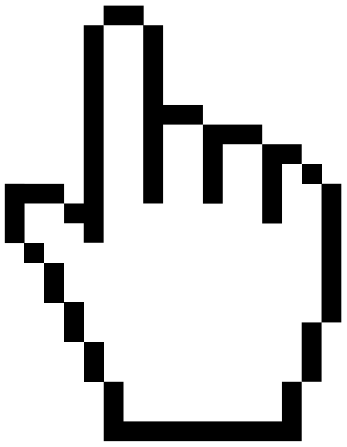
Dostęp państwa do danych użytkowników usług internetowych

Siedem problemów i kilka hipotez



FUNDACJA PANOPTYKON

Próba podsumowania

Od kilku lat toczy się w Polsce dyskusja na temat wykorzystywania danych telekomunikacyjnych (billingów, danych o lokalizacji) na potrzeby walki z przestępczością. Dzięki niej udało się zdiagnozować kilka niebanalnych problemów na styku praw człowieka, polityki bezpieczeństwa i interesów prywatnych firm. Niektóre z nich próbuje właśnie rozwiązać Ministerstwo Spraw Wewnętrznych, proponując zmiany w obowiązującym prawie.
A przecież państwo sięga nie tylko po dane przetwarzane przez operatorów telekomunikacyjnych: z podobnymi żądaniami muszą się mierzyć także dostawcy usług świadczonych drogą elektroniczną[1].

Faktem jest, że zawsze, kiedy państwo sięga po dane obywateli, które ci w zupełnie innym celu powierzają prywatnym firmom, pojawiają się problemy, a przynajmniej poważne dylematy. Przewidując, że nie zabraknie ich także w obszarze usług internetowych, postanowiliśmy przyjrzeć się zasadom, na jakich odbywa się przekazywanie danych danych osobowych obywateli, a zarazem użytkowników takich usług, na żądanie różnych organów państwa.

Kto i o co pyta? Jaka jest skala zapytań i czy to w ogóle ma znaczenie? W jakim trybie zapytania o dane trafiają do firm? Z jakich podstaw prawnych najczęściej korzystają organy państwa? Czy z perspektywy firm obowiązek przekazywania danych na żądanie organów państwa jest uciążliwy? Ile to kosztuje i kto za to płaci?

Z takimi pytaniami pół roku temu rozpoczęliśmy projekt, którego celem było lepsze poznanie tego, co się dzieje na styku firm świadczących usługi drogą elektroniczną i organów państwa. Przez kolejne miesiące analizowaliśmy przepisy prawa, rozmawialiśmy z firmami i organami państwa (najwięcej z policją), formułowaliśmy coraz bardziej szczegółowe pytania i zbieraliśmy dane.

Nie mamy wielu gotowych odpowiedzi – częściej stawiamy hipotezy, które domagają się zbadania. Mamy nadzieję, że zebrane przez nas informacje i dane staną się początkiem debaty publicznej i zainspirują dalsze działania o charakterze badawczym.

Naszymi partnerami w tym procesie było kilka firm świadczących usługi drogą elektroniczną: Agora, Google, INTERIA.PL i Onet (w kolejności alfabetycznej). Zgodnie z prawem żadna z tych firm nie ma obowiązku ewidencjonowania ani raportowania zapytań, jakie otrzymuje od organów państwa. Bez ich zaangażowania i dobrej woli poznanie praktyki funkcjonowania przepisów, które obligują firmy do przekazywania danych organom państwa, nie byłoby możliwe. Tym bardziej doceniamy ich otwartość na taką rozmowę.

[1] W tej kategorii mieszczą się wszelkie usługi internetowe: dostarczanie poczty elektronicznej, hosting, administrowanie forami, serwisy zakupowe i aukcyjne, wyszukiwarki, wszelkiego rodzaju komunikatory i portale internetowe (nawet niekomercyjne). Tego typu działalność podlega regulacji w ustawie o świadczeniu usług drogą elektroniczną (UŚUDE).

Niniejsze opracowanie jest próbą zebrania i podsumowania wniosków z tego procesu, który – ze względu na ograniczoną skalę i eksploracyjny charakter – miejscami przynosi więcej nowych pytań niż jednoznacznych odpowiedzi. Niemniej miał on dla nas duży walor poznawczy. Zachęcamy do zapoznania się z wnioskami, które publikujemy z intencją otwarcia potrzebnej debaty i zainspirowania szerzej zakrojonych działań badawczych.

Cele: co chcemy osiągnąć?

Naszym celem nie było zebranie i przedstawienie suchych informacji na temat skali zapytań o dane użytkowników, jakie organy publiczne kierują do firm świadczących usługi drogą elektroniczną. Doświadczenie z debaty na temat dostępu do danych telekomunikacyjnych nauczyło nas, że to nie liczby są najważniejsze. Przygotowywane przez nas zestawienia danych pochodzących z różnych źródeł, a ostatnio także raport Najwyższej Izby Kontroli, pokazały, że – mimo obowiązku raportowania nałożonego na operatorów telekomunikacyjnych – statystyki prowadzone bez spójnej metodologii są nierzetelne. W efekcie mogą wprowadzać w błąd i odciągać uwagę od poważniejszych problemów.

Naszym celem nie jest piętnowanie firm, które – poruszając się w ramach prawa – realizują żądania udostępnienia danych o użytkownikach. To, że przestrzegają obowiązującego prawa, zasługuje tylko na uznanie. Jeśli jeszcze dbają przy tym o przejrzystość, ich klienci mogą czuć się uspokojeni. Z drugiej strony obywatele po prostu mają prawo wiedzieć więcej na temat zasad, na jakich firmy muszą współpracować z organami państwa.

Zależy nam na rozpoczęciu merytorycznej i poważnej debaty publicznej. Kluczowe w tym kontekście jest zrozumienie i przedstawienie problemów, które wiążą się z dostępem policji, sądów, prokuratury i służb do danych, jakie przetwarzają firmy świadczące usługi drogą elektroniczną. Dlatego najwięcej uwagi poświęcaliśmy następującym pytaniom: Czy istniejące procedury są wystarczające? Jaka jest praktyka organów publicznych – na jakie podstawy prawne najczęściej się powołują? Czy w ocenie firm większość kierowanych zapytań okazuje się uzasadniona? Czy potrzeba dodatkowych mechanizmów kontroli nad działaniami policji i innych służb? Jakie koszty ponoszą firmy świadczące usługi drogą elektroniczną i czy zasadnie?

Próbujemy zainicjować publiczną dyskusję na temat zasad przekazywania danych użytkowników usług internetowych organom państwa po to, by te zasady ulepszyć. Diagnoza problemów jest tylko wstępem do wspólnego namysłu nad ich rozwiązaniem poprzez zmianę lub doprecyzowanie obowiązującego prawa.

Liczymy, że ta inicjatywa – z udziałem czterech wiodących firm – okaże się początkiem pewnej tendencji; że z czasem wszystkie liczące się na rynku firmy świadczące usługi internetowe zgodzą się z tym, że warto wyprzedzać pytania i otwarcie mówić o zasadach przekazywania danych na żądanie organów państwa. Otwarta debata na ten temat wydaje się korzystna dla wszystkich stron. Zderzając perspektywę firm, obywateli i organów państwa, jesteśmy w stanie zdiagnozować te problemy, które dotykają wszystkich, przez co okazują się możliwe do rozwiązania.

Kontekst: od debaty o danych telekomunikacyjnych do „afery podsłuchowej”

Bezpośrednią inspiracją dla przyjrzenia się praktykom przekazywania danych o obywatelach-użytkownikach usług internetowych były dla nas wnioski z debaty publicznej dotyczącej wykorzystywania przez organy państwa danych telekomunikacyjnych. Po ponad trzech latach debaty na ten temat – ożywiającej się za każdym razem, gdy Urząd Komunikacji Elektronicznej publikował zbiorcze statystyki pokazujące skalę zapytań o dane telekomunikacyjne obywateli (w tym billingi) – wciąż mamy wiele niewiadomych. Największą jest rzetelność i miarodajność generowanych statystyk, co ostatnio potwierdził druzgocący raport Najwyższej Izby Kontroli. Tym trudniej ustalić, w jakich celach organy państwa sięgają po dane telekomunikacyjne i jakiego rodzaju danych żądają od operatorów.

Mimo tych niewiadomych udało się zdiagnozować kilka konkretnych problemów – przede wszystkim to, że brakuje nadzoru ze strony niezależnego organu nad tym, kto, po co i o co pyta operatorów. Reakcją na tak postawioną diagnozę są zapowiadane przez MSW zmiany w obowiązującym prawie, szczególnie projekt stworzenia Komisji Kontroli Służb Specjalnych. W debacie publicznej pojawiły się też wątki ważne dla firm, takie jak problem zwrotu kosztów czy potrzeba ujednolicenia procedur, z jakich korzystają pytające o dane organy. Być może w kolejnym kroku ustawodawca podejmie te problemy.

Doświadczenie z debatą na temat zasad udostępniania danych telekomunikacyjnych przekonało nas, że zainteresowanie mediów i opiniotwórczych środowisk trudnym tematem może wyjść na dobre, nawet jeśli czasem cierpi na tym rzetelność przekazu. Wydaje się, że innej drogi do zmiany sytuacji na lepsze po prostu nie ma. Stąd pomysł podjęcia – w równie kompleksowy sposób – tematu ochrony prywatności użytkowników usług internetowych w kontekście działań wymiaru sprawiedliwości oraz organów ścigania i służb.

Ta decyzja zbiegła się w czasie z ujawnieniem informacji o tym, że amerykańskie służby na ogromną skalę uzyskiwały dostęp do danych przechowywanych przez największe firmy internetowe. Niniejsze opracowanie – zakorzenione w polskich uwarunkowaniach prawnych – nie jest głosem w dyskusji wywołanej rewelacjami Edwarda Snowdena.

Prawo obowiązujące w USA przewiduje, że dane klientów firm podlegających amerykańskiej jurysdykcji mogą być udostępniane służbom w zasadzie bez ograniczeń, o ile klient nie jest obywatelem USA. Mimo braku niezależnych mechanizmów kontroli nad ich działaniem polskie służby muszą każdorazowo uzasadnić swoje żądanie udostępnienia danych, wskazując odpowiednią podstawę prawną. Ani przepisy prawa, ani doświadczenie firm nie dają podstaw, aby sądzić, że w Polsce mamy do czynienia z masową inwigilacją użytkowników usług internetowych. Tę tezę uzasadniamy w szczegółowym opisie zasad udostępniania danych, który jest elementem drugiej części tego opracowania.

