

# Bezpowrotnie utracona prywatność

Szpiegują nas już nie tylko komputer i telefon, ale także samochód, droga, a wkrótce również soczewka kontaktowa lub ubranie. Które urządzenia ułatwiają nam życie, a które są dla nas groźne? Czy w cyberświecie ochrona danych ma sens?



DOROTA BOGUCKA

**N**ajwyraźniej tak, bo rośnie liczba państw, które wprowadzają do swojego prawa stosowne przepisy – dziś jest ich już 90, a w ponad 70 z nich działają organy ochrony danych. W tym roku po raz 33. w dniu 28 stycznia obchodziliśmy międzynarodowy Dzień Ochrony Danych Osobowych. Podczas zorganizowanej z tej okazji przez Generalnego Inspektora Ochrony Danych Osobowych konferencji rozmawiano o prawnych, technologicznych i edukacyjnych aspektach „Prywatności w cyfrowym świecie”.

## Zdażyć przed Europą

Państwa członkowskie Unii Europejskiej nie mają wątpliwości, że potrzebne jest nowoczesne prawo, które zaostrzy przepisy dotyczące m.in.

przekazywania danych obywateli państwom trzecim, wprowadzi sankcje i umożliwi równe traktowanie firm z Unii Europejskiej i spoza niej. „Doszliśmy do porozumienia i liczbę poprawek zmniejsziliśmy z kilku tysięcy do 90 – relacjonował prace w UE dr Rafał Trzaskowski, minister administracji i cyfryzacji – udało nam się znaleźć kompromis między potrzebami obywateli a interesem biznesu. Żeby wymagania ochrony danych nie szły w poprzek uznanym modelom biznesowym”.

Przykładem takiego kompromisu jest zgoda na profilowanie, które może wprawdzie prowadzić do dyskryminacji niektórych usługobiorców komercyjnych, ale jest niezbędne w takich dziedzinach, jak prace naukowe czy przewidywanie klęsk żywiołowych. Przyjęto zatem, że jest dopuszczalne pod warunkiem, że klient każdorazowo wyrazi zgodę, wiedząc, czym taka zgoda skutkuje.

Ze względu na kalendarz wyborów do Parlamentu Europejskiego Rada powinna skończyć prace do końca roku. Jeśli prace się przeciągną, co prawdopodobnie oznaczałoby powrót do kwestii już omówionych i przesunięcie wejścia nowego prawa w życie nawet do roku 2020, to zasadnym posunięciem będzie wcześniejsza nowelizacja polskiej ustawy o ochronie danych. Zdaniem ministra Trzaskowskiego nie ma również przeszkód, żeby już przystąpić do zmian w aktach wykonawczych, np. rozporządzeniu z 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

## Big data = big problem

„Kiedy na forum europejskim rozpoczęliśmy dyskusję o big data, to obawiano się, że nie zdolamy zapanować nad 7–8 gigabajtami danych. Dziś tyle danych mieści się na pendrive, który trzymam w ręku” – tak o skali zmian mówił dr Wojciech Rafał Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych. Gospodarz spotkania zaznaczył, że dzięki personalizacji danych i internetowi rzeczy ludziom będzie się żyło wygodniej.

Według prowadzącego debatę na temat „Granic personalizacji w świecie big data” Łukasza Bolikowskiego z Interdyscyplinarnego Centrum Modelowania Matematycznego i Komputerowego Uniwersytetu Warszawskiego, big data charakteryzuje duży rozmiar (volume), wysoka zmienność (velocity) i wysoka różnorodność (variety). „Do tej definicji dodałbym jeszcze istotną wartość (value)” – powiedział Dariusz Śpiewak, członek zarządu Zakładu Ubezpieczeń Społecznych. Instytucji, która operuje dziś bazą danych obejmującą 600 mln dokumentów, a w ciągu najbliższych 10 lat będzie musiała dziesięciokrotnie zwiększyć pojemność swoich serwerów. Korzystają z nich nie tylko płatnicy i analitycy społeczni, ale również komornicy, którzy kierują do ZUS-u 250 tys. zapytań miesięcznie. Trudno przecenić również znaczenie danych dla aktuariuszów i kontrolerów, jednak ze względu na ochronę prywatności obywateli niektóre kraje, w tym Niemcy i Czechy, zabraniają łączenia danych ubezpieczenia społecznego z innymi danymi personalnymi.

Dr inż. Jarosław Tworóg, wiceprezes zarządu Krajowej Izby Gospodarczej Elektroniki



i Telekomunikacji, zwrócił uwagę na konieczność zamknięcia systemów z obu stron, czyli chronienia danych wchodzących do systemu i wychodzących z niego. Przyznał również, że wraz z rozwojem technologii granice ochrony danych przesuwają się, a jedynym racjonalnym działaniem może się okazać ochrona danych stanowiących rdzeń ochrony demokracji.

Zdaniem Katarzyny Szymielewicz, prezes Fundacji Panoptykon, granica ochrony danych powinna przebiegać tam, gdzie wykorzystanie danych może wpływać na zachowania ludzi. Zgoda na personalizację danych nie ma znaczenia, jeśli wyrażający ją właściciel danych nie wie, jakie będą konsekwencje. „Wyzwaniem jest to, żeby firma pokazała nam algorytm przetwarzania danych” – powiedziała Szymielewicz, zwracając jednocześnie uwagę na problem gromadzenia danych o dzieciach, które nie są świadome, że profilowanie może mieć ogromne znaczenie dla ich przyszłości. Na przykład brytyjscy ubezpieczyciele już doszli do wniosku, że zamiast robić drogie testy DNA, lepiej i taniej jest obserwować zachowania na FB i na tej podstawie oceniać stan zdrowia (np. liczba wykrzykników przy poście świadczy o tym, że autorowi mogło skoczyć ciśnienie) i skłonność ubezpieczonego do ryzykownych zachowań.

