FUNDACJA PANOPTYKON

ROK Z USTAWĄ INWIGILACYJNĄ

Co się zmieniło?
Czy było się czego bać?

Liczyliśmy na reformę służb i zwiększenie kontroli nad tajnymi operacjami, a dostaliśmy ustawę, która słusznie dorobiła się przydomka „inwigilacyjna". Projekt nowego prawa pojawił się na przełomie 2015 i 2016 r. Kilka tygodni później protestowaliśmy przed Pałacem Prezydenckim, a ponad 33 tys. osób podpisało petycję, obawiając się przede wszystkim zwiększenia inwigilacji w sieci. Obywatelskie protesty na niewiele się zdały: ustawa została przyjęta 15 stycznia 2016 r., a weszła w życie 6 lutego.

Co wiemy po roku jej obowiązywania? Czy było się czego bać?

WSTĘP

Kontrowersje dotyczące sięgania przez służby specjalne po dane telekomunikacyjne sięgają 2003 r., kiedy to operatorzy telekomunikacyjni zostali zmuszeni do ich przechowywania i udostępniania Policji i służbom specjalnym. Od samego początku uprawnione podmioty miały swobodny dostęp do billingów i innych danych telekomunikacyjnych. Aby dowiedzieć się, do kogo dzwonił właściciel telefonu lub gdzie się znajdował, funkcjonariusze nie musieli nikogo pytać o zgodę. W szczególności nie musieli z takim pytaniem fatygować się do sądu. Z czasem okazało się, że operatorzy telekomunikacyjni otrzymują setki tysięcy, a nawet miliony takich zapytań rocznie – w rekordowym 2014 r. udostępnili dane ponad 2,35 mln razy.

Na skutek działania organizacji pozarządowych oraz Rzecznika Praw Obywatelskich 30 lipca 2014 r. Trybunał Konstytucyjny stwierdził, że możliwość sięgania przez Policję i inne służby po dane bez niezależnej kontroli narusza konstytucję. Niestety, w swoim wyroku Trybunał nie sformułował precyzyjnie, jak powinna wyglądać kontrola nad sięganiem po billingi. Powiedział tylko, że co do zasady powinna ona następować **przed** pobraniem danych przez służby, a sprawować ma ją niezależny organ, np. sąd. Orzeczenie Trybunału wchodziło w życie po 18 miesiącach. Tyle czasu mieli rządzący na zmiany prawne. Wyznaczony termin upłynął 7 lutego 2016 r.

Wskutek opieszałości poprzedniej ekipy z wymaganą przez TK zmianą prawa musiał się zmierzyć rząd PiS. Powołując się na presję czasu, „szybką ścieżką" (jako projekt poselski, niepoddany żadnej formie konsultacji) przepchnięto zmiany w ustawie o Policji i innych przepisach regulujących działanie służb. Częściowo wykonując wyrok Trybunału Konstytucyjnego, tzw. ustawa inwigilacyjna wprowadziła kilka kosmetycznych zmian, np. zobowiązanie służb do niszczenia pobranych, a już nieprzydatnych danych. Jednak w fundamentalnym wymiarze zawiodła pokładane w niej oczekiwania: nie wprowadziła niezależnej kontroli nad dostępem do danych telekomunikacyjnych ani nie ograniczyła możliwości ich wykorzystywania do konkretnych postępowań, w których rzeczywiście okazało się to konieczne.

Tak ukształtowana „reforma" służb spotkała się z powszechną krytyką – ze strony organizacji pozarządowych, Rzecznika Praw Obywatelskich, Naczelnej Rady Adwokackiej czy Biura Analiz Sejmowych. Nawet Biuro Trybunału Konstytucyjnego wydało oświadczenie, z którego wynika, że ustawa nie realizuje wyroku Trybunału Konstytucyjnego.

Protestowali też obywatele. Internetową petycję przeciwko ustawie podpisało ponad 33 tys. osób, miały miejsce też liczne demonstracje w tej sprawie. Jedna z nich – współorganizowana przez Amnesty International, Akcję Demokracja i Fundację Panoptykon – odbyła się przed Pałacem Prezydenckim. Wówczas Prezydent Andrzej Duda spotkał się z przedstawicielami protestujących. Podczas spotkania zapewnił, że widzi konieczność reformy uprawnień służb, oraz zadeklarował, że zaproponuje zmiany. Dotychczas nie zostały jednak podjęte żadne prace w tym kierunku.

Przyjęta 15 stycznia 2016 r. tzw. ustawa inwigilacyjna[1] wprowadziła trzy fundamentalne zmiany dotyczące uprawnień służb do pozyskiwania danych telekomunikacyjnych i internetowych.

1. **Ułatwiła dostęp do danych internetowych.**
2. **Wprowadziła mechanizm pozornej kontroli nad pobieraniem danych.**
3. **(Jeszcze bardziej) zmniejszyła przejrzystość działania służb.**

[1] Ustawa z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. 2016, poz. 147), dalej: tzw. ustawa inwigilacyjna, ustawa.

