Beata Marek

Rozmowa z dr Wojciechem Wiewiórowskim Generalnym Inspektorem Ochrony Danych Osobowych (Conversation with Polish Inspector General for the Protection of Personal Data)

Beata Marek: Zacznijmy od „ciasteczek". Otóż jednym z argumentów powoływanych przez ich przeciwników jest twierdzenie, że mechanizm ten działa poza wiedzą i zgodą użytkowników końcowych, a tym samym narusza ich prywatność. Czy zrewidowany art. 5 (3) dyrektywy 2002/58/WE e-privacy wpłynie na to, że te obawy nie będą już podnoszone?

Generalny Inspektor Ochrony Danych Osobowych: „Ciasteczka" są rzeczywiście problemem. Już na poziomie dyrektywy o prywatności i łączności elektronicznej tak naprawdę mamy do czynienia z pewnym błędem w założeniach. Przyjmuje się, że cookies to jednolite rozwiązanie czy też jedna grupa rozwiązań. Tymczasem cookies bardzo się od siebie różnią. O ile zarzuty dotyczące ochrony danych osobowych i ochrony prywatności rzeczywiście mają duży sens przy tzw. tracking cookies, o tyle przy innego rodzaju „ciasteczkach", które są dołączane do różnego rodzaju stron czy serwisów internetowych, te obawy nie są wystarczająco uargumentowane. To spowodowało swego rodzaju rozdarcie GIODO przy pracach nad nowelizacją Prawa telekomunikacyjnego, którą kwestie *cookies* były objęte. Gdybyśmy bowiem, z jednej strony, chcieli stosować literalne brzmienie przepisów dyrektywy, to nowe rozwiązania trzeba byłoby odnieść do wszystkich rodzajów cookies i jedynie rozwiązania typu *opt-in* uznać jako jedyne możliwe do zastosowania. Jednak z drugiej strony, spowodowałoby to konieczność wielokrotnego wyrażania zgody na ich stosowanie w serwisach internetowych. Moglibyśmy doprowadzić do sytuacji, w której literalne wdrożenie zapisów dyrektywy tak naprawdę działałoby przeciwko ochronie prywatności, ponieważ użytkownik ciągle pytany o zgodę dotyczącą cookies albo wyrażałby ją bez zastanowienia i godził się na wszystko, albo w ogóle zniechęciłby się do idei prywatności, gdyby miała prowadzić do stosowania tego typu rozwiązań.

Biorąc pod uwagę interpretacje ze strony Komisji i dyskusje, które toczyły się w innych krajach, zdecydowaliśmy się nie protestować przeciwko ostatecznemu rozwiązaniu, które pojawiło się w polskim Prawie telekomunikacyjnym, uznając je za akceptowalne. Aczkolwiek to określenie – akceptowalne - jest chyba jedynym, którego jestem w stanie użyć w stosunku do nowego brzmienia przepisu. Faktycznie powoduje on powstanie systemu opt-out, który jest pewnego rodzaju wyjątkiem od rozwiązań, które do tej pory były stosowane w polskim prawie. Można więc powiedzieć, że zaakceptowaliśmy propozycję kompromisową, zdając sobie sprawę z tego, że jako GIODO narażamy się na zarzuty niewystarczająco silnej ochrony prywatności, co było założeniem dyrektywy o prywatności i łączności elektronicznej. Aczkolwiek podkreślam, że patrząc na wypowiedzi przedstawicieli Komisji Europejskiej dotyczące interpretacji projektu, jestem zdania, że jest to uzasadnione odstępstwo od takiego literalnego brzmienia przepisów. Jak one będą działały w praktyce, również w odniesieniu np. do strony internetowej GIODO, to wciąż otwarte pytanie.

BM: Nawiązując do opinii Europejskiego Inspektora Ochrony Danych Osobowych w sprawie neutralności sieci, zarządzania ruchem oraz ochrony prywatności i danych osobowych (Dziennik Urzędowy C 034 , 08/02/2012 P. 0001 - 0017), w której dostrzeżono problem stosowania przez dostawców usług internetowych „polityki zarządzania ruchem" jestem ciekawa czy zdaniem dra w prawie należy bardziej szczegółowo określić obowiązki nakładane na providerów związane z neutralnością sieci?

GIODO: Jestem przeciwnikiem wprowadzania re-

gulacji prawnych dotyczących neutralności sieci. Uważam, że to powinna być część rozwiązań, które są najpierw sprawdzone na rynku, a dopiero potem ewentualnie podejmowane są jakiekolwiek decyzje prawne w tym zakresie. Z drugiej strony jestem przeciwny rozwiązaniom, które miałyby prowadzić do nadzoru i blokowania treści, które pojawiają się w Internecie.

BM: A czy dr zgadza się z twierdzeniem, że polskie przepisy dotyczące retencji danych pozwalają na zbyt łatwy dostęp do danych organom ścigania? Jak dostęp ten powinien być uregulowany w zgodzie z ochroną danych osobowych obywateli?

