Z dr. Wojciechem Rafałem Wiewiórowskim, Generalnym Inspektorem Ochrony Danych Osobowych (GIODO), rozmawiamy o wpływie nowych trendów technologicznych na ochronę danych osobowych oraz rozporządzeniu jej dotyczącym, nad którym pracuje obecnie Unia Europejska.

Dane osobowe w kontekście Big Data i internetu rzeczy

Jak nowe rozwiązania, takie jak Big Data czy internet rzeczy, wpływają na ochronę danych osobowych?
Big Data to bardziej hasło marketingowe, niż „rozwiązanie". Kryje się za nim stwierdzenie, że obecna ilość danych przekracza nasze możliwości samodzielnego ich przetwarzania i potrafią to jedynie zaawansowane systemy analityczne. Tym razem związane jest to z analizą danych dotyczących konkretnych osób. Tymczasem już w latach 70. XX wieku podawano te same powody, przygotowując prawodawstwo zmierzające do ochrony danych osobowych. To właśnie z powodu utraty możliwości samodzielnego kontrolowania przetwarzania takich danych powstały instytucje takie jak GIODO. Obecnie technologie są bardziej zaawansowane, ale problem pozostał ten sam.

Analityka biznesowa danych z Big Data, podobnie jak np. model cloud computing, nie jest sama w sobie zakazana. Trzeba jednak pamiętać, że gdy dotyczą danych objętych ochroną – ogólnie przez prawo ochrony danych osobowych, bądź szczególnie w ramach tajemnic prawnie chronionych takich jak tajemnica bankowa lub telekomunikacyjna – posiadacze takich danych nie mogą się nimi swobodnie dzielić. Nie można także ich łączyć, mimo że pojawiają się przykłady operatorów, którzy np. rozpoczęli działalność bankową. Prawo zabrania zestawiania danych pozyskanych na różne potrzeby bez zgody osób, których one dotyczą lub bez innej wyraźnej podstawy prawnej. W roku 2013 słyszałem wypowiedź przedstawiciela jednego z banków, który snuł wizję tego, że instytucja ta stanie się outsourcerem usług headhuntingowych i będzie oferować analizy przyszłych kandydatów do pracy. Dla mnie jest to herezja, bo banki czegoś takiego robić nie mogą! I w najbliższym czasie nie należy spodziewać się rozluźnienia tych zasad!

Prawdą jest natomiast, że organy ochrony danych osobowych de facto nie mają już możliwości zapanowania nad wszelkimi formami przetwarzania danych. Często możemy co najwyżej zwalczać szkody, które zostały dokonane z powodu naruszeń. Jest to o tyle trudne, że o szkodzie, w cywilistycznym znaczeniu tego słowa, można zaś mówić tylko wówczas, gdy można ją dokładnie określić i wyliczyć jej konsekwencje. Organy ochrony danych osobowych takie jak GIODO muszą natomiast zaoferować też obywatelom pomoc w dochodzeniu ich praw i skuteczne sposoby ochrony.

Czy aby na pewno zasada minimalizacji zbierania danych - będąca podstawą działania takich instytucji, jak GIODO, podstawą europejskiego systemu ochrony danych osobowych - **nie jest największą zbrodnią przeciwko ludzkości, której właśnie dokonujemy?**

Przed czym powinno się ich chronić?
Narzędzia analityczne, które są wykorzystywane do przetwarzania danych na nasz temat, pozwalają na zbieranie bardzo różnych danych z bardzo różnych źródeł i wywodzenia z nich wniosków, które nie są oczywiste. Niedawno miałem okazję oglądać zestawienie danych statystycznych, na podstawie którego wysnuwano wręcz absurdalne wnioski. Próbowano bowiem wykazać 100-proc. korelację między liczbą utonięć w stanie Connecticut a nakładami na edukację w sąsiadującym z nim stanie Massachusetts... Parafrazując stwierdzenie, że są kłamstwa, duże kłamstwa i statystyka, mamy dziś do czynienia z narzędziami analitycznymi, dużymi narzędziami analitycznymi i statystyką.

Poważnie mówiąc, najbardziej niepokojącą rzeczą dla rzeczników ochrony danych osobowych jest nie samo zestawianie pochodzących z różnych źródeł, danych, które są prawdziwe lub mamy co do nich przewidywania, że są prawdziwe, lecz analityka predykcyjna, w której z cech, które uważamy za prawdziwe, albo uprawdopodobnione próbujemy wnioskować o cechach, które jeszcze uprawdopodobnione nie są.

