podstawie złego prawa?**

Dlatego, że sądy nie są władzą ustawodawczą, tylko – jak nazwa wskazuje – sądowniczą. Sądy działają na podstawie prawa i w granicach prawa, nawet jeśli prawo jest wadliwe, jak w opisywanym przypadku. Sędziowie mogą jedynie podejmować ten temat w ramach swoich aktywności naukowych czy popularyzatorskich, co zresztą wielokrotnie czynili.

**10. Prawo i Sprawiedliwość znowelizowało prawo i wprowadziło rozwiązania, których domagał się przed laty Trybunał Konstytucyjny, więc skąd problem?**

*Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*, czyli tzw. ustawa inwigilacyjna, wdrożyła wytyczne TK z 2014 r. częściowo, przy okazji wprowadzając do polskiego prawa rozwiązania, o których sąd konstytucyjny w ogóle nie wspominał.

Wśród zaleceń TK znalazło się m.in. wprowadzenie obowiązku notyfikacyjnego, czyli konieczności „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". Tego rozwiązania do dzisiaj nie ma w polskim prawie.

Innym przykładem jest skrytykowana przez TK nieostrość sformułowań, którym posługuje się ustawodawca. Trybunał uznał za konieczne, aby „zdefiniować zamknięty i możliwe wąski katalog poważnych przestępstw", uzasadniających prowadzenie kontroli operacyjnej. Do dzisiaj jednak ABW może wnioskować o kontrolę operacyjną w związku z realizacją zadania rozpoznawania, zapobiegania i wykrywania „innych przestępstw godzących w bezpieczeństwo państwa". W odniesieniu do tego przepisu TK nie stwierdził jednak jego niezgodności z konstytucją w zakresie wskazanym przez wnioskodawców.

Trybunał wnosił także o stworzenie „zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach". Nie chodziło oczywiście o szczegóły techniczne sprzętu, tylko o nazwy rodzajowe, takie jak „podsłuch rozmów telefonicznych", „podsłuch i podgląd pomieszczeń i osób" czy „nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu". W konsekwencji wyroku w 2016 r. dodano wspomniany wcześniej ogólny katalog pięciu rodzajów kontroli operacyjnej. Jego znaczenie jest widoczne zwłaszcza dzisiaj, w dobie kontrowersji związanych z oprogramowaniem Pegasus. Powołując się na ten katalog, rzecznik ministra koordynatora Stanisław Żaryn stwierdził, że kształt, jaki przyjmuje kontrola operacyjna, ma „drugorzędne" znaczenie, a przepisy „nie przewidują ograniczeń dla rodzaju danych, które mogą zostać pobrane". Rzeczywiście, korzystając z ogólnego kształtu katalogu można argumentować, że ustawodawca *expressis verbis* nie wykluczył korzystania z narzędzia takiego jak Pegasus. Rzecznik Żaryn nie zauważył jednak, że znaczenie ma coś dokładnie odwrotnego – że go w jasny sposób nie dopuścił (zob. punkt 14.).

Mało przekonująco brzmią przy tym głosy oburzenia ze strony opozycyjnej PO. Przygotowany przez jej polityków projekt ustawy mającej wychodzić naprzeciw wyrokowi TK z 2014 r. (druk nr 967 z 25 czerwca 2015 r.) był rozwiązaniem równie wadliwym, co przyjęta ostatecznie „ustawa inwigilacyjna" z 2016 r.

Temat czynności operacyjno-rozpoznawczych z definicji ma charakter polityczny, ale nie „partyjny". Wadliwość procedur w zakresie kontroli operacyjnej jest wspólną odpowiedzialnością całości elit politycznych, a błędy, zaniechania i utrwalenie się niedobrej praktyki w równym stopniu obciążają zarówno rządzących, jak i opozycję.

**11. Dlaczego mamy wierzyć Citizen Lab? To jakaś tajemnicza instytucja, o której nikt nie słyszał.**

To, że o Citizen Lab dopiero niedawno dowiedzieli się użytkownicy polskiego Twittera, do tej pory skoncentrowani na rozpowszechnianiu antyszczepionkowych teorii spiskowych, nie oznacza, że jest to instytucja nowa, dziwna lub podejrzana. Citizen Lab powstało ponad dwadzieścia lat temu, działa na Uniwersytecie w Toronto, jednej z najlepszych uczelni na świecie (26. miejsce na świecie według rankingu QS 2022). Kluczowe jest przy tym słowo „na", ponieważ w sieci uparcie przedstawia się tę sprawę w taki sposób, jakby związki pomiędzy Citizen Lab a uniwersytetem były znikome. To nieprawda. Instytucja jest integralną częścią Munk School of Global Affairs and Public Policy, która z kolei jest integralną częścią Uniwersytetu w Toronto.