***

Ze względu na specyfikę zebranego materiału podzieliliśmy nasze opracowanie na dwie – w dużej mierze niezależne – części:

- **pierwsza** stanowi próbę interpretacji danych, które otrzymaliśmy od firm w ramach badania pilotażowego oraz od organów państwa (przede wszystkim służb) w odpowiedzi na wnioski o dostęp do informacji publicznej; jako kontekst zostały przywołane również dane zbierane od operatorów telekomunikacyjnych przez Urząd Komunikacji Elektronicznej;

- **druga** ma charakter problemowy – zbiera wnioski z analizy przepisów prawa oraz z rozmów, jakie na etapie przygotowania lub analizy ankiet przeprowadziliśmy z firmami świadczącymi usługi internetowe, a także rozmów z policją.

Zapraszamy do lektury!

I. Praktyka firm i organów państwa: analiza zebranych danych

W tej części opracowania:

- opisujemy zebrane informacje na temat skali i praktyki przekazywania danych o użytkownikach usług internetowych na żądanie organów państwa, które uzyskaliśmy dzięki współpracy z kilkoma wiodącymi firmami świadczącymi takie usługi;
- porównujemy odpowiedzi firm z informacjami, jakie – w trybie dostępu do informacji publicznej – uzyskaliśmy od organów państwa;
- zestawiamy skalę przekazywania danych o użytkownikach usług internetowych na żądanie organów państwa ze skalą udostępniania danych telekomunikacyjnych;
- stawiamy kilka hipotez, które uważamy za warte zbadania i poddania weryfikacji.

I. BADANIE PILOTAŻOWE: CO CHCIELIŚMY OSIĄGNĄĆ I CO SIĘ UDAŁO?

Podstawową trudnością w ocenie skali i praktyk sięgania po dane użytkowników usług internetowych jest to, że polskie prawo nie zobowiązuje ani firm świadczących takie usługi, ani organów państwa, które sięgają po dane, do prowadzenia statystyk i przygotowywania sprawozdań na ten temat. Jeśli firmy przygotowują takie sprawozdania – robią to z własnej woli, wychodząc naprzeciw społecznym oczekiwaniom. Licząc na taką otwartość, postanowiliśmy zadać kilka pytań wiodącym firmom, które świadczą usługi internetowe na polskim rynku.

Nikt przed nami nie rozmawiał z tego typu firmami na temat zapytań, jakie kierują do nich rozmaite organy państwa. Nic więc dziwnego, że nawet przedsiębiorstwa, które były otwarte na taką rozmowę, nie dysponowały jednolitą i usystematyzowaną wiedzą. W niektórych przypadkach okazało się, że dane, których szukamy – owszem – są, ale tylko w formie papierowej, a ich przeniesienie do formatu elektronicznego byłoby dla firmy bardzo czasochłonne. Zdając sobie sprawę z tego typu ograniczeń, postanowiliśmy zacząć od rozmowy z firmami i przeprowadzenia pilotażu. Chcieliśmy zweryfikować, czy dobrze stawiamy pytania, jak również sprawdzić, jakimi danymi firmy dysponują już dziś i czy są skłonne podzielić się tą wiedzą.

Dlaczego firmy miałyby otwarcie mówić o swoich praktykach przekazywania danych o użytkownikach usług internetowych na żądanie organów państwa, skoro prawo ich do tego nie obliguje? Chcieliśmy sprawdzić, czy na wzór międzynarodowych gigantów, takich jak Apple, Facebook i Google, zechcą ujawnić pewne zestawienia statystyczne. Gdyby nam się to udało, byłaby to pierwsza tego rodzaju inicjatywa, nie tylko w Polsce, ale i w Europie, nastawiona na poznanie realiów przekazywania danych przez firmy świadczące usługi drogą elektroniczną.

Naszym celem nie było stworzenie rankingu jawności wśród firm, dlatego też udzielone przez nie odpowiedzi poddaliśmy pseudonimizacji[2]**.** Chcieliśmy sprawdzić, czy ujawnienie konkretnych danych pozwoli zobaczyć, jak w praktyce funkcjonują przepisy związane z pozyskiwaniem informacji o użytkownikach usług internetowych, nawet jeśli przyniesie to więcej pytań niż odpowiedzi. Zdawaliśmy sobie sprawę z tego, że na wejściu trudno nam będzie zebrać wyczerpujące dane. Nasze cele koncentrowały się wokół stworzenia spójnej metody, którą będzie można wykorzystać w dalszych, szerzej zakrojonych działaniach badawczych, i rozpoczęcia otwartej dyskusji na temat zasad przekazywania danych o użytkownikach usług internetowych na żądanie organów państwa.

Nie mamy pewności co do tego, czy wszystkie dane, które udało nam się zebrać w ramach współpracy z firmami, są w pełnym zakresie porównywalne. Dołożyliśmy jednak starań, by na wstępie wyjaśnić możliwe niejasności i wątpliwości. Przygotowanie formularza ankiet dla firm poprzedziliśmy rozmowami z ich przedstawicielami, dzięki którym mogliśmy się dowiedzieć, jakie kategorie danych są zbierane przez poszczególne firmy oraz w jakim zakresie wewnętrzne zasady ich gromadzenia i sprawozdawczości są ze sobą zbieżne.

Rozmowy z firmami – analiza jakościowa
Zaproszone przez nas firmy uczestniczyły w tym przedsięwzięciu od samego początku, także na etapie przygotowania ankiet. Przeprowadziliśmy rozmowy, które pomogły nam zrozumieć zasady funkcjonowania wielu procesów i mają odzwierciedlenie w opisie praktyki stosowania przepisów w naszym kraju. Większość konkretnych problemów, które opisujemy w drugiej części tego opracowania, zdiagnozowaliśmy właśnie na podstawie rozmów z firmami, przeprowadzonych na etapie opracowywania formularza ankiet. To potwierdziło nasze założenie, że poznanie mechanizmów i zasad, na których opiera się przekazywanie danych o użytkownikach usług internetowych na żądanie organów państwa, jest ważniejsze niż sucha, ilościowa analiza tego zjawiska.

Ważniejsza niż skala pozyskanych danych okazała się możliwość postawienia diagnozy problemów i wypracowania wspólnych konkluzji.

[2] W tym przypadku: oddzielenie odpowiedzi na ankiety od danych bezpośrednio identyfikujących firmy i zastąpienie tych ostatnich liczbami porządkowymi.

Metoda

Do udziału w pilotażu zaprosiliśmy dwanaście firm, które są właścicielami najpopularniejszych polskojęzycznych portali internetowych. Podstawą doboru firm było badanie Megapanel PBI/Gemius (luty 2013). Rozstrzygająca była pozycja firmy na polskim rynku usług internetowych mierzona liczbą użytkowników – nie braliśmy pod uwagę jej lokalizacji ani pochodzenia. Stąd obok polskich w tej grupie znalazły się także firmy zagraniczne. Większość zaproszonych firm zadeklarowała chęć współpracy, jednak w trakcie realizacji projektu kilka z nich zrezygnowało z udziału.

Na wstępnym etapie przeprowadziliśmy rozmowy z przedstawicielami zaproszonych do współpracy firm, które nie tylko pomogły zebrać informacje na temat praktyk sięgania organów państwa po dane i wyzwań pojawiających się na tym tle, ale stanowiły podstawę do przygotowania formularzy ankiet, które zostały następnie przekazane firmom.

Każda z firm otrzymała dwie wersje ankiety: podstawową i rozszerzoną. W wersji podstawowej pytaliśmy o te informacje, które – zgodnie z uzyskaną wiedzą – były w posiadaniu większości z nich: Ile zapytań o dostęp do danych organy państwa skierowały do nich w ostatnim roku ogółem oraz w rozbiciu na rodzaje tych organów? Ile wniosków doczekało się odpowiedzi w postaci udostępnienia żądanych danych? Wersja rozszerzona zawierała pytania o liczbę kont, których dotyczyły żądania udostępnienia danych, oraz liczbę kont, w przypadku których dane rzeczywiście udostępniono. Pytaliśmy w niej też, ile razy żądano dostępu do konkretnych kategorii danych oraz ile razy te dane rzeczywiście udostępniano. Chodzi o takie kategorie, jak: dane abonenckie, dane podawane przy rejestracji, historię logowania, dane geolokalizacyjne, treść komunikacji publicznej, informacje o sieci kontaktów oraz plikach, jakie użytkownicy zamieszczają w chmurze.

W rozszerzonej wersji ankiety znalazły się też pytania dotyczące podstaw prawnych, na jakie powoływały się organy państwa przy żądaniu dostępu do danych, jak również stosunku firmy do danej podstawy prawnej na etapie weryfikacji zasadności wniosków. Pytaliśmy o procedurę stosowaną w przypadku odrzucenia wniosku ze względów formalnych oraz o to, czy firmy pobierają opłaty od podmiotów żądających dostępu do danych. Interesowało nas też, jakie obciążenie czasowe wiąże się z obsługą zapytań o dane oraz jakie kanały komunikacji z organami państwa dopuszcza dana firma.

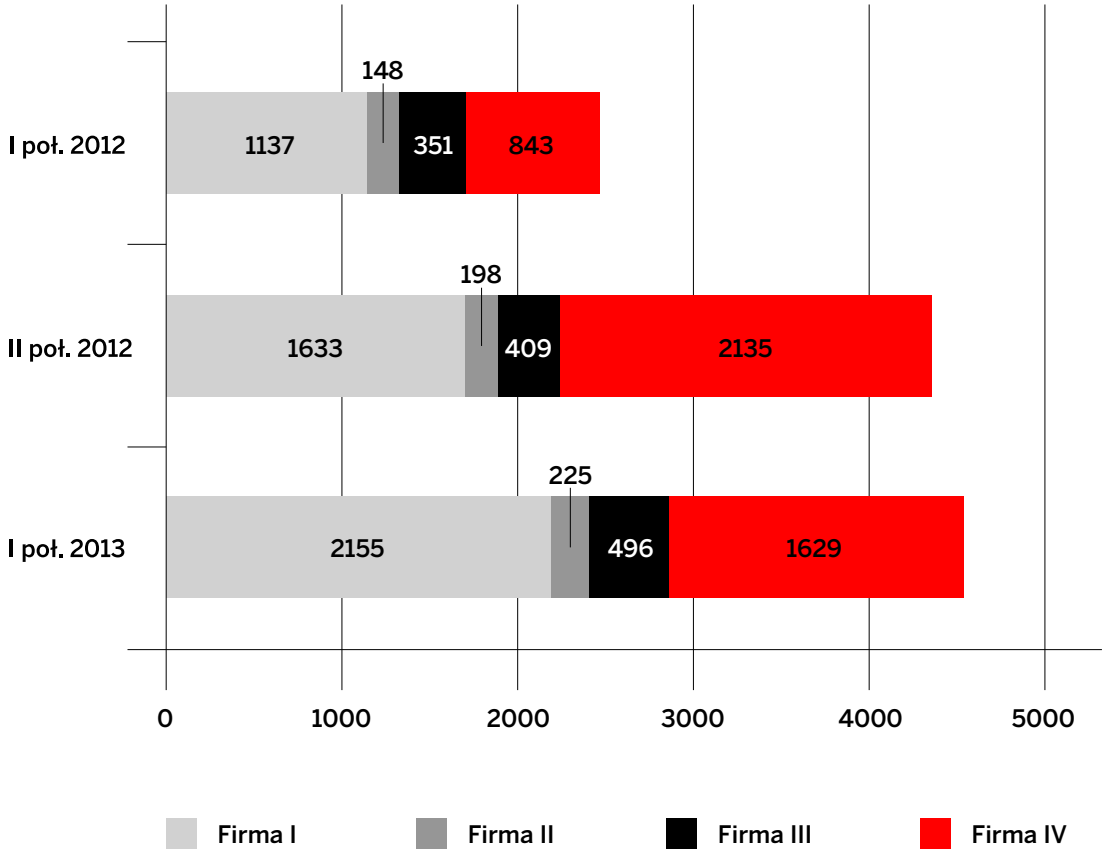
Żeby uzupełnić informacje, jakie przekazały nam firmy biorące udział w pilotażu, postanowiliśmy spytać drugą stronę – prokuraturę, policję i inne służby – o liczbę wniosków, jakie te organy kierują do firm świadczących usługi drogą elektroniczną. Dostaliśmy jedynie pojedyncze odpowiedzi, które dla ilustracji przedstawiamy w dalszej części tego opracowania.