Takie działanie, co prawda jest dopuszczalne, ale tylko w sytuacji, gdy wymaga tego prawo, albo wówczas, gdy istnieje zgoda ze strony osoby zainteresowanej. Musi być ona jednak poinformowana, że takie działania są podejmowane, na czym polegają oraz zawsze powinna mieć dostęp do informacji o tym, jakie dane na jej temat są zbierane i w jaki sposób są przetwarzane.

Bank czy firma ubezpieczeniowa mogą dokonywać takiej predykcji na potrzeby ustalenia naszej zdolności kredytowej, czy ryzyka ubezpieczeniowego. To wręcz nakazuje im prawo. Instytucja, która zajmuje się analizowaniem różnego rodzaju usług, przewidywaniem tego, co może się nam przydać w przyszłości, też może to robić, ale pod warunkiem, że dana osoba wie, jak ta instytucja to robi i ma możliwość zareagowania, gdy informacja, która jest przez tę instytucję stworzona, jest sprzeczna z prawem, nieprawdziwa lub niepełna.

Ponadto na takie działania klient musi wyrazić dobrowolną zgodę, co oznacza, że musi mieć realny i swobodny wybór. Niedawno uczestniczyłem w jednej konferencji dotyczącej nowoczesnych metod zarządzania informacją na rynkach finansowych, gdzie m.in. wspominano o planie wymiany – za zgodą klienta – informacji o wszystkich transakcjach danego klienta we wszystkich bankach w Polsce. Przygotowano nawet porozumienie „samoregulacyjne" ustalające, jak miałoby to być zrobione. Z tym, że efektem takiego porozumienia może być doprowadzenie do sytuacji, w której nie będzie na polskim rynku oferty, która nie przewidywałaby dzielenia się przez banki informacjami dotyczącymi klienta. Wówczas mogłoby się okazać, że „zgoda" klienta nie jest tak naprawdę dobrowolna, bo gdyby nie wyraził zgody, mógłby nie otrzymać danego produktu na rynku finansowym. To więc co banki nazywają samoregulacją, ja – z równą swadą – nazwałbym zmową kartelową.

Na co więc trzeba zwracać uwagę?
Po pierwsze, na zakres danych, który jest gromadzony. Po drugie, na to, jak dane są wykorzystywane, ze szczególnym uwzględnieniem analityki predykcyjnej. Po trzecie zaś na to, aby mieć zapewnione prawo dostępu do dotyczących nas danych wraz z prawem do ich usunięcia lub poprawienia, jeśli zostały zebrane bezprawnie, są nieprawdziwe lub niepełne.

Obecnie mamy do czynienia z inną rewolucją – internetu rzeczy. Czy to również stanowi zagrożenie dla naszych danych osobowych? Już dziś instalowane przez nas aplikacje zbierają i przekazują dane np. o naszej aktywności fizycznej, do których dostęp zapewne chcieliby mieć przedstawiciele firm ubezpieczeniowych, podobnie jak do danych z naszej inteligentnej lodówki...
Internet rzeczy to kolejna rewolucja, która nas czeka, a nie wiem na ile jesteśmy do niej przygotowani zarówno jako społeczeństwo, jak i samo biuro GIODO. Widać to, gdy zaczynamy uświadamiać sobie, że za kilka lat praktycznie każdy otaczający nas przedmiot, będzie w ten czy inny sposób komunikował się z internetem. Przedmiot ten za mniej lub bardziej świadomą naszą zgodą, albo dla mniej lub bardziej uświadomionego interesu administratora, będzie przesyłał informację o nas na zewnątrz.

W logistyce internet rzeczy jest już prawdą. W portach jest on robiony na poziomie kontenerów, ale schodzi obecnie na poziom palety czy wręcz opakowania od jogurtu. Wkrótce za pośrednictwem internetu będziemy w stanie sprawdzić, w jakim stanie jest ten jogurt, albo przynajmniej, kiedy mija jego termin do spożycia. To będzie oznaczało, że każdy z nas będzie w stanie skontaktować się ze swoją lodówką i odpytać ją, kiedy mija termin do spożycia znajdujących się w niej jogurtów. To oczywiście – samo w sobie – jest bardzo przydatną usługą, o ile wiemy, kto jeszcze – poza nami – te dane posiada.