GIODO: Zdecydowanie zgadzam się z opinią, że polskie przepisy dotyczące retencji danych telekomunikacyjnych wciąż nie są zadowalające. O tym, że to dla GIODO bardzo istotny problem, świadczy m.in. fakt, że już 2 lata temu tematem przewodnim Dnia Ochrony Danych Osobowych (28 stycznia 2011 r.) była właśnie ta kwestia. Uważaliśmy już wtedy, że korekta przepisów w tym zakresie jest absolutnie niezbędna. Niestety, wciąż jej nie ma, bo trudno za sukces uznać kosmetyczne zmiany przy ostatniej nowelizacji Prawa telekomunikacyjnego.

Uważam też, że dyrektywa jest napisana źle, przez co jest narzędziem nieadekwatnym i, co więcej, kompletnie nieskutecznym. Przypominam, że pojawiła się jako rozwiązanie z zakresu prawa ochrony konkurencji i miała doprowadzić do tego, by operatorzy na rynku europejskim mieli mniej więcej takie same obowiązki, niezależnie od tego, czy działają w Niemczech, Francji, Austrii czy w Estonii. Jednak kilka krajów Unii Europejskiej w ogóle jej nie wdrożyło, a te, które wprowadziły rozwiązania w tym zakresie, zastosowały je w sposób na tyle różny i na tyle różnie odnoszący się do obowiązków operatorów telekomunikacyjnych, że nawet z punktu widzenia ochrony konkurencji zakładany cel zupełnie nie został osiągnięty. Natomiast niektóre państwa zaczęły wykorzystywać ją jako narzędzie z zakresu bezpieczeństwa. Niemniej implementacja rozwiązań dotyczących retencji danych w wielu krajach wywołała burzliwe spory, jak np. w Bułgarii, Rumunii, Czechach, Szwecji, Austrii i na Węgrzech, a Niemcy nawet wycofali się z ich wdrożenia.

To powoduje, że jestem wielkim zwolennikiem zmiany dyrektywy, a tym samym jestem mocno niezadowolony z tego, że prace, które są w tym zakresie prowadzone, trwają tak długo i nie przynoszą żadnych realnych efektów.

Wracając do oceny rozwiązań, które przyjęto w Polsce, trzeba podkreślić, że były one najdalej idącymi z możliwych. Niemniej kwestia okresu obowiązkowej retencji danych jest tu, oczywiście, sprawą najmniej istotną. To, że wcześniej okres ten wynosił 24 miesiące, a po zmianie Prawa telekomunikacyjnego wynosi 12 miesięcy, nie oznacza, że sytuacja poprawiła się dwukrotnie czy też, że mamy o 50% lepsze rozwiązania niż wcześniej. W odniesieniu do rynku internetowego, problemem jest to, jakiego rodzaju dane mogą być zbierane. To nie jest określone wprost w przepisach polskich, toteż uznać można, że Polska nie dokonała wdrożenia dyrektywy w odpowiedni sposób.

Jeśli zaś chodzi o rynek telekomunikacyjny, to najpoważniejszym problemem jest kwestia dostępu do danych retencyjnych. Wątpliwości GIODO budzi przyjęte w Polsce rozwiązanie, które umożliwia niektórym służbom dostęp do danych telekomunikacyjnych przy pomocy specjalnego interfejsu. Nie przekonują mnie tłumaczenia, że ograniczono liczbę policjantów, którzy mają dostęp do tych danych, że istnieje śladowanie, które pozwala zweryfikować, który policjant, do których danych miał dostęp. O ile bowiem faktycznie takie rozwiązania wprowadzono w praktyce, o tyle nie przewidują ich polskie przepisy. Poza tym uważam, że jest to zbyt duży dostęp, do zbyt dużego zakresu danych, przy zbyt dużej liczbie zdarzeń, o które może chodzić. Niech świadczy o tym fakt, że kiedy GIODO zapytał się policji i służb, jakie przestępstwa uważają za poważne (ustawa ich nie wymienia, a zarazem dostęp do danych możliwy jest przy „przestępstwach poważnych"), to otrzymaliśmy bardzo różne odpowiedzi. Jedna ze służb wskazała, że wszystkie przestępstwa, którymi się zajmuje, są poważne. Druga przekazała informację, że „właśnie czeka na wytyczne GIODO dotyczące tego, co jest poważnym przestępstwem".

Od innych służb, które odpowiedziały na nasze pytanie, oraz od policji, otrzymaliśmy wewnętrzne instrukcje mówiące o tym, które przestępstwa należy traktować jako poważne. Abstrahując od faktu, że ten bardzo ważny element regulowany jest na poziomie aktów wewnętrznych, co jest sprzeczne z prawem, w tym z Konstytucją RP – powinno być to bowiem uregulowane w ustawie i rozwinięte w przepisach rozporządzenia - to te instrukcje były różne. Inną instrukcją posługuje się Policja, a innymi służby specjalne. To wyraźnie pokazuje, że jest konieczność ujednolicenia choćby rozumienia definicji poważnego przestępstwa. Inna sprawa, że przez nieprawidłową implementację dyrektywy doprowadziliśmy do tego, że dane te mogą być wykorzystywane w postępowaniach cywilnych, przede wszystkim w sprawach rozwodowych. Nie jest to z pewnością walka z terroryzmem, a więc kwestia zapewnienia bezpieczeństwa.