### Dziurawe aplikacje

Liczba użytkowników aplikacji mobilnych rośnie lawinowo. Z badań przytoczonych przez Artura Piechockiego z Polskiej Izby Informatyki i Telekomunikacji wynika, że w styczniu 2013 r. pobrano 1600 aplikacji, a we wrześniu 2013 r. było ich już 60 tys. Wiele z nich może być niebezpieczna, ponieważ bez wiedzy użytkownika zbierają i przekazują dane nie mające nic wspólnego z celem, do którego

**Co można zrobić, żeby uchronić się przed wpływem danych? Minimum to wprowadzenie dodatkowego hasła zabezpieczającego, wyłączenie interfejsów, których nie używamy, spicie się ze stroną producenta i szyfrowane backupy.**

zostały zainstalowane. „Jeśli korzystamy z Facebooka przez telefon, to musimy sobie zdawać sprawę z tego, że udostępniamy wszystkie numery, które mamy w bazie” – ostrzega Piotr Konieczny z Niebezpiecznik.pl. Ryzykowne może się okazać również kupowanie biletów, bo biletomaty wyposażone w szpiegujące oprogramowanie mogą zbierać numery używanych kart płatniczych. Aplikacje zainstalowane w urządzeniach mobilnych przesyłają bez wiedzy użytkowników dane nie tylko o położeniu, ale również o odwiedzanych stronach



GODO uczy najmłodszych, jak chronić dane osobowe

internetowych i połączeniach telefonicznych. Samo pojęcie urządzenia mobilnego należałoby rozszerzyć, bo wyposażone w komputery pokładowe auta także przekazują dane o sposobie jazdy do producenta. Niebezpiecznie może być również w banku. Przekonał się o tym uczestnik konferencji, który chciał skorzystać z e-kasy oferowanej przez jeden z banków, ale kiedy pobrał aplikację, to otrzymał pytanie o możliwość czytania danych o kontaktach i połączeniach. Użytkownik zawiadomił bank, potem producenta, ale żadna z tych instytucji nie poczuwa się do odpowiedzialności.

Co więc można zrobić, żeby uchronić się przed wypływem naszych danych? Minimum to wprowadzenie dodatkowego hasła zabezpieczającego, wyłączenie interfejsów, których nie używamy, spicie się ze stroną producenta i szyfrowane backupy.

### Moje dane, moja sprawa

Ochrona danych w szczególny sposób dotyczy dzieci, a już dziś 98% dziewięciolatków minimum raz na tydzień korzysta z internetu. Zdaniem Karoliny Szczepańskiej, nauczycielki informatyki ze Społecznej Szkoły Podstawowej nr 30 w Warszawie, ponieważ aż jedna czwarta uczniów deklaruje, że nawiązuje w ten sposób kontakty z nieznajomymi, to brama do przekazywania danych jest szeroko otwarta. Jej zdaniem również rodzice – wbrew deklaracjom – nie mają właściwej kontroli nad tym, jak ich pociechy korzystają z komputerów i telefonów. Do nauczycieli należy takie zaprezentowanie tematu ochrony danych, żeby był ciekawy dla uczniów. Przykładem mogą być prace – filmy i rysunki – które powstają w ramach projektu GODO „Twoje dane, Twoja sprawa”.

Prezes Fundacji Nowoczesna Polska Jarosław Lipszyc nie ma wątpliwości, że jedynym

sposobem na to, żeby młodzi i starsi użytkownicy panowali nad środowiskiem komunikacyjnym jest edukacja. Za tę skierowaną do przedsiębiorców odpowiada jego zdaniem państwo, które powinno wydać odpowiednie rekomendacje, ujawniać informacje o przypadkach sprzecznych z prawem działań firm na terytorium Polski i chronić przedsiębiorców przed szpiegostwem ze strony konkurencji.

Zdaniem Dariusza Jaszcuka, burmistrza miasta i gminy Mrozy, dużym problemem jest niespójność prawa w Polsce, która powoduje, że wiele informacji zawartych np. w rejestrze gruntów i innych zbiorach jest możliwa do pozyskania. Wysoko ocenił wysiłki nauczycieli informatyki (na podległym sobie terenie) idące w kierunku upowszechnienia wiedzy o niebezpiecznych zachowaniach, ale zwrócił również uwagę na to, że z czystej wygody i lenistwa rodzice nie chcą np. instalować routerów, które blokowałyby niepożądane treści. „Nie każdy problem da się rozwiązać technicznie” – uważa Michał „Rysiek” Woźniak, prezes Fundacji Wolnego i Otwartego Oprogramowania. Jego zdaniem, rodzice, którym trzeba wytłumaczyć, że umieszczając na FB śmieszne zdjęcia i filmiki swoich dzieci, bo chcą się nimi pochwalić, naprawdę okradają swe pociechy z godności. „My sami oddajemy naszą prywatność za ładny interface. Czyli robimy to, co kiedyś ci, którzy oddali Manhattan za 60 guldenów” – dodaje Woźniak. Jego zdaniem akcje edukacyjne przyniosą skutek dopiero wtedy, kiedy ludzie poznają rzeczywistą wartość danych. Według danych przytoczonych przez Małgorzatę Steiner z Ministerstwa Administracji i Cyfryzacji do 2020 r. wartość aplikacji opartych na przetwarzaniu cyfrowej tożsamości będzie wynosiła 330 mld euro. Łączna wartość cyfrowej tożsamości będzie wówczas stanowiła już 8% PKB. ■