Munk School została przez jednego z dziennikarzy nazwana „jakby uczelnią" i porównana... do Krajowej Szkoły Administracji Publicznej. Szkoły (*schools*) czy koledże (*colleges*) są po prostu jednostkami wewnątrz anglosaskich uniwersytetów, przyjmujących często postać uczelni kolegialnych (*colegiate university*), czyli swoistych federacji, których elementy składowe dysponują szerszą autonomią niż wydziały polskich uczelni. W ramach Uniwersytetu w Toronto działa kilka koledży oraz kilkanaście wydziałów i szkół. Munk School jest jedną z nich.

Citizen Lab nie jest, jak stwierdził jeden z polityków obozu władzy, „fundacyjką", tylko znanym i cenionym, interdyscyplinarnym ośrodkiem analitycznym zajmującym się szeroko pojętym bezpieczeństwem teleinformatycznym. Od lat zwraca uwagę na luki w oprogramowaniu komputerowym czy analizuje problem neutralność sieci.

Nie jest prawdą, że Citizen Lab pojawiło się „znikąd" i „nagle" wykryło problem inwigilacji w Polsce, na złość Prawu i Sprawiedliwości. Zanim świat dowiedział się o Pegasusie, Citizen Lab zajmowało się m.in. oprogramowaniem Remote Control System (RCS) grupy Hacking Team, którego ślady odkryło także w Polsce. Było to… w 2014 r. Opublikowany raport na ten temat zauważono i komentowano w polskiej prasie fachowej.

Nazwiska członków Citizen Lab są znane, można zapoznać się z ich dorobkiem i wykształceniem. W składzie znajdziemy prawników, informatyków, politologów czy dziennikarzy z renomowanych uczelni. Nic nie stoi na przeszkodzie, aby przeczytać dysertacje doktorskie członków zespołu: np. Jeffrey'a Knockela (doktorat z informatyki, University of New Mexico) czy Williama Marczaka (doktorat z informatyki, University of California, Berkeley). Poza posiadaniem stałej kadry, centrum korzysta też ze wsparcia zewnętrznych ekspertów.

W sieci wyśmiano sformułowanie „interdisciplinary laboratory", co dowodzi niezrozumienia, że w świecie nauki pojęcie „lab" oznacza po prostu komórkę badawczą, niekoniecznie związaną z noszeniem kitla i pracą przy mikroskopie.

Nie jest również prawdą, że „tajemnicze" jest finansowanie Citizen Lab. W pierwszej kolejności ośrodek jest finansowany przez Uniwersytet w Toronto. Poza tym korzysta ze wsparcia finansowego różnych podmiotów, publicznych i komercyjnych, np.: Canada Centre for Global Security Studies, Donner Canadian Foundation, Ford Foundation, Hewlett Foundation, Hivos, The Hopewell Fund, International Development Research Centre, John D. and Catherine T. MacArthur Foundation, Oak Foundation, Open Society Foundations, Psiphon Inc., The Sigrid Rausing Trust, Social Sciences and Humanities Research Council of Canada, czy the Walter and Duncan Gordon Foundation.

Argument, że finansowanie instytucji jest nietransparentne, jest absurdalny – rozlicza się ona przed władzami Munk School, a te przed władzami Uniwersytetu w Toronto. Na podobnej zasadzie można stwierdzić, że nietransparentny jest Uniwersytet Jagielloński – jego dokładnych rozliczeń finansowych również nie można znaleźć na stronie internetowej.

W sensie organizacyjnym Citizen Lab niczym nie różni się od innych instytucji eksperckich, które działają przy wielu uniwersytetach, także w Polsce, w tym na Uniwersytecie Jagiellońskim (np. Centrum Ewaluacji i Analiz Polityk Publicznych czy Interdyscyplinarne Centrum Analiz Społeczno-Prawnych).

Dyskredytowanie i ośmieszanie instytucji stało się popularne odkąd polscy dziennikarze „odkryli", że wspomagała ją finansowo fundacja George'a Sorosa, czyli wspomniana powyżej Open

Society Foundations. Rzecz w tym, że nikt tej współpracy nie ukrywał – wręcz przeciwnie, obie strony się nią chwalą.