1. UŁATWIONY DOSTĘP DO DANYCH INTERNETOWYCH

1.1. Co zmienia ustawa?

Na podstawie tzw. ustawy inwigilacyjnej Policja i inne służby mogą pozyskiwać **dane internetowe** bezpośrednio od firm z wykorzystaniem tzw. **bezpiecznego łącza**. Udostępnianie danych ma się odbywać bez udziału pracowników firmy lub przy niezbędnym ich udziale, jeżeli taka możliwość będzie zawarta w porozumieniu między służbą a firmą. Przepisy nie precyzują, czy „porozumienie" jest dobrowolne, czy firma może powiedzieć: „nie". Przed wejściem w życie ustawy istniała możliwość zawarcia takich porozumień wyłącznie z operatorami telekomunikacyjnymi. Przepisy nie precyzowały natomiast sposobu pozyskiwania danych internetowych.

Zgodnie z tzw. ustawą inwigilacyjną sięganie po dane internetowe stało się możliwe „w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych" (Policja) czy w celu realizacji ustawowych zadań, np. działalności analitycznej (Centralne Biuro Antykorupcyjne). Dotychczas dostęp do tego typu danych odbywał się na podstawie ustawy o świadczeniu usług drogą elektroniczną, zgodnie z którą firmy internetowe były zobowiązane do udostępniania tych danych uprawnionym organom, ale wyłącznie „na potrzeby prowadzonych przez nie postępowań".

Nie zmienił się natomiast zakres informacji, do jakich służby mają dostęp: różne rodzaje danych wymienione w ustawie o świadczeniu usług drogą elektroniczną uzyskały jedynie zbiorczą nazwę – danych internetowych. Temat ten budził ogromne kontrowersje na etapie prac parlamentarnych (w szczególności to, czy służby będą w stanie obchodzić tajemnicę korespondencji), w związku z tym do ustawy wprowadzono poprawkę precyzującą, że nowe zasady nie dotyczą **treści komunikatów**, np. e-maila.

1.2. Nasze wątpliwości i obawy

Wprowadzenie możliwości zdalnego pozyskiwania danych internetowych bezpośrednio od firm rodzi ryzyko masowej inwigilacji, czyli pozyskiwania przez służby ogromnych ilości danych „na wszelki wypadek". Pozyskiwanie danych w sposób „analogowy", z udziałem pracowników firm je przechowujących, utrudnia lub wręcz uniemożliwia pozyskiwanie danych w hurtowych ilościach. Zasysanie danych za pomocą bezpiecznego łącza eliminuje te ograniczenia.

Te obawy podsyca niejasność, w jakich sytuacjach służby mogą pozyskiwać dane internetowe. Dotychczas było to możliwe wyłącznie w ramach prowadzonych przez nie postępowań, co stanowi formalne ograniczenie dla służb, które powinny mieć chociaż sygnaturę prowadzonej sprawy. Tzw. ustawa inwigilacyjna wprowadziła drugą – niezwykle ogólną – przesłankę: pozyskiwanie danych m.in. w celu zapobiegania przestępstwom lub prowadzenia działalności analitycznej. Jednocześnie nie uchylono fragmentu ustawy o świadczeniu usług drogą elektroniczną mówiącego o udostępnianiu danych wyłącznie „na potrzeby prowadzonych postępowań". Relacja między tymi dwoma regulacjami jest niejasna.

Dodatkowe obawy budzi to, że nie wiadomo, co konkretnie mieści się w pojemnym worku „dane internetowe". Na pewno są to informacje na temat użytkowników, które pośrednicy internetowi (np. Interia, Onet czy Allegro) przechowują na podstawie ustawy o świadczeniu usług drogą elektroniczną. W tej kategorii mieszczą się dane niezbędne, by prawidłowo dostarczyć i rozliczyć usługę, np. imię, nazwisko i adres e-mail, oraz tzw. dane eksploatacyjne, które są konieczne, by „dopasować" usługę do sprzętu i oprogramowania użytkownika, czyli numer IP, informacje o systemie operacyjnym czy przeglądarce internetowej.

Niezbędne do świadczenia usługi może być także przechowywanie **treści korespondencji**, jeśli tego właśnie oczekuje klient – np. w ramach usługi poczty elektronicznej obejmującej przechowywanie danych na wirtualnym serwerze. Inny przykład danych osobowych zbieranych przez firmy internetowe to adres, pod który sklep internetowy dostarcza zakupiony towar. Jednak zasada jest wciąż ta sama – firma musi mieć jasny, wynikający ze specyfiki usługi, powód do przetwarzania tych informacji. Są wreszcie dodatkowe dane, które służą dopasowaniu wyświetlanych treści do cech użytkownika czy poprawiają jakość świadczonej usługi. Do tej kategorii zaliczają się wszystkie dane, które sami podajemy zaufanym dostawcom usług – chociażby portalom randkowym czy serwisom społecznościowym – o naszych zainteresowaniach.