II. CO WIEMY NA TEMAT SKALI ZAPYTAŃ O DANE?

Dyskusję o tym, ile organy państwa chcą wiedzieć o obywatelach i w jakim stopniu angażują do tego firmy świadczące usługi drogą elektroniczną, łatwo sprowadzić do liczb. To jednak niepotrzebne i niebezpieczne uproszczenie. Nie o samą skalę przecież chodzi, ale przede wszystkim o to, czy państwo pyta tylko wtedy, kiedy rzeczywiście ma do tego podstawy, a firmy – odpowiadają tylko wtedy, kiedy muszą.

Informacje na temat liczby zapytań pochodzących od publicznych instytucji zostały udostępnione przez wszystkie cztery firmy biorące udział w pilotażu. Dane zebrane dla analizowanych 18 miesięcy obrazuje wykres 1.

Wykres 1: Liczba zapytań skierowanych przez wszystkie uprawnione organy państwa do firm świadczących usługi drogą elektroniczną (na podstawie danych przekazanych przez cztery firmy)



Z przekazanych odpowiedzi wynika, że bezwzględna liczba zapytań o dane otrzymywanych przez poszczególne firmy znacząco się różni. Jak można wyjaśnić te różnice?

Hipotezą, która nasuwa się jako pierwsza, jest to, że liczba zapytań zależy od wielkości firmy i liczby klientów. W pewnym stopniu na pewno. Warto jednak zwrócić uwagę, że każda ze współpracujących firm prowadzi działalność na szeroką skalę i ma znaczącą pozycję na polskim rynku. Więcej światła na ten problem rzucają rozmowy z przedstawicielami firm. Wynika z nich, że kluczowym czynnikiem jest w tym przypadku model biznesowy i rodzaj świadczonych usług: im więcej możliwych sporów między użytkownikami i potencjalnych naruszeń prawa, tym więcej zapytań. Na przykład model biznesowy oparty na sprzedaży towarów i usług przez Internet z zasady zakłada większe ryzyko oszustw i sporów związanych z prawami autorskimi niż model zakładający prowadzenie portalu informacyjnego połączonego z forum dyskusyjnym. W tym drugim przypadku należy się spodziewać sporów między użytkownikami na tle naruszenia dóbr osobistych, w tym zniesławienia, które relatywnie rzadziej angażują organy państwa.

Z naszych rozmów z policją – która zaraz po prokuraturze pyta o dane użytkowników najczęściej – wynika, że kolejnym istotnym czynnikiem jest lokalizacja serwera i jurysdykcja, jakiej podlega firma. Firmy zagraniczne obecne na polskim rynku z zasady

odsyłają policję i inne organy państwa do swojej centrali. Nie wszyscy funkcjonariusze radzą sobie z taką procedurą. Jeśli mają wybór, wolą o to samo zapytać polską firmę. Dlatego w przypadku międzynarodowych korporacji takich jak Facebook czy Google liczba kierowanych do nich zapytań może okazać się mniejsza, niż można by oczekiwać na podstawie skali działania firmy.

Analiza danych przekazanych przez wszystkie firmy, które wzięły udział w pilotażu, prowadzi do wniosku, że w badanym okresie liczba zapytań, jakie kierują do nich organy państwa, konsekwentnie rośnie. Otwarte pozostaje pytanie o to, z czego wynika ten wzrost. Czy organy państwa miały więcej powodów, żeby pytać (np. w związku ze wzrostem liczby toczących się postępowań z udziałem klientów firm świadczących usługi drogą elektroniczną)? Wiele na to wskazuje.

Ze względu na wycinkowość danych poddanych analizie trudno wyrokować, czy zaobserwowany wzrost liczby zapytań jest szerszym i trwałym trendem. Jednak rozmowy, jakie przeprowadziliśmy z przedstawicielami firm i policji, sugerują, że taka teza jest uzasadniona. Wiele wskazuje na to, że wzrost liczby zapytań o dane użytkowników usług internetowych ze strony organów państwa to skutek uboczny wzrostu społecznej aktywności w Internecie. Wraz z przenoszeniem się różnych sfer życia do sieci przenosi się tam również przestępczość; rośnie też liczba sporów między obywatelami, które wynikają z aktywności internetowej.

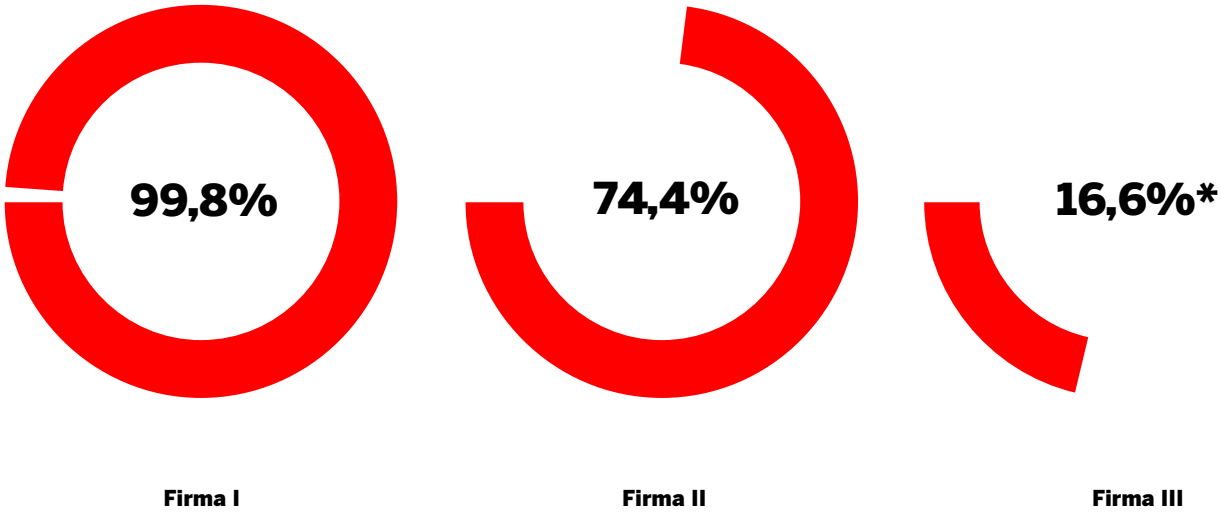
Tę intuicję potwierdzają liczne badania dotyczące aktywności użytkowników Internetu na przestrzeni ostatnich lat. Autorzy badania CBOS za 2012 rok stwierdzają: „Dynamicznie rośnie liczba internautów – już niemal dwie trzecie dorosłych deklaruje, że korzysta z sieci w celach pozazawodowych". Również realizowane w latach 2010–12 badania World Internet Project pokazują, że odsetek użytkowników Internetu w Polsce wzrasta z roku na rok. W 2012 r. z Internetu korzystało dwie trzecie badanych, w tym ponad 90% poniżej 30 roku życia. Badania aktywności dzieci i młodzieży – m.in. Generalnego Inspektora Ochrony Danych Osobowych oraz inne, zrealizowane przez firmę TNS we współpracy z Fundacją Orange i Fundacją Dzieci Niczyje – pokazują, że z Internetu powszechnie korzystają również dzieci. Można zaryzykować stwierdzenie, że wraz z dojrzewaniem kolejnych pokoleń aktywnych użytkowników Internetu będzie wzrastać liczba zapytań o ich dane na potrzeby rozmaitych postępowań.

Dlaczego skala zapytań o dane bywa zwodnicza?
Z rozmów z policją wiemy, że sama skala zapytań w niczym nie oddaje skali zainteresowania policji (czy innych służb) konkretnymi obywatelami. Wynika to z praktyki działań śledczych, które z zasady zaczynają się od szerzej zakrojonych poszukiwań po to, by na dalszym etapie zawęzić się do kręgu osób podejrzanych. Aby ustalić ten właściwy numer IP, zwykle trzeba zweryfikować lub porównać ze sobą wiele innych. To jednak nie znaczy, że policja interesuje się każdą osobą, której numer IP znalazł się w aktach sprawy. Byłaby to najkrótsza droga do sparaliżowania pracy organów ścigania. Dodatkowo dyskusję o skali zapytań, jakie organy państwa kierują do firm świadczących usługi drogą elektroniczną, utrudnia brak spójnej metody prowadzenia sprawozdawczości. Jak liczyć takie zapytania? Czy pytanie o każdy numer IP, nawet jeśli zmierza do ustalenia jednego sprawcy, liczyć osobno? Co w sytuacji, gdy jedno zapytanie (np. o numer IP) generuje kolejne, bardziej szczegółowe (np. o dane, które użytkownik podał w umowie), ale wciąż dotyczy tej samej sprawy? Wątpliwości można mnożyć.

III. JAK FIRMY REAGUJĄ NA ZAPYTANIA O DANE?

Porównanie liczby zapytań kierowanych przez instytucje publiczne z liczbą udzielanych odpowiedzi prowadzi o ciekawych wniosków. Okazuje się, że w przypadku trzech firm, które były w stanie przekazać odpowiednie dane, **odsetki udostępnień są bardzo zróżnicowane: od kilkunastu do kilkudziesięciu procent w skali 18 miesięcy**. Otwarte pozostaje pytanie o to, z czego mogą wynikać tak duże różnice w procencie udostępnianych danych.

