www.di.com.pl

Biznes powinien ustalić granicę personalizacji - wywiad z GIODO z okazji VIII Dnia Ochrony Danych

Marcin Maj, 28-01-2014,

Personalizacja bezrobotnych, rozpoznawanie twarzy, Edward Snowden, copyright trolling - Dziennik Internautów rozmawiał na te tematy z Wojciechem Wiewiórowskim, Generalnym Inspektorem Ochrony Danych Osobowych. Wywiad miał związek z obchodzonym dziś VIII Dniem Ochrony Danych.

Właśnie dziś obchodzimy **VIII Dzień Ochrony Danych**. To "święto nietypowe" ustanowiono po to, aby przypominać ludziom o znaczeniu danych osobowych i prywatności. 28 stycznia to rocznica otwarcia do podpisu Konwencji 108 Rady Europy z 1981 roku w sprawie ochrony osób w zakresie zautomatyzowanego przetwarzania danych osobowych. Jest to chyba najstarszy akt prawny o zasięgu międzynarodowym, który kompleksowo regulował zagadnienia związane z ochroną danych.

Z okazji Dnia Ochrony Danych zorganizowano w Warszawie konferencję "Prywatność w cyfrowym świecie", w czasie której będą omawiane takie problemy, jak aplikacje mobilne, granice personalizacji i edukacja cyfrowa. Dziennik Internautów rozmawiał wcześniej na te tematy z Wojciechem Wiewiórowskim, Generalnym Inspektorem Ochrony Danych Osobowych. Poniżej zapis tej rozmowy, który - mamy nadzieję - skłoni Was do refleksji nad współczesnymi problemami w zakresie prywatności. Wcześniej publikowaliśmy tylko fragment tego wywiadu dotyczący copyright trollingu.

* * *

Marcin Maj, Dziennik Internautów: Przed nowym rokiem, w grudniu, firma FacialNetwork udostępniła aplikację NameTag, która pozwala na wyciągnięcie danych sfotografowanej osoby z Facebooka, LinkedIn i tym podobnych serwisów. Gdy tylko zapoznałem się z działaniem tej aplikacji, zastanowiło mnie... co Pan by na to powiedział?

Dr Wojciech Wiewiórowski, GIODO: Tego typu aplikacje będą tworzone, jestem o tym całkowicie przekonany. Mogą być użyteczne, czego dowodzi pojawienie się na rynku takich rozwiązań, jak Google Glass. (...)

Jeśli chodzi o algorytmy służące rozpoznawaniu twarzy, to nie są one w tej chwili doskonałe, ale z pewnością będą ulepszane. Prace w tym zakresie są prowadzone zarówno przez firmy komercyjne, jak i przez instytucje naukowe. W Polsce klasycznym przykładem projektu, w którym pod uwagę brane jest wykorzystanie mechanizmu rozpoznawania twarzy, jest projekt

INDECT. Uczestniczące w nim osoby analizują, na ile w ogóle możliwe jest sprawne rozpoznanie twarzy poprzez porównanie jej z jakimś systemem dokumentów, takich chociażby jak zasoby policyjne (...)

Tak więc co do tego, że takie aplikacje będą powstawały, nie mam żadnych wątpliwości. Natomiast główne pytania, które nurtują rzeczników ochrony danych osobowych, brzmią: kto otrzymuje tego typu informacje i w jakim celu je wykorzystuje.

Działanie aplikacji, przy pomocy której osoba jedynie na własne potrzeby rozpoznawałaby, kim jest ten, kogo w tej chwili zobaczyła, można by uznać za mieszczące się w ramach tego, co nazywamy "użytkiem domowym i osobistym".

Każdy jednak, kto zna choćby podstawowe zasady działania aplikacji mobilnych, zdaje sobie sprawę z tego, że to przetworzenie danych (...) nie odbywa się w telefonie komórkowym, w smartfonie czy w jakimkolwiek innym urządzeniu mobilnym, które przy sobie mamy, lecz daleko poza nimi. Informacja jest bowiem wysyłana gdzieś w określone przez dewelopera miejsce, tam jest przetwarzana przy pomocy danych, które deweloper posiada i odsyłana z powrotem do tego, kto zażądał tego typu operacji, ale zapewne również przechowywana u dewelopera oraz w innych zbiorach, o których nie mamy pojęcia.

Główne pytania, które zawsze stawiają rzecznicy ochrony danych osobowych w stosunku do aplikacji mobilnych, brzmią: na ile ten, kto używa aplikacji, zdaje sobie sprawę z tego, co ona robi? Czy wie, co tak naprawdę i komu ujawnia w momencie, kiedy jakichś operacji dokonuje? Kim są podmioty, które mają dostęp do danych, do jakich celów je zbierają i wykorzystują?