Nie jest jasne, czy opisane kategorie informacji wyczerpują pojęcie danych internetowych, o których mowa w tzw. ustawie inwigilacyjnej. Można przecież przypuszczać, że Policja i inne służby pytają nie tylko o te dane, których przetwarzanie wprost dopuszcza ustawa o świadczeniu usług drogą elektroniczną, ale również o te, które firmy przetwarzają w oparciu o zgodę klienta lub własny uzasadniony interes (np. historię transakcji lub wyszukiwania, lokalizację).

Jednoznaczne wskazanie w ustawie, że nowe zasady udostępniania danych nie dotyczą treści komunikatów, nie uspokoiło wielu ekspertów pracujących w sferze nowych technologii, którzy wskazują, że – szczególnie w sytuacji dostępu online służb do baz danych – **firma może mieć poważne techniczne problemy z oddzieleniem metadanych od treści przekazu**. Często są one przechowywane w tym samym miejscu, a udostępnianie danych za pośrednictwem bezpiecznego łącza ma się odbywać bez udziału pracowników firmy.

1.3. Czego się dowiedzieliśmy?

Zbadaliśmy, czy uprawnione podmioty korzystają z nowej możliwości pozyskiwania danych internetowych za pomocą „bezpiecznego łącza" i czy zawarły w tym zakresie porozumienia z firmami internetowymi. Dowiedzieliśmy się, że:

- Policja od wejścia w życie ustawy nie zawarła żadnych porozumień z firmami;
- CBA od wejścia w życie ustawy nie zawarło żadnych porozumień z firmami;
- Żandarmeria Wojskowa zawarła 4 porozumienia z firmami;
- Agencja Bezpieczeństwa Wewnętrznego odmówiła odpowiedzi na nasze pytanie, zasłaniając się tajemnicą. Walczymy o tę informację przed sądem.

Nie udało nam się rozwiać wątpliwości dotyczących sytuacji, w jakich dopuszczalne jest pozyskiwanie danych. W trakcie prac parlamentarnych ze strony rządu padały deklaracje, że nadal będzie to możliwe wyłącznie na potrzeby prowadzonych postępowań. Jednak w ocenie Rzecznika Praw Obywatelskich, który skierował ustawę do Trybunału Konstytucyjnego, wystarczającą podstawą dla pobrania danych są przesłanki wskazane w tzw. ustawie inwigilacyjnej (np. działalność analityczna CBA).

W poszukiwaniu odpowiedzi na pytanie, jakiego rodzaju dane pobierają służby od dostawców usług internetowych, uzyskaliśmy od Ministerstwa Spraw Wewnętrznych i Administracji jedynie ogólną informację, że Policja dzieli pozyskiwane dane internetowe na dwie kategorie:

- raporty połączeń („raport połączeń wg określonych kryteriów");
- dane użytkowników („w szczególności ustalenia danych osobowo-adresowych dla zadanego numeru IP, dla zadanego adresu e-mail oraz ustalenie usługi Internet według danych, tj. PESEL, adres, REGON, NIP").

1.4. Nasze wnioski

Ustawa dała Policji i innym służbom narzędzia do masowego zbierania informacji o aktywności użytkowników Internetu. Służby, zawierając porozumienia z firmami internetowymi, mogą pobierać informacje na temat naszej aktywności za pośrednictwem bezpiecznych łączy, bez jakiejkolwiek uprzedniej kontroli. Najprawdopodobniej do pobrania danych niepotrzebne jest nawet wykazanie, że toczy się postępowanie, choćby formalnie uzasadniające pobranie danych. Cały mechanizm poddany jest pozornej kontroli ze strony sądów (por. punkt 2). Niestety nadal nie wiemy, o jakie konkretnie typy danych pytają służby i czy nie nadużywają swoich uprawnień, jeśli mają do dyspozycji bezpieczne łącza.

Nie wiemy też, czy Agencja Bezpieczeństwa Wewnętrznego skorzystała z możliwości zawarcia porozumienia z firmami internetowymi. Uznanie przez Agencję, że ujawnienie informacji o liczbie zawartych porozumień z firmami internetowymi zagraża bezpieczeństwu Polski (na tej podstawie odmówiono odpowiedzi na nasze pytanie), jedynie otwiera pole do spekulacji.

Żadnych porozumień z firmami internetowymi nie zawarła dotychczas Policja, która z racji na skalę swoich działań powinna być najbardziej zainteresowana ułatwionym dostępem do danych przydatnych do walki np. z oszustwami dokonywanymi za pośrednictwem Internetu. Co zaskakujące, takie porozumienia zawarła wielokrotnie mniejsza od Policji Żandarmeria Wojskowa.

W kontekście ryzyka masowej inwigilacji duże znaczenie ma to, czy polskie służby będą w stanie zawrzeć wspomniane porozumienia również z firmami internetowymi, które – formalnie – nie prowadzą działalności w Polsce. Chodzi przede wszystkim o największe amerykańskie korporacje, tj. Google'a czy Facebooka. Na ten moment nie wiemy o żadnym porozumieniu między polskimi służbami a amerykańskimi firmami, które pozwalałoby na bezpośredni dostęp do danych, a zawiłości jurysdykcyjne (do kogo skierować takie żądanie; czy zostałoby ono zaakceptowane przez amerykańskie sądy; czy taka współpraca byłaby możliwa bez międzynarodowego porozumienia na poziomie państw) wydają się działać na korzyść tych ostatnich i ich klientów. Niemniej jednak warto odnotować, że również wiodące internetowe firmy otrzymują coraz więcej zapytań od polskich służb tradycyjną drogą (por. punkt 3 dotyczący przejrzystości).