Wykres 2: Odsetek udostępnień danych użytkowników przez firmy świadczące usługi drogą elektroniczną w odpowiedzi na zapytania organów państwa w okresie 1.01.2012–30.06.2013 (na podstawie danych przekazanych przez trzy firmy)



Zestawienie to należy interpretować ostrożnie, ze względu na fakt, że *w przypadku firmy III odsetek udostępnień dotyczy stosunku liczby zapytań dotyczących kont użytkowników do liczby udostępnień dotyczących tychże kont, podczas gdy w przypadku pozostałych dwóch firm odsetek ten odnosi się do stosunku liczby zapytań do udostępnień dotyczących tych zapytań (bez względu na to jakiej liczby kont dotyczyły). Niemniej różnice między firmami są tak znaczące (nawet między firmą I i II, które podały analogiczne dane), że zasługują na szczególną uwagę.

Na podstawie rozmów, jakie przeprowadziliśmy z firmami i policją, mamy trzy – wzajemnie się niewykluczające – hipotezy wyjaśniające tę sytuację.

- Różnice w procedurach stosowanych przez firmy
  Prawo nie reguluje w sposób precyzyjny, jak powinien wyglądać i jakie warunki spełniać wniosek o dane użytkownika usług internetowych (por. analiza na s. 24). W związku z tym firmy same te warunki doprecyzowują i same oceniają, czy dany wniosek spełnia kryteria formalne. W efekcie może się zdarzyć, że niektóre z nich respektują wnioski, które inne uznałyby za „źle wypełnione". W sytuacji braku precyzyjnej regulacji są one skazane na własną ocenę i wdrażanie własnych procedur.

- Niespójność praktyk po stronie organów państwa
  Doświadczenie firm pokazuje, że różne organy państwa stosują różne standardy przygotowywania wniosków o dane: czasem do firmy trafia dobrze umotywowany, kompletny wniosek; innym razem pismo wymaga wyjaśnień – co może mieć odzwierciedlenie w statystykach.

- Różnice wynikające z jurysdykcji
  Internet jest zjawiskiem globalnym. To oznacza, że nie istnieją dla niego ani granice państw, ani granice jurysdykcji i porządków prawnych. Ponieważ część firm oferujących swoje usługi na terenie Polski ma swoje siedziby w innych państwach, różne są też procedury stosowane w relacjach między organami państwowymi a firmami zagranicznymi (por. analiza na s. 21–22).

Nie przesądzając, która z powyższych hipotez najlepiej odzwierciedla rzeczywistość, można zaryzykować stwierdzenie, że tak długo, jak wiemy bardzo niewiele na temat działań organów państwa wobec firm funkcjonujących na polskim rynku, ale podlegających różnym reżimom prawnym, rzetelne porównanie praktyk samych firm w zakresie przekazywania danych o użytkownikach na żądanie organów państwa będzie niemożliwe.

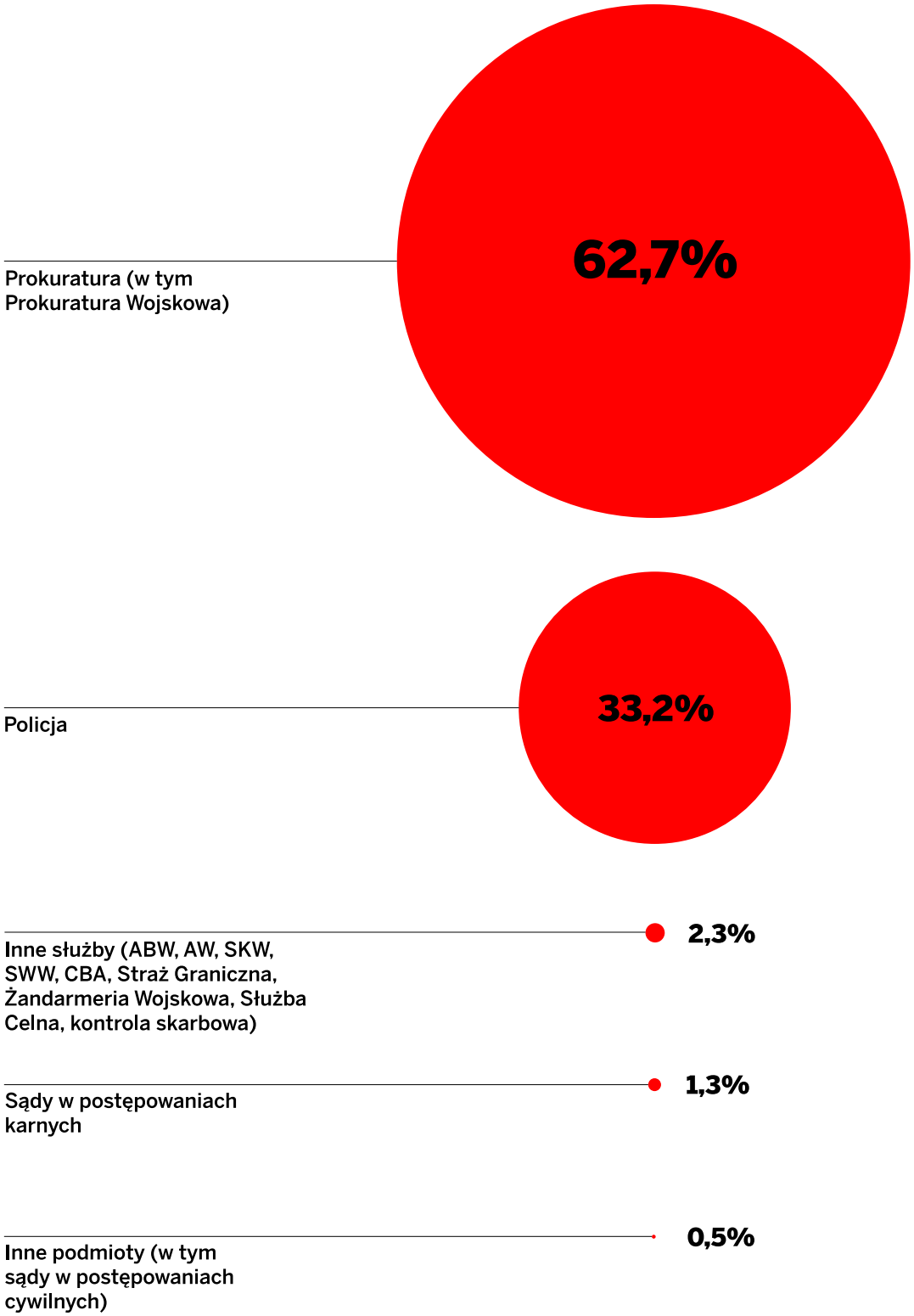
IV. KTO I DLACZEGO PYTA?

O wiele ciekawsza niż próba zbadania skali zapytań o dane użytkowników usług internetowych wydała nam się odpowiedź na pytanie o to, kto i w jakim celu domaga się przekazania takich danych.

Na podstawie rozmów z firmami udało się ustalić, jakie podstawy prawne są wykorzystywane przez organy państwa pytające o dane usługobiorców, jakie podstawy są przez firmy respektowane i jakie problemy rodzą się na tym tle. Wnioski z tej analizy zawarliśmy w drugiej części tego opracowania (por. s. 24). Niestety, okazało się, że żadna z firm biorących udział w pilotażu nie gromadzi szczegółowych danych na temat podstaw prawnych, na jakie powołują się organy państwa, a tym samym nie jest w stanie odtworzyć udziału poszczególnych podstaw prawnych w łącznej liczbie kierowanych zapytań.

Od trzech firm udało się natomiast uzyskać informacje na temat tego, jakie podmioty i jak często sięgają po dane usługobiorców. Poniższy wykres przedstawia udział poszczególnych organów w ogólnej liczbie zapytań, jakie trafiły do firm w analizowanym okresie.

Wykres 3: Udział zapytań poszczególnych organów państwa w łącznej liczbie zapytań skierowanych do firm świadczących usługi drogą elektroniczną w okresie 1.01.2012–30.06.2013 (na podstawie danych przekazanych przez trzy firmy)



Z odpowiedzi firm, które były w stanie przekazać nam odpowiednie dane, wynika, że niekwestionowanym liderem, jeśli chodzi o liczbę zapytań o dane użytkowników usług internetowych, jest prokuratura. Na drugim miejscu plasuje się policja.

Zapytania kierowane bezpośrednio przez sądy są o wiele rzadsze. Natomiast zapytania od służb – w tym ABW czy CBA – stanowią zupełny margines. Przy czym żadna z polskich firm nie zastrzegła, że nie może ujawnić pewnych kategorii zapytań o dane. W ich odpowiedziach służby specjalne pojawiły się na równi z policją i prokuraturą. Na tej postawie oraz na podstawie analizy przepisów prawa możemy zaryzykować tezę, że polskie firmy nie otrzymują zapytań od służb, których skali nie mogłyby ujawnić ze względu na obowiązującą je tajemnicę.

