

Śledzą nas.

Dlaczego na hasło „ACTA” tysiące ludzi wyszło na mróz protestować, a po ujawnieniu afery z amerykańską inwigilacją na gigantyczną skalę siedzą w domach? Nie wiedzą, co tak naprawdę jest groźne w internecie

Sylwia Czubkowska

Latwo jest straszyć, że wiedzą o nas wszystko, że Wielki Brat patrzy i że inwigilacja jest już permanentna. Trudniej jest przyznać się, że znaczna część z tej inwigilacji jest właściwie przydatna i potrzebna. A najtrudniej jest znaleźć granicę, by odróżnić ochronę od zagrożenia sterowania ludźmi.

Jeszcze w marcu 29-letni Michał pracował w call center. Zajmował się sprzedażą telewizyjnej platformy n. Gdy po połączeniu n z Cyfrą+ abonenci zaczęli się buntować i masowo krytykować nową ofertę, rozpisali się też o tym media. Michał jeden takich krytycznych tekstów polubił, co zaznaczył na Facebooku, na swojej osobistej tablicy. Dwa dni później musiał odejść z pracy, bo uznano, że „działa na szkodę firmy”.

Kilka dni temu w jednym z wydawnictw podczas zebrania pewna pracownica dostała wydruk swojej dyskusji pod tekstem zalinkowanym na Facebooku. Razem ze znajomą ironicznie odnosiły się w niej do umoralniających opinii, jakie pojawiły się tekstach publikowanych przez to wydawnictwo. Usłyszała kaganie, że to niedopuszczalne, by nie podzielać ideałów swojego pracodawcy. A warto dodać, że konto na Facebooku miała zabezpieczone najwyższymi ustawieniami prywatności.

Takie historie jeszcze dwa lata temu budziły sensację, głośnym echem odbijały się pierwsze przypadki zwolnionych z powodu Naszej Klasy, Facebooka czy Twittera. Dziś już coraz więcej osób ma świadomość, że zachowanie na ich profilach wcale nie jest sferą tak bardzo prywatną. Że nauczyciel, pracodawca obecny lub potencjalny, nawet policja albo bank może zajrzeć na konto i wyciągnąć z niego wnioski. Ale dopiero odłam wybuchła afera z PRISM, czyli ściśle tajnym do niedawna amerykańskim programem szpiegowskim, który daje amerykańskiemu wywiadowi dostęp do danych zgromadzonych na serwerach największych firm internetowych, wiemy też, że

równie łatwy dostęp do naszych danych mają amerykańskie służby specjalne.

Zdaje się, że zasięg inwigilacji internetu nie ma już granic. Gigabajty korespondencji, terabajty zdjęć, znajomi znajomych spleceni w społecznościową sieć, z której można wyciągnąć naprawdę szczegółowe informacje o każdym z nas. A gdy się już do nich zyska dostęp, można szybko, łatwo i precyzyjnie budować profile: klientów, idealnych odbiorców reklamy, najlepszych pracowników. Ale także profile terrorystów czy przestępców. Choćby tylko potencjalnych. Choćby tylko w oparciu o przewidywania z cyfrowych śladów. Brzmi strasznie? A nie jest takie nieprawdopodobne. Warto więc zadać sobie pytanie – czy przejmujemy się tym, co się dzieje z naszymi danymi, i czy mamy dobre rozeznanie w tym, o jakie dane powinniśmy się martwić.

Polska bez PRISM. Chyba

Na hasło ACTA tysiące ludzi wyszło na mróz i w tradycyjny sposób krzyczało o cenzurze i potajemnych układach władzy. Drugie tyle bawiło się w hakerów i uczestniczyło w atakach czy raczej blokadach witryn rządowych. Jeszcze więcej zakładało fanpage'e protestacyjne, pisało na forach, Facebooku czy Twitterze, co myśli o rządzie, który chce ograniczyć prawa do ściągania filmów, muzyki i książek, choćby z nielegalnych źródeł.

