TELEFONICZNA KOPALNIA INFORMACJI. PRZEWODNIK

FUNDACJA
PANOPTYKON

TELEFONICZNA KOPALNIA INFORMACJI. PRZEWODNIK

AUTORZY:
Wojciech Klicki, Anna Obem, Katarzyna Szymielewicz

WSPÓŁPRACA:
Małgorzata Szumańska

Publikacja powstała dzięki wsparciu:

OPEN SOCIETY FOUNDATIONS

HEINRICH BÖLL STIFTUNG WARSZAWA

FUNDACJA IM. STEFANA BATOREGO

w ramach programu
„Demokracja w Działaniu”

SPIS TREŚCI

Telefoniczna kopalnia informacji to nieocenione źródło wiedzy o życiu każdego z nas – o tym, gdzie jesteśmy, z kim się przyjaźnimy i jakie mamy zwyczaje. Z tych informacji państwo może korzystać w dowolny sposób.

Mamy go przy sobie bez przerwy – ukryty w torebce lub kieszeni spodni telefon komórkowy to nie tylko wygodne narzędzie komunikacji. To również nadajnik, który nieustannie rejestruje informacje o naszym położeniu i naszej komunikacji ze światem. Podobnie jest z Internetem, w którym każda aktywność pozostawia ślad. Tak skonstruowana jest sieć.

Potencjał monitorowania komunikacji między ludźmi organy ścigania dostrzegły już w XIX w. – wówczas stacje telegrafu były zobligowane do przetrzymywania przez rok kopii przesyłanych depesz. Bogactwo cyfrowych śladów, jakie generujemy w XXI w., jest bez porównania bardziej kuszące. Z tej pokusy narodziły się współczesne programy gromadzenia, przechowywania i analizowania tego, co przepływa przez sieci telekomunikacyjne.

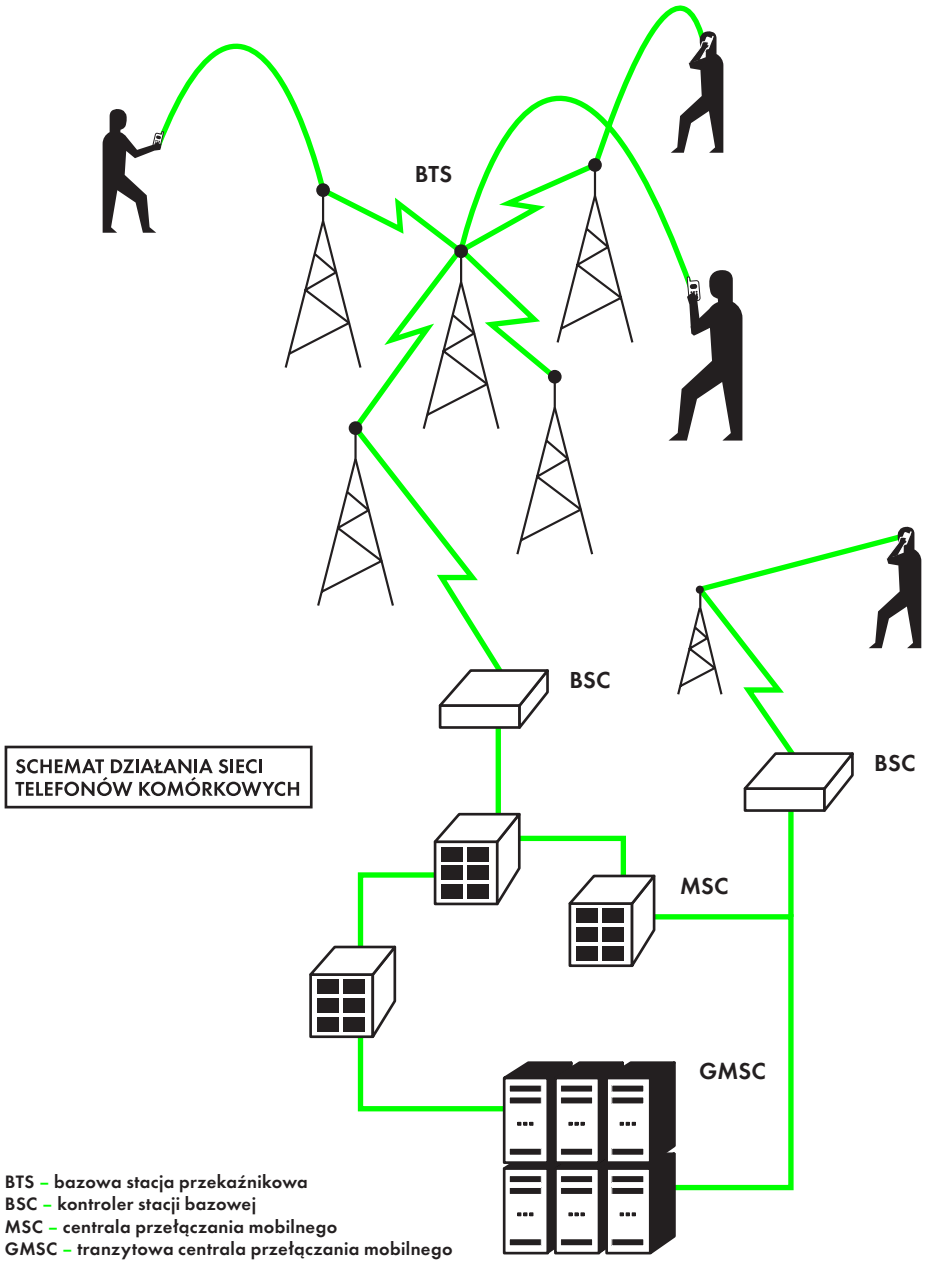
Retencja danych telekomunikacyjnych, której poświęcony jest ten przewodnik, polega na przechowywaniu przez określony czas informacji o tym, gdzie się znajdujemy, z jakich urządzeń korzystamy i z kim się kontaktujemy. Te okruchy informacji, tzw. metadane, pozwalają odtworzyć szczegółowy obraz naszego życia: codziennych zwyczajów, powiązań biznesowych, relacji intymnych, szlaków komunikacyjnych. Prawo zmusiło operatorów telekomunikacyjnych do przechowywania i udostępniania tych danych organom ścigania. Wszystko to miało służyć walce z poważnymi przestępstwami, przede wszystkim z terroryzmem. Szczegółowe dane o naszej komunikacji zaczęły być zatrzymywane na wszelki wypadek. Wszyscy zostaliśmy uznani za potencjalnych przestępców (i to poważnych!).

Retencja danych telekomunikacyjnych to prawdopodobnie najmocniej ingerujący w naszą prywatność instrument, który jak dotąd został przyjęty w Unii Europejskiej. W Polsce policja i inne służby mogą sięgać po metadane nawet w najbardziej błahych sprawach, jeżeli tylko dojdą do wniosku, że to konieczne do przeciwdziałania przestępczości. W praktyce ich możliwości związane z analizowaniem danych telekomunikacyjnych są w zasadzie nieograniczone. Co więcej, nie potrzebują do tego zgody sądu ani prokuratora!

Jak powstają bazy danych, do których sięgają służby? Czego na nasz temat można się z nich dowiedzieć? Czy gromadzenie metadanych jest tak niewinne, jak podnoszą entuzjaści tego rozwiązania? Czy retencja danych to środek mający uzasadnienie w walce z przestępczością, czy raczej nieproporcjonalne naruszenie praw i wolności każdego z nas? Na te pytania spróbujemy odpowiedzieć w naszym przewodniku.

Rozdział 1

Architektura sieci



SCHEMAT DZIAŁANIA SIECI TELEFONÓW KOMÓRKOWYCH

BTS – bazowa stacja przekaźnikowa
BSC – kontroler stacji bazowej
MSC – centrala przełączania mobilnego
GMSC – tranzytowa centrala przełączania mobilnego

Telefon podłączony do sieci komórkowej i komputer podłączony do Internetu ze swej natury są niewyczerpanymi źródłami informacji o użytkowniku. Generuje je każda rozmowa telefoniczna, każde połączenie z Internetem. Oprowadzanie po telekomunikacyjnej kopalni informacji zaczniemy od początku – od tego, jak powstają cyfrowe ślady.

Jak działa sieć komórkowa?