Wszystkie powyższe stwierdzenia nie oznaczają oczywiście, że Citizen Lab powinno być traktowane jako nieomylna wyrocznia. Na razie nikt jednak nie wykazał, że komórka myliła się w sprawie Pegasusa.

**12. Jeśli nawet polskie służby używały Pegasusa, to korzystanie z niego musiała poprzedzić zgoda wyrażona przez właściwy sąd. A skoro tak, to nie ma mowy o nielegalności tego narzędzia.**

Nie wiemy, czy rzeczywiście korzystanie z Pegasusa było poprzedzone złożeniem wniosku o zarządzenie kontroli operacyjnej.

Ale nawet jeśli tak było, to nie zmienia to faktu, że stosowanie tego narzędzia jest niezgodne z polskim prawem. Argumentów na rzecz tego stwierdzenia jest wiele i mają one charakter zasadniczy. Wystarczy ograniczyć się do trzech.

Po pierwsze, kontrola operacyjna ma być stosowana selektywnie, wobec konkretnej osoby, przy możliwie niewielkiej inwazyjności względem osób trzecich. Tymczasem oprogramowanie takie jak Pegasus jest „kombajnem" (*harvester*) pobierającym (także w czasie rzeczywistym) wiele danych wszelkiego rodzaju – w tym przy użyciu kamery i mikrofonu. Oznacza to podsłuchiwanie, nagrywanie czy obserwowanie osób postronnych, które przypadkiem znalazły się w pobliżu osoby z zainfekowanym telefonem: na poczcie, w szpitalnej poczekalni, w autobusie czy na sali wykładowej. Nie może być mowy o spełnieniu ustawowego wymogu dotyczącego uzyskiwania i utrwalania obrazu lub dźwięku osób z „pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne". Dlatego właśnie Pegasusa nazywa się systemem do „totalnej" czy „masowej" inwigilacji i dlatego jego stosowanie jest nie do pogodzenia z polskim porządkiem prawnym w obecnym kształcie.

Po drugie, kontrola operacyjna odnosi się do przyszłości. Wydając postanowienie o jej zarządzeniu, sąd uruchamia „zegar". Od tego momentu służba dysponuje określonym w postanowieniu czasem: może być to tydzień, miesiąc czy trzy miesiące[7]. Analogicznie jest z czytaniem korespondencji czy podsłuchem w pomieszczeniach. Pegasus, łamiąc zabezpieczenia telefonu czy tableta (*remote jailbreak*), umożliwia dostęp do wielu typów danych, w tym nagrań, zdjęć, SMS-ów, MMS-ów i maili, także tych poprzedzających wydanie postanowienia o zarządzeniu kontroli operacyjnej. Umożliwia nawet dostęp do treści pochodzących z aplikacji, które oferują szyfrowanie danych (np. popularnych komunikatorów WhatsApp i Signal).

[7] Maksymalny okres stosowania kontroli operacyjnej przez zdecydowaną większość instytucji bezpieczeństwa wynosi w Polsce 18 miesięcy, ale realizuje się go fazami. Pierwsza, domyślna faza nie może być dłuższa niż trzy miesiące, a każda kolejna realizowana jest w trybie przedłużenia. Pierwsze przedłużenie nie może być dłuższe niż trzy miesiące, a łączna długość wszystkich kolejnych przedłużeń nie może przekroczyć roku. Każde przedłużenie, czyli uruchomienie kolejnej fazy kontroli, wymaga odpowiedniego uzasadnienia i odbywa się w trybie analogicznym do zarządzenia kontroli – postanawia o tym sąd, działając na wniosek właściwej instytucji, po uzyskaniu zgody prokuratora. Instytucje kontrwywiadowcze (ABW, SKW) są z tego górnego limitu wyłączone.