BM: Pozostając jeszcze na chwilę w temacie retencji danych chciałabym się spytać dra czy mrożenie danych ma szansę zastąpić retencję danych? Jeśli tak to w czym jest lepszy ten model archiwizacji danych?

GIODO: Retencja jako zjawisko i tak będzie istniała. To nie jest tak, że jestem przeciwny rozwiązaniu, jakim jest retencja danych. Jest ona potrzebna choćby dla rozpatrywania reklamacji klientów. Co do mrożenia to jest oczywiście idea, którą bardzo popiera np. Panoptykon. Natomiast ja przyznaję, że wciąż nie do końca rozumiem, czym różni się proponowane mrożenie od rozwiązań, które istnieją dzisiaj i które też powodują, że pewien zestaw danych, o który wnioskowała policja miałby zostać zachowany na jej potrzeby.

Oczywiście rozumiem, że w przypadku mrożenia danych pozostawałyby one po stronie operatora, a policja mogłaby do nich tylko ewentualnie sięgać, a w przypadku dzisiejszych rozwiązań dane te są transportowane do policji i tam przetwarzane. Jeżeli tylko o to chodzi, to mrożenie podoba mi się bardziej, choć nakłada na operatorów telekomunikacyjnych dodatkowe obowiązki. Powstaje w związku z tym pytanie, czy można nakazać operatorom telekomunikacyjnym przechowywanie danych, które tak naprawdę są potrzebne policji. Być może jest to ciekawe i dobre rozwiązanie. Nie jestem jednak przekonany, czy ono tak naprawdę wiele zmienia. Dla mnie najbardziej istotną kwestią jest to, w jakich sprawach można sięgać do danych oraz czy można to robić bez żadnej kontroli zewnętrznej, choćby *post factum*. Tu jest bardzo poważny problem dodatkowy, który trzeba byłoby rozważyć. Rozumiem zastrzeżenia ze strony policji i służb, że dane z retencji niekiedy potrzebne są natychmiast, w tym znaczeniu, że nie ma czasu na przeprowadzenie procedury, która miałaby zezwalać na dostęp do tych danych, że przeprowadzenie tego typu procedury byłoby de facto fikcją. Być może więc pomysłem jest dokonywanie oceny *post factum*, czyli oceny, w jakich sytuacjach i celach dane retencyjne zostały wykorzystane. Gdyby wówczas okazało się, że zostały one pozyskane lub wykorzystane nieprawidłowo, można byłoby nakazać ich zniszczenie. To rozwiązanie jest jednak bardzo niewygodne dla policji, ponieważ każda kontrola post factum zakłada, że w momencie kiedy okaże się, że funkcjonariusz zażądał danych, które nie były potrzebne albo nie było żadnych podstaw do ich uzyskania, to powinna pojawić się kara. Jest to zatem dla policji i służb niewątpliwie temat trudny, ponieważ mogący wpływać na ograniczanie działań tam, gdzie one faktycznie byłby potrzebne.

BM: Nie ulega wątpliwości, że podniesione przez dra postulaty zarówno w odniesieniu do frywolnej interpretacji „poważnego przestępstwa" oraz zakresu i sposobu pozyskiwanych danych są bardzo ważne i wymagają podjęcia konkretnych działań na drodze legislacyjnej. Mam nadzieję, że wydarzy się to w niedalekiej przyszłości.

W kolejnym pytaniu chciałabym się odnieść do zyskującej na znaczeniu chmury. W czasie kryzysu każdy podmiot szuka oszczędności i m.in. dlatego od pewnego czasu obserwujemy tzw. „boom" na usługi w chmurze. Martwi mnie jednak fakt, że wielu przedsiębiorców wciąż jeszcze nie zdaje sobie sprawy z zagrożeń chmury oraz obowiązków wynikających z przepisów o ochronie danych osobowych. Pomimo swej niewiedzy decyduje się na

outsourcing w chmurze – co może wywołać przysłowiowe gradobicie (np. nie są zawierane umowy powierzania albo outsourcowane są dane osobowe poza Europejski Obszar Gospodarczy sprzecznie z przepisami ustawy). Jakie zdaniem dra są największe zagrożenia związane z chmurą i co jest absolutnym „must have" przy przejściu do tego modelu biznesowego?