Za prawidłowe funkcjonowanie sieci komórkowej odpowiada wiele urządzeń i baz danych, które komunikują się ze sobą. W dużym uproszczeniu: sieć składa się z „komórek", czyli obszarów objętych zasięgiem danej stacji BTS (bazowej stacji przekaźnikowej, ang. *base transceiver station)*. Telefony komórkowe, które przemieszczają się razem z właścicielami, w zasadzie bez przerwy „meldują się" stacjom BTS w swoim otoczeniu. Dzięki tej ciągłej komunikacji możliwe jest zestawianie połączeń między telefonami w ramach jednej lub wielu sieci. **W zasięgu jednej stacji przekaźnikowej w tym samym momencie mogą znajdować się setki, a nawet tysiące osób.**

Stacja BTS to odbiornik i nadajnik radiowy. Telefony komórkowe łączą się z nią bez względu na to, czy prowadzimy akurat rozmowę, czy nie. Stacja BTS komunikuje się następnie z urządzeniem zwanym kontrolerem BSC (kontroler stacji bazowej, ang. *base station controller*), który odpowiada za przełączanie poruszającego się telefonu między kolejnymi stacjami BTS. Jednemu kontrolerowi może podlegać kilkadziesiąt stacji BTS. Następnie kontroler BSC łączy się z centrum zarządzania połączeniami w danej sieci – centralą MSC (centrala przełączania mobilnego, ang. *mobile switching center*).

Telefon loguje się do najbliższej stacji bazowej (BTS), która informację o tym przekazuje do kontrolera stacji bazowej (BSC). Kontroler BSC, który odpowiada za przełączanie poruszającego się telefonu między stacjami BTS, przekazuje informację dalej, do centrali przełączania mobilnego (MSC). Ta zaś odpowiada za uwierzytelnienie abonentów, rozpoczynanie i kończenie rozmów oraz zarządzanie przełączaniem poruszającego się telefonu.

Jeśli chcemy porozmawiać z abonentem innej sieci, centrala łączy się z kolejnym urządzeniem: centralą tranzytową (tranzytową centralą przełączania mobilnego, ang. *gateway mobile switching center,* GMSC). Dopiero z tego miejsca nasze połączenia są przekierowywane do central MSC innych operatorów, a za ich pośrednictwem do odpowiednich stacji BTS i z powrotem.

Każda rozmowa telefoniczna, każde połączenie z Internetem zostawia ślad. Te ślady, zebrane i poddane analizie, są niewyczerpanym źródłem informacji o naszym życiu.

Co nas identyfikuje w sieci komórkowej?

W sieci telekomunikacyjnej nie identyfikuje nas imię i nazwisko. Stacja BTS rozpoznaje telefon po tymczasowym numerze naszej karty SIM (TMSI). Pełnymi danymi każdego abonenta dysponuje tylko centrala MCS, która „zna" nasz numer telefonu, numer urządzenia, którym się posługujemy, i stały numer naszej karty SIM. Na zewnątrz sieci przekazywane są tylko dane niezbędne do zrealizowania połączenia, czyli numer karty SIM (IMSI) oraz – w przypadku połączeń przychodzących – nasz numer telefonu.

Każdy abonent sieci komórkowej ma przypisane dwa podstawowe numery: międzynarodowy numer telefonu (MSISDN) oraz unikatowy numer karty SIM (IMSI). Numer IMSI przesyłany jest tylko podczas logowania się telefonu do sieci (np. po jego włączeniu). Po uwierzytelnieniu abonentowi przydzielany jest tymczasowy numer karty SIM (TMSI), który od tej pory pełni rolę podstawowego identyfikatora wymienianego między jego telefonem a siecią. To zmniejsza ryzyko poznania numeru IMSI przez osoby nieuprawnione.

Jakie dane o nas posiada operator telekomunikacyjny?

- dane abonenckie, czyli informacje, które podaliśmy w umowie;
- numer telefonu (MSISDN);
- stały i tymczasowy numer karty SIM (IMSI, TMSI);
- numer urządzenia, którym się posługujemy (IMEI);
- informacje o naszym bieżącym położeniu (dane geolokalizacyjne): telefon loguje się do stacji BTS niezależnie od tego, czy akurat prowadzimy rozmowę;
- historię wszystkich połączeń wychodzących i przychodzących (billing);
- historię wysłanych i odebranych wiadomości SMS.

Jak działa Internet?

Komunikując się przez Internet, również zostawiamy ślady. Im dalej w sieć, tym więcej cennych informacji o naszym życiu. Na podstawie samych tylko danych telekomunikacyjnych, o których mowa w tym przewodniku, można odtworzyć szczegółowy obraz aktywności każdego użytkownika.

Internet to zbiór sieci umożliwiających transmisję danych między podłączonymi do nich urządzeniami. Jest on „siecią sieci" – składa się z tysięcy połączonych ze sobą sieci, których głównym zadaniem jest transport danych między nadawcą a odbiorcą. Internet przypomina galaktykę pełną ciał o różnym charakterze i rozmaitych powiązaniach.

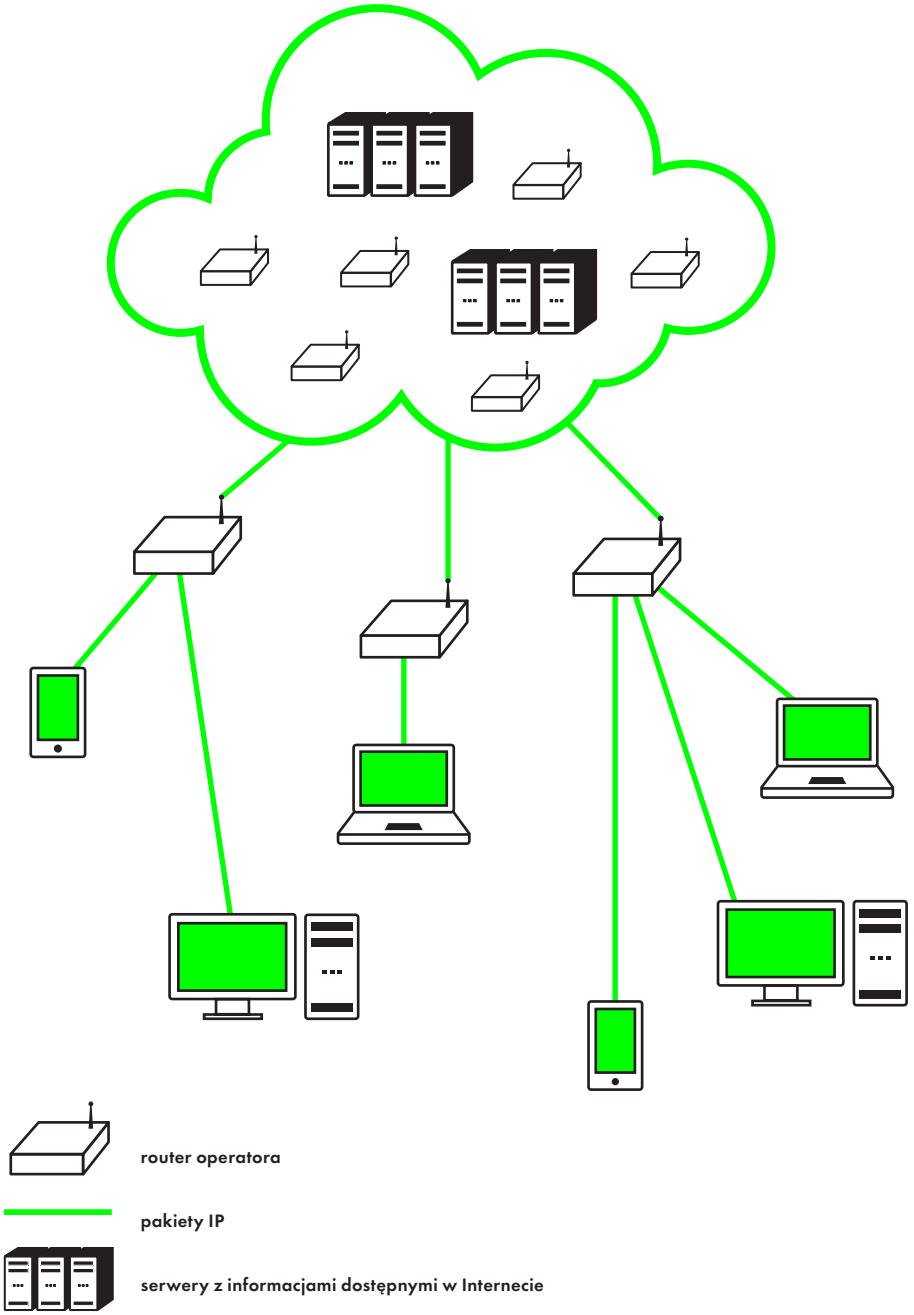
Podstawowymi elementami sieci internetowej są tzw. urządzenia końcowe, które komunikują się ze sobą. W tej kategorii mieści się wszystko, co sami jesteśmy w stanie podłączyć do Internetu (komputery osobiste, telefony komórkowe, tablety itp.), jak również wszelkiego rodzaju urządzenia serwujące nam treści (np. serwery WWW, serwery poczty elektronicznej). Komunikacja w sieci internetowej jest możliwa dzięki urządzeniom, których zadaniem jest kierowanie ruchem i transport danych: routerom, serwerom proxy, serwerom DNS.

