Ustawa zwana inwigilacyjną – skandal czy burza w szklance wody?

9 stycznia 2016

Policja i służby uzyskają uprawnienie do inwigilacji internautów? PiS i jego sojusznicy chcą, żeby można było śledzić wszystko, co robimy w Internecie? A może nic się nie zmieni? Wątpliwości wokół „danych internetowych", o których mowa w projekcie nowelizacji ustawy o policji procedowanym obecnie w Sejmie, narastają. Naszym zdaniem projekt jest fatalny, ale jego krytyka czasami idzie za daleko.

O CZYM MÓWIMY?

Niewątpliwie jednym ze źródeł nieporozumienia jest niejasność pojęcia „danych internetowych". Są to informacje, które pośrednicy internetowi (np. Interia czy Onet) przechowują na temat swoich użytkowników na podstawie ustawy o świadczeniu usług drogą elektroniczną. Część z nich to dane niezbędne, by prawidłowo dostarczyć i rozliczyć usługę, np. imię i nazwisko i adres e-mail oraz tzw. dane eksploatacyjne, które są konieczne, by „dopasować" usługę do sprzętu i oprogramowania użytkownika, czyli numer IP, informacje o systemie operacyjnym czy przeglądarce internetowej. Niezbędne do świadczenia usługi może być także przechowywanie treści korespondencji, jeśli tego właśnie oczekuje klient – np. w ramach usługi poczty elektronicznej obejmującej przechowywanie danych na wirtualnym serwerze.

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 usługi, powód do przetwarzania tych informacji. Są wreszcie dodatkowe dane, które służą np.

dopasowaniu wyświetlanych treści do cech użytkownika, poprawiające jakość usługi. Do tej kategorii zaliczają się wszystkie dane, które sami podajemy portalom – chociażby randkowym o naszych zainteresowaniach.

SKĄD OBAWY?

W gorącej dyskusji na temat „danych internetowych" należy odróżnić fakty od mitów. Mitem jest twierdzenie, że projekt przyznaje służbom zupełnie nowe uprawnienia, a policja i służby nie miały dotychczas dostępu do danych internetowych. Mogły go wykorzystywać i to robiły – podstawą prawną był przepis mówiący o możliwości uzyskania dostępu do danych na „potrzeby prowadzonych postępowań". Działo się to bez jakiejkolwiek kontroli – kiedy firma otrzymywała pismo wskazujące, że dane są potrzebne do jakiegoś postępowania, nie mogła zadawać zbędnych pytań.

A jednak projekt ustawy ułatwia policji i innym służbom dostęp danych internetowych. Dlaczego? Po pierwsze – mimo że nie znika przepis dotyczący „prowadzonych postępowań", policja będzie mogła sięgać po dane „w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych". Kryteria te są niezwykle szerokie: analizowanie ruchu na serwisach umożliwiających wymianę plików może być bowiem uznane za „zapobieganie przestępstwom", a weryfikacja tożsamości użytkowników portali hazardowych – za przejaw troski o ich zdrowie.

Druga zmiana ma jednak – przynajmniej potencjalnie – większe znaczenie. Otóż zamiast dotychczasowej drogi pisemnej (np. pismo wysłane pocztą) , udostępnianie danych internetowych będzie mogło się odbywać drogą elektroniczną, bez udziału pracowników firmy. Wystarczy, że taka możliwość zostanie przewidziana w porozumieniu zawartym z Komendantem Głównym Policji. To kopia rozwiązania stosowanego od lat wobec firm

telekomunikacyjnych, które billingi i inne dane telekomunikacyjne udostępniają za pomocą takich „bezpiecznych łączy”. W tym kontekście musi się pojawić pytanie, czy wygoda i szybsze tempo udostępniania danych nie doprowadzi to do radykalnego wzrostu skali zapytań? Jeśli tak, mamy konkretny powód do niepokoju. Dodatkowo, projekt przewiduje, że koszt udostępniania danych będzie spoczywał na firmach, co dotychczas nie było jednoznaczne. To kolejne ułatwienie w dostępie do danych internetowych, które może się przełożyć na inflację zapytań.