GIODO: W odniesieniu do chmury często używam motta (które powinni stosować Ci, którzy chcieliby z usług chmurowych korzystać) mojego rodzinnego miasta czyli Gdańska – nec temere nec temide (pol. bez strachu, ale z rozwagą). Tak dokładnie trzeba podchodzić do usług chmurowych. Jest oczywiste, że ten model biznesowy będzie coraz częściej stosowany przy różnego rodzaju usługach. Nie można też twierdzić, że w ogóle nie należy z chmury korzystać, bo ona jest niebezpieczna. Trzeba korzystać, ale z rozsądnym spojrzeniem na to, co się dzieje. W 2012 roku unijni rzecznicy ochrony danych osobowych opublikowali dwa zestawy wskazań dotyczących tego, jak podchodzić do usług chmurowych. Pierwsze to memorandum sopockie, które zostało wydane przez tzw. Grupę Berlińską (grupę do spraw ochrony prywatności w telekomunikacji). Drugie to opinia Grupy Roboczej Art. 29 (zrzeszającej odpowiedników GIODO z wszystkich państw UE) przyjęta w lipcu 2012 r. Dokumenty te zwracają uwagę na najważniejsze kwestie, które przy stosowaniu *cloud computing*u powinny być brane pod uwagę. Uwzględnić trzeba m.in. to, że czym innym jest ochrona danych osobowych w chmurze, a czym innym ochrona tajemnic prawnie chronionych. Umieszczanie w chmurach danych, które są objęte tajemnicą lekarską, adwokacką czy radcowską lub innymi rodzajami tajemnic prawnie chronionych albo informacji, które są informacjami niejawnymi w rozumieniu ustawy o ochronie informacji niejawnych może powodować problem z punktu widzenia tych przepisów. Najprostszym przykładem jest niemożność umieszczania w chmurze, która znajduje się poza Polską, informacji niejawnej, która ze względu na bezpieczeństwo państwa chroniona jest odpowiednią klauzulą.

Z punktu widzenia ochrony danych osobowych jest dla mnie oczywiste, że podmiot, który decyduje się na skorzystanie z usługi albo infrastruktury chmurowej, powinien rozważyć, czy musi zastosować art. 31 ustawy o ochronie danych osobowych odnoszący się do powierzania przetwarzania danych. W niektórych sytuacjach należy bowiem zawrzeć umowę w tym zakresie, a w niektórych nie trzeba. Gdy mamy do czynienia z danymi tzw. zwykłymi i są one szyfrowane i w tej postaci przenoszone do infrastruktury chmurowej, to można się zastanawiać, czy po stronie dostarczyciela chmury w ogóle dochodzi do przetwarzania danych, czy jest on tylko hosterem. Niemniej jeżeli mówimy o rozwiązaniu typu SaaS, jest to już znacznie mniej prawdopodobne. Nawet jeżeli umieścimy zaszyfrowaną informację, to i tak będzie ona odszyfrowana przez oprogramowanie, które będzie działało w chmurze, po to, by mogła zostać przetworzona. A to już oznacza, że ktoś przynajmniej teoretycznie może do tej informacji mieć dostęp.

Zwracam więc uwagę na konieczność przeprowadzenia analizy każdego z rozwiązań chmurowych, które ma być zastosowane oraz z zasady unikania umów adhezyjnych (umów, których nie negocjujemy). Warto pamiętać jednocześnie, że możliwość negocjowania umowy spoczywa na administratorze danych osobowych (dalej ADO). ADO, przekazując dane przetwarzającemu – procesorowi, nie gubi odpowiedzialności za te dane, w stosunku do których decyduje o celach i środkach ich przetwarzania. Cały czas ta odpowiedzialność zarówno za dane, jak i sposób ich przetwarzania spoczywa na nim. W związku z tym ADO musi sobie zapewnić kontrolę nad tym, w jaki sposób dane są przetwarzane przez podmiot, któremu zostały powierzone. I tu ciekawostka. Z reguły umowy, które trafiają do ADO zamierzających skorzystać z usług chmurowych, nie zawierają żadnych klauzul dotyczących możliwości przeprowadzenia kontroli. Natomiast gdy ADO wskaże, że taką kontrolę chciałby sobie zapewnić, to okazuje się, że istnieje również druga wersja umowy, która już zawiera rozwiązania dotyczące kontroli. Zatem to, że w umowie, którą nam przedstawiono, nie znajdują się takie rozwiązania, a nam wydaje się, że niemożliwe jest przeprowadzenie zewnętrznej kontroli, nie wyłącza wcale naszej

odpowiedzialności za to, że zrezygnujemy z jednego z podstawowych obowiązków, które leżą po stronie ADO.

BM: No właśnie. W praktyce widać, że nie ma jednolitej polityki po stronie providerów w zakresie podejścia do klienta oraz informowania go.

GIODO: I dobrze. Rynek konkurencji polega na tym, że różne podmioty mają różną politykę. Wręcz niepokoiłaby mnie sytuacja gdyby powstał kartel. Dlatego polityki są różne. Dobrze żeby były dobre.

BM: Nie miałam na myśli stworzenia kartelu. Mi chodziło o obecną sytuację gdzie jest skrajnie różna polityka informacyjna po stronie providerów. Moim zdaniem powinny być pewne obowiązki informacyjne nałożone na wszystkich usługodawców takie same. Np. informowania o tym, że provider nie posiada własnej infrastruktury informatycznej tylko „dzierżawi ją". Miałam taki przypadek, że zwrócił się do mnie podmiot, któr miał problem z providerem oferującym usługę chata w modelu SaaS. Usługodawca nie wyrażał zgody na podpisanie umowy powierzania zasłaniając się twierdzeniem „jesteśmy zarejestrowani w GIODO, a zatem nie ma potrzeby takiej umowy zawierać". Dodam, że działał w IaaS co zatajał przed potencjalnym klientem (odpowiednia umowa podpowierzania także nie zostałaby zawarta). Dodatkowo dane były przetwarzane poza Europejskim Obszarem Gospodarczym o czym potencjalny klient nie został poinformowany (to wykazał przeprowadzony przeze mnie audyt).

