Dziennik Internautów
WYWIAD

Jak Big Data wpływa na prywatność? Czego zabrakło w Ustawie o Policji? - wywiad z Generalnym Inspektorem Ochrony Danych Osobowych

Marcin Maj, 26.01.2016

Big Data niewątpliwie przynosi korzyści, ale pewne obawy może wzbudzać pozyskiwanie danych na nasz temat z innych źródeł - zauważa dr Edyta Bielak–Jomaa (GIODO) w rozmowie z Dziennikiem Internautów. Tematem rozmowy była również tzw. ustawa inwigilacyjna (nowelizacja ustawa o Policji) oraz unijna reforma ochrony danych.

Nasza redakcja od kilku lat angażuje się w coroczne obchody **Dnia Ochrony Danych Osobowych**, który przypada na 28 stycznia (w rocznicę otwarcia do podpisu Konwencji 108 Rady Europy). W tym roku obchody dnia obejmują wiele imprez. O niektórych już pisaliśmy, a informacje o innych znajdziecie na stronie GIODO.

W tym roku tematem przewodnim obchodów jest zagadnienie Big Data. Dziennik Internautów miał okazję krótko rozmawiać na ten temat z dr Edytą Bielak-Jomma, Generalnym Inspektorem Ochrony Danych Osobowych. Rozmawialiśmy też o innych bieżących tematach takich jak nowelizacja Ustawy o Policji.

Marcin Maj, DI: W tym roku głównym zagadnieniem Dnia Ochrony Danych osobowych jest „Big Data". Nierzadko można spotkać się z opiniami, że tak naprawdę Big Data jest zjawiskiem nie do opanowania. Mowa o przetwarzaniu wielu danych na ogromną skalę i na całym świecie, w różnych krajach i na różnych kontynentach. Co mogą zrobić organy ochrony danych, takie jak GIODO, aby do świata Big Data wprowadzić dbanie o prywatność?

dr Edytą Bielak-Jomaa, GIODO: Rozwój nowych technologii i globalizacja niewątpliwie spowodowały, że skala pozyskiwania, gromadzenia i wymiany informacji, w tym danych osobowych, osiągnęła niebotyczne rozmiary. Doskonalone i coraz powszechniej wykorzystywane są narzędzia analityczne, służące do zbierania z wielu źródeł licznych danych i informacji oraz wywodzenia z nich wniosków. To rodzi poważne zagrożenie dla prywatności i ochrony danych osobowych. Nie sposób jednak nie zauważyć innego aspektu tego zjawiska, jakim są korzyści, które dzięki Big Data odnosi nie tylko sektor biznesu, ale i my wszyscy.

Mówiąc to, mam na myśli m.in. rozwiązania smart city wspomagające zarządzanie siecią transportu miejskiego czy sterowanie ruchem ulicznym, ale także aplikacje, z których tak chętnie korzystamy, bo zdobywamy informacje np. o korkach ulicznych, o mogących nas zainteresować wydarzeniach odbywających się blisko miejsca naszego aktualnego pobytu czy o stanie naszego organizmu w czasie wysiłku fizycznego. Przedsiębiorcy korzystający z rozwiązań analityki biznesowej danych wskazują zaś na znaczną redukcję kosztów swojego działania czy możliwość podejmowania szybszych i lepszych decyzji w sferze zarządzania.

Rozwoju Big Data nie powstrzymamy, niemniej pilnie należy podjąć dyskusję, w jaki sposób korzystać z udogodnień, jakie się z tym wiążą, przy jednoczesnym zapewnieniu maksimum prywatności i właściwej ochrony danych osobowych. Uważam, że jest to jedno z poważnych wyzwań, jakie stoją przed organami ochrony danych osobowych, w tym GIODO.

Za niepokojące uważam przede wszystkim to, że niejednokrotnie dane na nasz temat pozyskiwane są nie bezpośrednio od nas, lecz z innych źródeł, bez naszej wiedzy i zgody. Są natomiast zestawiane i analizowane w celu stworzenia naszego profilu. Często na ich podstawie wyciągane są fałszywe wnioski, co do naszych cech oraz możliwych zachowań. W tym kontekście szczególnie groźna jest automatyzacja tego procesu. Trzeba wypracować takie rozwiązania, dzięki którym zapewnione będzie nasze prawo do informacji na temat tego, kto i ile o nas wie oraz w jakim celu gromadzi dotyczące nas dane, a także prawo do dostępu do nich i możliwość ich poprawiania. Istotne jest także właściwe zabezpieczanie owych wielkich zbiorów danych.