2. MECHANIZM POZORNEJ KONTROLI NAD POZYSKIWANIEM DANYCH

2.1. Co zmienia ustawa?

Zgodnie z tzw. ustawą inwigilacyjną kontrolę nad pozyskiwaniem danych telekomunikacyjnych, pocztowych lub internetowych sprawuje właściwy sąd okręgowy. Policja lub służba specjalna przekazują im w okresach półrocznych sprawozdania obejmujące liczbę przypadków pozyskania danych, ich rodzaj, a także kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane. W ramach prowadzonej kontroli **sąd może zapoznać się z materiałami uzasadniającymi pobranie danych**.

Opisany mechanizm kontroli nie dotyczy jednak danych, które znajdują się w prowadzonym przez operatorów telekomunikacyjnych wykazie abonentów (tzw. dane abonenckie). Znajdują się w nim wszystkie dane podawane przy zawieraniu umowy (np. imię i nazwisko, numer konta, adres). Dostęp do tych danych jest wyłączony spod opisanej wyżej kontroli.

2.2. Nasze wątpliwości i obawy

Na pozór tzw. ustawa inwigilacyjna wprowadziła fundamentalną zmianę względem dotychczasowej sytuacji, w której nikt nie sprawował kontroli nad udostępnianiem danych. Jednak konstrukcja i skuteczność tego mechanizmu kontrolnego budzi ogromne wątpliwości. Czy sąd jest w stanie rzetelnie skontrolować działania służb, jeśli dostaje o nich informacje w trybie hurtowym i na dodatek po upływie kilku miesięcy? Na jakiej podstawie powinien wybrać sprawy do bliższego przyjrzenia się, skoro (fizycznie) nie jest w stanie zbadać każdej?

Wątpliwości budzi też wyłączenie spod jakiejkolwiek kontroli dostępu do danych abonenckich. Co prawda, nie ingerują one tak mocno w prywatność jak inny rodzaje danych (np. billingi czy informacje o lokalizacji), niemniej wciąż stanowią istotną pulę informacji na nasz temat. Z orzeczenia Trybunału Konstytucyjnego, które wymusiło przyjęcie tzw. ustawy inwigilacyjnej, wynika, że dopuszczalne jest zróżnicowanie zasad kontroli w zależności od charakteru danych. Niedopuszczalne jest jednak wyłączenie niektórych kategorii danych spod jakiejkolwiek kontroli. Ma ona zapewnić przecież, by konstytucyjne prawo do prywatności było ograniczane tylko wtedy, gdy jest to konieczne i proporcjonalne.

2.3. Czego się dowiedzieliśmy?

Przekazywanie 6-miesięcznych sprawozdań sądom odbywa się na podstawie wytycznych Ministra Spraw Wewnętrznych i Administracji. Co ciekawe, jak poinformowało samo MSWiA, resort „nie brał udziału w opracowaniu ww. dokumentu". Projekt wytycznych został przekazany Ministerstwu przez ministra Mariusza Kamińskiego w celu zatwierdzenia.

Zgodnie z wytycznymi Policja i uprawnione podmioty składają co 6 miesięcy do sądów okręgowych sprawozdanie w ujęciu sumarycznym oraz w ujęciu szczegółowym w podziale na prowadzone sprawy. Pierwsze sprawozdania dotyczyły okresu od 7 lutego do 30 czerwca 2016 r., kolejne – następnych 6 miesięcy.

Udało się nam uzyskać sprawozdania szczegółowe złożone do sądów przez Komendę Stołeczną Policji oraz Komendę Wojewódzką Policji w Białymstoku. Dotyczą one okresu 7 lutego – 31 czerwca 2016 r. Sprawozdanie warszawskiej policji, którego wycinek zamieszczony jest na następnej stronie, składa się z 4097 pozycji. Znamy też ogólne sprawozdanie Komendy Wojewódzkiej Policji w Opolu. Pozostałe komendy wojewódzkie, a także służby specjalne, odmówiły nam udostępnienia swoich sprawozdań (o przyczynach odmowy więcej w następnej części).

Uzyskaliśmy informację, że 5 sądów okręgowych przeprowadziło już swoje kontrole. 3 z nich zakończyły się pozytywnie: sądy okręgowe w Poznaniu, Kielcach i że wynik kontroli jest niejawny.

W odpowiedzi na pytanie o sposób przeprowadzenia kontroli kielecki sąd okręgowy poinformował nas, że zapoznał się z materiałami uzasadniającymi udostępnienie Komendzie Wojewódzkiej Policji w Kielcach danych w 10 losowo wybranych sprawach.