Podstawowym nośnikiem informacji w sieci są pakiety IP (Internet Protocol). Można je porównać do wagoników, które są przesyłane między różnymi urządzeniami, by wreszcie trafić pod wskazany przez wysyłającego adres. Każda informacja, którą wysyłamy lub pobieramy przez Internet, podróżuje rozbita na pakiety IP, zawierające część danych, oraz adresy IP nadawcy i odbiorcy, które umożliwiają ich doręczenie. Dopiero kiedy pakiety docierają do adresata, są łączone w całość.

Każde urządzenie końcowe – telefon, tablet czy komputer – w momencie podłączenia się do sieci u danego operatora dostaje niepowtarzalny adres IP. W przypadku sieci Wi-Fi lub sieci lokalnych (np. sieci komputerów w domu lub w firmie) kilka urządzeń posługuje się tym samym adresem. To powoduje, że z zewnątrz są postrzegane jak jedno urządzenie.

Ponieważ numerów IP jest dziś mniej niż urządzeń, które łączą się z siecią, wykorzystywane są dynamiczne adresy IP – przypisywane urządzeniu tylko na czas danej sesji. Adres zwalnia się w momencie rozłączenia z siecią i może być wykorzystany przez inne urządzenie. Dlatego nie można powiedzieć, że każdy adres IP bezpośrednio identyfikuje użytkownika Internetu lub jego urządzenie. Kojarząc jednak adres IP z innymi informacjami, które posiada operator sieci telekomunikacyjnej, można ustalić, które urządzenie korzystało w danym momencie z danego numeru IP.

SCHEMAT DZIAŁANIA INTERNETU



Operator, który podłącza nas do Internetu, widzi adresy wszystkich urządzeń, z którymi się komunikujemy – serwerów, z których pobieramy treści, i komputerów, do których przesyłamy informacje.

Informacją, która jednoznacznie identyfikuje urządzenie w sieci, jest adres MAC. To wizytówka, którą „legitymuje się" ono u operatora, prosząc o przyznanie adresu IP. Gdy tylko urządzenie połączy się z siecią i uzyska własny adres IP, może rozpocząć przesyłanie danych. Każdy ruch w Internecie – każde kliknięcie, zapytanie wpisane w wyszukiwarkę, odebranie lub wysłanie wiadomości, wyświetlenie strony internetowej, pobranie treści – wiąże się z transmisją danych.

Co dostawca Internetu wie o użytkowniku?

Operator telekomunikacyjny podłączający nas do Internetu zna numer MAC urządzenia i adres IP, który sam mu przypisał. Ale to nie koniec: wszystkie pakiety danych, jakie wysyła lub odbiera użytkownik, w pewnym momencie przechodzą przez routery operatora. Operator widzi adresy IP wszystkich urządzeń, z którymi komunikuje się jego klient: serwerów WWW, innych komputerów itp. Jeśli komunikacja nie jest szyfrowana, może także przeczytać zawartość przesyłanych pakietów IP: treść maili, wiadomości i czatów, hasła i loginy do aplikacji internetowych itp.

Z informacji przekazanych gazecie „The Guardian" przez Edwarda Snowdena wynika, że amerykańska Agencja Bezpieczeństwa Wewnętrznego (NSA) miała płacić firmom internetowym za pozostawianie w oprogramowaniu tzw. luk bezpieczeństwa (ang. *back door*), dzięki którym analitycy NSA mieli mieć dostęp także do szyfrowanej komunikacji. Zwolennicy wolnego oprogramowania uznali tę informację za kolejny argument przemawiający za upowszechnieniem otwartych rozwiązań, twierdząc – nie bez racji – że jeśli kod źródłowy jest dostępny dla każdego, trudno w nim umieścić luki bezpieczeństwa.

Metadane = obraz codziennej aktywności

„Przy obecnym poziomie rozwoju techniki na podstawie danych telekomunikacyjnych towarzyszących przekazom informacji można zbudować profile osobowości i śledzić mobilność nieomal wszystkich obywateli”. Trybunał Konstytucyjny, Niemcy

Treść komunikacji objęta jest tajemnicą i poddane szczególnej ochronie. Jednak już same metadane (czyli nie treść rozmowy, ale informacje o rozmowie, przede wszystkim: z kim, gdzie i kiedy się odbyła) wystarczają, żeby zbudować szczegółowy profil aktywności każdego użytkownika sieci. Potwierdził to eksperyment niemieckiego polityka Maltego Spitza oraz badania naukowców z Massachusetts Institute of Technology.

Malte Spitz chciał zweryfikować, jak szczegółowy profil jego osoby można uzyskać w oparciu o dane, które zgodnie z niemieckim prawem przechowywał na jego temat operator telekomunikacyjny. Po długiej batalii prawnej (operator nie chciał udostępnić żądanych informacji) doszło do zawarcia ugody. Malte Spitz uzyskał z bazy danych operatora 35 000 rekordów, które szczegółowo dokumentowały sześć miesięcy jego życia. Te dane, poddane obróbce graficznej, pozwoliły zwizualizować szlaki komunikacyjne polityka i częstotliwość jego telefonicznych interakcji. W połączeniu z publicznie dostępnymi danymi z takich źródeł jak Twitter czy tradycyjne media bez większych trudności można było odtworzyć także cele podróży Maltego Spitza i kontekst, w jakim kontaktował się z otoczeniem.

Zespół Fundacji Panoptykon próbował na polskim gruncie powtórzyć eksperyment Maltego Spitza. Niestety bezskutecznie. W polskich przepisach prawo dostępu do swoich danych osobowych nie zostało sformułowane w sposób jasny i jednoznaczny. Na tej podstawie operatorzy nie uwzględnili wniosków członków zespołu Fundacji i nie udostępnili żądanych danych telekomunikacyjnych.

Natomiast naukowcy z renomowanego Massachusetts Institute of Technology ustalili, że na podstawie danych telekomunikacyjnych tylko z jednego miesiąca można odtworzyć sieć kontaktów i w 90% przypadków ustalić tożsamość osób należących do tej sieci. Co więcej, aż w 95% przypadków na podstawie danych telekomunikacyjnych można przewidzieć, gdzie dana osoba znajdzie się w ciągu kolejnych 12 godzin.

Rozdział 2

Potencjał w rękach władz

Często problemem nie jest sama technologia, tylko to, do czego zostanie ona wykorzystana. Stało się tak również w przypadku telefonów komórkowych – politycy, działając pod hasłami „wojny z terroryzmem", postanowili, że dane telekomunikacyjne powinny być przechowywane przez operatorów, a potem udostępniane policji i innym służbom w celu walki z poważnymi przestępstwami. Przedstawiamy podstawowe zasady przyjęte w tzw. dyrektywie retencyjnej i najważniejsze problemy, jakie wynikają z obowiązkowej retencji danych telekomunikacyjnych.

„Dyrektywa retencyjna jest bez wątpienia najbardziej ingerującym w prywatność prawem kiedykolwiek przyjętym w Unii Europejskiej". Peter Hustinx, Europejski Inspektor Ochrony Danych

Krótka historia dyrektywy retencyjnej

Po zamachach na World Trade Center z 11 września 2001 r. cały świat zawojowała idea gromadzenia danych telekomunikacyjnych do celów zwalczania przestępczości i zapobiegania terroryzmowi. Na fali retoryki „wojny z terroryzmem" wiele państw przyjęło regulacje nakładające na operatorów obowiązek zbierania i udostępniania danych telekomunikacyjnych sądom, policji i innym służbom. Z pozoru niewinna architektura sieci, którą opisaliśmy wcześniej, zaczęła być na masową skalę wykorzystywana jako narzędzie inwigilacji.

W Polsce obowiązek retencji danych wprowadzono już w 2003 r. Na mocy rozporządzenia Ministra Infrastruktury z 24 stycznia 2003 r. operatorzy mieli obowiązek przechowywać dane telekomunikacyjne przez 12 miesięcy. Chociaż ograniczenie konstytucyjnych praw i wolności – a retencja jest właśnie takim ograniczeniem – powinno być wprowadzone w drodze ustawy, rozporządzenie obowiązywało w tym kształcie aż do 2009 r.

Ograniczenia 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. (Art. 31. Konstytucji RP z 1997 r.)

Kolejny zamach – z 11 marca 2004 r. w Madrycie – poruszył opinię publiczną w Europie i stał się katalizatorem wprowadzenia powszechnego obowiązku retencji danych we wszystkich państwach członkowskich Unii Europejskiej. 25 marca 2004 r. Rada Europejska przyjęła Deklarację w sprawie zwalczania terroryzmu, w której zobowiązała unijne organy prawodawcze do przygotowania odpowiednich zmian w przepisach.