DI: Pana zdaniem samo pojawienie się takich rozwiązań wymaga jakichś szczególnych interwencji organów ochrony danych osobowych, czy po prostu trzeba spokojnie to nowe zjawisko obserwować?

GIODO: Na pewno trzeba obserwować. Na pewno trzeba też pytać. Powołam się tutaj ponownie na przykład Google Glass. Gdy Google rozpoczął testowanie tych okularów, rzecznicy ochrony danych osobowych, nie tylko z Europy, ale również m.in. z Kanady, Meksyku, Izraela, Australii, Korei Południowej czy Nowej Zelandii, wystosowali do tego przedsiębiorcy wspólny list, w którym zażądali wyjaśnienia m.in. tego, jaką informację na

temat działania tego urządzenia utrzymuje użytkownik, z czego zdaje sobie sprawę i jakie podmioty trzecie mają dostęp do danych zbieranych przez Google.

Należy więc spodziewać się tego, że rzecznicy ochrony danych będą uważnie śledzili kwestię działania aplikacji mobilnych i ich wpływu na prywatność użytkowników. Oczywiście nie każdy rzecznik ochrony danych osobowych jest przygotowany do tego zadania z czysto technologicznego punktu widzenia. Odpowiednie do tego celu laboratorium mają nasi koledzy np. z Francji czy z Kanady, dlatego w ramach współpracy rzeczników staramy się delegować tego typu zadania do wykonania przez organy, które są do tego najlepiej przygotowane.

DI: Jeden z tematów umieszczonych w agendzie konferencji organizowanej przez GIODO z okazji VIII Dnia Ochrony Danych Osobowych brzmi "Granice personalizacji w świecie Big Data". Szczerze powiem, że nie wiem, gdzie te granice są, tzn. ja osobiście mam wrażenie, że żadna firma ich sobie nie postawi.

GIODO: Mamy dwie możliwości. Pierwsza to taka, że firmy jednak zaczną stawiać granice personalizacji danych, a przynajmniej zaczną stawiać sobie pytania, do jakiego momentu mają zamiar dojść i dlaczego do tego momentu mogą dojść. Druga możliwość jest taka, że te granice będą wyznaczone przez przepisy prawne, a ich egzekwowaniem zajmą się organy będące regulatorami, ale sytuacji tej wcale nie uważam za doskonałą ani słuszną.

Jestem bowiem zwolennikiem tego, by przy każdym przedsięwzięciu związanym z przetwarzaniem danych osobowych dokonywać analizy jego wpływu na prywatność, czyli czegoś, co nazywa się Privacy Impact Assessment. Oznacza to, że przed rozpoczęciem działań trzeba odpowiedzieć sobie na pytania, które dotyczą owej personalizacji, a potem stosować się do tego, do czego tak naprawdę sami się zobowiązaliśmy, wyznaczając cele i sposoby przetwarzania danych.

Dla zilustrowania tej kwestii podam przykład działania jednego z tzw. operatorów systemu dystrybucyjnego, a więc przedsiębiorstwa zajmującego się dostarczaniem energii elektrycznej, związany z instalacją inteligentnych liczników energetycznych. Inteligentny licznik energetyczny, szczególnie podłączony do sieci HAN, jest w stanie przekazać bardzo dokładną informację dotyczącą sposobu zachowania osoby, m.in. tego, jakich używa sprzętów, kiedy ma je włączone czy wyłączone, a nawet jaki film w telewizji ogląda (co zostało udowodnione w warunkach laboratoryjnych).

Firma owa, świadoma wpływu, jaki na ochronę prywatności ma instalacja inteligentnych liczników energetycznych, przeprowadziła analizę tego, wymagającego poważnych nakładów finansowych, przedsięwzięcia, ustalając, jakie dane są jej naprawdę potrzebne do świadczenia usług (...). I to wcale nie zostało zrobione w ramach specjalnie prowadzonego Privacy Impact Assessment, lecz było normalną częścią analizy ryzyka przedsięwzięcia.

Rzecznicy ochrony danych osobowych będą optowali za tym, aby tego rodzaju analizy ryzyka przeprowadzać przy każdym działaniu związanym z przetwarzaniem danych osobowych. Zdaję sobie sprawę, że zaraz może pojawi się wątpliwość, czy każdy, nawet gdy przygotowuje niewielką aplikację mobilną, będzie coś takiego robił. Uważam, że powinien, a zachętą do tego może być wprowadzenie jakiegoś systemu certyfikacji, choćby poprzez sklepy, które takie aplikacje sprzedają.