GIODO: Oczywiście taki przypadek jest karygodny. To, że ktoś zarejestrował swój zbiór w rejestrze prowadzonym przez GIODO, po pierwsze, nie oznacza, że na pewno wypełnia obowiązki wynikające z ustawy, po drugie ten usługodawca wyraźnie wskazał, że jego zbiór został zarejestrowany, co oznacza, że nasze dane osobowe chce dołączyć do swojego zbioru. Innymi słowy on będzie ADO, a więc podmiotem, który będzie decydował o celach i środkach przetwarzania danych. Jeżeli więc ktoś nam mówi, że ma już przecież zgłoszoną bazę, to oznacza to, że nie traktuje nas jak ADO, tylko uważa, że to on nim będzie. Z pewnością w tym momencie powinno zapalić się nam już nie żółte, ale czerwone światełko. Natomiast dotknęła Pani innego problemu, który może się pojawić, i z którym bardzo trudno sobie radzić. To jest sytuacja, w której tym providerem usług chmurowych nie jest tak naprawdę dostarczyciel chmury. On zaś jest tylko pośrednikiem w kontakcie z tymi, którzy chmurę „posiadają". Dostarcza usługę, którą stworzył, ale nie na swoich zasobach. Taka sytuacja jest niekiedy nazywana stosem chmur. Polega na tym, że my tak naprawdę kontaktujemy się z obłoczkiem, a ten obłoczek będzie nasze dane przetwarzał w chmurach, których sam nie jest właścicielem. I to jest bardzo skomplikowana sytuacja. Musimy zdawać sobie sprawę z tego, jakie umowy i z jakimi podmiotami ma zawarte usługodawca, z którym chcemy zawrzeć umowę. Może się okazać, że tylko on działa na terenie Polski, a chmury umieszczone są poza obszarem EOG.

BM: Dokładnie. Projekt rozporządzenia unijnego zaprezentowanego w styczniu 2012r., które ma zastąpić unijną dyrektywę z 1995 r. jest uważany za dość rewolucyjny. Czy faktycznie tak jest?

GIODO: Moim zdaniem, projekt nie jest nadzwyczaj rewolucyjny, choć pojawiają się w nim pewne nowe zasady. Swego rodzaju rewolucją jest zapewne to, że zniknie 27 ustaw krajowych, a zamiast nich pojawi się jeden akt prawny na poziomie europejskim. To, oczywiście, jest uproszczenie, bo ustawy odnoszące się do ochrony danych osobowych w poszczególnych krajach będą musiały istnieć. Rozporządzenie nie reguluje bowiem sposobu ukształtowania organu ds. ochrony danych osobowych ani kwestii kontroli sądowej. Natomiast pojawia się wiele rozwiązań nowych, bardzo dobrych – np. wiążące reguły korporacyjne. Mi, jako GIODO, bardzo ich brakuje. Obecnie ani polskie, ani europejskie prawo nie przewiduje bowiem istnienia BCR, więc pojawienie się ich w rozporządzeniu jest bardzo dobrym rozwiązaniem. Z drugiej jednak strony niektóre z zasad, które przewidziano rozporządzeniu jako nowe, są albo rozwinięciem zasad już istniejących, albo próbą doprecyzowania pewnych filozoficznych pomysłów, które do tej pory były wyrażane w doktrynie. Za takie przypadki uważam zasadę przenaszalności danych (ang. portability),

prawo do bycia zapomnianym, privacy by design i privacy by default. W tym zakresie niewątpliwie pojawiają się nowe rozwiązania . Wielokrotnie jest to uszczegółowienie i odniesienie do nowych rozwiązań technologicznych, co czasem powoduje problem, np. przy zasadzie przenaszalności danych. O ile jest ona zrozumiała, oczywiście przy wszystkich zastrzeżeniach, w przypadku przenoszenia pomiędzy portalami społecznościowymi, o tyle nie bardzo wiem, jak miałaby funkcjonować, jeżeli dotyczyłaby np. ubezpieczycieli. Czy to oznacza, że wszystkie informacje, które posiada o mnie ubezpieczyciel A mogę od niego zabrać i przekazać darmowo ubezpieczycielowi B? Są sytuacje, w których możemy mieć co do tego wątpliwości. Przykładowo jeżeli oferta, która została mi przedstawiona, bazuje na badaniach lekarskich, za które zapłacił ubezpieczyciel A, to mimo iż są to dane o mnie, czyli powinienem mieć do nich dostęp. Natomiast wcale nie jest takie oczywiste, czy mogę je zabrać ubezpieczycielowi A i przedstawić ubezpieczycielowi B.