Zamach w londyńskim metrze z 7 lipca 2005 r. jeszcze wzmocnił pozycję zwolenników ograniczenia wolności i prywatności w imię walki z terroryzmem. Zamach w jednej z największych europejskich stolic do tego stopnia zburzył poczucie bezpieczeństwa Europejczyków, że nie było miejsca na głosy krytyczne. Rok później **przyjęto dyrektywę retencyjną** (oficjalnie: Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE). **Zobowiązała ona wszystkie państwa członkowskie Unii Europejskiej do stworzenia przepisów obligujących operatorów telekomunikacyjnych do przechowywania i udostępniania organom ścigania danych swoich klientów.**

Retencja danych miała być wykorzystywana wyłącznie w celu walki z „poważną przestępczością", a więc nie w celach prewencyjnych czy związanych z drobnymi

naruszeniami prawa. Jednak niektóre państwa, w tym Polska, wdrożyły ten obowiązek w szerszym zakresie (a więc niezgodnie z celami dyrektywy), czyniąc z retencji danych uniwersalne narzędzie działania policji i innych służb.

Operatorzy zostali zmuszeni do przechowywania i udostępniania organom ścigania wszystkich metadanych, które nasze urządzenia „zostawiają" w sieciach telekomunikacyjnych. Peter Hustinx, Europejski Inspektor Ochrony Danych, nazwał tę konstrukcję „bez wątpienia najbardziej ingerującym w prywatność prawem kiedykolwiek przyjętym w Unii Europejskiej".

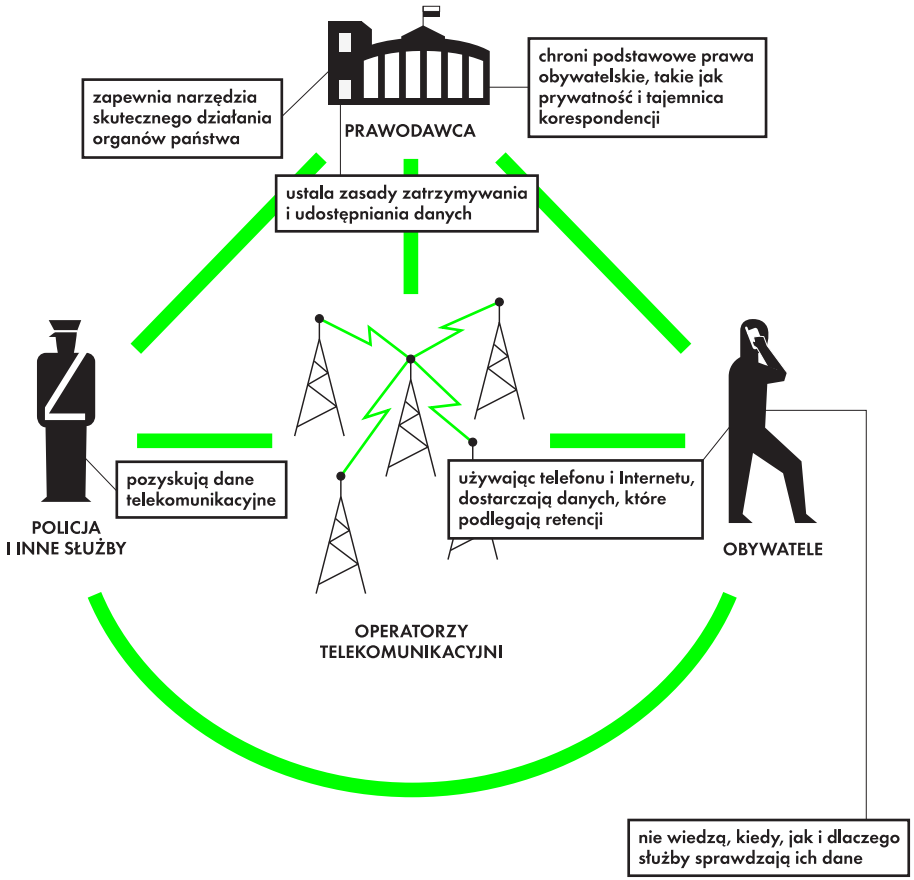
Konieczność przechowywania części danych telekomunikacyjnych wynika z potrzeb samych operatorów. Na długo zanim prawo narzuciło obowiązek ich zatrzymywania dla celów bezpieczeństwa, operatorzy zachowywali część informacji o ruchu na potrzeby rozliczeń, reklamacji, logistyki czy komunikacji z klientami. Wprowadzenie obowiązkowej retencji danych bardzo jednak zmieniło sytuację, ponieważ drastycznie wykroczyło poza to, co niezbędne. Dlatego właśnie rozwiązanie to godzi w podstawowe prawa każdego z nas.

Opinia publiczna, w większości niezorientowana w technicznych aspektach funkcjonowania sieci, łatwo dała się przekonać, że skoro retencja będzie dotyczyć „tylko" informacji o połączeniach, a nie treści komunikacji, nie stanowi poważnego zagrożenia dla prywatności.

Podstawowe założenia dyrektywy retencyjnej:

- operatorzy są zobowiązani do przechowywania danych telekomunikacyjnych swoich klientów,
- organy ścigania mogą mieć dostęp do tych danych w związku ze ściganiem poważnych przestępstw,
- dane przechowywane są przez okres od 6 do 24 miesięcy.

GŁÓWNI AKTORZY I DANE TELEKOMUNIKACYJNE W OBECNYM STANIE PRAWNYM



Czas przechowywania danych

Przed wprowadzeniem dyrektywy retencyjnej prawodawstwa poszczególnych państw przewidywały różne okresy przechowywania danych. W Polsce w 2003 r. wprowadzono retencję danych przez okres jednego roku. W 2005 r. grupa posłów zaproponowała jednak wydłużenie okresu zatrzymywania danych aż do 15 lat. Oczywiście ze względów bezpieczeństwa. Po burzy, którą ta propozycja wywołała w środowisku operatorów telekomunikacyjnych, projekt trafił do kosza.

Dyrektywa retencyjna, obowiązująca od 2006 r., określa okres zatrzymywania danych na nie mniej niż 6 miesięcy i nie więcej niż 2 lata. Najkrótszy, 6-miesięczny, okres retencji obowiązuje m.in. na Litwie i Słowacji. W Irlandii i we Włoszech wprowadzono 2-letni okres retencji. Również **polskie władze początkowo zdecydowały się na maksymalny, 2-letni, okres retencji. Dopiero w styczniu 2013 r., na fali społecznej krytyki, został on skrócony do 12 miesięcy.**

Z informacji, które co roku publikuje Urząd Komunikacji Elektronicznej, wynika, że policja i służby rzadko sięgają po dane starsze niż 12 miesięcy – w 2012 r. było tak tylko w 8% przypadków.

Koszty obowiązkowej retencji danych

Dyrektywa nie rozstrzygnęła jednoznacznie, kto ma ponosić koszty obowiązkowej retencji danych. Jedynie osiem państw członkowskich wprowadziło różne formy zwrotu kosztów udostępniania danych. W pozostałych krajach koszty przechowywania danych i obsługi zapytań ponoszą operatorzy, którzy przerzucają je na klientów. Doświadczenie różnych krajów pokazuje, że zachodzi istotna współzależność między obowiązkiem zwrotu kosztów, jakie generują zapytania o dane, a ich liczbą: im mocniej obciąża to budżet pytających, tym mniej pytają.

Szacuje się, że w Polsce ponoszone przez operatorów roczne koszty obowiązkowej retencji danych wynosić mogą nawet 74 mln złotych rocznie.

Jak dowiedział się amerykański senator Edward J. Markey, działający na terenie Stanów Zjednoczonych operator AT&T, który zrealizował 99% ze 181 tys. zapytań, otrzymał za to wynagrodzenie w wysokości 8,3 mln dolarów.

Wrażliwe informacje o życiu 500 milionów Europejczyków są zatrzymywane i przechowywane bez względu na to, czy są oni podejrzani o popełnienie przestępstwa.

Wątpliwości prawne

Dyrektywa to akt prawny, który nie obowiązuje bezpośrednio – państwa członkowskie mają obowiązek jego implementacji, czyli wdrożenia do przepisów krajowych. Mają przy tym pewien margines swobody. Niektóre państwa Unii Europejskiej, jak Austria i Szwecja, długo uchylały się od implementacji dyrektywy retencyjnej – Szwecja zrobiła to dopiero w 2012 r. pod presją kary finansowej, którą nałożył na nią Trybunał Sprawiedliwości Unii Europejskiej. W Niemczech, Rumunii i Czechach sądy konstytucyjne uznały przepisy krajowe za niezgodne z ich konstytucjami. Niebawem zbadają tę sprawę również sądy konstytucyjne Słowenii i Polski.

Rumuński sąd konstytucyjny uznał, że zasada prewencyjnego gromadzenia danych o obywatelach godzi w domniemanie niewinności i jest sprzeczna z prawem do prywatności i wolności wypowiedzi.

„Przy obecnym poziomie rozwoju techniki na podstawie danych telekomunikacyjnych towarzyszących przekazom informacji można zbudować profile osobowości i śledzić mobilność nieomal wszystkich obywateli" – orzekł niemiecki Federalny Sąd Konstytucyjny i stwierdził, że retencja danych telekomunikacyjnych stanowi poważne ograniczenie prawa do prywatności.