Przy niektórych platformach, np. platformie Apple, aplikacje przechodzą swoistą certyfikację przy wejściu na listę produktów w oficjalnym sklepie online. Ta certyfikacja nie jest prowadzona pod kątem ochrony prywatności, lecz zgodności z tym, jakie produkty Apple sam oferuje swoim klientom. Trochę trudniejsze jest to w przypadku Androida, ale też można sobie wyobrazić sytuację, w której klient będzie w stanie ustalić, czy przeprowadzono tego typu analizę i jakie są jej wyniki. Sądzę, że takie certyfikowane aplikacje byłyby chętniej używane niż te, które takiej certyfikacji nie posiadają.

DI: Jeśli chodzi o personalizację usług państwa, mam pytanie o profilowanie osób bezrobotnych. Czy Pana zdaniem administracja będzie częściej dokonywała profilowania?

GIODO: Myślę, że tak i to wcale nie byłoby złe. Jestem zwolennikiem sytuacji, w której przynajmniej niektóre usługi publiczne będą w lepszy sposób dostosowane do potrzeb konkretnej osoby, która jest klientem administracji. Usługi dotyczące aktywizacji bezrobotnych są bardzo dobrym przykładem tego typu działań, które inaczej powinny wyglądać w przypadku profesora szkoły wyższej, który utracił zatrudnienie, inaczej w przypadku osoby, która ma wykształcenie zawodowe (...).

Nie jestem przeciwnikiem samej personalizacji. Natomiast uważam, że jeżeli taka przymusowa personalizacja następuje, to po pierwsze, zgodnie z art. 51 Konstytucji RP, musi być uregulowana w ustawie. Parlamentarzyści muszą zadecydować, że jest to niezbędne w demokratycznym państwie prawnym, a jednocześnie w ustawie określić, jakie dane są zbierane, do czego mogą być wykorzystywane, kto ma do nich dostęp, jak długo są przechowywane, jakie prawa przysługują osobie, której dane dotyczą. Co do zasady, powinna ona mieć dostęp do danych na swój temat, choć zdaję sobie sprawę, że przy działaniach CBA w wielu przypadkach może być to niemożliwe. Niemniej jeżeli osoba, której profil jest tworzony, ma dostęp do takich danych, np. zbieranych przez urząd pracy, kolejną ważną kwestią jest to, czy ma prawo je poprawić. Czy np. zajrzawszy do tych danych i zobaczywszy, że zawierają pewne informacje ocenne ze strony urzędu pracy, ma prawo powiedzieć „ja się z tą oceną nie zgadzam".

Ocena może bowiem nie być dokonana na podstawie prawdziwych danych, lecz być tylko pewnym opartym na danych statystycznych przewidywaniem tego, w jaki sposób mogę funkcjonować (tzw. profil predykcyjny). Dlatego osoba, która jest w ten sposób profilowana, powinna móc poprawić dane, które jej dotyczą.

Te kwestie powinny być, moim zdaniem, uregulowane na poziomie ustawy. Tego, niestety, w przypadku propozycji Ministerstwa Pracy i Polityki Społecznej na temat profilowania bezrobotnych nie ma. Stąd wynika pewien konflikt. Nie dotyczy on samego pomysłu personalizacji i pomocy w stosunku do osób bezrobotnych, bo to rzeczywiście się sprawdza w wielu krajach Europy i świata, tylko tego, jakie będą gwarancje, że nie dojdzie do naruszenia praw człowieka.

DI: Edukacja cyfrowa to kolejny temat, który ma być podejmowany w tegorocznych dyskusjach z okazji Dnia Ochrony Danych. Jakie problemy wiążą się z edukacją cyfrową w świetle ochrony danych?

To bardzo ważna kwestia, bo wszyscy mówimy o edukacji, lubimy używać tego pojęcia jako swego rodzaju buzzworda, podnosząc, że nie chodzi o to, by wszystko uregulować w przepisach prawa i karać za ich naruszanie, lecz chodzi o to, by edukować.

