

Więcej zaufania, mniej inwigilacji

Pracownik Google fotografuje park
wulkaniczny w centralnej Francji



Francis Campagnoni/LA MONTAGNE/PHOTOPQR/FORUM

Nie mogę się zgodzić na zakaz zakrywania twarzy podczas zgromadzeń, bo państwo nie może podejrzewać każdego obywatela – mówi w rozmowie z Anną Mazgal **WOJCIECH RAFAŁ WIEWIÓROWSKI**, Generalny Inspektor Ochrony Danych Osobowych

Przed kim chroni nas G1000?

Kiedy w latach 70. i 80. w krajach zachodniej Europy tworzono przepisy dotyczące ochrony danych osobowych, to państwo postrzegano jako Wielkiego Brata,

który może chcieć przetwarzać zbyt dużo informacji na nasz temat. Dziś zaufanie do państwa wzrosło, a przepisy coraz bardziej służą ochronie naszej prywatności w relacjach z biznesem.

Obywatele coraz częściej godzą się na utratę prywatności w stosunkach łączących ich z organami państwa, o ile czują, że służy to ich bezpieczeństwu. Już w latach 70. XX wieku w Niemczech

ingerencję w prywatność uzasadniano zwalczaniem terroryzmu spod znaku organizacji Baader-Meinhof.

A teraz w Polsce używa się tych argumentów?

Padają w debacie na temat projektu ustawy o zgromadzeniach. Jako GIODO nie mogę się zgodzić na zakaz zakrywania twarzy podczas zgromadzeń. Wydaje mi się, że państwo nie powinno być nieufne wobec własnych obywateli. Nie może z zasady uważać każdego za podejrzanego.

Czy w ingerencjach polskiego państwa w prywatność obywateli widać jakąś konsekwencję?

Uważam, że przetwarzanie danych osobowych przez państwo, szczególnie w dobie rozwoju nowoczesnych technologii, rodzi wiele istotnych problemów. Właśnie dlatego tematem przewodnim obchodów Dnia Ochrony Danych Osobowych w 2012 r. było hasło „Co państwo wie o obywatelach? Zasady przetwarzania danych osobowych w rejestrach publicznych”.

W przypadku przetwarzania danych osobowych przez państwo dochodzi bowiem do zderzenia dwóch sprzecznych celów. Z jednej strony chcielibyśmy, żeby administracji publicznej nie trzeba było podawać wielokrotnie tych danych, które już raz jej przekazaliśmy. Zatem chcielibyśmy, aby tworzone przez nią systemy informacyjne były interoperacyjne, a dane przepływały między organami administracji.

Z drugiej jednak strony chcielibyśmy, aby każdy sam decydował o tym, kto i jakie informacje o nim posiada. Tymczasem państwo, realizując pierwszy z tych

celów, doprowadza do sytuacji, w której możliwe jest łączenie się z poszczególnymi rejestrami publicznymi, a urzędnicy – w ramach swoich uprawnień – mogą korzystać z wielu źródeł informacyjnych, zdobywając dane na swoje potrzeby.

To brzmi sensownie, gdzie zatem czai się niebezpieczeństwo?

Idea nie jest zła, ale w praktyce niesie ze sobą poważne zagrożenia. Gdy konkretny urząd otrzymuje dostęp do jakiegoś rejestru, to zazwyczaj jest to dostęp do całej jego zawartości, a nie tylko do potrzebnej informacji. A jeśli systemy i rejestry są połączone, to wiemy, że potencjalnie jest gdzieś taka osoba w państwie, która może dotrzeć do wszystkich tych zasobów z jednego komputera. Nie twierdzę, że nie ma potrzeby nadania komuś takich uprawnień. Ale chciałbym wiedzieć dokładnie, kto to jest i kto go kontroluje.

Do tej pory najsukcesowniejszym strażnikiem naszych danych gromadzonych przez administrację publiczną był chaos. Teraz jednak systemy informacji i rejestry są porządkowane i systematyzowane. To konieczne, tyle tylko że jedynymi osobami, które wiedzą, co w którym systemie się znajduje, nie są prawodawcy ani urzędnicy, tylko informatycy i autorzy logarytmów. Chciałbym wiedzieć, kto tych ludzi zatrudnia i czy państwo wie, jakie systemy informacyjne posiada i jak są one połączone.

A także kto jest „odzwierciedlającym” rozdającym urzędnikom uprawnień dostęp.

No właśnie, kto nim jest?

Wbrew pozorom sznurki nie zbiegają się w ABW albo w CBA. Mnóstwo z nich zbiega się u wójta, burmistrza, prezydenta miasta lub wojewody, którzy mają dostęp np. do rejestru PESEL, ewidencji gruntów i budynków, rejestru związanego z podatkami lokalnymi i wielu, wielu innych.