Z kolei zdaniem czeskiego Trybunału Konstytucyjnego skala i zakres obowiązku zatrzymywania danych były zbyt szerokie w stosunku do celu retencji, a przepisy nie chroniły obywateli wystarczająco przed potencjalnymi nadużyciami ze strony organów publicznych.

Sądy z Austrii i Irlandii uznały, że zbieranie informacji o wszystkich, którzy korzystają z sieci telekomunikacyjnych, może naruszać prawa człowieka (w tym Kartę praw podstawowych Unii Europejskiej). Ich wątpliwości rozstrzygnie Trybunał Sprawiedliwości Unii Europejskiej. Jeśli sędziowie dojdą do wniosku, że podstawowe założenie dyrektywy – prewencyjne zbieranie danych o wszystkich – jest niezgodne z Kartą praw podstawowych Unii Europejskiej, europejscy politycy będą musieli na nowo zastanowić się, jak walczyć z przestępczością przy użyciu nowych technologii, nie naruszając przy tym praw swoich wyborców.

Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. (Art. 7 Karty praw podstawowych Unii Europejskiej)

Skutki społeczne

W ramach obowiązkowej retencji danych wrażliwe informacje na temat sieci kontaktów (włącznie z biznesowymi), przemieszczania się i życia prywatnego (np. kontaktów z osobami bliskimi, lekarzami, prawnikami, doradcami zawodowymi, psychologami, telefonami zaufania) 500 milionów Europejczyków są zatrzymywane i przechowywane.

Dzieje się tak bez względu na to, czy jesteśmy podejrzani o popełnienie przestępstwa. **To odwrócenie jednej z podstawowych zasad rządów prawa: domniemania niewinności.** Retencja danych telekomunikacyjnych podważa zasadę poufności w kontaktach profesjonalnych, stwarzając ryzyko wycieku lub nadużycia informacji. Umożliwia też ominięcie zasady ochrony źródeł dziennikarskich: na podstawie samych billingów służby z łatwością mogą określić, skąd dziennikarz zdobył informacje do konkretnej publikacji. Stąd już tylko krok do ograniczenia wolności prasy i (auto)cenzury.

Skuteczność

Nigdy nie udowodniono, że obowiązkowe przechowywanie danych telekomunikacyjnych rzeczywiście jest niezbędne do zapewnienia bezpieczeństwa. Badania Instytutu Maxa Plancka prowadzą do wprost przeciwnych wniosków. Wynika z nich, że tzw. **zamrażanie danych przechowywanych przez dostawców usług telekomunikacyjnych w celach komercyjnych, czyli mniej inwazyjna dla praw i wolności obywatelskich alternatywa dla retencji, jest metodą skuteczną w 99,99% prowadzonych spraw.** Właśnie ten instrument został przewidziany w Konwencji Rady Europy o zwalczaniu cyberprzestępczości.

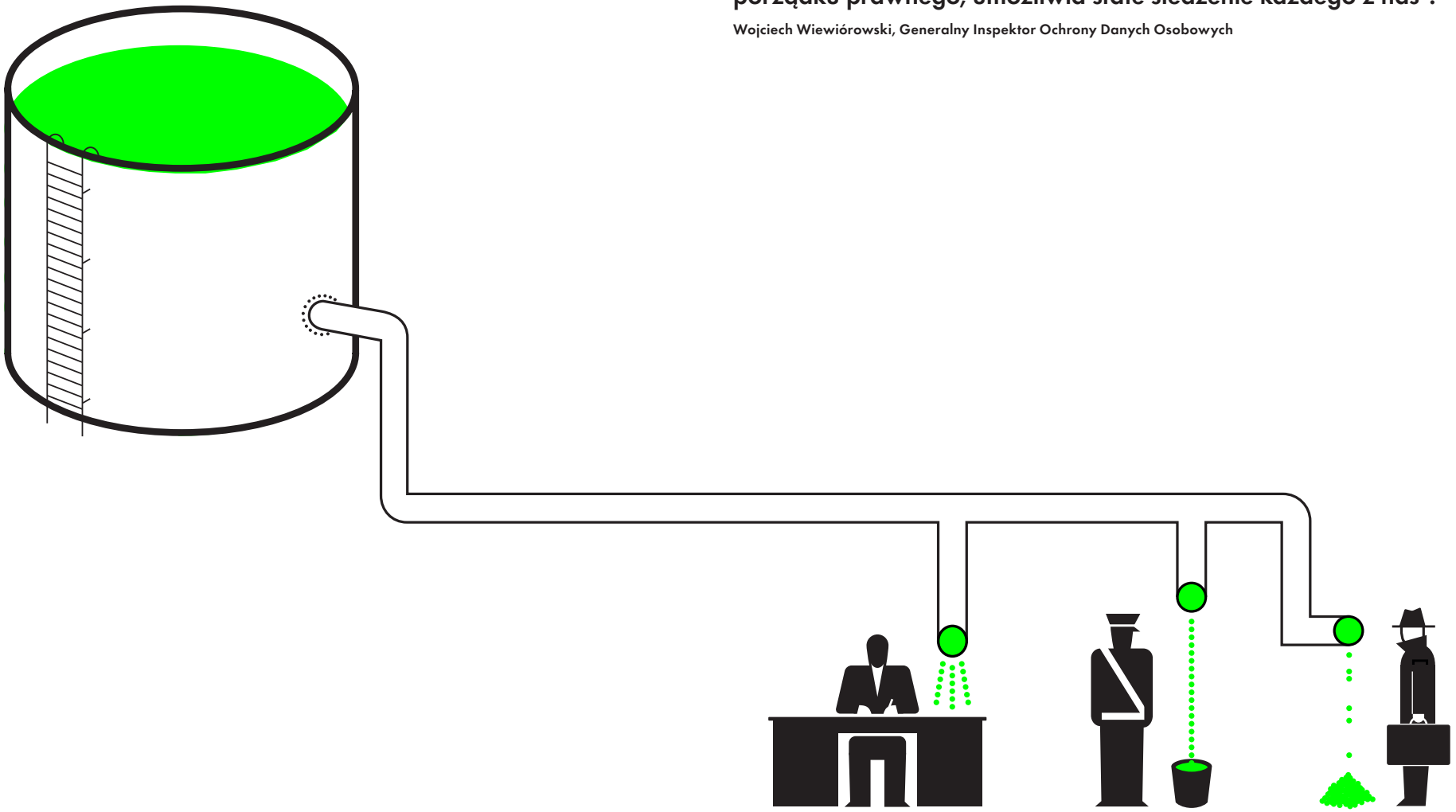
Zamrażanie danych (ang. *quick freeze*) to zatrzymywanie przez operatora telekomunikacyjnego wskazanych danych na wniosek uprawnionej służby w związku z konkretnym, już toczącym się, postępowaniem. Zamrożenie dokonywane jest natychmiastowo, bez oczekiwania na decyzję sądu, co skutecznie zapobiega utracie cennych danych, które inaczej mogłyby zostać skasowane, jako zbędne dla operatora. Aby jednak uzyskać dostęp do zamrożonych danych, potrzebna jest zgoda sądu.

Porównanie sytuacji w krajach, które wprowadziły obowiązek zatrzymywania danych z państwami, którego tego nie zrobiły, nie potwierdza wpływu tego obowiązku na skuteczność ścigania przestępstw. Dla organów ścigania kluczowa jest dostępność danych, a ta nie jest ściśle uzależniona od obowiązku retencji. Okazuje się, że dane przechowywane przez dostawców usług telekomunikacyjnych w celach komercyjnych, w połączeniu z mechanizmami szybkiego ich zamrażania w razie potrzeby, z zasady jest wystarczająca.

W 2011 r. Komisja Europejska opublikowała raport oceniający pierwsze lata funkcjonowania dyrektywy retencyjnej. Okazało się, że żaden kraj w Unii Europejskiej nie wdrożył dyrektywy w pełni zgodnie z intencją, jaka przyświecała europejskiemu prawodawcy. Wiele krajów, w tym Polska, wykorzystała ten instrument, żeby ułatwić pracę policji i służbom kosztem praw podstawowych swoich obywateli. Dane zgromadzone przez Komisję Europejską na potrzeby oceny dyrektywy – w tym uzyskane od polskiej policji – nie potwierdziły, że retencja jest niezbędna do skutecznej walki z przestępczością. W tym samym czasie ukazał się raport-cień przygotowany przez koalicję European Digital Rights. Wynika z niego, że dzięki retencji danych obywatele w zasadzie nic nie zyskali w sferze bezpieczeństwa, a wiele stracili w sferze prywatności.