Inaczej do sprawy podszedł sąd w Poznaniu, w którym kontrola zasadności pobrania danych odbyła się wyłącznie na podstawie sprawozdania:

„Kontrolę przeprowadził Przewodniczący Wydziału XVI Karnego Sądu Okręgowego w Poznaniu i nie stwierdził żadnych uchybień ani nieprawidłowości. W związku z powyższym nie było potrzeby zapoznania się z materiałami uzasadniającymi udostępnienie Policji danych telekomunikacyjnych, pocztowych lub internetowych". Podobnie w Gdańsku kontrola została przeprowadzona bez pobierania jakichkolwiek materiałów.

Sprawa nr	Jednostka	Kategoria		Dane telekomunikacyjne			Dane pocztowe	Dane internetowe		Razem w ramach sprawy
		Rodzaj/Podstawa prawna		Raporty połączeń	Lokalizacje stacji abonenckich	Inne niż raporty połączeń, lokalizacje stacji abonenckich, niebędące danymi użytkowników	Dane o użytkownikach i usługach	Raporty połączeń	Dane użytkowników	
		Wg ustawy o Policji	Kwalifikacja prawna/ Działania ratownicze/ poszukiwawcze							
OR-01/02/2016	KPP LEGIONOWO	art. 20c ust.1 ziwp	284Kk;286Kk	12	0	9	0	0	0	21
OS-69/15	KPP LEGIONOWO	art. 20c ust.1 ziwp	286Kk	20	2	0	0	0	0	22
SWD-6457/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	281Kk	17	4	1	0	0	0	22
71/15	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	22	4	0	0	0	0	26
8/14	KPP LEGIONOWO	art. 20c ust.1 ziwp	59UOPN	17	10	0	0	0	0	27
5/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	29	0	0	0	0	0	29
21/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	29	0	0	0	0	0	29
REJ. 09/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	278Kk	29	0	0	0	0	0	29
17/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	30	0	0	0	0	0	30
SWD 7394	KPP LEGIONOWO	art. 20c ust.1 ziwp	278Kk	30	0	0	0	0	0	30
69/15	KPP LEGIONOWO	art. 20c ust.1 ziwp	286Kk	28	2	1	0	0	0	31
2/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	32	0	0	0	0	0	32
4/11	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	30	5	0	0	0	0	35
20/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	278Kk	40	0	0	0	0	0	40
RO-3/15	KPP LEGIONOWO	art. 20c ust.1 ziwp	56UOPN;59UOPN;63UOPN;62UOPN	28	15	1	0	0	0	44
6/15	KPP LEGIONOWO	art. 20c ust.1 ziwp	278Kk;279Kk	45	0	1	0	0	0	46
SWD-12462/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	28	17	1	0	0	0	46
KP-S-54/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	278Kk	40	8	0	0	0	0	48
SWD-9330/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	286Kk	70	1	0	0	0	0	71
OR-1/15	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	40	37	0	0	0	0	77
1/15	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk	65	45	5	0	0	0	115
16/16	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk;280Kk	110	0	8	0	0	0	118
4/15	KPP LEGIONOWO	art. 20c ust.1 ziwp	279Kk;279Kk	213	1	1	0	0	0	215
KPP-WNP-2418/2102/16	KPP MIŃSK MAZ.	art. 20c ust.1 dp	CZYNNOŚCI POSZUKIWAWCZE	1	0	0	0	0	0	1
OP-96/15	KPP MIŃSK MAZ.	art. 20c ust.1 dp	CZYNNOŚCI POSZUKIWAWCZE	1	0	0	0	0	0	1
RO-3/14	KPP MIŃSK MAZ.	art. 20c ust.1 ziwp	258Kk	0	0	1	0	0	0	1
SWD-8103/2016	KPP MIŃSK MAZ.	art. 20c ust.1 ziwp	278Kk	1	0	0	0	0	0	1
2DS-256/16	KPP MIŃSK MAZ.	art. 20c ust.1 ziwp	197Kk	0	2	0	0	0	0	2

2.4. Nasze wnioski

Konstrukcja mechanizmu kontrolnego wprowadzonego przez tzw. ustawę inwigilacyjną sprawia, że nie gwarantuje on realnej kontroli nad działaniami służb. Zebrane przez nas informacje o jego działaniu na poziomie konkretnych sądów potwierdzają tę diagnozę.

Na etapie pobierania danych Policja i inne uprawnione organy nie muszą się liczyć z żadną formą kontroli. Następnie same decydują o tym, jakie informacje trafią do sprawozdania, które zobaczy sąd. W ramach swoistego obowiązku sprawozdawczego przygotowują one prostą tabelę, ale nie muszą uzasadniać, dlaczego pobranie danych w konkretnych sprawach było konieczne. Wreszcie: ustawa nie nałożyła na same sądy **obowiązku realnej weryfikacji** tego, czy raportowane im pobrania danych były zasadne. Sędziowie mają w tym zakresie swobodę, z której w różny sposób korzystają.