To prawda. Dlatego osoba, która porusza się po cyfrowym świecie, powinna mieć wiedzę nie tylko czysto techniczną, ale także dotyczącą tego, jak w wirtualnej rzeczywistości chronić swoją prywatność i dane osobowe. Powinna np. zdawać sobie sprawę z tego, że synchronizowanie tabletu z komputerem pokładowym w samochodzie to nie tylko synchronizowanie muzyki, ale również kalendarza, listy spotkań i listy adresowej, które w tym momencie staną się dostępne dla każdego mechanika w serwisie samochodowym. W przypadku lekarza, adwokata czy radcy prawnego rodzi to poważny problem związany z zachowaniem tajemnicy zawodowej.

Edukacja w cyfrowym świecie oznacza zatem edukację dotyczącą wszystkich etapów życia i ról, które gramy w społeczeństwie, które w coraz większym stopniu jest społeczeństwem cyfrowym.

Natomiast jeśli chodzi o edukację skierowaną do dzieci i młodzieży, to jako przykład podam program „Twoje dane – Twoja sprawa", który Biuro GIODO realizuje wspólnie z ośrodkami metodycznymi dla nauczycieli. Otóż my wcale nie zabiegamy, by do podstawy programowej wprowadzić dodatkowy przedmiot, jakim będzie ochrona danych osobowych albo ochrona prywatności, bo byłaby to próba tworzenia kolejnego przysposobienia obronnego albo kolejnej lekcji wychowawczej. Natomiast zależy nam na tym, by upowszechnić podejmowanie tematyki ochrony danych osobowych i prywatności podczas lekcji z bardzo różnych, czasem nieoczywistych, przedmiotów. Np. gdy na lekcji języka angielskiego uczymy się Present Perfect Continuous albo "trzeciego conditionala", to możemy to robić zarówno na czytance dotyczącej Big Bena albo mostu londyńskiego, jak i na czytance dotyczącej prywatności w sieci (...).

Jeżeli podczas zajęć z biologii uczymy o genetyce, to dlaczego przy tej okazji nie informować o tym, że genom to specyficzna informacja o nas, informacja, której nigdy nie zmienimy, w przeciwieństwie do imienia, nazwiska czy środowiska, w którym przebywamy. To taka ciekawostka, która pojawia się przypadku choćby świadków koronnych - wszystko można im zmienić poza genomem. W momencie, kiedy będziemy mogli rozpoznawać osoby na podstawie danych genetycznych, ten problem będzie coraz bardziej widoczny.

Jako GIODO uczestniczyłem w pracach specjalnego zespołu przy Ministrze Nauki i Szkolnictwa Wyższego, który zajmuje się badaniami genetycznymi i biobankowaniem. Jednak wiele kwestii z tego zakresu wymaga jeszcze uregulowania. To również ogromne pole do edukacji, de facto edukacji cyfrowej, bo większość danych jest już przetwarzanych w postaci elektronicznej, także w sektorze ochrony zdrowia, w którym informatyzacja postępuje z roku na rok. Dlatego lekarzy trzeba nauczyć właściwego postępowania z danymi osobowymi.

DI: Ostatnio często można spotkać się ze stwierdzeniem, że Edward Snowden rozruszał nasze myślenie o prywatności. Czy Pana zdaniem ta cała seria wycieków miała korzystny wpływ na dyskusję o prywatności, czy też zepchnęła ją na jakieś niepotrzebne tematy?

GIODO: Na pewno miała korzystny wpływ w tym znaczeniu, że temat przestał być tematem niszowym, stał się zaś tematem z pierwszych stron gazet. Natomiast każda sytuacja, w której temat niszowy staje się tematem z pierwszych stron gazet, powoduje, że dyskusja w pewnym stopniu się „tabloidyzuje". Wówczas dochodzi do tego, że miesza się kwestie związane z działaniem systemów służących do masowej inwigilacji społeczeństwa, takich jak np. PRISM czy XKeyscore, z zagadnieniami dotyczącymi podsłuchiwania telefonu Angeli Merkel. Tymczasem mnie naprawdę niespecjalnie interesuje to, w jaki sposób służby specjalne Republiki Federalnej Niemiec chronią telefon Pani Kanclerz, czy umieją to robić (...) Natomiast czym innym jest wywiad czy kontrwywiad, a czym innym sytuacja, kiedy prowadzona jest masowa inwigilacja społeczeństwa.

Zatem z jednej strony bardzo dobrze, że pojawiły się dyskusje dotyczące tych zagadnień, z drugiej strony, trzeba oczywiście uważać, by nie sprowadzić ich do kwestii związanych ze szpiegostwem. Ja nie wiem, czy Snowden jest dobry czy zły, jakie są motywy i podstawy jego działania – dobre czy złe. Natomiast bez wątpienia sprowokował bardzo istotną dyskusję.