Na ile pomocne w tym wszystkim może być unijne rozporządzenie o ochronie danych osobowych, którego formalne uchwalenie przez Radę i Parlament Europejski ma nastąpić w pierwszej połowie 2016 r.?

W tym względzie istotne mogą być m.in. dwa mechanizmy mające na celu zwiększenie ochrony naszej prywatności - *privacy by design* (*prywatność w fazie projektowania*), zakładający, że narzędzia i usługi powinny być tak konstruowane, by od samego początku uwzględniały potrzebę ochrony prywatności obywateli, oraz *privacy by default* (*prywatność w ustawieniach domyślnych*), który odnosi się przede wszystkim do usług i aplikacji kierowanych do konsumentów.

Mechanizm ten wskazuje, iż podstawowe ustawienia powinny chronić prywatność użytkownika i dawać mu swobodę decydowania w tym zakresie. Rozwinięciem praktycznych aspektów ochrony prywatności w fazie projektowania jest zaś dokonywanie oceny ryzyka i skutków wpływu projektu na prywatność oraz poziom ochrony danych (*privacy impact assessment*). Do jej przeprowadzania administrator danych lub podmiot przetwarzający są zobowiązani wówczas, gdy operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów. Żeby przynosiła ona oczekiwane rezultaty, powinna być przeprowadzana, jeszcze zanim jakieś urządzenia czy systemy zostaną wprowadzone do użycia. Ważne jest, by zakres dokonywanej oceny był

szeroki i wykraczający poza problemy ściśle prawne oraz by odbywała się ona w sposób systematyczny.

Istotne znaczenie może też mieć przyjęcie koncepcji *risk based approach*, która zakłada, że im większe jest ryzyko związane z przetwarzaniem danych osobowych, tym większy powinien być zakres obowiązków ciążących na administratorze. W tym kontekście do zwiększonej dbałości o dane osobowe będą zobowiązani administratorzy korzystający właśnie z takich rozwiązań technologicznych, jak np. Big Data czy chmura obliczeniowa (*cloud computing*). O wymogu przywiązywania szczególnej wagi do zabezpieczenia danych decydowała będzie również sama treść gromadzonych informacji. Im zakres przetwarzanych danych jest szerszy, bądź znajdują się w nim dane osobowe wrażliwe, tym poziom zabezpieczenia danych powinien być wyższy.

Skoro jesteśmy już przy kwestii unijnej reformy ochrony danych osobowych - czy polski GIODO przygotowuje się w jakiś sposób do jej wdrożenia?

Zmiany, jakie czekają nas po wejściu w życie unijnego rozporządzenia o ochronie danych osobowych, będą rewolucyjne. Jest to bowiem akt prawny, który obowiązywać będzie w całości w sposób bezpośredni. To oznacza nie tylko to, że jego przepisów nie trzeba będzie implementować do polskiego systemu prawnego, ale również i to, że do nich będziemy musieli dostosować przepisy polskich ustaw i rozporządzeń. Prawdopodobnie część z nich trzeba będzie uchylić, gdyż w znacznej części normy prawne w zakresie ochrony danych osobowych będą wynikać bezpośrednio z nadrzędnych przepisów unijnego rozporządzenia ogólnego, a część zmodyfikować w sposób, który zagwarantuje zgodność z unijną regulacją.

W ocenie GIODO, to olbrzymie wyzwanie dla ustawodawcy, który musi dokonać przeglądu wielu regulacji sektorowych, za które odpowiadają poszczególne resorty, i ocenić, które z przepisów należy ewentualnie zmienić oraz czy są obszary, które wymagają wprowadzenia nowych unormowań. Dla lepszego uzmysłowienia skali możliwych zmian warto wskazać, iż ze wstępnych szacunków wynika, że przeanalizowania może wymagać ponad 800 aktów prawnych, w których znajdują się odniesienia do ochrony danych osobowych. Ponadto należy zaznaczyć, że rozporządzenie przewiduje także przypadki, kiedy poszczególne kwestie pozostawione są do uregulowania lub doprecyzowania przez prawo krajowe. Przykładowo są to m. in. takie szczegółowe zagadnienia sektorowe, jak chociażby przetwarzanie danych osobowych na potrzeby zatrudnienia, ochrony zdrowia czy w celach statystycznych i naukowych.