Pozorność kontroli nad dostępem do danych doskonale obrazuje praktyka sądów w Gdańsku i Poznaniu. Zapoznały się one z tabelami i wyłącznie na tej podstawie uznały pobieranie danych za uzasadnione. A przecież z tabeli, która jest suchym zestawieniem liczb, w żadnym razie nie wynika, czy pobranie danych w konkretnej sprawie było konieczne. Taka forma sprawozdawczości nie zabezpiecza też przed nadużyciami, na przykład pobieraniem „przy okazji" danych niezwiązanych ze sprawą.

Pozorność stworzonego w ustawie mechanizmu kontroli potęguje też duży odstęp czasu, jaki następuje pomiędzy pobraniem danych a weryfikacją tych działań przez sąd. Ustawa nie narzuciła też sędziom konkretnych kryteriów kontroli – przede wszystkim nie wprowadziła zasady, zgodnie z którą pobranie danych jest uzasadnione tylko wówczas, gdy inne środki – mniej ingerujące w prywatność – okazały się nieprzydatne. W konsekwencji nie wiadomo nawet, jakimi kryteriami sądy powinny się kierować, gdyby (z własnej inicjatywy) zdecydowały się na przeprowadzenie kontroli w konkretnej sprawie.

Niemniej za pozytywny sygnał można uznać działanie Sądu Okręgowego w Kielcach. Już samo zapoznanie się przez sędziego z materiałami uzasadniającymi pobranie danych w 10 losowo wybranych sprawach może wywołać wśród funkcjonariuszy poczucie, że ktoś patrzy im na ręce. Prawdopodobieństwo weryfikacji ich działań przez sąd z nieistniejącego staje się realne.

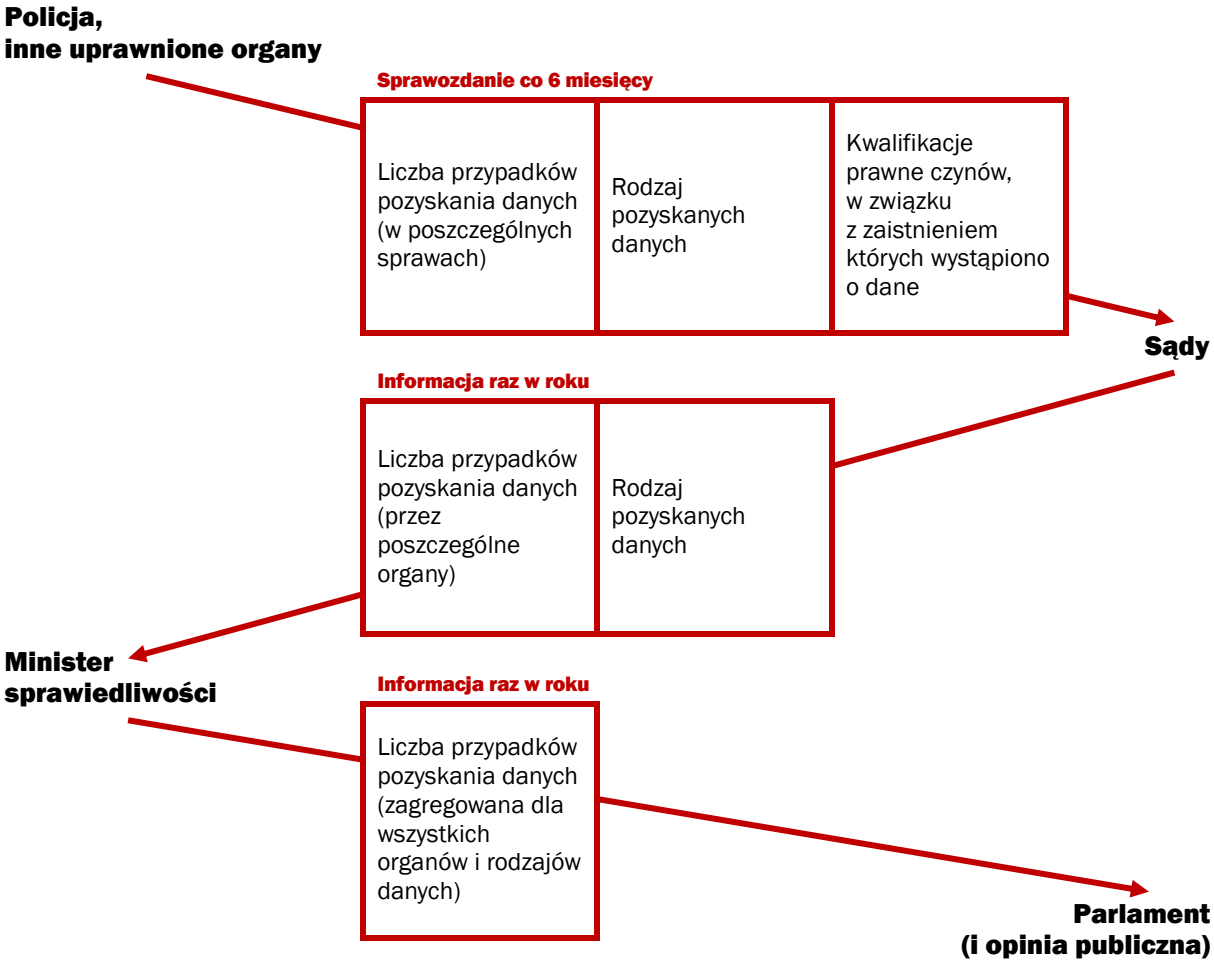
Ustawa nie wprowadziła żadnego mechanizmu (choćby pozornej) kontroli nad sięganiem po dane abonenckie. A zatem tym, do kogo należy dany telefon, gdzie ta osoba mieszka i jaki posiada numer konta, funkcjonariusze mogą się interesować bez ryzyka, że ktoś ich złapie za rękę i z tego działania rozliczy. Co więcej, również opinia publiczna nie pozna danych na temat skali tego typu zapytań (więcej w następnym punkcie).