Dodatkowo sprawę komplikuje wdrażanie unijnych zasad dotyczących ponownego wykorzystania informacji pochodzących z sektora publicznego. W efekcie informacja publiczną staje się duża liczba danych pochodzących z rejestrów publicznych, zawierających również dane osobowe. Podmioty z sektora gospodarczego lub non profit mogą pozyskiwać informacje publiczne i powtórnie je wykorzystywać, także w celach komercyjnych.

O ile organy władzy publicznej są uprawnione do przetwarzania danych osobowych tylko wówczas i tylko w takim zakresie, na jaki zezwalają im przepisy prawa, na podstawie których działają, o tyle gdy posiadane przez nie dane osobowe zostaną uwolnione do przestrzeni publicznej, sytuacja jest odwrotna: można z nimi zrobić wszystko, czego prawo wyraźnie nie zakazuje. Moim zdaniem nie jesteśmy do tego przygotowani.

Są jeszcze rejestry centralne, takie jak System Informacji Oświatowej czy planowany System Informacji Medycznej. Czy dostęp do tak dużych zbiorów danych nie zagraża naszej prywatności?

Budowanie rejestrów centralnych jest niebezpieczne z dwóch powodów. Istnieje możliwość, że Wielki Brat – państwo – będzie nas śledził, ale ja bym nie przesadzał z tym zagrożeniem. Poza służbami specjalnymi i policją, które mogą mieć w tym pewien interes, to organy takie jak Ministerstwo Zdrowia nie są chyba zainteresowane, by śledzić np. historię naszych operacji plastycznych.

Ktoś jednak mógłby zestawić dane z różnych rejestrów publicznych, w tym SIM, budując nasz profil. Istnieje też niebezpieczeństwo wycieku, np. ataku „Man in the middle”, kiedy podstawiony np. przez prywatną firmę człowiek wykrada dane przesyłane między dwiema komunikującymi się stronami. To doświadczenie niektórych krajów, które wprowadziły centralne rejestry. Izrael stracił tak kontrolę nad odpowiednikiem naszej bazy PESEL.

Dane o nas to towar o rosnącej wartości?

Informacja o nas i naszych zainteresowaniach oraz życiowych doświadczeniach ma swoją cenę, jej przetwarzanie umożliwia robienie dobrego interesu. Najmniejszym problemem jest spam, jaki możemy otrzymywać, gdy ktoś pozyska nasze dane osobowe. →

REKLAMA

Fundacja Warszawskie Hospicjum dla Dzieci opiekuje się nieuleczalnie chorymi dziećmi w ich własnych domach. Hospicjum istnieje dzięki wsparciu ludzi, którym bliski jest los ciężko chorych dzieci. Przekaż 1 % podatku dzieciom z Warszawskiego Hospicjum dla Dzieci.

KRS: 0000097123

Fundacja
Warszawskie
Hospicjum  dla Dzieci

Twój 1% - mój powrót do domu

www.hospicjum.waw.pl



➔ Poważnym problemem może być natomiast utrata kontroli nad danymi, których pozyskanie przez osoby lub podmioty nieuprawnione może nam zaszkodzić. Do takich danych zaliczyłbym informacje dotyczące naszej sytuacji finansowej, numeru karty kredytowej czy konta bankowego, dokonywanych operacji finansowych czy też informacji o długach i ich spłaceniu. Dostęp do tych informacji powinien być limitowany, a mam wrażenie, że zbyt często są one rozdawane.

Druga grupa to informacje o naszym stanie zdrowia. Wiele instytucji, zwłaszcza ubezpieczeniowych, chciałoby mieć do nich dostęp, by obniżyć ryzyko swojej działalności. Rozumiem ich interes biznesowy, jednak ubezpieczenie to umowa, która wiąże się z ryzykiem po obu stronach.

Trzecia grupa to dane dotyczące naszego zachowania, które mogą pochodzić z bardzo wielu źródeł, np. systemów wideonadzoru, urządzeń, które emitują sygnał radiowy, czy inteligentnych liczników energetycznych.

Taki licznik zagraża mojej prywatności?

On informuje m.in., kiedy jest pani w domu. Na etapie badań naukowych jest pozyskiwanie z niego informacji np. o tym, który odcinek „Star Treka” oglądamy.

Czy użytkownicy portali społecznościowych są świadomi, jak krążą w sieci informacje zamieszczane na Facebooku?

