

# Nadchodzi rewolucja internetu rzeczy

Z Generalnym Inspektorem Ochrony Danych Osobowych, dr. Wojciechem Rafałem Wiewiórowskim rozmawia Dorota Bogucka



**D**zień Ochrony Danych Osobowych to okazja do zastanowienia się nad tym, czy uczymy się chronić swoje dane osobowe. Z badań wynika, że w ostatnim roku o 19% wzrosła liczba osób, które nie podają swoich danych w portalach społecznościowych, wiedząc, że to niebezpieczne. Czy ocenia Pan, że świadomość znaczenia ochrony danych się poprawia?

Jestem ostrożny w ocenianiu takich statystyk, ponieważ mam wrażenie, że to, co ludzie deklarują, nie jest tożsame z tym, co faktycznie robią. Jeśli świadomość zagrożeń rozumiemy jako myślenie od czasu do czasu o tym, że coś złego może się wydarzyć, to rzeczywiście ona rośnie. Jeżeli natomiast spojrzymy na to, co ludzie robią w serwisach społecznościowych i jakie informacje za ich pośrednictwem przekazują, to można mieć wątpliwości, czy ta świadomość w jakikolwiek sposób się zmienia. Jestem ostatnią osobą, która chciałaby komukolwiek zakazać budowania swojej pozycji społecznej, również w internecie, poprzez udostępnianie nawet intymnych informacji o sobie. Ale warto zwrócić uwagę, że niektóre z tych informacji mogą powodować niebezpieczeństwo dla tej osoby. Stałe informowanie o tym, gdzie jadą kolacje, gdzie przebywam, jest informacją, że w tym czasie nie ma mnie w domu albo przed którą restauracją jest zaparkowany mój

samochód. Istnieje też poważne niebezpieczeństwo, że informacje przekazane do systemów społecznościowych mogą być wykorzystane w inny sposób, niż byśmy chcieli. Na dowód tego bardzo często podaję przykład osoby, która umieściła w sieci swoje zdjęcie, jak skacze ze spadochronem. To był żart, fotomontaż, bo takiego zdarzenia nigdy nie było, ale po śmierci tej osoby rodzina dowiedziała się, że fotografia ta została dołączona do dokumentacji ubezpieczeniowej jako dowód złamania warunków umowy ubezpieczenia na życie, ponieważ ubezpieczony deklarował, że nie będzie uprawiał sportów ekstremalnych.

Pamiętajmy, że o ile w dowolny sposób możemy upubliczniać informacje o sobie, o tyle nie mamy prawa decydować za innych, jakie ich zdjęcia, filmy i jakie informacje o nich udostępnić, np. w serwisach społecznościowych. Nasze prawo do autonomii informacyjnej nie rozciąga się na osoby trzecie.

**Największym problemem jest to, że spółki udostępniają sobie dane, często bez wiedzy klientów, którzy są potem nagabywani przez różne firmy. Te punkty w umowach konsumenckich są pisane takim językiem, że klient nie wie, co podpisuje.**

Tak, to prawda. Wymienianie się danymi osobowymi jest dozwolone w momencie, kiedy osoba

zgodzi się na przekazywanie danych. Jednak umowy z klauzulami o wyrażeniu zgody są często konstruowane w taki sposób, żeby osoba wyraziła zgodę na wykorzystywanie jej danych osobowych, nie będąc świadoma, co naprawdę zrobiła. Klasycznym tego przykładem jest zgoda na przekazywanie danych podmiotom współpracującym z firmą, której przekazujemy dane. Dzieje się tak np. przy zawieraniu umów o kartę lojalnościową, kartę punktową, rozwiązanie rabatowe, przy okazji konkursów itp. Wtedy z reguły godzimy się na blankietowe rozwiązanie, jakim jest przekazywanie danych podmiotom współpracującym z tym podmiotem, któremu udostępniamy dane. Trzeba pamiętać, że podpisując taką zgodę, klient godzi się, żeby jego dane zostały wprowadzone do dowolnej bazy, która będzie sprzedawana, rozdawana, dzierżawiona, wypożyczana. Zgody są czasem sformułowane w sposób nieprecyzyjny albo wprowadzający w błąd, niekiedy mamy też do czynienia z ich wymuszaniem. Na przykład klient słyszy, że jeżeli nie udzieli zgody, to nie skorzysta z usługi. Innym, szczególnie ohydny, moim zdaniem, sposobem pozyskiwania danych jest podkładanie podpisanej już zgody czy zaznaczonego okienka z tą zgodą przy operacji, która nie dotyczy przekazywania danych. Z tym mamy do czynienia zarówno na rynku finansowym, jak i IT.