A na hasło PRISM owszem, też przeszła fala oburzenia, powstało nawet kilka zabawnych memów, firmy szybko wyparły się udziału w grze danymi ich użytkowników, ale to tyle. Większego poruszenia, a już na pewno takiego, jak półtora roku temu, nie widać.

Na jednym ze slajdów prezentujących działanie PRISM, które wyciekły do mediów, jest grafika pokazująca, jak kręgosłup światowego internetu biegnie przez USA. Płynnie tędy większość światowego transferu danych. Służby Stanów Zjednoczonych nie muszą się więc specjalnie głowić, jak się dostać do obywateli innych państw, bo ich działania i tak trafiają w strefę oddziaływania

amerykańskiego prawa. A ono chroni prywatność Amerykanów – i tylko ich. Potwierdza to Wojciech Rafał Wiewiórowski, generalny inspektor ochrony danych osobowych: – PRISM tak naprawdę nie jest wielkim zaskoczeniem. Oczywiście nie wiedzieliśmy, że tak właśnie nazywa się system do cyfrowej inwigilacji, ale wszyscy, którzy zdawali sobie sprawę, jak wygląda ochrona bezpieczeństwa w Stanach Zjednoczonych, mieli też świadomość, że musi funkcjonować tego typu rozwiązanie – mówi. – Dodatkowo ten system nie działa poza prawem. Wręcz przeciwnie, jest osadzony w przepisach amerykańskich i, co ważne, służy głównie do inwigilacji obywateli krajowców. Bo do podsłuchiwanie czy czytania e-maili obywatela USA potrzebna jest zgoda sądu, a do podobnej kontroli cudzoziemca już nie. To jest ta wyraźna różnica między Europą a Stanami Zjednoczonymi. O ile w Europie chronimy prawa człowieka, o tyle w USA chroni się prawa Amerykanów – dodaje Wiewiórowski.

– Protesty przeciwko PRISM? Nie wydaje mi się – zastanawia się Rafał Trzaskowski, poseł do Parlamentu Europejskiego. – Owszem, to jest oburzające działanie, ale działanie rządu amerykańskiego. Europejczycy i Polacy mają świadomość, że ich rządy działają inaczej. Przy ACTA protesty wybuchły ze względu na niejawną proces podpisywania tej umowy. Ludzi również mocno oburzył pomysł wzmocnienia ochrony praw autorskich, jak i to, że zrobiono to ponad ich głowami. Tym razem jednak w Europie prace nad nowym rozporządzeniem w sprawie danych prowadzone są w sposób przejrzysty. Szczególnie w Polsce są bardzo szeroko konsultowane. Każda opinia, każdy głos krytyczny są jawne. I to uspokaja nastroje – uważa poseł.

Podobnie uważa Wiewiórowski, który podkreśla, że prawdziwe oburzenie i poruszenie powstało dopiero wtedy, gdyby okazało się, że to polski rząd ma swój własny

PRISM. – Kilka miesięcy temu jednak posłowie z komisji innowacyjności i nowych Technologii oficjalnie pytali Ministerstwo Sprawiedliwości, MSW i Komendę Główną Policji, czy są u nas prowadzone podobne działania. Otrzymałi zapewnienia, że nie. Gdyby jednak okazało się, że te działania są prowadzo-



ACTA została odczytana jako zamach na prawa ekonomiczne. A cóż to takiego są dane osobowe?



No i co z tego

ne, reakcja mogłaby być dużo ostrzejsza – mówi Wiewiórowski i podkreśla, że protesty wokół ACTA dowodzą, iż ludzie potrafią się zorganizować, jeżeli mają poczucie, że władza podejmuje ważne decyzje ponad ich głowami.

Inaczej jednak widzi to Katarzyna Szymielewicz, szefowa Fundacji Panoptykon, która chyba najgłośniej w Polsce mówi o zagrożeniach związanych z ochroną naszej prywatności. – To nie jest tak, że nie ma zainteresowania PRISM, że ludzie się nie oburzyli, bo oburzyli się. W Stanach wybuchła naprawdę poważ-

na debata o granicach inwigilacji w cyfrowym świecie. Jej uczestnicy nie muszą masowo wychodzić na ulice, by pokazać swoje niezadowolenie. Podobnie w Europie: wiele grup obywatelskich domaga się od instytucji europejskich zwiększenia gwarancji ochrony prywatności w relacjach z USA – tłumaczy Szymielewicz.