Po trzecie, kontrola operacyjna musi być zorganizowana w postaci szczelnego systemu. Wszystkie systemy teleinformatyczne, w ramach których mają być przetwarzane informacje niejawne, muszą zostać do tego dopuszczone, czyli uzyskać akredytację bezpieczeństwa teleinformatycznego. W zakresie informacji o klauzuli „poufne" lub wyższej (a takie związane są z kontrolą operacyjną) udzielają jej ABW i SKW. Nie wiemy, czy akredytacja Pegasusa miała miejsce, co prowadzi do dwóch pytań. Jeśli nie, to jak to możliwe, że jest używany przez służby? A jeśli tak, to jak to możliwe, że wydano w jego sprawie świadectwo akredytacji? Aplikacja Pegasus izraelskiej firmy NSO Group Technologies to po prostu udostępniana na zasadach subskrypcji komercyjna aplikacja typu spyware[8], pozwalająca pozyskiwać dane „na skróty", z pominięciem usługodawców telefonicznych czy z branży internetowej. Informacje zebrane z zainfekowanego urządzenia przesyłane są do jednego z serwerów Pegasusa (Pegasus Data Server), a później trafiają na „pulpit" (Pegasus Working Station) właściwej instytucji. Wiele wskazuje więc na to, że dane zebrane w Polsce trafiają poza jej granice. Prowadzi to do możliwości „wypływania" informacji niejawnych do odbiorców zewnętrznych. W przestrzeni publicznej zwraca się uwagę na związki firmy z izraelskimi służbami, czemu sprzyja fakt, że jeden z jej założycieli służył w Mossadzie. W odpowiedzi na globalne kontrowersje izraelski rząd odciął się jednak od NSO Group, podkreślając, że jest to prywatne przedsiębiorstwo.

Właściwie każdy z tych argumentów w oderwaniu od pozostałych jest wystarczający, aby stwierdzić nielegalność używania Pegasusa nad Wisłą. W połączeniu tworzą one jaskrawy przykład naruszenia prawa – nie tylko ustawowego, ale także konstytucyjnego.

Nie wspominając już o trybie nabycia prawa do korzystania z tej usługi. To odrębny problem prawny i – wiele na to wskazuje – odrębne naruszenie procedur.

**13. Pegasus nie jest pierwszym i z pewnością nie będzie ostatnim oprogramowaniem tego rodzaju. Na pewno z tego i podobnych narzędzi korzystają służby innych państw. Skąd więc problem?**

Zgadza się – istnieją podobne oprogramowania i wiemy, że służby po nie sięgają. Przykładowo amerykańskie Federalne Biuro Śledcze przyznało niedawno, że nabyło „ograniczoną licencję" na dostęp do Pegasusa, ale wyłącznie w celu „testowania i oceny" usługi, m.in. pod kątem konsekwencji dostania się jej w niepowołane ręce. Z pewnością nie jedna służba policyjna i specjalna posłużyła się tym lub podobnym oprogramowaniem w celach operacyjnych czy w związku ze ściganiem sprawców przestępstw. Nie ma to jednak bezpośredniego związku z sytuacją w Polsce, problem dotyczy bowiem stosowania Pegasusa w odniesieniu do polskich przepisów.

Legalność trzeba rozważać na dwóch płaszczyznach: generalnej dopuszczalności tego rodzaju narzędzi do prowadzenia kontroli operacyjnej i sposobu korzystania z nich w jej remach. Nawet

[8] Oprogramowanie szpiegujące (*spying software* – spyware) to typ złośliwego lub szkodliwego oprogramowania (*malicious software* – malware). Do tej kategorii należą też m.in. różne rodzaje oprogramowania blokującego dostęp do sprzętu lub usługi (*ransom software* – ransomware), oprogramowanie reklamowe (*advertising-supported software* – adware), a także wirusy, robaki i trojany.

bowiem prawnie dopuszczone do użytku narzędzie służb, niezależnie czy mowa o pałce służbowej czy oprogramowaniu komputerowym, może być stosowane niezgodne z prawem. Do tego dochodzą kontrowersje natury politycznej, które także mogą zaowocować konsekwencjami prawnymi. Gdyby potwierdziło się, że szef sztabu wyborczego opozycji był inwigilowany w trakcie kampanii, uprawnione byłyby pytania o uczciwość wyborów parlamentarnych 2019 r.

Przekonującym nie jest również stwierdzenie, że polskie instytucje bezpieczeństwa korzystały lub wciąż korzystają z narzędzi o podobnej do Pegasusa funkcjonalności. Jeśli tak, to dotyczy ich dokładnie ten sam problem, czyli brak odpowiedniego umocowania prawnego. Ponadto dowodzenie, że w ustawach kompetencyjnych nie może znaleźć się dokładny wykaz narzędzi informatycznych jest argumentem ad absurdum. Nie tego dotyczy postulat – chodzi o brak ustawowej ogólnej nazwy rodzaju kontroli operacyjnej, która obejmowałaby tego typu narzędzia, a nie o specyfikację techniczną konkretnych narzędzi.