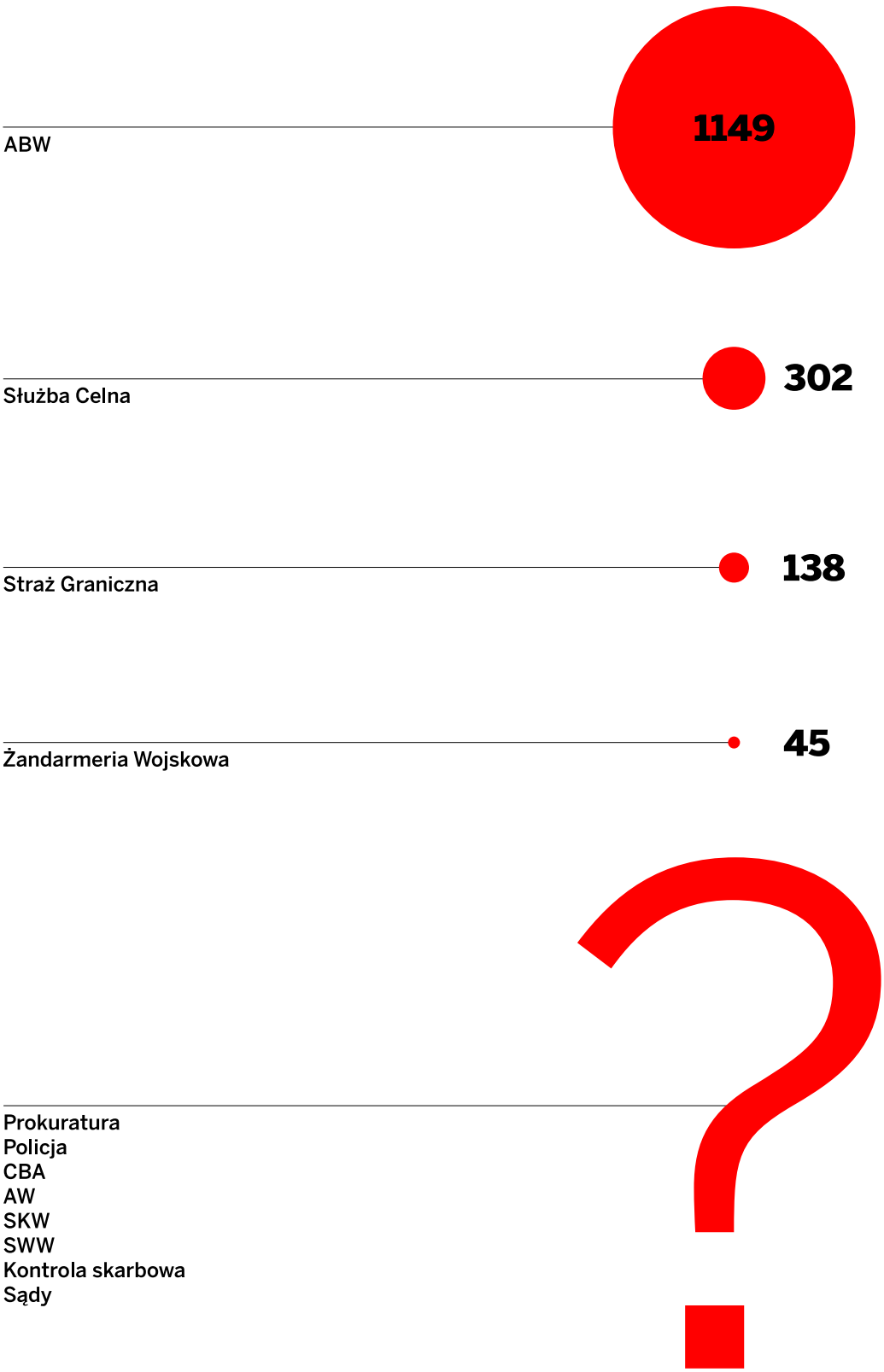
Zdecydowana większość zapytań o dane użytkowników usług internetowych przechodzi przez wymiar sprawiedliwości lub organy ścigania, które pozyskują dane na potrzeby postępowań karnych. Zakładając, że przekazane informacje są rzetelne, a państwo nie stosuje metod niejawnego sięgania po dane gromadzone przez firmy, nie ma przesłanek, by sądzić, że polskie służby realizują programy masowej inwigilacji w zakresie pobierania informacji o osobach korzystających z usług internetowych.

Ze względu na niewielką liczbę firm, które wzięły udział w pilotażu, postanowiliśmy przyjrzeć się zapytaniom o dane użytkowników Internetu również od strony organów państwa. W tym celu skierowaliśmy analogiczne pytania do: policji, prokuratury, ABW, Agencji Wywiadu, CBA, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Służby Celnej, kontroli skarbowej, Straży Granicznej i Żandarmerii Wojskowej. W trybie dostępu do informacji publicznej zapytaliśmy te instytucje m.in. o to, ile zapytań o dane obywateli – w tym samym czasie – skierowały do firm świadczących usługi drogą elektroniczną.

Niestety, akurat w tych instytucjach, które według danych uzyskanych od firm pytają najwięcej, nasze wnioski o dostęp do informacji publicznej napotkały na opór. Policja poinformowała nas, że nie zbiera tego typu danych, a więc nie może ich nam przekazać. Podobnie odpowiedziała Prokuratura Generalna: ponieważ prawo nie nakłada na nią takiego obowiązku, na poziomie centralnym nie prowadzi ewidencji wszystkich zapytań kierowanych przez poszczególne prokuratury do firm świadczących usługi drogą elektroniczną. Rzeczywista i precyzyjna skala zapytań, jaką generują te instytucje, pozostaje zatem wielką niewiadomą.

Natomiast udało nam się uzyskać dane na temat liczby zapytań kierowanych do firm świadczących usługi drogą elektroniczną od służb, które teoretycznie mają najwięcej powodów, żeby takie informacje uznać za poufne lub z innych powodów niedostępne. Zestawienie ich odpowiedzi prezentujemy poniżej.

Wykres 4: Liczba zapytań skierowanych przez poszczególne uprawnione organy państwa do firm świadczących usługi drogą elektroniczną w okresie 1.01.2012–30.06.2013 (na podstawie danych uzyskanych od organów państwa)



Nie ulega wątpliwości, że bez analogicznych danych od prokuratury i policji bardzo trudno oszacować skalę zapytań o dane użytkowników usług internetowych w Polsce. Na podstawie zebranych danych możemy jednak zaryzykować tezę, że same służby – poza policją – pytają mało. Ten wniosek ma oparcie nie tylko w danych przekazanych przez firmy, ale także w odpowiedziach służb udzielonych w trybie dostępu do informacji publicznej. W skali kraju podane przez nie liczby zapytań o dane użytkowników usług internetowych to margines całego zjawiska.

V. KONTEKST: UDOSTĘPNIANIE DANYCH TELEKOMUNIKACYJNYCH

Żeby umieścić dyskusję o udostępnianiu danych użytkowników usług internetowych w szerszym kontekście, wracamy do punktu wyjścia: skali zapytań o dane obywateli, z którą mierzą się operatorzy telekomunikacyjni.

Wykres 5: Liczba zapytań skierowanych do operatorów telekomunikacyjnych przez wszystkie uprawnione organy państwa w 2011 i 2012 r. (na podstawie danych zebranych przez Urząd Komunikacji Elektronicznej)

Mimo że – jak wielokrotnie podkreślaliśmy – suche liczby niewiele mówią o interesujących nas problemach i trudno w oparciu o nie wyciągać daleko idące wnioski, samo porównanie skali zapytań o te dwie kategorie danych daje do myślenia.

Zestawienie danych publikowanych przez Urząd Komunikacji Elektronicznej oraz danych, jakie w trybie dostępu do informacji publicznej uzyskaliśmy od poszczególnych organów państwa, pokazuje, że zainteresowanie danymi generowanymi w sieciach telekomunikacyjnych jest zdecydowanie większe niż w przypadku usług świadczonych drogą elektroniczną.

Tabela: Liczba zapytań skierowanych przez poszczególne uprawnione organy państwa w latach 2011-12 (na podstawie danych uzyskanych od organów państwa)

	do firm świadczących usługi drogą elektroniczną	do operatorów telekomunikacyjnych
Policja	brak danych	2894760
CBA	brak danych	195300
ABW	1299	241902
AW	brak danych	——
SKW	brak danych	brak danych
SWW	brak danych	——
Straż Graniczna	192	716726
ŻW	32	12259
Kontrola skarbowa	brak danych	6963
Służba Celna	268	26
Prokuratura	brak danych	brak danych
Sądy	brak danych	brak danych

Z perspektywy tej analizy najciekawsze wydaje się porównanie liczby zapytań o dane telekomunikacyjne kierowanych przez poszczególne uprawnione organy z analogicznym zestawieniem dotyczącym danych użytkowników usług internetowych, szczególnie że w przypadku zapytań kierowanych przez służby do operatorów telekomunikacyjnych udało nam się uzyskać interesujące nas dane od policji (także w trybie dostępu do informacji publicznej). Jeśli przyjąć założenie, że struktura zapytań w przypadku obu rodzajów danych – danych abonentów telekomunikacyjnych i danych użytkowników usług internetowych – jest w miarę podobna, potwierdza się wniosek wynikający z odpowiedzi uzyskanych od firm (por. wykres 3): policja interesuje się danymi obywateli w dużo większym stopniu niż inne służby.

Zdecydowana większość ingerencji w prywatność użytkowników usług internetowych jest związana z postępowaniami karnymi i odbywa się pod kontrolą wymiaru sprawiedliwości, ponieważ wszelkie dane zebrane przez policję ostatecznie trafiają do akt postępowania albo są niszczone jako nieprzydatne.

Drugi ciekawy wniosek dotyczy ogromnej dysproporcji między liczbą zapytań, które organy państwa kierują do firm świadczących usługi drogą elektroniczną, a liczbą tych, które trafiają do operatorów telekomunikacyjnych. Porównanie tych danych wydaje się potwierdzać to, czego dowiedzieliśmy się z rozmów z policją: do firm świadczących usługi internetowe organy ścigania z zasady kierują przede wszystkim pytania o numer IP. Ustalenie numeru IP użytkownika to zwykle pierwszy trop w sprawie, jeśli dotyczy ona korzystania z usług internetowych. Jeśli tylko jest taka możliwość, na etapie rozpracowania sprawy i gromadzenia dowodów policja i prokuratura wykorzystują bardziej wiarygodne i mówiące więcej dane, które są gromadzone przez operatorów telekomunikacyjnych (por. analiza na s. 23). Drugim czynnikiem, który może mieć wpływ na dużą skalę zapytań o dane telekomunikacyjne, jest możliwość bezpośredniego sięgania po dane przechowywane przez operatorów za pomocą specjalnych interfejsów, ułatwiających i przyspieszających dostęp do tych danych. W przypadku sięgania po dane użytkowników usług internetowych organy państwa nie mają takiej możliwości i za każdym razem muszą je uzyskać od firmy świadczącej usługi.

II. Udostępnianie danych: formalne zasady i praktyczne problemy

W tej części opracowania:

- wyjaśniamy podstawowe zasady gromadzenia danych przez firmy i ich udostępniania organom państwa;
- opisujemy praktyczne problemy i dylematy, z którymi muszą mierzyć się firmy przekazujące dane na żądanie organów państwa;
- diagnozujemy siedem kluczowych problemów, które wymagają zmian w przepisach obowiązującego prawa.