Rzeczywiście w Stanach zamiast protestów zaczęła się dyskusja o jawności zbierania i przetwarzania danych. W pierwszej kolejności głos w sprawie inwigilacji zabrały też organizacje, które tradycyjnie strzegą prywatności. Electronic Frontier Foundation, Mozilla, Reddit oraz kilkadziesiąt innych organi-

Pokolenie digital native deklaruje, że ochrona prywatności jest ważna, jednak bez oporu publikuje informacje o sobie w internecie

zacji uruchomiły inicjatywę StopWatching.us, w której ramach zbierane są podpisy pod listem do Kongresu wzywającym do poprawienia prawa oraz publikowania dokładnych informacji o skali inwigilacji w USA. Ale także giganci, którzy według informacji, jakie wyciekły o PRISM, współpracują ze służbami, czyli Google, Microsoft czy Facebook, wiedząc, że skandal nie służy budowaniu zaufania do ich usług, szybko zaczęli deklorować, że będą przynajmniej publikować dane o tym, ile tajnych nakazów zmusza ich do ujawniania informacji.

– W efekcie ludzie dosyć racjonalnie uznali, że nie ma co karać Google'a czy Facebooka za to, że na zgodne z prawem wnioski udostępniali rządowi informacje. Przecież są zarejestrowani w USA, więc obo-

wiązuje ich tamtejsze prawo – mówi Szymielewicz.

Czy Big Data są takie złe

Co ciekawe, nawet ci oburzeni podkreślają, że nie chodzi o całkowite zaprzestanie działań w zakresie nadzoru, nawet tego elektronicznego. Chodzi jedynie o to, aby obywatele mieli świadomość, co dokładnie robią służby dla ich bezpieczeństwa.

– Przecież ogromna część z tych działań jest naprawdę prowadzona dla dobra ogółu – przekonuje poseł Trzaskowski. – Albo przynajmniej dla usprawnienia działania pewnych instytucji. Mnie na przykład nie przeszkadza, że Amazon, wiedząc, jakie książki już w nim kupilem, zna mój gust i proponuje mi kolejne dopasowane do tego mojego cyfrowego wizerunku czytelnika. Clou problemu leży w tym, żeby ktoś, komu nie pasuje takie wykorzystywanie jego danych do profilowania, mógł to kontrolować i zabronić przetwarzania informacji o sobie – tłumaczy europoseł.

Nasze dane mogą być też niezwykle przydatne choćby przy zarządzaniu państwem. – Przydają się w sytuacjach kryzysowych, takich jak klęski żywiołowe. Są niezbędne do skutecznej walki z terroryzmem, zorganizowaną przestępczością czy cyberprzestępczością. – Ale nawet takie cele muszą być jasno sprecyzowane i musimy dać obywatelom pełną kontrolę nad ich danymi, ale tak by nie piętrzyć przy tym niepotrzebnych przeszkód dla przedsiębiorców – dodaje Trzaskowski i tłumaczy, że nazbyt skrajne prawo zamiast chronić ludzi, może tylko doprowadzić do problemów. Podaje przykład prawa do bycia zapomnianym. Jego najostrzejszą interpretacją, czyli zobowiązanie internetowych przedsiębiorców do wykasowywania danych użytkowników na ich życzenie, mogłoby doprowadzić nawet do upadku serwisu Allegro. Ta platforma aukcyjna działa w oparciu o pewność co do tego, że opinie o sprzedawcach i kupujących są przejrzyste. – I gdyby nagle wszyscy byli użytkownicy tego serwisu zażądali usunięcia wszystkich swoich danych, także opinii o innych użytkownikach, zachwiałoby to tym modelem biznesowym – tłumaczy Trzaskowski.