Jestem generalnie zwolennikiem tego rozporządzenia. Uważam, że to dobry pomysł, również od strony formalnej. Czeka nas jednak jeszcze poważna dyskusja co do ostatecznego kształtu przepisów. Ta dyskusja już się toczy i my jako Biuro GIODO uczestniczymy w niej jako eksperci po stronie polskiej, biorąc udział m.in. w spotkaniach Grupy Roboczej ds. wymiany informacji i ochrony danych DAPIX. Bierzemy także aktywny udział w pracach Parlamentu Europejskiego. Podczas dwudniowej konferencji PE z 27 parlamentami krajowymi, miałem zaszczyt wygłosić wykład na temat dyrektywy, czyli drugiego aktu, który jest dołączony do pakietu proponowanych zmian. Uważam, że jest to regulacja, która jest w Polsce niezbędna. Oczywiście wiem o wszystkich zastrzeżeniach, które zgłaszają inne kraje członkowskie, ale wszystko, co proponuje dyrektywa, jest lepsze niż przepisy obecnie obowiązujące w Polsce. W związku z tym jestem absolutnym zwolennikiem rozwiązań, które tam zaproponowano.

BM: A co dr sądzi o projektach typu Google Glass oraz Facedeals?

GIODO: Są to bardzo ciekawe projekty. Szczerze mówiąc, w jakimś stopniu brakuje mi tego typu rozwiązań technicznych na rynku. Rozwiązań, dzięki którym miałbym taką rozszerzoną rzeczywistość, która umożliwiałaby natychmiastowy dostęp do Wikipedii czy innego rodzaju serwisów, dotyczących np. każdego kościółka czy komina, które znajdują przy drodze, którą jadę. Jestem osobą, która dużo podróżuje i szukam czasem informacji o miejscowościach – czasem nawet bardzo małych – przez które przejeżdżam. Np. niedawno, podczas jednej z podróży, zastanowił mnie ogromny komin stojący w polu pod Pruszkowem. Okazało się, że istnieje blog poświęcony kominom w Polsce. Można było znaleźć tam dokładne informacje o tym kominie i o tym, że powstał w związku z planowaną budową elektrociepłowni, która, jak się okazało, w efekcie nigdy nie powstała. No, ale domyślam się, że nie chce mnie Pani pytać o kominy ani informacje o XVII-wiecznych kościołach, tylko o te dane, które są danymi osobowymi. O dane, które przy pomocy Google Glass miałyby być dostępne. No i to już jest problem poważny. Z jednej strony, oczywiście, możemy powiedzieć, że każdy musi się samodzielnie zgodzić na to, żeby jego dane były możliwe do wyszukiwania przy pomocy różnego rodzaju aplikacji robionych na potrzeby takich rozwiązań.

Problem polega nawet nie na dobrowolności, lecz na tym, na ile jesteśmy poinformowani o tym, na co tak naprawdę się godzimy. Nie neguję rozwiązania jako takiego. Rozumiem jego przydatność. Sam pewnie chętnie bym z niego skorzystał, aczkolwiek bardzo ostrożnie i rozważnie. Pamiętajmy, że serwis typu Google Glass nie różni się aż tak bardzo od tego, co możemy znaleźć w Internecie. Przy pomocy tej usługi zostaną wyszukane informacje, które już dzisiaj umieszczamy w Internecie i są wyszukiwane choćby na potrzeby reklamy behawioralnej. Cały czas przypomina mi się sytuacja, z którą miałem do czynienia kilka miesięcy temu, kiedy w Internecie przypadkowo trafiłem na informację o książce, którą czytałem w dzieciństwie - „Feniks i dywan". Przez kilka minut przeszukiwałem Internet, by znaleźć informacje o niej, bo chciałem ją przeczytać swojej córce. Znalazłem wszystkie wydania, które ukazały się na rynku. Jakież było moje zdziwienie, gdy

przez następną godzinę, gdy korzystałem z zupełnie innych tematycznie serwisów, wszystkie reklamy behawioralne odnosiły się do pobliskich salonów z dywanami. Okazało się, że zostałem zgeolokalizowany i to w dodatku jako osoba szukająca dywanów. Dobrze, że nie pokazano mi, gdzie można kupić feniksy. Sądzę, że informacja, która trafiła na potrzeby reklamy behawioralnej, była zbliżona do tego, co otrzymałbym w serwisie Google Glass. W tym przypadku wyszedłbym na ulicę, a serwis pamiętałby, że niedawno szukałem feniksów i dywanów w związku z czym należy mnie poinformować, w którą stronę należy się udać, żeby owe dywany znaleźć. Oczywiście, należy pamiętać, że gdzieś odkłada się informacja dotycząca tego, czego posiadacz tych konkretnych okularów szukał w ostatnim czasie.

BM: W jaki sposób kontrolować podmioty, które zbierają aż tyle informacji na rynku europejskim? Czy jest to realnie możliwe?

GIODO: Jest to możliwe. Z jednej strony ze względu na fakt, że każdy z nas może wystąpić o to, aby dostać komplet informacji o sobie, które znajdują się w posiadaniu danej firmy. O ile jeszcze 3 czy 4 lata temu osoby, które ubiegały się o takie informacje, były wyśmiewane, o tyle obecnie firmy zdają sobie sprawę z tego, że obowiązek udzielenia informacji istnieje i są zobowiązane go respektować. Z drugiej strony większość firm ma swoje przedstawicielstwo europejskie, a GIODO poprzez współpracę z swoimi odpowiednikami w UE, a czasami poza Unią (równie dobrze współpraca wygląda jeżeli chodzi o Kanadę, Australię czy Nową Zelandię, coraz lepiej w przypadku Stanów Zjednoczonych gdzie Federal Trade Commision jest coraz bardziej aktywna na rynku prywatnym) ma możliwość wpłynięcia na to jak wyglądają polityki prywatności tego typu serwisów. Oczywiście w tym momencie przytaczam przykłady dotyczące dużych serwisów. Gorzej jest w przypadku serwisów, które oferują gry online czy wirtualne światy (część gier tworzy de facto takie światy, społeczności przywiązane do określonej gry), a których właścicielami są firmy mające siedziby w bardzo egzotycznych miejscach na świecie.