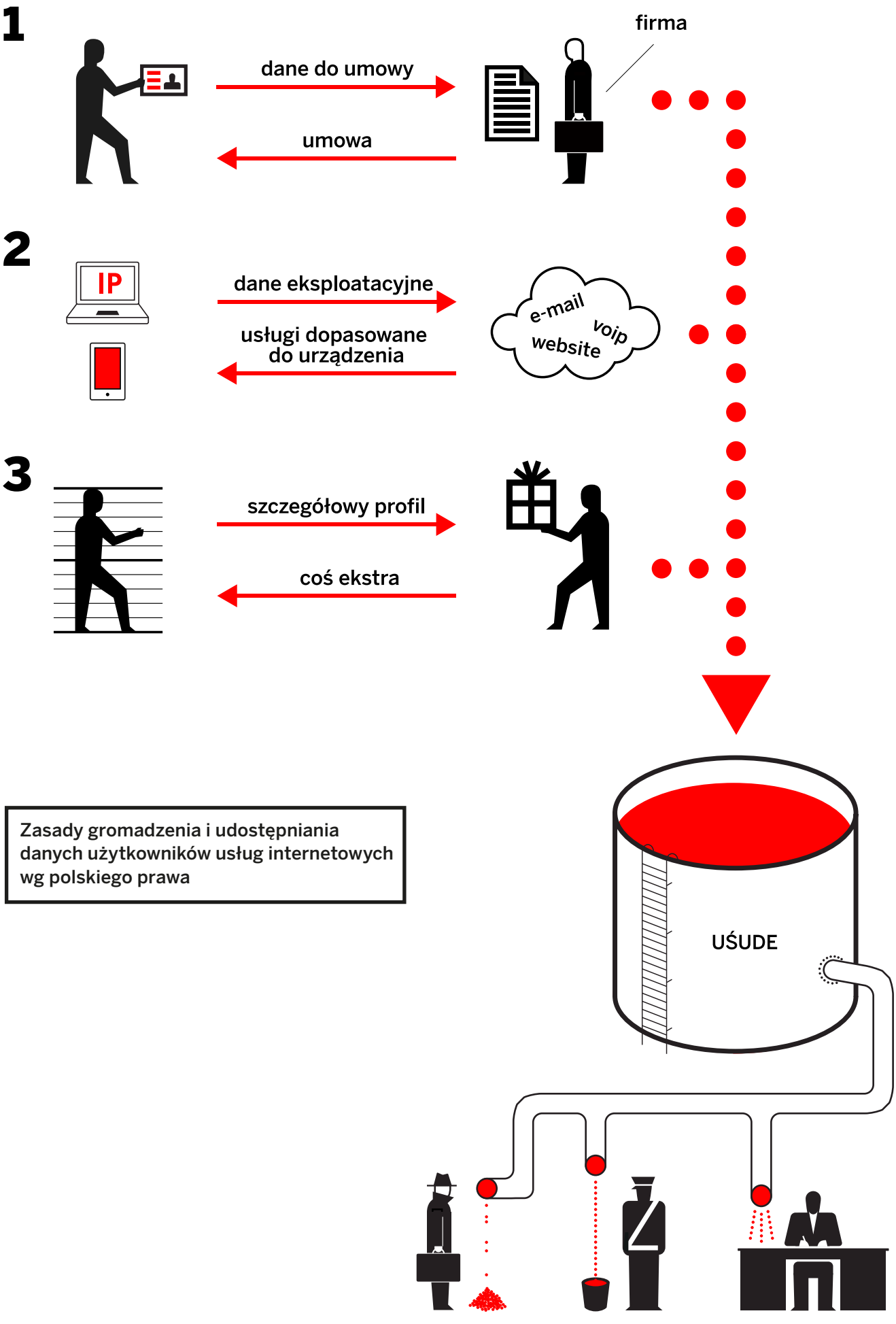
I. CO FIRMY WIEDZĄ O UŻYTKOWNIKACH?

Każdy ruch w Internecie zostawia ślad. Ten ślad może być rejestrowany przez dostawcę usługi, z której korzysta obywatel-użytkownik. Im więcej takich danych gromadzi firma, tym więcej informacji na temat obywateli-użytkowników mogą pozyskać także organy państwa, o ile tylko mają do tego podstawę prawną. Dlatego naturalnym punktem wyjścia do rozmowy o zasadach dostępu do danych użytkowników usług internetowych powinno być przypomnienie, jakie dane na temat użytkowników usług internetowych mogą być przetwarzane przez same firmy.

Dane niezbędne

To, jakie dane o swoich klientach może przetwarzać polska firma świadcząca usługi drogą elektroniczną, jest ściśle uregulowane przepisami. Co do zasady są to informacje niezbędne, by prawidłowo dostarczyć i rozliczyć świadczoną usługę. W tej kategorii mieszczą się:

- dane osobowe, które są niezbędne do zawarcia umowy: np. nazwisko, PESEL, adres e-mail (por. infografika – 1);
- dane „eksploatacyjne", które są konieczne, by „dopasować" usługę do sprzętu i oprogramowania użytkownika: np. numer IP, informacje o ustawieniach przeglądarki i zainstalowanym oprogramowaniu (por. infografika – 2).



Zasady gromadzenia i udostępniania danych użytkowników usług internetowych wg polskiego prawa

Niezbędne do świadczenia usługi może być także przechowywanie treści korespondencji, jeśli tego właśnie oczekuje klient – np. w ramach usługi poczty elektronicznej, wykorzystującej hosting danych na wirtualnym serwerze. To oczywiście nie znaczy jeszcze, że firma ma prawo czytać nasze e-maile i wykorzystywać ich treść w innych celach niż te, które wynikają bezpośrednio z umowy.

Innym przykładem danych osobowych zbieranych przez firmy może być adres, pod który sklep internetowy dostarcza zakupiony towar. Jednak zasada jest wciąż ta sama – firma musi mieć jasny, wynikający ze specyfiki swojego działania, powód do przetwarzania tych informacji.

W Polsce zasady zbierania i przechowywania danych o klientach regulują: ustawa o świadczeniu usług drogą elektroniczną i ustawa o ochronie danych osobowych. Tych reguł nie muszą jednak przestrzegać firmy, które nie podlegają polskiej jurysdykcji, nawet jeśli działają na polskim rynku.

Dodatkowe dane

Może się zdarzyć, że firma chce zbierać dane, które nie są niezbędne do świadczenia zamówionej przez użytkownika usługi – np. służące lepszemu dopasowaniu reklam czy poprawiające jakość usług (por. infografika – 3). W tym kontekście takie informacje, jak historia aktywności w serwisie, szczegółowy profil użytkownika czy informacje o kontaktach z innymi użytkownikami, mogą być bardzo atrakcyjne.

Jeśli firma chce przetwarzać dane osobowe, które nie są jej niezbędne do realizacji usług – może to zrobić wyłącznie za zgodą użytkownika. W praktyce oznacza to, że powinna poinformować każdego użytkownika, jakie dodatkowe informacje chce o nim zbierać i zapytać, czy akceptuje on takie warunki dostarczania usług.

Zasad, jakie wynikają z ustawy o świadczeniu usług drogą elektroniczną i ustawy o ochronie danych osobowych, nie muszą przestrzegać firmy, które nie podlegają polskiej jurysdykcji (zarejestrowane poza Polską i nieprzetwarzające danych na terenie Polski). W ich przypadku zasady zbierania i przetwarzania danych użytkowników określa prawo kraju pochodzenia.

II. ZASADY UDOSTĘPNIANIA DANYCH ORGANOM PAŃSTWA

Informacje, które są niezbędne z perspektywy firm, jak również te, które użytkownicy usług internetowych przekazują im dobrowolnie, mogą się okazać równie atrakcyjne z perspektywy państwa. Najczęstszym powodem takiego zainteresowania jest walka z przestępczością, a konkretnie potrzeba zebrania dowodów w dochodzeniu przeciwko danej osobie. Zasady, na jakich organy państwa mogą wykorzystywać dane gromadzone przez firmy, również określa prawo.

Z jednej strony ustawa o świadczeniu usług drogą elektroniczną nakłada na wszystkie firmy świadczące takie usługi obowiązek „udzielania informacji o przetwarzanych danych organom państwa na potrzeby prowadzonych przez nie postępowań" (art. 18 ust. 6 UŚUDE). Podobnie jak ograniczenia dotyczące zbierania i przetwarzania danych osobowych obowiązki wynikające z tej ustawy dotyczą tylko firm podlegających polskiej jurysdykcji. Firmy zagraniczne stosują się do takich zasad, jakie określa prawo kraju, w którym są zarejestrowane.

Jednak obowiązki firm wynikające z ustawy o świadczeniu usług drogą elektroniczną to tylko jedna strona medalu. Prawo przyznaje bowiem poszczególnym organom państwa wyraźne uprawnienia, na podstawie których mogą się domagać od firm wydania danych osobowych użytkowników usług internetowych. W relacji z tymi organami – wyposażonymi w kompetencje władcze – wszystkie firmy działające na terytorium Polski są równe. Również firmy zagraniczne muszą się stosować do postanowień sądu i prokuratora czy wniosków kierowanych przez policję na podstawie jej przepisów kompetencyjnych.

Zgodnie z kodeksem postępowania karnego (art. 218 i 236a) prokurator i sąd mają prawo zażądać danych, jeśli mają one znaczenie dla konkretnego postępowania. Z kolei – zgodnie z ustawą o Policji (art. 20 ust. 2a) – policja może pobierać i przetwarzać dane osobowe o osobach podejrzanych bez ich wiedzy i zgody. Analogiczne rozwiązanie przewidują tzw. ustawy kompetencyjne, regulujące działanie poszczególnych służb (m.in. ABW, CBA, kontroli skarbowej, Służby Celnej). Przepisy regulujące funkcjonowanie policji i innych służb inaczej traktują tylko niektóre rodzaje danych (np. dane bankowe lub ubezpieczeniowe), natomiast nie przewidują odrębnych reguł postępowania z danymi użytkowników usług internetowych. Stąd wniosek, że dostępu do tych danych (jako kategorii danych osobowych) służby mogą żądać na podstawie ogólnych przepisów dotyczących pobierania danych osobowych.

Polskie przepisy nie pozwalają na swobodny dostęp organów państwa do baz danych, w których firmy gromadzą dane użytkowników usług internetowych. Prokuratura, policja i inne służby mogą pozyskiwać tylko informacje na temat konkretnych osób. Za każdym razem muszą też przedstawiać odpowiedni wniosek lub postanowienie, ze wskazaniem podstawy prawnej.

Różne standardy ochrony elektronicznej korespondencji

W polskim prawie standard ochrony korespondencji nie jest jednolity. Zależy on od tego, jaki status ma przechowująca ją firma. Operatorów telekomunikacyjnych obejmuje tzw. tajemnica telekomunikacyjna. W praktyce oznacza to, że sam operator nie może się zapoznać z treścią przechowywanej korespondencji (np. wiadomości SMS) ani słuchać realizowanych rozmów; nie może też na to pozwolić innym podmiotom, chyba że tajemnicę telekomunikacyjną uchyli swoim postanowieniem sąd karny. Przepisy regulujące zasady świadczenia usług internetowych – w tym poczty elektronicznej – nie przewidują analogicznej ochrony. Tajemnica telekomunikacyjna nie chroni zatem korespondencji przechowywanej przez firmy świadczące usługi drogą elektroniczną.