Istnieje mit o utracie znaczenia prywatności: podobno już nie zależy nam na niej tak jak kiedyś. Polemizowałbym z tym, choć widzę, jak zachowują się ludzie w sieci, sam jestem aktywnym użytkownikiem serwisów społecznościowych. Niemniej znaczna większość ankietowanych obywateli uważa, że prywatność powinna być chroniona, i domaga się prawa do posiadania kilku tożsamości. Uważamy, że mamy prawo zachowywać się inaczej jako ojciec, inaczej



Robert Gardziński

„Mam prawo domniemywać, że Ministerstwo Kultury oraz organizacje zbiorowego zarządzania prawami autorskimi uważają, iż wkrótce otrzymają uprawnienia do przetwarzania danych osobowych

WOJCIECH RAFAŁ WIEWIÓROWSKI

jako pracownik, a jeszcze inaczej jako klient.

Inna kwestia, czy w ogóle jesteśmy w stanie zachować prywatność w tak zmieniającym się świecie. Oczywiście możemy dobrowolnie poddać się kontroli państwa albo przedsiębiorcy, uznając,

że przecież nie mamy nic do ukrycia, bo zachowujemy się poprawnie. Tyle że jest to podejście obce kulturze, w której się wychowaliśmy. Idea anioła stróża obecna w naszej kulturze nigdy nie była łączona z inwigilacją. Oczywiście naruszeń prywatności nie da się

w pełni zwalczyć, podobnie jak naszej niefrasobliwości, z jaką sami udostępniamy w sieci swoje dane osobowe. Mamy prawo popełniać głupstwa, ale musimy ponosić ich konsekwencje. Nie oznacza to jednak, że o naszą prywatność nie powinniśmy walczyć i prawnie próbować ograniczyć niepożądane zachowania w tym zakresie.

Jak globalna ocena nowej polityki prywatności Google, która integruje ponad 60 regulaminów różnych produktów firmy w jedną, spójną całość?

Inspektorzy ochrony danych osobowych z całej UE poprosili Google o przesunięcie terminu obowiązywania nowych zasad, a prośbę tę poparła Komisja Europejska. Chcemy w ciągu dwóch tygodni przygotować wspólne stanowisko w tej sprawie. Nie chodzi o ewidentne problemy z nową polityką prywatności, tylko o sam fakt, że Google jest wielkim graczem na rynku europejskim. Lepiej także dla Google, że otrzyma od nas jedno spójne stanowisko, zamiast 27 różnych, jak przy wprowadzaniu usługi Street View, w której zdjęcia ulic i budynków udostępnione są w Internecie.

Na czym polega reforma prawa ochrony danych proponowana przez Komisję Europejską?

To prawdziwa rewolucja. W UE obowiązywać będzie jedno rozporządzenie dotyczące ochrony naszych danych osobowych i będzie bezpośrednio stosowane we wszystkich krajach członkowskich. Uzupełnieniem rozporządzenia będzie dyrektywa regulująca odmienności w zakresie ochrony danych w policji i wymiarze sprawiedliwości w sprawach karnych. Rozporządzenie w zasadzie zastąpi 27, a po przystąpieniu Chorwacji 28 ustaw o ochronie danych osobowych, choć nie do końca, bo harmonizacja dotyczy tylko prawa materialnego. Nie obejmuje procedur i kontroli sądowej.

W rozporządzeniu pojawia się m.in. zasada „one stop shop”,

która polega na tym, że podmiot, wykonując pewnego rodzaju działania wspólnie z organem ochrony danych osobowych w swoim kraju, może uznawać, że te działania zostały wykonane w stosunku do 27 krajów członkowskich. To oznacza, że nie musi ich wykonywać 27 razy, bo np. jeśli zarejestruje zbiór danych osobowych – nawet tzw. wrażliwych – w jednym kraju, to automatycznie rejestracja ta zostanie dokonana w 26 pozostałych krajach członkowskich. Jednocześnie liberalizuje się przepisy dotyczące rejestracji zbiorów danych zawierających dane osobowe tzw. zwykłe. Pozostanie jednak obowiązek rejestracji zbiorów danych zawierających dane wrażliwe.

Nowa jest konieczność zgłaszania incydentów dotyczących ochrony danych. Dzisiaj np. bank, który utraci dane swoich klientów, nie ma obowiązku zgłaszania tego komukolwiek.

Klientom też nie?

Banki robią to tylko dlatego, że ujawnienie przez osoby trzecie informacji o utracie danych rujnuje ich reputację. Instytucje finansowe czy ubezpieczeniowe po prostu kalkulują, co im się bardziej opłaca: informować klientów czy nie. Lepiej, żeby miały taki obowiązek.

Dla Polaków największą nowością będzie wprowadzenie kar administracyjnych za naruszenia – bardzo dotkliwych, rzędu miliona euro czy pięciu procent obrotu przedsiębiorstwa. W tej chwili najwyższa kara, którą w wyjątkowych sytuacjach możemy wyegzekwować, to 50 tys. zł grzywny w celu przymuszenia do wykonania decyzji administracyjnej GODO. Wszystkie te zmiany mogą zacząć obowiązywać już w 2014 r.