BM: Czy zgadza się dr z twierdzeniem, że prawo do bycia zapomnianym może prowadzić do ograniczenia wolności słowa w Internecie?

GIODO: Tak, zgadzam się z takim twierdzeniem. Uważam, że powinniśmy bardzo ostrożnie podchodzić do tego zagadnienia. W ostatnim czasie miałem dwa duże wystąpienia na ten temat. Pierwsze na konferencji zorganizowanej przez Agencję Praw Podstawowych w Wiedniu, drugie podczas dnia otwartego biura GIODO w Dąbrowie Górniczej gdzie zwracałem uwagę na tę kolizję, która występuje pomiędzy prawem do bycia zapomnianym, a wolnością wypowiedzi, pamiętając przede wszystkim, że nasz przepis konstytucyjny dotyczący swobody wypowiedzi jest tym samym przepisem, w którym zapisane jest prawo do przetwarzania informacji. W związku z tym to jest nie tylko wolność słowa, ale również wolność przetwarzania informacji. Na czym polega problem? Poprzez wycofanie informacji o sobie (mówię teraz tylko o informacji legalnie umieszczonej w sieci) możemy tak naprawdę wpływać na to, jak wygląda pamięć historyczna. Dwa przykłady, które dobrze to ilustrują. Po pierwsze przypadek, gdzie zabójca aktora Waltera Sedlmayra zażądał od Wikipedii usunięcia informacji o tym, że jest mordercą (tłumacząc to tym, że ma on problem z powrotem do społeczeństwa, gdyż jego nazwisko jest ciągle łączone z przestępstwem dokonanym wiele lat wcześniej). Co ciekawe, niemiecka Wikipedia wycofała dane osobowe zabójcy, ale bez trudu można znaleźć te dane w angielskiej wersji Wikipedii oraz w archiwach gazetowych. Drugi przykład dotyczy wspomnianego przeze mnie wcześniej blogu o kominach. Jest tam także napisane, kto nie wybudował elektrociepłowni i kto podejmował decyzje, skutkujące różnymi opisanymi w blogu konsekwencjami. Zapewne te osoby również mogłyby wystąpić, w ramach prawa do bycia zapomnianym o to, żeby ich dane zostały usunięte z Internetu.

Jeszcze może dodam, że w tej chwili toczy się postępowanie dotyczące z jednej strony neutralności sieci, a z drugiej strony prawa do bycia zapomnianym. Dotyczy ono Maxa Mosleya (jest to dobrze znane nazwisko wszystkim osobom, które interesują się wyścigami samochodowymi, jako że był on szefem Formuły 1). W pewnym momencie w sieci

pojawiły się zdjęcia oraz nagrania dotyczące sfery prywatnej Maxa Mosleya. Wytoczył on sprawę, w której zażądał odszkodowania oraz usunięcia materiałów z serwisów należących do gazety i wygrał ją. Ale informacja się klonuje. Max Mosley od kilku lat dąży do usuwania tych materiałów z różnych miejsc w sieci i skutecznie w jakimś stopniu je usuwa. Ta informacja jednak w dalszym ciągu się klonuje i pojawia w nowych miejscach. Jaki jest nowy pomysł Maxa Mosleya? Pozwał Google. Uznał, że ten podmiot powinien doprowadzić do sytuacji, gdy w wynikach wyszukiwania nie będą znajdowały się informacje dotyczące zdarzenia, które niewątpliwie narusza prywatność Maxa Mosleya. Google odpowiada, że może nawet by się na to zgodził w przypadku Maxa Mosleya, natomiast co stanie się, jeżeli pozostałe 6 mld ludzi na Ziemi zgłosi zastrzeżenia co do informacji, które na ich temat pojawiają się w różnych miejscach w sieci. Czy też mają być filtrowane z wyników wyszukiwania?

W związku z tym próba wpłynięcia na usunięcie danych z Internetu nie dość, że jest nieskuteczna, to może wywołać efekt przeciwny – tzw. efekt Barbry Streisand, polegający na tym, że jak coś bardzo chce się ukryć, to ukrywana treść staje się bardziej widoczna. Barbra Streisand zaprotestowała kiedyś przeciwko albumowi zdjęć wybrzeża Kalifornii, gdzie znajdowało się zdjęcie jej posiadłości. Ten album nie był specjalnie popularny do czasu, kiedy Barbra Streisand zaprotestowała. Wtedy wszyscy zainteresowali się przede wszystkim tym, czegóż to ona nie chciała pokazać.