Natomiast co do tabloidyzacji tego zdarzenia, to niestety nie ominęła ona także polskiego parlamentu, czego dowodzą wypowiedzi posłów po posiedzeniu sejmowej Komisji ds. Służb Specjalnych, jakie w sprawie Snowdena odbyło się z udziałem przedstawicieli służ specjalnych. Jeśli posłowie tej Komisji twierdzą, że Polska nie podlegała monitoringowi ze strony USA, to nie wiem, czy wiedzą, co mówią.

To, że takiemu monitoringowi Polska podlega, jest dla mnie zupełnie oczywiste. Pytać możemy jedynie o to, czy polskie służby specjalne współpracowały ze służbami amerykańskimi. Może się tego dowiemy, podobnie jak tego, czy istniał podsłuch na telefonach posłów i premiera. Natomiast to, że dane w komunikacji, która jest prowadzona przez serwery amerykańskie, zbierane są przez służby specjalne jest dla mnie zupełnie oczywiste.

DI: Ostatnie moje pytanie dotyczy zjawiska, które częściowo tylko zahacza o problemy prywatności. Chodzi mi o copyright trolling, czyli zgłaszanie naruszeń praw autorskich do organów ścigania. Wyciąganie danych i dochodzenie na własną rękę…

GIODO: …zbieranie danych teoretycznie na potrzeby postępowania karnego, lecz faktyczne używanie ich w postępowaniu cywilnym - tak spojrzałbym na to jako prawnik.

Na początek muszę zaznaczyć, że tego typu działanie ze strony profesjonalnych adwokatów bądź radców prawnych uważam za głęboko nieetyczne. Niestety, jest to wykorzystywanie organów publicznych, takich jak prokuratura czy policja, do wykonywania działań, do których nie są one powoływane.

Rzeczywiście jest to problem. Wynika on z tego, że o ile prawo karne stanowi, że informacja dotycząca osób naruszających prawa autorskie musi być udzielona przez dostarczyciela usług internetowych albo przez operatora telekomunikacyjnego policji, o tyle nie ma takiego przepisu w prawie cywilnym.

Niezależnie zatem od tego, czy mówimy o naruszeniu praw autorskich, czy np. czyjegoś dobrego imienia albo wizerunku firmy, to działanie jest dokładnie takie samo. Podejmowana jest próba pozyskania danych na potrzeby postępowań karnych tylko po to, żeby wykorzystać je na potrzeby postępowań cywilnych. O ile jestem w stanie w jakimś stopniu zrozumieć takie

działanie ze strony osób indywidualnych, o tyle zdecydowanie potępiam takie próby podejmowane przez osoby zajmujące się tego typu działalnością profesjonalnie. Uważam, że powinniśmy zająć się tym, na ile osobom, które chcą rzeczywiście dochodzić swoich praw przed sądem cywilnym, należy ułatwić dostęp do danych, które byłyby do tego potrzebne.

Mówiąc w sposób bardzo prawniczy, należałoby przeprowadzić dyskusję dotyczącą prawidłowego skierowania pozwu. Jakiś czas temu Naczelna Rada Adwokacka przedstawiła propozycję, która - jak sądzę - jest warta rozważenia, choć wymaga sporych zmian w Kodeksie postępowania cywilnego. Chodzi mianowicie o możliwość złożenia tzw. ślepego pozwu, czyli pozwu bez określenia pozwanego, z jednoczesnym wystąpieniem o udzielenie informacji, która mogłaby doprowadzić do zidentyfikowania takiej osoby.

Ważne jest bowiem, by rozróżni dwie sytuacje. Pierwsza to ta, kiedy rzeczywiście zamierzamy wytoczyć sprawę sądową przeciwko komuś i mamy uzasadniony interes, by określone informacje, w tym dane osobowe, pozyskać. Druga to sytuacja, kiedy po prostu chcemy jedynie dowiedzieć się, kto naruszył nasze prawa.

Na dowód tego, że sprawa nie jest prosta, podam przypadek dotyczący osoby, która próbowała pozyskać dane internauty publikującego w sieci informacje dotyczące jej spraw rodzinnych. W jej opinii bowiem kwestie te przedstawiane były w sposób nieprawdziwy i obraźliwy. Osoba ta była naprawdę zdeterminowana, żeby złożyć pozew o ochronę dóbr osobistych, aż do momentu, w którym dowiedziała się, że osobą zamieszczającą wpisy jest jej własny syn. Ostatecznie uznała, że wytaczanie sprawy sądowej tylko po to, by w sądzie prać rodzinne brudy, nie jest dobrym pomysłem.