Jakie ma to konsekwencje w praktyce? Na szczęście policja i inne służby, mimo braku ograniczenia tajemnicą telekomunikacyjną, nie mogą swobodnie sięgać po treść korespondencji – ich przepisy kompetencyjne narzucają w takich sytuacjach szczególny tryb, bez względu na to, kto przechowuje korespondencję. Zdarza się jednak, że sądy cywilne – traktując wszelkie informacje posiadane przez firmy jako „dokument" – żądają od firmy świadczącej usługi drogą elektroniczną ujawnienia korespondencji jej użytkowników. Powołują się przy tym na przepisy kodeksu postępowania cywilnego, umożliwiające sądom dostęp do dokumentów w celach dowodowych. Mimo, że firmy nie przechowują korespondencji swoich użytkowników i nie są w posiadaniu tego typu „dokumentów", odmowa wykonania postanowienia sądu cywilnego może się wiązać z koniecznością zapłacenia grzywny.

Obywatel nie zawsze wie, że był „sprawdzany"

Czy obywatele wiedzą o tym, kto i kiedy sięga po dotyczące ich dane? To zależy od tego, kto pyta. Sądy i prokuratorzy działający na podstawie kodeksu postępowania karnego muszą wydać postanowienie, które doręczane jest nie tylko firmie, ale i osobie, której ono dotyczy. Przepisy pozwalają sądom i prokuratorowi odroczyć doręczenie takiego postanowienia ze względu na dobro postępowania, ale obowiązek poinformowania obywatela, że był „sprawdzany", nie znika. Zupełnie inne reguły obowiązują w tzw. postępowaniu przedprocesowym: ani policja, ani służby nie muszą informować osoby, której dane wykorzystały w ramach czynności operacyjnych. Tę wiedzę mają jedynie firmy, do których służby zwracają się z wnioskami i zapytaniami.

Najczęściej poszukiwana informacja: adres IP

Z rozmów z praktykami wiemy, że z całego katalogu dostępnych danych policję i prokuratorów najczęściej interesuje numer IP. W przeciwieństwie do danych, które użytkownicy sami podają firmom świadczącym usługi internetowe, tę informację trudno zmienić czy zafałszować. Na podstawie numeru IP organy ścigania są w stanie dokonać kolejnych ustaleń – adresu czy nazwiska osoby podejrzanej. Ze względu na większą wiarygodność danych, które posiadają operatorzy telekomunikacyjni, kolejne („drążące") zapytania trafiają zwykle do nich. Wynika to m.in. z tego, że do zawarcia niektórych typów umów z operatorem telekomunikacyjnym potrzebne jest okazanie dokumentu.

III. NIEPEWNE PROCEDURY I PODSTAWY PRAWNE

Prawo nie określa precyzyjnie elementów, jakie powinien zawierać wniosek o dane, który organy państwa kierują do prywatnej firmy. To powoduje wątpliwości interpretacyjne, które firmy muszą rozstrzygać wg własnej oceny i na własne ryzyko.

Aby otrzymać informacje o danym użytkowniku usług internetowych, służby i inne organy państwa zawsze muszą się powołać na konkretną podstawę prawną. Jedną z najczęściej

powoływanych podstaw jest niezwykle lakoniczny art. 18 ust. 6 UŚUDE, który brzmi: „Usługodawca udziela informacji o danych, o których mowa w ust. 1–5, organom państwa na potrzeby prowadzonych przez nie postępowań". I właśnie wokół tego przepisu toczy się swoisty spór interpretacyjny.

Ten przepis nakazuje firmom przekazywać dane na żądanie „organów państwa", ale nie precyzuje, jakie podmioty mieszczą się w tej kategorii (w praktyce pojawiła się wątpliwość na temat tego, czy np. izba lekarska lub leśniczy to też organ państwa uprawniony do pobierania danych). Jednak zdaniem samych organów – w tym policji – art. 18 ust. 6 UŚUDE jest dość precyzyjny i nie wymaga zmiany. Według informacji przekazanych nam przez policję na podstawie tego właśnie przepisu (a nie ustawy o Policji) Komendant Główny Policji upoważnił grupę funkcjonariuszy do pobierania danych od firm świadczących usługi internetowe – szczególnie do weryfikowania numerów IP.

Inne zdanie na ten temat mają niektóre firmy – twierdzące, że do wydania danych potrzebują jeszcze wyraźnej podstawy prawnej po stronie pytającego organu. **Z rozmów z firmami wynika, że praktyka różni się w zależności od przedsiębiorstwa: niektóre odpowiadają na zapytania oparte wyłącznie o art. 18 ust. 6 UŚUDE, inne domagają się dodatkowo wskazania podstawy prawnej wynikającej z tzw. ustawy kompetencyjnej** (regulującej zasady działania policji lub innych służb).

To jednak nie koniec wątpliwości interpretacyjnych. Prawo nie określa precyzyjnie elementów, jakie powinien zawierać wniosek o dane, który organy państwa kierują do prywatnej firmy (np. wskazanie sygnatury sprawy, w jakiej toczy się postępowanie; podpis funkcjonariusza; pieczęć instytucji). Nie jest też zdefiniowane, jak powinna zachować się firma, jeśli otrzyma wniosek niekompletny (zwrócić do uzupełnienia, a może odmówić wydania danych?), ani jak należy działać w sytuacjach nagłych – np. zagrożenia życia – kiedy brakuje czasu na nadmierne formalności. W efekcie decyzja o tym, czy prosić organy państwa o dodatkowe wyjaśnienia, czy – ze względu na uzasadnione okoliczności – po prostu zrealizować wniosek, zależy wyłącznie od oceny danej firmy.

Obowiązujące przepisy nie precyzują też tego, jaką drogą organy państwa mogą kierować do firm świadczących usługi internetowe zapytania o dane ich użytkowników. Także w tej sferze praktyka – i firm, i organów państwa – jest różna. Do mniejszych firm organy państwa nadal wysyłają zapytania pocztą tradycyjną; w kontaktach z większymi firmami, które mogą sobie pozwolić na wdrożenie bezpiecznych kanałów komunikacji elektronicznej, wykorzystuje się również tę formę komunikacji. Policja potwierdza, że z niektórymi firmami nawiązała bezpieczne, szyfrowane połączenia właśnie w celu sprawniejszego przekazywania wniosków o dane. Nie ma jednak mowy o bezpośrednim dostępie do baz danych, czyli interfejsie pozwalającym na samodzielne pobieranie danych. W nagłych przypadkach – np. zagrożenia życia – mogą się natomiast zdarzać odpowiedzi na zapytania złożone przez telefon.

Spór o zwrot kosztów

Konieczność odpowiadania na zapytania organów państwa generuje koszty. Związane są one np. ze zbieraniem informacji, o które pyta dany organ, wydrukowaniem setek stron wyciągów i przesłaniem ich tradycyjną pocztą. Prawo nie precyzuje, czy firmom należy się zwrot poniesionych wydatków. Firmy stosują różne metody radzenia sobie z tym

problemem: część z nich pobiera opłaty za przekazywanie danych, a część realizuje je na własny koszt. Zdarza się też, że firmy egzekwują zwrot kosztów na drodze sądowej.

Nadużycia w związku z dostępem do danych

Znane są przypadki zgłaszania zawiadomień o popełnieniu przestępstwa naruszenia praw autorskich do prokuratury przez stowarzyszenia zajmujące się ochroną praw autorskich tylko po to, by z pomocą organów ścigania dotrzeć do danych osobowych domniemanych „piratów". Mając takie informacje, stowarzyszenia lub ich pełnomocnicy kierują żądanie zapłaty za naruszenie praw autorskich już bezpośrednio do użytkownika, co może być odebrane jako forma szantażu. Takie działanie wykorzystuje mechanizmy procesu karnego i organy państwa w sporze o charakterze cywilnym, a więc stanowi nadużycie prawa.

IV. MECHANIZMY KONTROLI

Polskie prawo nie przewiduje jednolitego mechanizmu kontroli działań organów państwa, kiedy w grę wchodzi wykorzystywanie danych użytkowników usług internetowych czy też innych kategorii danych osobowych. Kontrola niezależnego organu – np. sądu – jest zasadą tylko w przypadku niektórych typów postępowań; w przypadku innych – takiej kontroli brak.

W postępowaniu karnym prawo przewiduje kilka niezależnych mechanizmów kontroli. Przede wszystkim o przekazaniu danych decyduje sąd lub prokurator, ale zawsze pod kontrolą sądu – czyli niezależnego organu. Dodatkowo postanowienie o sięgnięciu po dane osobowe jest doręczane osobie, której dotyczy. Doręczenie może być odroczone do czasu zakończenia postępowania, jeśli jest to niezbędne ze względu na dobro sprawy. Jednak sam obowiązek poinformowania o tym, że dane były wykorzystywane w sprawie, nie znika. Co więcej – osobie, której postanowienie dotyczy, przysługuje zażalenie, które rozpoznaje sąd.

Analogicznych „bezpieczników" i mechanizmów kontroli nad sięganiem po dane o użytkownikach usług internetowych nie ma na etapie czynności operacyjnych prowadzonych np. w celu zapobiegania przestępczości lub rozpracowywania środowiska przestępczego. Takie czynności ze swojej natury są tajne. Informacja o tym, że służby, prowadząc czynności operacyjne, interesowały się danymi użytkownika usług internetowych, dotrze do niego tylko pod warunkiem, że zostanie wszczęte postępowanie karne. Jeśli zebrane dane nie dadzą ku temu wystarczających podstaw, również informacja o pobraniu danych przez policję i służby nie dotrze do użytkownika.

Na etapie czynności operacyjnych policja i inne służby mogą sięgać po dane o użytkownikach usług internetowych bez zewnętrznej kontroli ze strony prokuratora lub sądu. Co więcej, służby specjalne nie są kontrolowane nawet przez Generalnego Inspektora Ochrony Danych Osobowych. Zapytania o dane przechodzą jednak przez system kontroli wewnętrznej. Z informacji, jakie uzyskaliśmy od policji wynika, że żaden funkcjonariusz nie może samodzielnie spytać o dane – potrzebuje do tego zgody przełożonego, która może jednak przyjąć formę stałego upoważnienia.