BM: Niewątpliwie potęga Google tkwi w ilości i różnorodności informacji oraz m.in. skali ich odbioru. Z powodzeniem można powiedzieć, że na Google spoczywa też swego rodzaju odpowiedzialność w zakresie dostarczania tychże informacji. Ingerowanie w treści znajdujące się w Internecie jest sprawą bardzo delikatną i powinno mieć moim zdaniem zawsze incydentalny charakter.

Na koniec przenieśmy się na chwilę myślami do przyszłości. Czy zdaniem dra e-administracja będzie opierała się wyłącznie na biometrycznych systemach uwierzytelniania znanych z filmów *science fiction*? Przykładowo będzie liczył się odcisk palca, skan siatkówki oka, a nie posiadany dowód osobisty czy złożony podpis na dokumencie.

GIODO: Mam nadzieję, że nie. Mam nadzieję, że biometria będzie jedną z opcji, którą będzie można stosować. Natomiast nie będzie się przymuszało do tego, aby wszystkie dane biometryczne i to wszystkich obywateli były przetwarzane w systemach. Ja, oczywiście, nie chcę się wypowiadać na temat tego, czy skan siatkówki oka może być niebezpieczny ze względu na stan pseudo-nauki, jaką jest irydologia. Tak czy inaczej nie wiemy, jak te dane biometryczne mogą być wykorzystane w przyszłości.

Pamiętajmy, że niektóre z danych biometrycznych, a szczególnie dane genetyczne, w jeden zasadniczy sposób różnią się od jakichkolwiek danych osobowych. Są naprawdę niezmienne. Nawet imię i nazwisko, nr PESEL, nr NIP można zmienić w ekstremalnych sytuacjach w życiu. Natomiast genomu nie zmienimy. W związku z tym, jeżeli raz skompromitujemy genom czy pewne rodzaje informacji biometrycznych, to nigdy więcej nie będziemy mogli ich odtworzyć w sposób neutralny na nowo. Tym samym zalecałbym dużą ostrożność w przypadku biometrii.

Trudno jest też dobrze zdefiniować dane biometryczne. W niektórych przypadkach jesteśmy pewni, że mamy do czynienia z danymi biometrycznymi, a w niektórych nie. Przykładowo kartka z odręcznym pismem zawiera dane biometryczne. Można pismo ocenić grafologicznie. Można też zmierzyć np. nacisk na kartkę. Ale czy skan lub kserokopia takiego dokumentu zawierają w dalszym ciągu dane biometryczne? A w końcu czy to oznacza, że każdy własnoręcznie podpisany dokument zawiera dane biometryczne? Zalecałbym dużą ostrożność. Tam gdzie biometria miałaby służyć do identyfikacji osoby i w szczególności do uwierzytelniania się w systemach należałoby zachować dużą ostrożność i dać możliwość wyboru. Już dzisiaj pojawiają się np. bankomaty biometryczne w Polsce, ale są bardzo rozsądnie wprowadzane. Można pozostać przy zwykłej karcie bankomatowej, a można zrezygnować z karty i posługiwać się danymi biometrycznymi. Do

momentu, w którym nie ma preferencji w stosunku do danych biometrycznych, czyli np. nie dostaje się lepszej oferty, jeżeli stosuje się dane biometryczne, to można mówić, że jest to dobrowolnie wyrażona zgoda osoby.

BM: Dziękuję za rozmowę.

GIODO: Również dziękuję za rozmowę.

PATRONAT MEDIALNY

Z przyjemnością zapraszamy Państwa na wyjątkowe wydarzenie jakim jest debata:

Ochrona prywatności w obliczu nowych technologii

20 marca 2013r.
Collegium Iuridicum II
Biblioteka Uniwersytetu Warszawskiego (ul. Lipowa 4)
WSTĘP NIEODPŁATNY

Organizatorem wydarzenia jest fundacja Bezpieczna Cyberprzestrzeń przy wsparciu radcy prawnego Artura Piechockiego oraz interdyscyplinarnego koło naukowego badań nad Internetem i nowoczesnymi technologiami „Cyberlaw". Formuła spotkania bazuje na przedstawianiu dwóch odmiennych poglądów na dany temat z zakresu ochrony prywatności w obliczu nowych technologii, prezentowanych przez dwóch ekspertów.

PROGRAM DEBATY:

1. Generalny Inspektor Ochrony danych Osobowych Wojciech Wiewiórowski – wykład wstępny;
2. Arwid Mednis (Wierzbowski/Eversheds), adwersarz - Katarzyna Szymielewicz (Fundacja Panoptykon) – ochrona przed naruszeniami a prawo do prywatności;
3. Xawery Konarski (Traple, Konarski, Podrecki), adwersarz - Igor Ostrowski (Salans) – ochrona danych osobowych/prywatność a reklama behawioralna;
4. Tomasz Grzegory (Google), adwersarz - Mariusz Grzesiuk (Onet.pl) – ochrona danych osobowych/prywatność w usługach świadczonych drogą elektroniczną, mi.in. cookies;
5. Grzegorz Wanio (Olesiński), adwersarz - Maciej Kołodziej (naszaklasa.pl) – ochrona danych osobowych/prywatność w serwisach społecznościowych.

PATRONAT HONOROWY:

Generalny Inspektor Ochrony Danych Osobowych
Dziekan WPiA UW
Polska Izba Informatyki i Telekomunikacji