Niezbędne też będzie wprowadzenie nowych uregulowań proceduralnych określających m.in. status i kompetencje organów ds. ochrony danych osobowych. Ze względu na niezwykle krótki, bo 2-letni, okres vacatio legis, po którym rozporządzenie wejdzie w życie, należy się do tego dobrze przygotować. Oprócz dokonania zmian w przepisach polskiego prawa, konieczne będą zmiany organizacyjne w Biurze GIODO w celu dostosowania do realizacji jego nowych zadań.

Nowością – z punktu widzenia polskiego prawa – będzie możliwość nakładania przez organ ds. ochrony danych kar finansowych na te podmioty, które naruszają przepisy o ochronie danych osobowych. To powinno przyczynić się do przestrzegania obowiązującego prawa, w tym większej dbałości o bezpieczeństwo danych osobowych. To zresztą nie jedyne rozwiązanie, które ma temu służyć. Projekt unijnego rozporządzenia przewiduje też bowiem większą odpowiedzialność i rozliczalność podmiotów przetwarzających dane osobowe,

zobowiązując je m.in. do zgłaszania poważnych naruszeń ochrony danych osobowych krajowemu organowi nadzorczemu tak szybko, jak tylko jest to możliwe.

Jednym z głównych założeń unijnej reformy ochrony danych jest wzmocnienie pozycji krajowych organów ochrony danych osobowych oraz współpracy między nimi, tak aby zagwarantować spójne egzekwowanie przepisów i jednolite stosowanie przepisów w całej UE. W związku z tym przepisy rozporządzenia ogólnego o ochronie danych wprowadzają rozwiązania, które w szczególności: - poprzez ustanowienie systemu „punktu kompleksowej obsługi" w zakresie ochrony danych w UE, umożliwiają administratorom danych w UE kontakt jedynie z jednym krajowym organem ochrony danych, mianowicie z krajowym organem ochrony danych w państwie członkowskim, w którym znajduje się główna siedziba przedsiębiorstwa;

- stworzenie warunków do szybkiej i skutecznej współpracy między krajowymi organami ochrony danych, przewidujących między innymi wymóg prowadzenia przez te organy dochodzeń i inspekcji na wniosek innego organu oraz wzajemnego uznawania swoich decyzji;

- ustanowienie mechanizmu spójności na szczeblu UE, aby zagwarantować, że decyzje krajowych organów ochrony danych niosące szersze skutki w wymiarze europejskim w pełni uwzględniały stanowisko innych odnośnych krajowych organów ochrony danych i były w pełni zgodne z prawem UE;

- nadanie Grupie Roboczej Art. 29 statusu niezależnej Europejskiej Rady Ochrony Danych, aby zwiększyć jej wkład w spójne stosowanie przepisów o ochronie danych i stworzyć solidną podstawę do współpracy organów ochrony danych.

W Polsce mieliśmy ostatnio gorący okres. Zmiana rządu, a potem prace nad ustawą o policji, która również ociera się o kwestię prywatności. Czy GIODO śledził te wydarzenia? Jakie jest stanowisko GIODO na temat tego projektu?

GIODO z uwagą śledzi wszystkie wydarzenia i prace związane z szeroko pojętą kwestią ochrony prywatności i danych osobowych, a problematyka retencji danych telekomunikacyjnych od kilku lat była przedmiotem szczególnego zainteresowania Generalnego Inspektora. Debata, która obecnie się toczy, jest zatem swego rodzaju kontynuacją wcześniejszych dyskusji w tym zakresie.

Przy formułowaniu przez GIODO uwag zarówno do projektu, który jest aktualnie przedmiotem prac parlamentarnych, jak i do projektu, który był przedstawiany jesienią 2015 r., istotne znaczenie mają dwa bardzo ważne wyroki – Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r., stwierdzający nieważność tzw. dyrektywy retencyjnej (2006/24), oraz Trybunału Konstytucyjnego z 30 lipca 2014 r. Zawarte w nich zalecenia i wskazówki nie są jednak wdrażane w projektowanych przepisach.