3. 3. (JESZCZE) MNIEJ PRZEJRZYSTOŚCI

3.1. Co się zmieniło?

Do wejścia w życie tzw. ustawy inwigilacyjnej Urząd Komunikacji Elektronicznej publikował przekazywane przez operatorów telekomunikacyjnych informacje o łącznej liczbie zapytań, jakie otrzymali oni od Policji i innych uprawnionych organów. Dane te, zbierane na potrzeby corocznego raportu przygotowywanego przez UKE dla Komisji Europejskiej, były znane opinii publicznej. Z tego właśnie źródła wiedzieliśmy, ile łącznie zapytań otrzymali operatorzy, a na ile z nich byli w stanie odpowiedzieć; a także dzięki niemu poznaliśmy „wiek" danych, które znalazły się w zainteresowaniu uprawnionych podmiotów (ile czasu upłynęło od zarejestrowania danych do ich pobrania).

Ustawa uchyliła jednak przepis ustawy – Prawo telekomunikacyjne, z którego wynikał ten obowiązek sprawozdawczy UKE. W zamian „w celu zapewnienia opinii publicznej niezbędnych informacji" (cytat z uzasadnienia) tzw. ustawa inwigilacyjna nałożyła na ministra sprawiedliwości obowiązek corocznego przedstawiania parlamentowi zagregowanej informacji na temat przetwarzania danych. Niestety, zakres informacji zawarty w owej „zagregowanej informacji" będzie o wiele węższy niż ten, do którego zdążyliśmy się przyzwyczaić. Niżej przedstawiamy uproszczony schemat przekazywania danych o działalności służb.



Drugim źródłem informacji dla opinii publicznej na temat szczegółów zainteresowania Policji i innych służb były raporty Fundacji Panoptykon, która co roku – w drodze dostępu do informacji publicznej – uzyskiwała informacje na temat działań poszczególnych służb, zbierała je, analizowała i publikowała.

Zarówno informacje przedstawiane przez UKE, jak i te pozyskiwane i publikowane przez Fundację Panoptykon, obejmowały zapytania służb o wszystkie rodzaje danych: dane abonenckie, billingi i lokalizacje.

3.2. Nasze wątpliwości i obawy

Tzw. ustawa inwigilacyjna wprowadziła na pozór niewinny przepis, zgodnie z którym sprawozdania służb do sądów przekazywane są „z zachowanie przepisów o ochronie informacji niejawnych". Nie przesądza to jednoznacznie, czy informacje zawarte w sprawozdaniu są informacjami niejawnymi. Jednak taka interpretacja jest możliwa, a jej przyjęcie pociąga za sobą daleko idące konse-

kwencje: informacje niejawne nie podlegają udostępnieniu w trybie dostępu do informacji publicznej. Innymi słowy, jeśli służby uznałyby sprawozdanie za informację niejawną (na podstawie przytoczonego przepisu), obywatele nie mieliby dostępu do statystyk o liczbie zapytań o dane.

Jeszcze gorzej sytuacja wygląda z danymi abonenckimi, których przewidziane w tzw. ustawie inwigilacyjnej sprawozdania służb w ogóle nie obejmują. Ich liczba, wraz z liczbą innych zapytań, zbierana jest wyłącznie w rejestrze prowadzonym przez same służby na potrzeby wewnętrzne (np. przez szefa ABW). Zgodnie z ustawą taki rejestr jest prowadzony z zachowaniem przepisów o ochronie informacji niejawnych, a więc zawarte w nim dane nie podlegają udostępnieniu.

3.3. Czego się dowiedzieliśmy?

Większość komend wojewódzkich Policji (z wyjątkiem komendy stołecznej oraz komendy w Białymstoku), a także służby specjalne (ABW, CBA) odmówiły nam udostępnienia przekazanych sądom sprawozdań, zawierających pełne zestawienie przypadków pozyskiwania danych telekomunikacyjnych i internetowych. Co znamienne, w ubiegłych latach m.in. ABW udostępniała nam analogiczną informację, nie dostrzegając w tym zagrożenia dla interesu państwa. Zdaniem Agencji sytuacja zmieniła się po wejściu w życie tzw. ustawy inwigilacyjnej, a aktualnie sporządzane sprawozdanie jest niejawne (czyli jego ujawnienie zagrażałoby bezpieczeństwu państwa). Dlatego na nasz wniosek o udostępnienie informacji publicznej otrzymaliśmy decyzję odmowną. Zaskarżyliśmy ją do sądu. Uważamy, że te same informacje z roku na rok nie mogły zmienić swojego charakteru i nagle zacząć stanowić zagrożenia dla bezpieczeństwa państwa. Co więcej, naszym zdaniem tzw. ustawa inwigilacyjna nie przesądziła jednoznacznie, czy sprawozdanie ma charakter niejawny; wynika z niej tylko, że jest przekazywane do sądu w trybie przewidzianym ustawą o ochronie informacji niejawnych.