Rozdział 3

Retencja danych w praktyce



W poprzednim rozdziale opisaliśmy, jakie założenia obowiązkowej retencji danych zostały przyjęte w Unii Europejskiej. Jednak aby polski policjant mógł wykorzystywać dane telekomunikacyjne, nie wystarczą przepisy unijne – niezbędne było ich wdrożenie do polskiego prawa. Zrobiono to w sposób, który premiował wygodę działania policji i innych służb kosztem naszej prywatności. Teraz przyjrzymy się praktyce sięgania po dane telekomunikacyjne i związanym z tym zagrożeniom.

„Regulacja, która w zamyśle miała ułatwić ściganie poważnych przestępstw, poprzez błędną implementację do polskiego porządku prawnego, umożliwia stałe śledzenie każdego z nas".

Wojciech Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych

Wojna z terroryzmem po polsku

Polska wdrożyła dyrektywę retencyjną w 2009 r., nowelizując prawo telekomunikacyjne. Atmosferę, w jakiej wdrożono w Polsce obowiązek zatrzymywania danych o wszystkich użytkownikach sieci telekomunikacyjnych, doskonale oddaje oficjalne uzasadnienie tej nowelizacji: „Polska jest lub może być wykorzystywana jako zaplecze logistyczne lub punkt tranzytowy dla ugrupowań terrorystycznych. Z uwagi na położenie geograficzne Polski, na szlakach wschód–zachód i północ–południe, istnieje bardzo duże prawdopodobieństwo wykorzystania terytorium naszego państwa właśnie w ten sposób".

Drugi z oficjalnych powodów nawiązywał do obecności polskich żołnierzy w Afganistanie, która miała się wiązać z ryzykiem stworzenia nowego szlaku przemytu heroiny przez terytorium Polski: „W sytuacji uczestnictwa polskich żołnierzy w przemycie narkotyków mogłaby zostać zagrożona sojusznicza wiarygodność Polski. Polscy żołnierze pomagaliby bowiem pośrednio, nie wiedząc o tym, finansować działalność al-Kaidy oraz talibów".

W najgorętszym okresie „wojny z terroryzmem" takie argumenty padały na podatny grunt. Jednak z perspektywy kilku lat trudno zgodzić się, by ryzyko przestępczej działalności wąskiej grupy żołnierzy przebywających w Afganistanie było dobrym uzasadnieniem dla ograniczenia praw i wolności obywateli 38-milionowego państwa.

Retencyjna wolna amerykanka

Z raportu Komisji Europejskiej oceniającego funkcjonowanie dyrektywy retencyjnej wynika, że z dostępnych możliwości Polska wybrała rozwiązanie najmniej korzystne z punktu widzenia ochrony praw i wolności obywateli. Wprowadzono najdłuższy, 2-letni (skrócony w 2013 r. do 12 miesięcy), okres retencji przewidziany dyrektywą, przy jednoczesnym braku zewnętrznej kontroli nad tym, kto i w jakim celu sięga po dane telekomunikacyjne. W porównaniu z dyrektywą polskie prawo poszerzyło też wachlarz celów, w jakich te dane mogą być wykorzystywane: z poważnych przestępstw na wszystkie przestępstwa, a nawet wykroczenia i działania prewencyjne.

Prawo telekomunikacyjne nakłada obowiązek retencji danych na operatorów; natomiast konkretne zasady, na jakich poszczególne organy uzyskują dostęp do tych danych, regulują tzw. ustawy kompetencyjne (czyli przepisy określające zasady ich działania). Prawo dostępu do danych telekomunikacyjnych mają w Polsce sądy, prokuratura, policja i inne (liczne!) służby: Centralne Biuro Antykorupcyjne,

Agencja Bezpieczeństwa Wewnętrznego, Straż Graniczna, Żandarmeria Wojskowa, Służba Kontrwywiadu Wojskowego, kontrola skarbowa i Służba Celna.

Jeśli bazy danych telekomunikacyjnych porównać do domu, to dostać się do nich można różnymi drogami: przez drzwi frontowe, tylne wejście lub okna. Od frontu do domu wchodzą sądy i prokuratorzy prowadzący postępowanie karne. Muszą oni wydać specjalne postanowienie, o którym informowana jest osoba, której dane są pobierane. Co prawda doręczenie tego postanowienia można odroczyć, ale właściciel telefonu czy komputera prędzej czy później dowie się, że był obiektem zainteresowania prokuratora lub sądu.

Z okien próbują korzystać sądy cywilne i np. prywatni detektywi, którzy nadużywają prawa lub wprost je łamią, sięgając po billingi mimo braku odpowiednich podstaw. Najwyższa Izba Kontroli, która sprawdziła, jak w praktyce wykorzystywane są dane telekomunikacyjne, spotkała się z przypadkami żądania przez sądy billingów w sprawach rozwodowych bez uzyskania koniecznej w takim wypadku zgody abonenta. Ani prawo telekomunikacyjne, ani przepisy kodeksu postępowania cywilnego nie dają podstaw do wydania przez sąd w sprawie cywilnej postanowienia dowodowego obligującego operatora do przetworzenia i przekazania temu sądowi danych objętych tajemnicą telekomunikacyjną. Zdarza się nawet, że na operatorów, którzy w takiej sytuacji nie dostarczyli sądowi billingów, nakładane są grzywny za niewykonanie polecenia sądu.

Największy problem stanowią tylne drzwi: są otwarte na oścież, a policja i inne służby korzystają z nich bez żadnej kontroli – tak często, jak same uznają za stosowne. Wbrew intencjom twórców dyrektywy retencyjnej umożliwiają one dostęp do danych nie tylko w celu wykrywania poważnych przestępstw, ale też w drobnych sprawach lub w ogóle bez prowadzonego postępowania, np. w „celach analitycznych". Policja i służby nie muszą też informować o pobraniu danych osoby, której to dotyczy.

Z raportu Komisji Europejskiej wynika, że tylko w Polsce, na Słowacji i na Łotwie można sięgać po dane telekomunikacyjne bez jakiejkolwiek kontroli – sądu, prokuratora lub niezależnego organu administracyjnego. Dla kontrastu: niemieckie służby mogą pozyskiwać dane telekomunikacyjne tylko w drodze nakazu sądowego, którego ważność jest ograniczona do 3 miesięcy. W uzasadnionych przypadkach nakaz może zostać wydłużony o kolejne 3 miesiące.

Sąd orzekający w sprawie dziennikarza Bogdana Wróblewskiego przeciwko CBA (patrz s. 38) uznał, że bezprawnie „billingując" (pobierając jego dane telekomunikacyjne), Biuro sięgnęło po wygodny instrument prawny, który nie wymagał zwiększonego nakładu pracy funkcjonariuszy: nie było konieczne uzyskanie zgody sądu ani poinformowanie dziennikarza o podjętych działaniach.

Z bazy operatora na biurko funkcjonariusza

W praktyce jest kilka dróg, którymi dane telekomunikacyjne mogą trafić z bazy danych prowadzonej przez operatora na biurko policjanta. Mogą być przekazane na pisemny wniosek komendanta głównego policji, ustne żądanie uprawnionego funkcjonariusza lub za pośrednictwem zabezpieczonego połączenia internetowego między policją a konkretnym operatorem (tj. za pomocą specjalnego interfejsu). Znakomita większość danych przepływa tą ostatnią drogą: szybko, sprawnie, bez zbędnej papierowej korespondencji. Uprawnieni do tego funkcjonariusze pobierają dane bezpośrednio z baz danych operatorów, nawet bez czynnego udziału tych ostatnich.

Systemy informatyczne mogą być zbudowane tak, że po stronie operatora nie zostaje nawet ślad po tym, że dane zostały pobrane. Uprawnienia do korzystania z interfejsu i innych dróg pozyskiwania danych o obywatelach każdy organ określa w swoich wewnętrznych przepisach. W przypadku policji dostęp do danych ma ok. 500 funkcjonariuszy, w tym ok. 200 pracowników Centralnego Biura Śledczego.

W Stanach Zjednoczonych każdy operator zatrudnia do obsługi zapytań o dane telekomunikacyjne specjalny zespół prawników, techników od obróbki danych i specjalistów od sieci komórkowych, który czeka w gotowości do rozpatrzenia i przygotowania odpowiedzi na setki zapytań, składanych codziennie przez amerykańskie organy ścigania. W Polsce ten wysiłek organizacyjny jest ograniczony do minimum: funkcjonariusze przez specjalny interfejs pobierają dane bezpośrednio z systemu operatora, który nie bierze w tym czynnego udziału.

Skala sięgania po dane: wielka niewiadoma

Łatwy dostęp służb do danych telekomunikacyjnych – bez kontroli sądu, bez ponoszenia kosztów i bez konieczności informowania sprawdzanego – znajduje odbicie w skali korzystania z danych telekomunikacyjnych przez polskie służby, która jest wielokrotnie większa niż w innych krajach europejskich. Choć to, co stoi za tymi „imponującymi" liczbami, wciąż jest w dużym stopniu zagadką.