Podam inny przykład, przedmiotu, który jest już na rynku – soczewki stale badającej poziom cukru we krwi. To świetne rozwiązanie dla osób, które mają problem z cukrzycą. Do tej pory poziom cukru badały 3-4 razy dziennie. Teraz odbywać się to będzie co kilkanaście sekund czy kilka minut. To przedmiot, którego istnienia użytkownicy właściwie nie zauważają, ponieważ de facto jest przeznaczony do innego celu.

Dopóki do informacji zbieranych przez soczewkę ma dostęp wyłącznie osoba, której te dane dotyczą, nie budzi to mojego sprzeciwu. Gdy zna ją również lekarz, który tę osobę leczy, wydaje się to bardzo logiczne. W momencie jednak, kiedy trafia ona do producenta takiej soczewki, rozumiem powód, co nie oznacza, że jestem z tego szczęśliwy. Jeśli zdam sobie sprawę z tego, że jest to soczewka produkowana przez Google, zaczynam się zastanawiać, z jakimi jeszcze danymi zostaną powiązane te informacje i w jaki sposób będą przekazane do osób trzecich.

Szczególnie ta ostatnia kwestia jest niezwykle istotna z punktu widzenia ochrony danych osobowych. Zwłaszcza po takich informacjach, jak ta ujawniona na początku tego roku, że firma Ford zbiera dane o działaniu samochodu, który już dawno znajduje się na innym kontynencie. Dane te zaś przesyłane są do producenta, a nie sprzedawcy, czy tego, kto prowadzi naprawy gwarancyjne. Słysząc, że o zaginionym samolocie malezyjskich linii lotniczych najwięcej wiedział producent jego silnika, zdajemy sobie sprawę z tego, że to, co dzisiaj jeszcze jest dla nas dziwnym rozwiązaniem, za kilka lat będzie czymś zupełnie normalnym.

Najbardziej niepokojącą rzeczą dla rzeczników ochrony danych osobowych jest nie samo zestawianie pochodzących z różnych źródeł danych, które są prawdziwe lub mamy co do nich przewidywania, że są prawdziwe, lecz analityka predykcyjna. Analityka predykcyjna, w której z cech, które uważamy za prawdziwe, albo uprawdopodobnione próbujemy wnioskować o cechach, które jeszcze uprawdopodobnione nie są.

NAJWAŻNIEJSZE PLANOWANE ZMIANY W OCHRONIE DANYCH OSOBOWYCH W UE

1. Zamiast 28 ustaw implementujących dyrektywę dotyczącą ochrony danych osobowych pojawi się jedno, unijne rozporządzenie.
2. Przedsiębiorca, który działa w kilku krajach europejskich – jest to szczególnie istotne w branży IT – będzie „rozliczał" się ze swoich obowiązków przed swoim organem krajowym.
3. Skargi na przedsiębiorcę mogą wpływać do różnych organów krajowych, ale one między sobą mają już rozwiązać sprawę, jednocześnie lokalnie informować konsumenta, co dzieje się z jego sprawą.
4. Rezygnacja (z wyjątkiem danych wrażliwych) ze zgłaszania prowadzonego zbioru do rejestru GIODO, na rzecz poddania ocenie tego, jak wygląda przetwarzanie danych osobowych w danej firmie i jakie może mieć niepokojące skutki dla osób, których dane są przetwarzane.
5. Obowiązek zgłaszania incydentów bezpieczeństwa (utraty, zniszczenia lub kradzieży danych) dla wszystkich firm, dziś dotyczy to tylko operatorów.
6. Nakładanie przez GIODO kar administracyjnych, czego do tej pory nie było w systemie polskim, a co sprawdzało się w systemach francuskim, brytyjskim.

I tu pojawia się bardzo poważne pytanie, które stawiają producenci tego typu rozwiązań, czy aby na pewno zasada minimalizacji zbierania danych – będąca podstawą działania takich instytucji, jak GIODO, podstawą europejskiego systemu ochrony danych osobowych – nie jest największą zbrodnią przeciwko ludzkości, której właśnie dokonujemy? Za kilkadziesiąt lat być może będziemy potrzebowali tych danych. Może dom, który będzie się miał mną opiekować za 30-40 lat, będzie potrzebował informacji o tym, co jadłem w roku 2014, jakiej muzyki słuchałem i na którym koncercie byłem w ostatni poniedziałek...

Czy Unia Europejska myśli o zmianie tych przepisów?
Jeśli chodzi o zmianę przepisów dotyczących ochrony danych osobowych, to obecnie trwają prace nad reformą systemu

ochrony danych osobowych w Unii Europejskiej. Przygotowywane jest rozporządzenie, które – cały czas wierzę – zostanie pod koniec 2014 lub na początku 2015 roku uchwalone i pewnie około roku 2017 wejdzie w życie. Rozporządzenie to w oczywisty sposób nie odwołuje się do konkretnych technik, czy modeli biznesowych, które są dziś stosowane na rynku, jak np. cloud computing. Zanim bowiem wejdzie w życie, może obecnie modele zastąpią już inne.