**14. To są wszystko nadinterpretacje ludzi niechętnych obecnej władzy. W którym miejscu w polskim prawie jest wprost napisane, że służbom nie wolno używać Pegasusa?**

W polskim prawie nie jest też wprost napisane, że osobie przesłuchiwanej nie można świecić lampą prosto w oczy lub kopać ją pod stołem. Regulacje szczegółowe wynikają z szerszych unormowań, odczytywanych w relacji do całości systemu prawnego. Zasada „co nie jest prawem zabronione, jest dozwolone" odnosi się do obywateli, a nie do organów władzy publicznej. W ich przypadku jest dokładnie na odwrót.

**15. W całej sprawie chodzi o to, aby „wybić kły" polskim służbom, tym samym wydając polskie państwo i obywateli na pastwę bandytów i terrorystów.**

Nikt na żadnym etapie nie postulował i nie postuluje odebrania służbom uprawnień do prowadzenia czynności operacyjno-rozpoznawczych, w tym kontroli operacyjnej. Technika operacyjna stosowana jest przez służby każdego państwa i nie sposób wyobrazić sobie, jak bez niej wyglądałyby działania zapobiegawcze i wykrywcze, ustalanie sprawców przestępstw oraz uzyskiwanie i utrwalenie dowodów.

Kontrola operacyjna jest niezbędna, ale potrzebny jest nadzór nad nią prowadzony przez niezależny, wyspecjalizowany organ. O to chodzi w całej dyskusji, to właśnie postulują naukowcy, eksperci oraz TK, RPO i NIK: prowadzić, ale ucywilizować.

Do tego zmierzają dwie aktualne propozycje legislacyjne. Pierwszą z nich jest datowany na 11 stycznia br. poselski projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, skierowany do Sejmu przez grupę posłów opozycji z Markiem Biernackim na czele. Projektodawcy zmierzają do wprowadzenia postulowanego przez TK obowiązku notyfikacyjnego, który nie obejmowałby jednak ABW i SKW oraz – co logiczne – AW i SWW. Projektowi nie nadano jeszcze numeru druku, znajduje się on obecnie w fazie konsultacji. Ruszyły też prace związane z petycją złożoną kilka miesięcy temu przez Fundację Panoptykon. Jej autorzy postulują, aby Senat

podjął inicjatywę ustawodawczą dotyczącą „wprowadzenia kontroli nad działaniami inwigilacyjnymi policji i służb specjalnych". 9 lutego nad petycją pochyliła się senacka Komisja Praw Człowieka, Praworządności i Petycji, a dwa dni wcześniej do izby wyższej parlamentu wpłynęło pismo RPO popierające wnioskodawców. Fundacja postuluje „powołanie organu nadzorczego, którego zadaniem będzie weryfikacja zgodności z prawem podejmowanym przez służby działań ingerujących w prawa i wolności jednostki, szczególnie czynności operacyjno-rozpoznawczych" oraz „stworzenie mechanizmu informacyjnego do powiadamiania obywateli i obywatelek, że w przeszłości byli przedmiotem zainteresowania ze strony służb".

Odbyło się już dziewięć posiedzeń senackiej komisji ds. Pegasusa, czyli Komisji nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych. Ciągle nie wiadomo, czy powstanie sejmowa komisja śledcza.

Dodatkową komplikacją jest obecny kształt i rola TK. Przez cały okres III RP sąd konstytucyjny był kluczowym wehikułem pożytecznych zmian w zakresie prawa policyjnego. Obecnie kierowanie do niego wniosków o zbadanie zgodności przepisów inwigilacyjnych z ustawą zasadniczą byłoby nie tylko bezcelowe, ale wręcz mogłoby okazać się szkodliwe. Zachodzi bowiem uzasadniona obawa, że uznałby on nawet wyraźnie wadliwe rozwiązania za zgodne z konstytucją, tym samym wykrzywiając linię orzeczniczą i konserwując obecny stan rzeczy. Warto dodać, że w TK zasiada od niedawna Bogdan Święczkowski, były szef ABW (od września 2006 r. do listopada 2007 r.). Natomiast wiceprezesem jest Mariusz Muszyński, który wedle doniesień prasowych w pierwszej połowie lat 90. miał być funkcjonariuszem Zarządu Wywiadu Urzędu Ochrony Państwa. Można złośliwie zauważyć, że w składzie TK brakuje jeszcze reprezentanta wojskowych służb specjalnych.

Rozemocjonowanie debaty publicznej dotyczącej Pegasusa i inwigilacji nie sprzyja tworzeniu dobrego prawa, ale historia kształtowania się instytucji czynności operacyjno-rozpoznawczych dowodzi jednego: do nowelizacji w tym obszarze dochodzi przede wszystkim w takich właśnie okolicznościach.