Co roku Urząd Komunikacji Elektronicznej publikuje informacje pokazujące skalę zapytań o dane telekomunikacyjne, jakie operatorzy otrzymują od sądów, prokuratury, policji i innych służb. W kwietniu 2010 r. polską opinię publiczną poruszyła wiadomość o „milionie billingów" – UKE podał wtedy informację, że operatorzy telekomunikacyjni w 2009 r. otrzymali od uprawnionych podmiotów ponad milion zapytań o dane telekomunikacyjne. W kolejnym roku ta liczba wyniosła ponad 1,3 mln. W 2011 r. wszyscy uprawnieni sięgali po dane telekomunikacyjne ponad 1,87 mln razy, zaś w 2012 r. – 1,72 mln.

W ostatnich latach liczba żądań danych telekomunikacyjnych wzrosła, chociaż w tym samym okresie nie stwierdzono równie dynamicznego przyrostu poważnych przestępstw w Polsce. Wzrost liczby zapytań nie wpłynął również na poprawę wykrywalności przestępstw.

Tymczasem policja i inne służby (bez sądów, prokuratury i Służby Kontrwywiadu Wojskowego) zapytane przez Fundację Panoptykon „przyznają się" do znacznie większej liczby zapytań: ponad 1,92 mln w 2011 r. i 2,13 mln w 2012 r. Jak wyjaśnić różnice między danymi przekazywanymi przez UKE i same służby – nie wiadomo. Wiadomo tylko tyle, że w Polsce wciąż brakuje rzetelnego źródła danych na temat zapytań o dane telekomunikacyjne. Ten wniosek potwierdził raport Najwyżej Izby Kontroli z czerwca 2013 r. Same liczby nie pozwalają na rzetelną ocenę skali ingerencji służb w naszą prywatność. Do tego konieczna byłaby przynajmniej informacja, co oznacza „zapytanie", które każdy z pytających organów i odpowiadających operatorów definiuje inaczej.

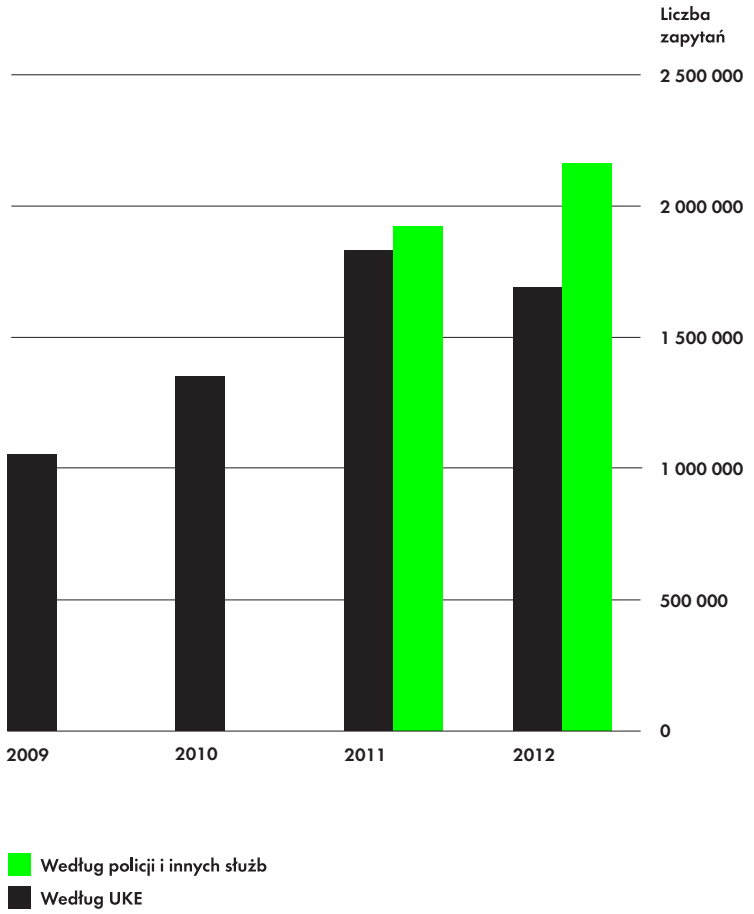
Z raportu Komisji Europejskiej oceniającego funkcjonowanie dyrektywy retencyjnej wynika, że w Niemczech służby sięgają po dane telekomunikacyjne aż 35-krotnie rzadziej niż w Polsce. Według polskiego MSW nie można jednak porównywać tych danych, ponieważ nie wiadomo, w jaki sposób w inne państwa liczą swoje „sprawdzenia telekomunikacyjne".

Przedstawiciele służb podają liczne argumenty uzasadniające tak wysoką liczbę zapytań – chociażby konieczność kierowania każdego zapytania do czterech największych operatorów, ponieważ nigdy nie wiadomo, u którego z nich zarejestrowany jest dany numer.

Według szefa CBA Pawła Wojtunika rośnie liczba zapytań, ale nie liczba pozyskiwanych danych. Szef CBA przyczyn tego (pozornego?) wzrostu ingerencji w prywatność obywateli upatruje w tym, że w Polsce można anonimowo kupić kartę pre-paid. Jego zdaniem przestępcy wykorzystują karty jednorazowo, co utrudnia ustalenie ich tożsamości i zmusza służby do sięgnięcia po więcej danych telekomunikacyjnych. Dlatego, wzorując się na rozwiązaniu funkcjonującym m.in. w Niemczech, CBA postuluje wprowadzenie obowiązku rejestracji kart pre-paid. Pozostaje jednak pytanie, czy taka propozycja jeszcze bardziej nie narusza prawa do prywatności.

Nikt w Polsce nie jest w stanie policzyć, ile zapytań o dane obywateli służby i inne uprawnione organy kierują do operatorów. Nie była tego w stanie ustalić nawet Najwyższa Izba Kontroli.

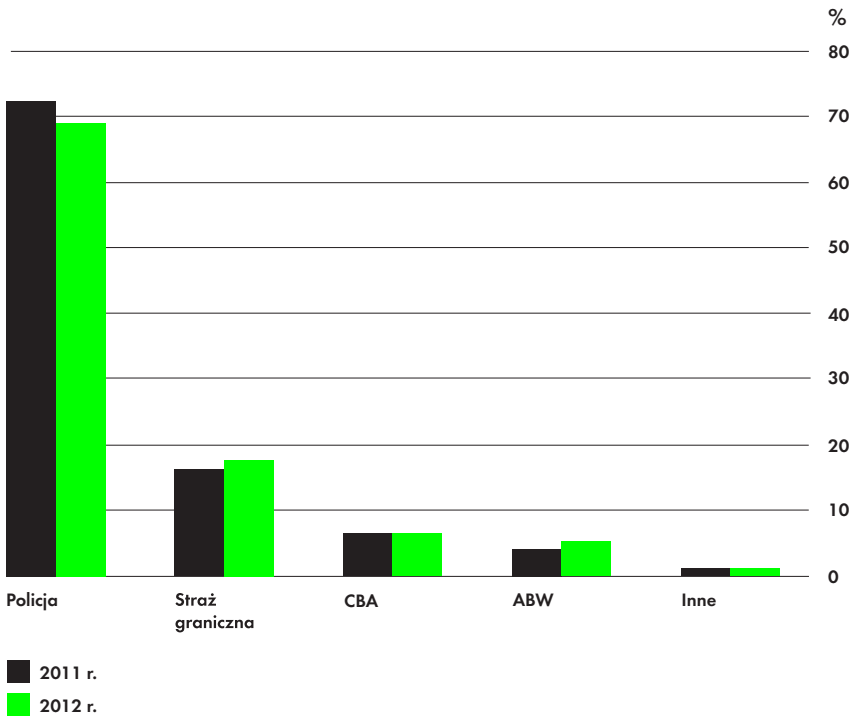
Łączna liczba zapytań o dane telekomunikacyjne w Polsce



Nie ma w Polsce ośrodka, który dysponowałby kompletnymi i w 100% rzetelnymi danymi o skali zapytań, jakie służby i inne uprawnione organy kierują do operatorów. Dane publikowane przez UKE są opracowane na podstawie informacji przekazywanych przez operatorów telekomunikacyjnych. Jednak według UKE nie wszyscy operatorzy realizują ten obowiązek.

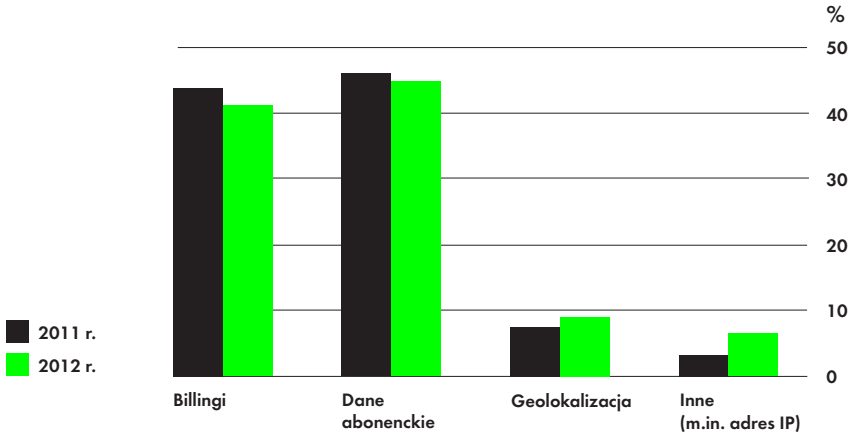
Dane zebrane przez Fundację Panoptykon obejmują zapytania policji, Straży Granicznej, ABW, CBA, Żandarmerii Wojskowej, kontroli skarbowej i Służby Celnej, nie zawierają natomiast zapytań Służby Kontrwywiadu Wojskowego (nie udostępniła danych), sądów i prokuratury.