Unia Europejska z jednej strony wzmacnia ochronę danych osobowych, a z drugiej ratyfikuje porozumienie ACTA, które umożliwia przekazywanie danych osobowych o klientach między prywatnymi firmami.

Podczas gdańskiej debaty o ACTA powiedziałem, że zdaję sobie sprawę z tego, że mogę być traktowany jako paranoik, któremu ubzdurało się, że ktoś próbuje dokonać zamachu na wolności obywatelskie. Sam uznałbym, że nim jestem, gdyby nie to, że widziałem, jakie działania były podejmowane wraz z przyjmowaniem ACTA, również w Polsce.

W zeszłym roku Ministerstwo Kultury i Dziedzictwa Narodowego uczestniczyło w przygotowaniu porozumienia pomiędzy operatorami telekomunikacyjnymi, dostawcami usług internetowych a organizacjami zbiorowego zarządzania prawami autorskimi. Jego elementem była możliwość przekazywania tym organizacjom danych osobowych osób, które np. wymieniają się plikami w Internecie.

W przygotowaniu tej umowy brały udział podmioty, które nazywają siebie przedstawicielami twórców, choć – moim zdaniem – z perspektywy prawa polskiego nimi nie są. Zwłaszcza jeśli chodzi o BSA (Business Software Alliance – przyp. A.M.), które wystawiło ministerstwu prywatny certyfikat potwierdzający, że nie jest ono „złodziejem”. To zaskakujące, że resort przyjmuje certyfikat, który nie jest, jak w przypadku ISO, certyfikatem międzynarodowej organizacji normalizacyjnej, ale dokumentem od prywatnej firmy, która jest stroną porozumienia opracowywanego w MKiDN.

Jakie były losy tego porozumienia?

Próba jego zawarcia została w zeszłym roku zablokowana m.in. przez GODO. Brak jest podstaw prawnych do wymiany pomiędzy tymi organizacjami danych osobowych użytkowników Internetu. Ministerstwo Kultury i Dziedzictwa Narodowego w tym samym czasie zgłosiło projekt uchwały wyrażającej zgodę na podpisanie ACTA i zawiesiło prace nad zablokowanym porozumieniem do czasu pojawienia się nowych

podstaw prawnych. Mam prawo domniemywać, że MKiDN oraz organizacje zbiorowego zarządzania prawami autorskimi uważają, że wkrótce otrzymają uprawnienia do przetwarzania danych osobowych.

Co to może w praktyce oznaczać?

Możliwe, że za dwa lata spotkamy się w sądzie, gdzie organizacja zbiorowego zarządzania prawami autorskimi będzie twierdziła, że ma prawo przekazywać za granicę dane osób naruszających prawo własności intelektualnej, a operatorzy telekomunikacyjni oraz GODO, że jest to absolutnie niedopuszczalne. Jeżeli tak się stanie, to chciałbym wiedzieć, do czego Polska się zobowiązała, składając podpis pod ACTA. Czy podpisała traktat, który miał zmieniać prawo polskie, czy też umowę, która jedynie petryfikuje „doskonały europejski system ochrony praw własności intelektualnej” i ma zamiar rozszerzać tę ideę na pozostałe kontynenty świata? Jeśli to drugie rozwiązanie jest prawdziwe, to napiszmy to wprost, tak jak napisała to Rada Unii Europejskiej, przyjmując ACTA. Co ciekawe, ci sami urzędnicy działający w ramach polskiej prezydencji potrafili napisać uzasadnienie dla Rady UE. Uzasadnienia dotyczącego podpisania tego traktatu przez Polskę nikt nie widział.

Dlaczego porozumienie ACTA nie było konsultowane przez GODO?

Tego nie wiem, choć wydaje mi się, że jako organ wydający dane osobowe powinienem być w ten proces włączony. Niemniej nie obrażam się z tego powodu. Uważam nawet, że ratyfikacja tego traktatu jest możliwa – ale pod warunkiem, że ktoś udowodni, iż jest to naprawdę niezbędne. Zwłaszcza że artykuł 31 Konstytucji RP stanowi, iż ingerencja w prawa i wolności obywatelskie może być dokonywana tylko wtedy, kiedy jest to niezbędne w demokratycznym państwie prawa.

**Poradnik PIT 2011
JUŻ W KIOSKACH**

Jak łatwo i szybko rozliczyć PIT 2011

- jaki formularz wybrać i jak przesłać go do urzędu skarbowego
- ulgi i odliczenia, z których wolno korzystać
- jak poprawiać błędy w zeznaniu
- wspólne rozliczenie: z małżonkiem i z dzieckiem



Wewnątrz broszury znajdziesz kod do programu do rozliczenia PIT

RZECZPOSPOLITA

rp.pl/hity