W 2013 r. zbadaliśmy skalę zapytań o dane internautów. Szczegółowe informacje otrzymaliśmy wówczas od Agencji Bezpieczeństwa Wewnętrznego. Okazało się, że w 2012 r. ABW zwróciła się z 692 pytaniami do 71 firm, co daje w zaokrągleniu 10 pytań do jednej firmy w skali roku. Dla porównania w tym samym roku ABW zadała operatorom telekomunikacyjnym 115 652 pytań, z których większość trafiła do jednego z 4 największych operatorów w Polsce. A więc bezpieczne łącza z największymi firmami telekomunikacyjnymi były realnie obciążone kilkudziesięcioma tysiącami pobrań danych. Dlaczego projekt przewiduje analogiczne ułatwienia w dostępie do danych internetowych, skoro skala zjawisk jest nieporównywalna? Jakie względy uzasadniają tworzenie takiej technologicznej infrastruktury na koszt firm internetowych – a w efekcie, na koszt ich klientów? A może sama łatwość sięgania po dane sprawi, że słupki z liczbą zapytań poszybują w górę?

Dodatkowym powodem do niepokoju jest nieprecyzyjność pojęcia „danych internetowych”, które według niektórych obejmuje także przekazywane przez firmy maile. Udostępnianie treści komunikacji w taki sam sposób, jak pozostałych danych internetowych, stanowiłoby wyłom w zasadzie, że na czytanie korespondencji policja i służby muszą uzyskiwać zgodę sądu. Najmniejsze wątpliwości w tej sprawie powinny być wyeliminowane w trakcie prac nad projektem.

Na marginesie dyskusji na temat danych internetowych pojawiają

się także obawy dotyczące możliwości korzystania przez służby z tzw. trojanów służących zdalnemu przeszukiwaniu komputerów. Dzisiaj możliwe jest to za zgodą sądu, a właściciel sprzętu jest o tym informowany. Projekt pogarsza ten standard – co krytykuje m.in. Helsińska Fundacja Praw Człowieka – zrównując przeszukanie komputera z kontrolą operacyjną, np. podsłuchem. Oznacza to, że do przeprowadzenia tej czynności nadal potrzebna będzie zgoda sądu, ale właściciel komputera może się nigdy o tym nie dowiedzieć.

KONTROLA, KONTROLA, KONTROLA

Oceniając proponowane zmiany, należy wyraźnie rozróżnić dwie kwestie: możliwość szybkiego udostępnienia danych i problem braku realnej kontroli nad jej praktycznym wykorzystaniem. Sama możliwość szybkiego udostępnienia danych – przynajmniej w teorii – nie jest niczym złym: w niektórych sytuacjach (np. reagowania na próby samobójcze) jest wręcz konieczna. Problemem będzie dopiero jej nadużywania przez policję i służby w sprawach, które nie uzasadniają takiej ingerencji w prywatność użytkowników Internetu. Sęk w tym, że w sytuacji braku niezależnej kontroli nad pobieraniem danych przez służby takie ryzyko nadużyć staje się bardzo realne. Teoretycznie projekt wprowadza następczą kontrolę sądu, jednak ze względu na ogromną liczbę spraw będzie ona fasadowa lub bardzo wyrywkowa – podobnie jak przy sięganiu po dane telekomunikacyjne, np. billingi.

Nie ma przeszkód, żeby ujednolicić zasady dostępu do dwóch podobnych rodzajów danych: telekomunikacyjnych i internetowych. Takie rozwiązanie wydaje się logiczne i sami niejednokrotnie je rekomendowaliśmy. Nie powinno być to jednak równanie w dół. Zasady dostępu powinny przewidywać silną i skuteczną kontrolę niezależnego organu nad tym, kto zagląda w nasze billingi i dane internetowe. Najlepiej, jeśli tym organem byłby sąd, sprawdzający zasadność zapytań zanim zostaną one zrealizowane. Wtedy „bezpieczne łącza” nie będą nam tak straszne.

Autorstwo: Wojciech Klicki, Katarzyna Szymielewicz
Źródło: Panoptykon.org