3.4. Nasze wnioski

Ustawa ograniczyła zakres publicznie dostępnych informacji o tym, jak często i po jakie kategorie danych telekomunikacyjnych sięgają uprawnione organy[2]. Wynika to z dwóch okoliczności:

- sprawozdania składane parlamentowi przez ministra sprawiedliwości na podstawie tzw. ustawy inwigilacyjnej obejmują mniej informacji niż te przygotowywane dotychczas przez Urząd Komunikacji Elektronicznej;
- faktycznie ograniczona została możliwość samodzielnego zdobycia tego typu informacji przez obywateli, w drodze dostępu do informacji publicznej.

Kategoria informacji	**Przed ustawą**	**Po ustawie**
Łączna liczba zapytań	T (1,2)	T (ale nieobejmująca danych abonenckich)
Liczba zapytań – różne kategorie danych	T (2)	N
Liczba zapytań pochodzących od konkretnej służby	T (2)	N
„Wiek" danych, których dotyczyły pytania	T (1)	N
Liczba zapytań o dane abonenckie	T (2)	N

Źródło: 1 – UKE, 2 – Panoptykon

[2] Ograniczenie, które sygnalizujemy, nie dotyczy danych internetowych, które nie były objęte istniejącym dotychczas obowiązkiem sprawozdawczym (wynikającym z ustawy – Prawo telekomunikacyjne).

Przejrzystość statystyk dotyczących sięgania przez uprawnione organy po dane o komunikacji obywateli ma kolosalne znaczenie: jest to namiastka społecznej kontroli nad funkcjonowaniem służb specjalnych. Nie ma powodów, by opinia publiczna nie mogła poznać statystyk pokazujących jedynie skalę ingerowania przez organy państwa w prywatność użytkowników telefonów czy Internetu. Tak dotychczas uważały sądy i – co ciekawe – większość służb specjalnych. Teraz trend się odwrócił i ci, którzy jeszcze niedawno nie widzieli przeszkód w podzieleniu się z nami informacją o swoich działaniach, dziś wymawiają się ochroną informacji niejawnych.

Tymczasem zostają nam próby interpretowania kolejnych tzw. raportów przejrzystości, regularnie publikowanych przez takie firmy, jak Google czy Facebook. Z raportu tej ostatniej firmy wynika, że polskie władze jedynie w I połowie 2016 r. aż 991 razy prosiły o informację na temat użytkowników portalu. To dwukrotny wzrost względem analogicznego okresu w 2015 r., kiedy tych pytań było 492. Nie znamy jednak wersji drugiej strony: same służby nie informują, ile razy pytały o dane internetowe ani jakiego typu spraw to dotyczyło. Jesteśmy więc skazani na spekulacje, z czego może wynikać tak gwałtowny wzrost zainteresowania służb naszą aktywnością w sieci (zaobserwowany na przykładzie konkretnej firmy, ale zapewne nie ograniczający się do jej klientów).

PODSUMOWANIE

Rok obowiązywania tzw. ustawy inwigilacyjnej potwierdza obawy, że dzięki stworzonym przez nią mechanizmom możliwa jest masowa inwigilacja polskiego Internetu. Nie wiadomo jednak, czy są one w ten sposób wykorzystywane. Zweryfikowanie tej hipotezy nie jest możliwe ze względu na daleko posunięte utajnienie działań służb w tej sferze, które tzw. ustawa inwigilacyjna jedynie pogłębiła (m.in. ograniczając dotychczas funkcjonujący mechanizm sprawozdawczy). Pewne jest natomiast, że stworzony przez nią mechanizm sądowej kontroli nad pozyskiwaniem danych jest pozorny.

Dalsze losy tzw. ustawy inwigilacyjnej leżą w rękach sędziów:

- zasiadających w Trybunale Konstytucyjnym, do którego ustawę skierował Rzecznik Praw Obywatelskich;
- pracujących w sądach administracyjnych, przed którymi toczyć się będą spory o jawność informacji statystycznych o skali zainteresowania służb naszymi danymi;
- pracujących w sądach okręgowych, do których trafiają sprawozdania służb: to od ich determinacji i pracowitości zależy, czy mechanizm pozornej kontroli nad działaniami służb nabierze choć trochę znaczenia.

Analiza danych i opracowanie
Wojciech Klicki

Współpraca
Katarzyna Szymielewicz
Małgorzata Szumańska

Korekta
Urszula Dobrzańska

Fundacja Panoptykon
Warszawa 2017