I dlatego nawet przeciwnicy rozbudowującej się e-inwigilacji przyznają, że zarówno publiczne, jak i komercyjne zastosowania Big Data niosą z sobą sporo korzyści. Oczywiście najbardziej widać to na polu czysto komercyjnym głównie w reklamie. Ale przetwarzanie Big Data to nie tylko biznes. Rick Smolan, autor książki „The Human Face of Big Data”, podaje przykład firm farmaceutycznych, które części leków nie wprowadzają na rynek. Dlaczego? Ponieważ małej części populacji zamiast pomóc, mogą zaszkodzić. W efekcie do chorych często nie trafia potrzebna pomoc. Można temu zaradzić, analizując genotyp konkretnych pacjentów i przewidując tym samym, jak zachowa się lek. Dzięki dostępowi do tetrabajtów naszych danych analiza

genotypu, która na początku zajmowała dekadę, dziś może zostać przeprowadzona w zaledwie tygodniu.

A może jednak tak naprawdę po prostu tematem Big Data zainteresowana jest tylko wąska grupa ludzi? Może reszcie jest po prostu wygodnie z tymi wszystkimi korzyściami, które niesie z sobą gromadzenie danych?

Palenie albo prywatność

ACTA budziła emocje, bo została odczytana jako zamach na prawa ekonomiczne, jako odebranie możliwości taniego czy też bezpłatnego dostępu do filmów, muzyki, książek. A dane osobowe, coż to takiego ważnego?

Taki właśnie obraz przebiega z badania przeprowadzonego przez Homo Homini dla DGP. Respondenci mieli w nim ocenić, jak bardzo wrażliwe, a tym samym także niezbędne do ochrony są różne informacje na ich temat. Data urodzenia, dane o zdrowiu, numer PESEL, hasła do serwisów społecznościowych. W wynikach badania wyraźnie widać różnice w pojęciu do ochrony prywatności w zależności od wieku – inny jest stosunek osób młodych, do 25. roku życia, a inny tych, którzy mają 45 lat i więcej. Okazuje się, że choć ci drudzy są w mniejszym stopniu aktywnymi internautami, rzadziej mają profile w serwisach społecznościowych, to oni bardziej obawiają się o bezpieczeństwo swoich danych. Często zresztą na wyrost, z lekką paranoicą, bo za dane szczególnie wrażliwe uważają już nawet swój adres e-mailowy czy imię i nazwisko. – Polacy powyżej 45. roku życia po prostu pamiętają, że demokracja nie zawsze istniała. Są świadomi, że zebrane – nawet w złośliwym celu – dane można wykorzystać nie tylko dla dobra społeczeństwa. Pokolenie digital native tego doświadczenia nie ma. I choć jego przedstawiciele pytani w ankietach zapewniali, że ochrona danych jest dla nich ważna, to praktycznie nie mają oporów przed udostępnianiem dużej ilości informacji o sobie – tłumaczy Wiewiórowski.

A więc ci, którzy potencjalnie mogliby się najbardziej oburzać i protestować, wcale nie czują się zagrożeni. – Świetnie wytłumaczył to Cory Doctorow w „Guardianie”. Stosunek ludzi do ochrony swojej prywatności porównał do palenia papierosów. Lekarze ciągle ostrzegają, że palenie może spowodować raka, a i tak ogromna rzesza ludzi nadal pali, bo lubi, doraźną przyjemność przedkłada nad mgliste zagrożenie, które może ich dotknąć w przyszłości – mówi Katarzyna Szymielewicz, która zapewnia, że sama też widzi korzyści, jakie niesie z sobą racjonalne zarządzanie informacją. – Ale to nie oznacza, że jako społeczeństwo mamy ślepo ufać każdemu, kto w imię efektywności, wygody czy bezpieczeństwa sięga po nasze dane – tłumaczy i dodaje, że jeżeli ktoś woli mieć przyjemność z funkcjonowania w serwisach społecznościowych, udostępniania w nich swoich zdjęć, korzystania ze sprofilowanych reklam internetowych, to nie ma sprawy. Chodzi tylko o to, by jak z tymi papierosami, był świadomy, do czego to może doprowadzić.



ARTUR BARANOWSKI/STAST NEWS