Statystyki i sprawozdawczość

Firmy dostarczające usługi internetowe nie mają obowiązku informowania nikogo o tym, jak często organy państwa pytają je o dane użytkowników i ile z tych zapytań zostaje ostatecznie zrealizowanych. Obowiązek przekazywania tego rodzaju informacji mają natomiast operatorzy telekomunikacyjni, którzy w rozumieniu przepisów są innym rodzajem podmiotów. Dane pochodzące od nich gromadzi Urząd Komunikacji Elektronicznej i – jak się okazuje – jawność tych statystyk nie utrudnia pracy organom ścigania ani wymiarowi sprawiedliwości. Z drugiej strony nie ulega wątpliwości, że najlepszym źródłem takich statystyk są organy państwa i to przede wszystkim one powinny gromadzić i udostępniać opinii publicznej informacje na temat żądań, jakie kierują do prywatnych podmiotów.

V. PODSUMOWANIE: KLUCZOWE PROBLEMY

Analiza przepisów prawa oraz informacji zebranych od firm i innych podmiotów przetwarzających dane użytkowników Internetu dały nam podstawy do opisania systemowych problemów związanych z przekazywaniem danych na żądanie organów państwa. Szczegółowo omówiliśmy je powyżej; natomiast w tym miejscu chcemy je podkreślić i podsumować.

Problem pierwszy: skala zapytań jest niemożliwa do oszacowania

Brakuje danych obrazujących skalę sięgania po dane użytkowników usług internetowych. Ponieważ firmy świadczące usługi drogą elektroniczną nie mają obowiązku prowadzenia ewidencji zapytań, jakie kierują do nich organy państwa, i publikowania sprawozdań na ten temat, robią to tylko niektóre – z własnej inicjatywy oraz według własnych zasad. Co gorsze, takiego obowiązku nie mają także organy państwa, w związku z czym tylko niektóre dysponują odpowiednimi danymi. W efekcie nie wiemy, ile jest zapytań o dane użytkowników usług internetowych, czego konkretnie dotyczą, kto je kieruje i ile z nich zostaje zrealizowanych. Tym trudniej ocenić, czy np. możliwość korzystania z danych użytkowników usług internetowych ma rzeczywisty wpływ na walkę z przestępczością albo pracę operacyjną służb.

Problem drugi: firmy muszą same rozstrzygać poważne wątpliwości interpretacyjne

Prawo nie precyzuje tego, jakie kryteria formalne powinien spełniać wniosek o dane i w jakim trybie powinien zostać przekazany firmie (np. czy dopuszczalna jest forma elektroniczna). Na tę niepewność nakładają się problemy interpretacyjne, związane z kluczową podstawą sięgania po dane przetwarzane przez firmy świadczące usługi drogą elektroniczną: art. 18 ust. 6 UŚUDE. W praktyce cały ciężar oceny tego, czy wniosek o dane został odpowiednio przygotowany i czy przywołana przez pytającego podstawa prawna jest wystarczająca, spoczywa na prywatnym przedsiębiorcy. W efekcie trudno mówić o spójnym standardzie ochrony prywatności użytkowników – każda firma dokonuje takiej oceny według własnego uznania. Brak precyzji przepisów utrudnia też

wypracowanie jednolitej metody gromadzenia danych do celów statystycznych – np. nie wiadomo, jak liczyć wniosek, który zawiera pytania o wielu użytkowników. Tego typu wątpliwości można by mnożyć.

Problem trzeci: brak kontroli nad pobieraniem danych przez służby

Brakuje zewnętrznego nadzoru i niezależnych mechanizmów weryfikacji tego, czy służby (np. ABW czy CBA) korzystają z danych użytkowników usług internetowych zgodnie z prawem. Ten problem wielokrotnie podkreślała Rzecznik Praw Obywatelskich, a ostatnio w swoim raporcie zauważyła też Najwyższa Izba Kontroli – żaden organ w Polsce nie kontroluje, czy służby rzeczywiście działają w granicach i na podstawie przepisów prawa. To dotyczy także (choć nie tylko) wykorzystywania danych użytkowników usług internetowych. Tam, gdzie w grę wchodzą dane osobowe, problem braku nadzoru nad działaniem służb pogłębia to, że sami obywatele nie mają możliwości zweryfikowania, czy służby pytały firmy o ich dane. Dla porównania: w postępowaniu oskarżony ma prawo do informacji o tym, że jego dane były pobierane na potrzeby sprawy i może nawet złożyć w związku z tym zażalenie.

Problem czwarty: różne procedury udostępniania danych obowiązujące w firmach

Polskie prawo przewiduje, z jednej strony, konkretne ograniczenia dla firm, jeśli chodzi o możliwość gromadzenia danych o użytkownikach usług internetowych, z drugiej – na te same firmy nakłada obowiązek udostępniania danych osobowych na żądanie uprawnionych organów. Nie wszystkie z tych reguł stosują się do firm zagranicznych: mimo że w takim samym stopniu muszą one respektować prawo karne i współpracować z sądami czy policją, nie podlegają obowiązkom wynikającym z ustawy o świadczeniu usług drogą elektroniczną. W praktyce mają wobec państwa podobne obowiązki, ale działają w oparciu o inne procedury. Ta rozbieżność reguł – bez względu na to, które w praktyce okazują się lepsze ze względu na ochronę danych użytkowników – powoduje, że nie możemy rzetelnie porównać praktyk wszystkich firm działających na polskim rynku.

Problem piąty: brak jasnych regulacji dotyczących zwrotu kosztów obsługi zapytań

Brak jasnych regulacji dotyczących zwrotu kosztów obsługi zapytań od organów państwa powoduje, że firmy muszą się mierzyć z dodatkowym problemem: albo zaakceptować to dodatkowe obciążenie, albo domagać się zwrotu kosztów na drodze sądowej. W przypadku pobierania danych telekomunikacyjnych (od operatorów telekomunikacyjnych) prawo rozstrzyga problem kosztów na niekorzyść operatorów: przepisy wyraźnie mówią, że dane są wydawane nieodpłatnie. Analogicznego przepisu nie ma w przypadku firm świadczących usługi drogą elektroniczną. W efekcie między firmami a organami państwa nierzadko dochodzi do sporów interpretacyjnych. Co do zasady sądy przyznają rację firmom i potwierdzają ich prawo do zwrotu poniesionych kosztów, jednak niejasność przepisów generuje dodatkowe koszty (procesów sądowych) i pochłania czas.

Problem szósty: niejednolity standard ochrony poczty elektronicznej i danych telekomunikacyjnych

W polskim prawie standard ochrony korespondencji zależy od tego, jaki status ma przechowująca ją firma. Korespondencję (np. wiadomości SMS) przesyłaną przez operatorów telekomunikacyjnych chroni tajemnica telekomunikacyjna. Korespondencja elektroniczna

(np. e-maile) przechowywana przez firmy świadczące usługi drogą elektroniczną nie podlega analogicznej ochronie. Dlatego w praktyce zdarza się, że sądy cywilne – traktując wszelkie informacje posiadane przez firmy jako „dokument" – żądają od firmy świadczącej usługi drogą elektroniczną ujawnienia korespondencji jej klientów. Podobnego żądania nie mogłyby skierować do operatora telekomunikacyjnego.

Problem siódmy: instrumentalne wykorzystywanie postępowania karnego do „wyciągania" danych osobowych

Doświadczenia firm potwierdzają, że zdarza się instrumentalne wykorzystywanie postępowania karnego i kompetencji prokuratury przez podmioty zajmujące się ochroną praw autorskich. Polega to na tym, że wszczęcie postępowania karnego (poprzez złożenie zawiadomienia o popełnieniu przestępstwa) ma jeden cel: ustalić dane osobowe użytkownika, który rzekomo naruszył prawa autorskie. Takie dane (znajdujące się w aktach postępowania) są następnie wykorzystywane do „dochodzenia praw" na własną rękę – najczęściej użytkownik dostaje groźny list z żądaniem zapłaty. To nieetyczna praktyka, głęboko ingerująca w prawa obywateli-użytkowników.

***

Dane o użytkownikach usług internetowych to tylko jedne z wielu rodzajów danych osobowych, które przetwarzają prywatne firmy i do których mogą uzyskiwać dostęp podmioty publiczne. Przepisy regulujące funkcjonowanie policji i innych służb inaczej traktują tylko niektóre rodzaje danych (np. dane bankowe lub ubezpieczeniowe), natomiast wszystkie pozostałe są pobierane na tych samych zasadach. Dlatego niektóre z zasygnalizowanych powyżej problemów mają charakter systemowy: nie dotyczą jedynie sięgania przez policję i inne służby po dane o użytkownikach usług internetowych. Dotyczy to zwłaszcza braku możliwości oszacowania, jaka jest skala zapytań o dane oraz braku kontroli nad pobieraniem danych przez służby.

Kluczowi uczestnicy projektu – podziękowania

Dziękujemy firmom: **Interia.pl**, **Onet** i **Agora** za poświęcenie czasu i namysł nad odpowiedziami oraz pełną gotowość do rozmowy o tym, jak przepisy nakazujące udostępnianie danych użytkowników funkcjonują w praktyce. Ich doświadczenie było dla nas szczególnie istotne, ponieważ te firmy działają na gruncie rodzimego prawa. Ważne było również to, że do projektu dołączyła firma **Google**, która już od kilku lat z własnej inicjatywy publikuje raporty przejrzystości, a jej doświadczenia są reprezentatywne dla firm zagranicznych. Doceniamy też chęć włączenia się do projektu ze strony firmy **Facebook**, która swój pierwszy raport przejrzystości opublikowała w tym roku – mamy nadzieję, że jest to początek stałej dobrej praktyki. Niestety, ze względu na niewystarczający zakres udostępnionych danych nie mogliśmy włączyć jej odpowiedzi do niniejszego opracowania.

Praca nad koncepcją była przedsięwzięciem ponadsektorowym. Pomogło nam **Ministerstwo Administracji i Cyfryzacji** – pod jego auspicjami odbyło się pierwsze spotkanie robocze, a Minister Michał Boni publicznie podkreślał konieczność zbadania skali zainteresowania organów państwa danymi użytkowników usług internetowych. Pomoc pro bono zaoferowała kancelaria **Bird & Bird**, która pośredniczyła w przekazywaniu danych między firmami a Fundacją Panoptykon. Kancelaria dokonała pseudonimizacji wypełnionych ankiet, dzięki czemu nie możemy przypisać udzielonych odpowiedzi konkretnym firmom.

Fundacja Panoptykon | panoptykon.org

FUNDACJA
PANOPTYKON

Autorki
Katarzyna Szymielewicz, Małgorzata Szumańska

Współpraca
Wojciech Klicki, Anna Mazgal, Anna Walkowiak

Korekta
Urszula Dobrzańska

Projekt graficzny
Filip Zagórski

Warszawa 2013

Publikacja udostępniona na licencji Creative Commons
Uznanie autorstwa – Na tych samych warunkach 3.0 Polska

Publikacja zawiera wnioski z projektu, który został zrealizowany
przez Fundację Panoptykon przy wsparciu finansowym firmy Google