Od kogo pochodzą pytania o dane telekomunikacyjne?



Fundacji Panoptykon udało się ustalić, po jakiego rodzaju dane telekomunikacyjne służby sięgają najczęściej. Z informacji zebranych od policji i innych służb wynika, że najbardziej interesują je tzw. dane abonenckie, czyli wszystkie dane, które podajemy operatorom przy okazji podpisywania umowy. Poza imieniem i nazwiskiem wśród tych danych może się znaleźć adres, PESEL czy numer konta. Tuż za danymi abonenckimi plasują się billingi, czyli wykazy połączeń, dzięki którym można ustalić, z kim i jak często się kontaktujemy. Znacznie rzadziej policja i inne służby pytają o dane geolokalizacyjne, czyli położenie telefonu w określonym czasie. Prawdopodobnie do tej kategorii zaliczają się również tzw. zrzuty z BTS, czyli informacje o wszystkich użytkownikach znajdujących się w określonym momencie w zasięgu danej stacji bazowej.

Rodzaje danych telekomunikacyjnych, których dotyczą pytania



Przegląd dostępnych liczb na temat skali sięgania przez policję i inne służby po nasze dane telekomunikacyjne nie pozwala na wyciągnięcie prostych wniosków. Tak naprawdę nie wiemy, jak często wykorzystywany jest ten instrument, ilu osób dotyczy i jak często bywa nadużywany.

Nadużycia

Sytuacja, w której służby nie muszą nikogo pytać o zgodę i pobierają dane telekomunikacyjne wtedy, gdy jest im wygodnie, stwarza duże ryzyko nadużyć. Nie wiadomo, co dzieje się z danymi wydobywanymi przez różne służby do „celów analitycznych". Ministerstwo Sprawiedliwości nie prowadzi statystyk w zakresie korzystania przez sądy i prokuratury z danych telekomunikacyjnych. Tylne drzwi, otwarte dla policji i służb, mogą być wykorzystywane w celach nieprzewidzianych dyrektywą retencyjną ani polskim prawem – w sposób, którego nie kontroluje ani wymiar sprawiedliwości, ani tym bardziej opinia publiczna.

Najgłośniejsze sprawy, w których bezprawnie pozyskiwano dane telekomunikacyjne, dotyczyły dziennikarzy. Okazało się chociażby, że w latach 2005–2007 ABW, CBA i policja zbierały dane na temat rozmów telefonicznych co najmniej dziesięciorga dziennikarzy. Obie służby zaprzeczyły, ale prokurator uzyskał z systemu operatora potwierdzenie złożenia zapytań przez CBA i ABW. W maju 2010 r. śledztwo w tej sprawie umorzono „z powodu niewykrycia przestępstwa".

W procesie o naruszenie dóbr osobistych, który Centralnemu Biuru Antykorupcyjnemu wytoczył Bogdan Wróblewski, dziennikarz „Gazety Wyborczej", sąd określił działanie CBA jako „typowe inwigilowanie w niewiadomym celu". Prawdopodobnie funkcjonariusze próbowali dowiedzieć się, kto informował Wróblewskiego o nieprawidłowościach w CBA. O tym, że CBA zagląda do jego billingów, Bogdan Wróblewski dowiedział się przez przypadek. W zakończonym w 2013 r. procesie sąd nakazał CBA publikację przeprosin.

Informacje o połączeniach telefonicznych dziennikarzy okazały się interesujące także dla amerykańskiego Departamentu Sprawiedliwości, który potajemnie uzyskał dostęp do spisów rozmów z 20 numerów telefonicznych należących do dziennikarzy agencji Associated Press. W kwietniu i maju 2012 r. – tj. w okresie, którym interesował się wywiad – wspomnianymi numerami posługiwało się około 100 osób zajmujących się m.in. tematyką rządową. Rząd odmówił składania wyjaśnień. Według Associated Press władze nie pierwszy raz poszukiwały informacji na temat źródeł dziennikarskich, jednak wcześniej zawsze robiły to w porozumieniu z agencją lub po uzyskaniu nakazu sądowego.

Konieczne zmiany w prawie

„Wygoda działania służb, a nie względy konieczności, decydują o ingerencji w konstytucyjną wolność i ochronę tajemnicy komunikowania się". **Irena Lipowicz, Rzecznik Praw Obywatelskich**

Polskie przepisy regulujące obowiązkową retencję danych telekomunikacyjnych trzeba zmienić – co do tego zgadzają się nie tylko organizacje pozarządowe, Rzecznik Praw Obywatelskich i Generalny Inspektor Ochrony Danych Osobowych, ale także Prokurator Generalny, Minister Administracji i Cyfryzacji, a nawet – przynajmniej w wystąpieniach medialnych – Minister Spraw Wewnętrznych.

W 2011 r. specjalny rządowy zespół pod kierownictwem ministra Jacka Cichockiego opublikował Raport dotyczący retencji danych telekomunikacyjnych. Z dość zachowawczych zapowiedzi zmian zawartych w raporcie – wprowadzenia

obowiązku niszczenia danych, zwiększenia nadzoru prokuratury, powołania specjalnego organu nadzorującego działalność służb oraz skrócenia okresu retencji do roku – udało się zrealizować tylko tę ostatnią. Pomimo przygotowania pod koniec 2013 r. przez Ministerstwo Spraw Wewnętrznych projektu ustawy o Komisji Kontroli Służb Specjalnych najważniejsze problemy – brak zewnętrznej kontroli nad sięganiem po dane oraz możliwość robienia tego w nawet najbardziej błahych sprawach – wciąż czekają na rozwiązanie.

„Jesteśmy już na tyle dojrzałą demokracją, aby można było rozważyć stworzenie instytucjonalnych mechanizmów kontroli zewnętrznej najbardziej wrażliwej aspektów pracy służb specjalnych". **Rządowy Raport dotyczący retencji danych telekomunikacyjnych**

Rzecznik Praw Obywatelskich zakwestionowała zgodność polskich przepisów dotyczących retencji z konstytucją. Jej wniosek do Trybunału Konstytucyjnego z 1 sierpnia 2011 r. został poparty przez Prokuratora Generalnego i Marszałek Sejmu. Na razie nie został on jednak rozpatrzony.

Dane telekomunikacyjne – mimo że nie zawierają treści rozmowy – są objęte tajemnicą komunikowania się. Może być ona ograniczona tylko w przypadkach ściśle określonych przez ustawę i tylko wtedy, gdy jest to niezbędne do zapewnienia porządku i bezpieczeństwa publicznego. Zdaniem Rzecznik Praw Obywatelskich polskie przepisy naruszają konstytucję, ponieważ:

- **pozwalają na arbitralne sięganie przez policję i inne służby po dane bez konieczności uzyskiwania zgody sądu lub innego zewnętrznego organu kontrolnego;**
- **nie nakładają obowiązku określenia, czy nie da się osiągnąć tych samych celów w sposób mniej ingerujący w prywatność;**
- **nie zawierają gwarancji ochrony tajemnic: lekarskiej, adwokackiej czy dziennikarskiej;**
- **w przypadku niektórych służb (np. ABW i CBA) nie nakładają obowiązku niszczenia danych, nawet jeśli nie są już one potrzebne.**

Konieczność zmian i ograniczenia dowolności, z jaką polskie służby sięgają po dane telekomunikacyjne, potwierdziła też Najwyższa Izba Kontroli, która skontrolowała tę kwestię. NIK negatywnie oceniła m.in. to, że jedynym podmiotem oceniającym zasadność sięgnięcia po dane telekomunikacyjne jest… sam podmiot pobierający dane.

TELEFONICZNA KOPALNIA INFORMACJI. PRZEWODNIK

AUTORZY:
Wojciech Klicki, Anna Obem, Katarzyna Szymielewicz

WSPÓŁPRACA:
Małgorzata Szumańska

KOREKTA:
Urszula Dobrzańska

PROJEKT GRAFICZNY:
Filip Zagórski

SKŁAD:
Sylwia Sieczkowska

DRUK:
Drukarnia Moś i Łuczak,
Poznań, PL

WYDAWCA:

FUNDACJA PANOPTYKON

panoptykon.org

Warszawa 2013