**A czy to, że klient zgodzi się na wprowadzenie swoich danych do obrotu, uniemożliwia mu już wszelkie dalsze działania zmierzające do ochrony danych?**

Teoretycznie nie, ale praktycznie bardzo go utrudnia. Zgodę, jak każdą inną czynność prawną tego typu, można odwołać. Ustawa o ochronie danych osobowych od 2011 r. zawiera przepis, który wprost stanowi, że zgoda może być cofnięta w każdym czasie. W praktyce, jeżeli zgody na przetwarzanie danych udzieliliśmy tylko podmiotowi A, to jej wycofanie nie jest specjalnie skomplikowane. Można tego dokonać w tej formie, w jakiej została ona udzielona, albo w inny dogodny sposób, najlepiej taki, byśmy byli potem w stanie udowodnić, że to zrobiliśmy. Ale jeśli zgodziliśmy się na dzielenie się tymi danymi ze współpracującymi podmiotami, to musimy ich wszystkich poszukać, co jest niewykonalne. Powiedzmy, że zorientowaliśmy się, że nasze dane są w obrocie, kiedy skontaktowała się z nami firma X, ale jak zaczniemy szukać, to okaże się, że bazę kupiła od firmy Y, a ta z kolei kupiła ją od firmy B, która rzeczywiście zebrała dane od nas. Czasem ten łańcuszek jest jeszcze dłuższy i żeby odwołać zgodę, musielibyśmy skontaktować się z każdym



z tych podmiotów, który bazę kupił. Teoretycznie takie działanie jest możliwe, ale praktycznie tylko wtedy będziemy mogli skorzystać z tego prawa, kiedy wiemy, kto nasze dane przetwarza. Jeśli oddaliśmy nasze dane do swobodnego obrotu, wycofanie zgody będzie bardzo trudne.

#### Czy klienci często skarżą się na podmioty, które łamią prawo?

Tak, liczba skarg rośnie lawinowo. W 2013 r. rozpocząłem postępowania w ok. 1,5 tys. spraw, natomiast pytań o interpretację przepisów wpłynęło ponad 4 tys. W niektórych segmentach to kilkakrotnie więcej, niż otrzymywaliśmy cztery lata temu. Ale nie uważam, aby drastycznie pogorszyło się to, w jaki sposób nasze dane są przetwarzane. To raczej ludzie są coraz bardziej świadomi swoich praw.

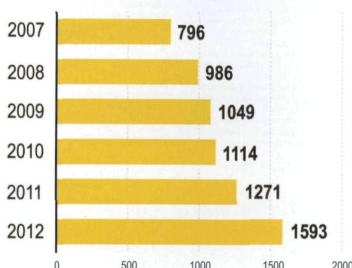
**Czy zatem operatorzy, firmy, które dopuszczają się naruszenia prawa, są świadome, że grożą im kary. Ostatnio we Francji Google został ukarany kwotą 200 tys. USD za nieinformowanie o zmianie polityki prywatności. Czy w Polsce sankcje mogą być dotkliwe?**

Przeciwko Google postępowania prowadziło sześć organów ochrony danych osobowych w różnych krajach. Kary finansowe zostały nałożone nie tylko we Francji, ale także w Hiszpanii, Belgii i Holandii. W Polsce Generalny Inspektor ma uprawnienia do nakładania kar wyłącznie w postępowaniu egzekucyjnym w administracji. Ale administratorzy danych w naszym kraju wiedzą, że Generalny Inspektor może podjąć decyzję, która będzie miała jeszcze bardziej dotkliwe skutki. W przypadku stwierdzenia naruszeń może bowiem zakazać przetwarzania danych albo nakazać zmianę sposobu ich przetwarzania. Takie decyzje są przez GIODO wydawane również w stosunku do podmiotów sektora ICT, np. wobec dostawców usług internetowych i firm telekomunikacyjnych.

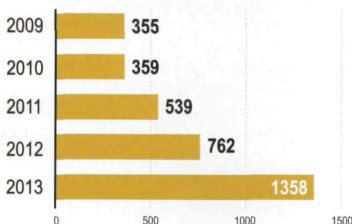
GIODO od dawna zwraca uwagę, że istnieje odwrotna dyskryminacja, jeżeli chodzi o polskich – czy może raczej europejskich – przedsiębiorców, prowadzących działalność w internecie. Muszą poddać się działaniom regulatorów europejskich, jakim nie muszą się poddawać podmioty działające spoza terenu Unii Europejskiej. To było bardzo widoczne, kiedy polska spółka NK, prowadząca serwis społecznościowy, dołożyła wszelkich starań, żeby dostosować się do unijnych prawnych standardów z zakresu ochrony danych osobowych i prywatności, podczas gdy podmioty działające spoza Europy nie musiały tego zrobić.