Niewątpliwie jednak nowelizacja przepisów o ochronie danych osobowych próbuje odpowiedzieć na wątpliwości, które pojawiają się dziś. Świadczy o tym także ostatnie orzeczenie w sprawie Google Spain *(Trybunał Sprawiedliwości Unii Europejskiej uznał, że można żądać usunięcia niektórych wyników wyszukiwania wyświetlanych po wpisaniu w okno wyszukiwarki imienia i nazwiska. – przyp. red.)*. Trybunał uznał, że 28 różnych organów ochrony danych, w 28 krajach członkowskich UE może wydać 28 różnych decyzji na temat czegoś, co tak naprawdę jest usługą skierowaną do całego świata. Wskazuje to, że dobrze byłoby wprowadzić jakiś porządek do tego systemu, choćby poprzez zastąpienie 28 ustaw o ochronie danych osobowych jednym rozporządzeniem na poziomie europejskim.

Nadal jednak utrzymane zostałyby krajowe instytucje ochrony danych osobowych?
Tak, z tego względu, że większość trafiających do nich spraw ma charakter lokalny, dotyczy firm i podmiotów publicznych działających w danym kraju. Współpraca między poszczególnymi organami to jednak główny cel, który chce osiągnąć Unia Europejska.

Na czym dokładnie polega reforma?
Wdraża ona kilka podstawowych założeń, wzmacniając część zasad, które były przewidziane w obowiązującym już prawie europejskim, zmieniając nieco sposób ich realizowania. Po pierwsze, zamiast 28 ustaw implementujących dyrektywę pojawia się jedno, unijne rozporządzenie. Dzięki temu, teoretycznie, różnica między tym, jak działa polski organ ochrony danych osobowych, a jak hiszpański czy estoński, będzie znacznie mniejsza. Podobnie będą orzekać sądy.

Po drugie, wprowadza się zasadę, że przedsiębiorca, który działa w kilku krajach europejskich – jest to szczególnie istotne w branży IT – będzie „rozliczał" się ze swoich obowiązków przed swoim organem krajowym. Jednocześnie skargi do niego mogą wpływać do różnych organów krajowych, ale one między sobą mają już rozwiązać sprawę, jednocześnie lokalnie informować konsumenta, co dzieje się z jego sprawą. Z drugiej strony spowoduje, że przedsiębiorca nie będzie musiał załatwiać swoich spraw jednocześnie w kilku krajach Unii Europejskiej.

Kolejna kwestia to rezygnacja ze zgłaszania prowadzonych zbiorów do rejestru GIODO, na rzecz poddania ocenie tego, jak wygląda przetwarzanie danych osobowych w danej firmie i jakie może mieć niepokojące skutki dla osób, których dane są przetwarzane. Raczej dokonujemy samooceny, niż zgłaszamy się do jakiegoś rejestru. Nawet, jeśli zbieramy te dane do celów marketingowych. Samo zgłoszenie nic tak naprawdę nie znaczy, ani dla tego rejestru, ani dla przedsiębiorcy. Wyjątkiem mają być zbiory, w których gromadzone są dane sensytywne wymienione w obecnym art. 27 ustawy o ochronie danych osobowych, np. dane o zdrowiu, wyznaniu czy poglądach politycznych.

Możliwe jest też zbieranie danych w ramach tzw. internetu rzeczy. Trzeba jednak znaleźć jedną z 6 podstaw prawnych, którą przewiduje obowiązująca dziś dyrektywa, np. gdy jest taki wymóg prawny lub gdy istnieje „uzasadniony interes" administratora danych osobowych. Tego specjalnie nie zmieni nowe rozporządzenie.

Nowością – z punktu widzenia polskiego prawa – będzie obowiązek zgłaszania incydentów bezpieczeństwa. Obecnie istnieje on tylko w Prawie telekomunikacyjnym. Incydent bezpieczeństwa oznacza sytuację, w której dane zostały zniszczone, skradzione lub z innego powodu wyciekły. Nowością będzie też nakładanie przez GIODO kar administracyjnych, czego do tej pory nie było w systemie polskim, a co sprawdzało się w systemach francuskim, brytyjskim.

Adam Jadczak