Rozwiązania europejskie idą w kierunku poddania podmiotów działających spoza Unii Europejskiej rozwiązaniom, które występują w prawie europejskim. Do tego zmierzają zmiany zaproponowane przez Komisję Europejską i przyjęte przez Parlament Europejski w zakresie nowych ram prawnych ochrony danych osobowych w Unii Europejskiej. Zresztą amerykańskie organy regulacyjne też przyznają sobie prawo do regulowania działalności, która jest prowadzona spoza terytorium Stanów Zjednoczonych, ale kierowana na obszar Stanów Zjednoczonych. Także Europa uznaje, że wszystkie osoby, które

#### Skargi skierowane do GIODO



#### Decyzje wydane przez GIODO

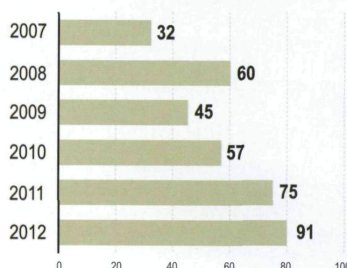


prowadzą jakiś biznes na terenie Unii, powinny być poddane prawu europejskiemu.

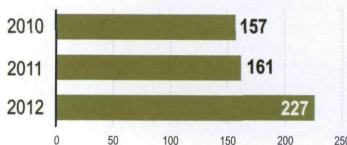
**Tylko że technologia jest zawsze o krok przed prawem. Dzisiaj już mamy aplikacje, które rozpoznają, identyfikują przypadkowych przechodniów. Jak się to ma do ochrony danych?**

Prawo nigdy nie będzie nadążało za rzeczywistością. To nigdy nie nastąpi i chyba dobrze, żeby nie nastąpiło. Bolesne jest dla mnie to, że nie dyskutuje się nad tym, jakie kwestie trzeba rozstrzygnąć i w jaki sposób. Nie uważam, że powinniśmy np. tworzyć ustawę o cloud computingu, bo gdy ją stworzymy, to być może ten model przetwarzania danych przestanie już w ogóle działać, zastąpiony czymś nowym. Mamy do czynienia z rewolucją. Z pewnością technologie związane z rozpoznawaniem twarzy będą się rozwijały. Najbardziej istotne jest to, kto może takie informacje zebrać, kto może je przekazać i kto będzie dokonywał ich obróbki. Bardzo wiele urządzeń zostało stworzonych po to, żeby odbierając dane ze świata rzeczywistego, łączyły je z rozproszonymi informacjami, które są w internecie. Jednak tak naprawdę rewolucja dokona się wtedy, kiedy do codziennego użytku wejdzie internet rzeczy. Wtedy, kiedy przedmioty zaczną się – często wbrew naszej woli – porozumiewać między sobą. Jeżeli przewiduje się, że w ciągu najbliższych dziesięciu, dwunastu lat każde urządzenie, które człowiek kiedykolwiek wytworzył, zostanie opatrzone chipem i będzie w stanie komunikować się z internetem, to musimy się przygotować na to, że te przedmioty zaczną

#### Skargi dotyczące sektora telekomunikacji



#### Skargi dotyczące sektora internetu



Źródło: GIODO

„mówić”. Będą przekazywać informacje, że szklanek należy napelnić i ktoś lub jakieś urządzenie będzie dokonywało kolejnego działania – przetworzenia tych informacji. To ułatwi nam życie, ale będzie rodziło nowe problemy w obrocie danymi i ich ochronie. Takie są wyzwania stojące przed osobami zajmującymi się ochroną danych w Europie i na świecie.

#### No właśnie, czy nadal chce Pan być Europejskim Rzecznikiem Ochrony Danych?

Procedura wyboru Europejskiego Inspektora Ochrony Danych została zahamowana. Doszło do pewnego rodzaju impasu między Komisją Europejską a Parlamentem Europejskim, wskutek czego podjęto decyzję, że procedura wyboru zostanie rozpoczęta od nowa. Czyli możemy powiedzieć, że jesteśmy w punkcie startu, tam gdzie byliśmy we wrześniu zeszłego roku. Jeżeli będzie taka możliwość formalna, a wszystko wskazuje, że będzie, to wystartuję również w kolejnym konkursie. ▶



Pod honorowym patronatem GIODO odbędzie się **Semafor 2014. VII Forum Bezpieczeństwa i Audytu IT**, organizowane przez ISSA, ISACA oraz Computerworld w terminie 27-28 marca 2014 r. Aby zgłębić wyzwania bezpieczeństwa IT w kontekście aktualnych top trendów: Big Data, technologie mobilne, chmura i sieci społecznościowe, dołącz do grona uczestników. [semafor.computerworld.pl](http://semafor.computerworld.pl)