W opinii GIODO, zaproponowana w projekcie forma kontroli nad pozyskiwaniem przez policję i służby specjalne danych telekomunikacyjnych, pocztowych lub internetowych jest niewystarczająca. Proponowany model przewiduje jedynie fakultatywną kontrolę następczą realizowaną przez sądy. Tymczasem, w opinii GIODO, jej dopuszczalność można uznać jedynie wyjątkowo, w ściśle określonych sytuacjach, w których zachodzi potrzeba natychmiastowego działania służb. Co do zasady zaś kontrola ta powinna być uprzednia i niezależna. GIODO wskazuje też, że projektowana forma kontroli nie gwarantuje w sposób

realny przestrzegania zasad niezbędności, adekwatności, i celowości, a przede wszystkim nie blokuje możliwości pozyskiwania danych nawet wtedy, gdy miałoby ono nastąpić z naruszeniem tych zasad. Tymczasem ETS wskazywał, że dostęp do tego typu danych powinien być ograniczony tylko do sytuacji, gdy jest to niezbędne w celu zapobiegania, wykrywania oraz ścigania poważnych przestępstw, zaś prawo powinno je definiować.

Kolejną kwestią, która budzi zastrzeżenia Generalnego Inspektora jest brak określenia w projekcie okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane telekomunikacyjne, pocztowe i internetowe. Stoi to w sprzeczności z wyrażoną w ustawie o ochronie danych osobowych zasadą ograniczenia czasowego, zgodnie z którą dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. Projekt przewiduje jedynie, iż dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisyjnemu i protokolarnemu zniszczeniu. Nie został natomiast uregulowany sposób postępowania z danymi wykorzystanymi w postępowaniu, w tym kwestia weryfikacji potrzeby ich dalszego przetwarzania. W praktyce może prowadzić to do nieuzasadnionego, bezterminowego przechowywania danych. Okres przetwarzania danych telekomunikacyjnych, pocztowych i internetowych powinien zatem być określony w sposób precyzyjny, tak, aby wyeliminować ryzyko nadużyć.

Generalny Inspektor wskazuje także na konieczność uzupełnienia projektu o obowiązek informacyjny wobec osób, których dane zostały pozyskane przez Policję i służby. Ma to szczególne znaczenie w odniesieniu do osób, wobec których nie zapadł wyrok lub którym nie zostały oficjalnie postawione zarzuty, jak również osób trzecich, których kontrola operacyjna czy pozyskanie danych bezpośrednio nie dotyczyło, bowiem osoby te nie będą miały świadomości, że jakiekolwiek działania wobec nich zostały podjęte. Uwagi GIODO zostały szczegółowo opisane i wyjaśnione w, dostępnych na naszej stronie internetowej pismach, skierowanych m.in. do Marszałka Sejmu RP oraz przewodniczącego Sejmowej Komisji Administracji i Spraw Wewnętrznych.

Czy GIODO posiada jakąś listę priorytetów lub zadań na najbliższy czas? Jeśli tak, to co się na niej znajduje?

Finalizujemy właśnie prace nad raportem na temat ochrony danych osobowych w Polsce, w którym przedstawiamy wyzwania, jakie czekają nas w tym obszarze w najbliższym czasie. Zostanie on przekazany odpowiednim instytucjom i organom w naszym państwie. Po pierwsze, wskazujemy w nim, że wkrótce formalnie uchwalone zostanie unijne rozporządzenie w zakresie ochrony danych osobowych, które spowoduje rewolucyjne zmiany w tej dziedzinie, do których wszyscy odpowiednio musimy się przygotować. Po drugie wymieniamy pewne grupy zagadnień, które GIODO będzie traktował w sposób priorytetowy ze względu na zagrożenia i wyzwania, jakie rodzą w sferze ochrony danych osobowych i prywatności.

Osobna część jest poświęcona zadaniom GIODO, zarówno tym realizowanym obecnie, jak i tym, które będą nałożone m.in. wspomnianym unijnym rozporządzeniem o ochronie danych osobowych czy wchodzącym w życie w lipcu 2016 r. rozporządzeniem Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. Wskazujemy ponadto, iż w ostatnim okresie znacząco wzrosło obciążenie urzędu, szczególnie ze względu na lawinowo rosnącą liczbę wpływających do Biura skarg i spraw, podkreślając konieczność dokonania pewnych

zmian systemowych, tak by urząd mógł sprostać wszystkim nałożonym przepisami prawa obowiązkom.

Co zaś do priorytetów i wyzwań związanych z ochroną danych osobowych, to w dużej mierze wynikają one z szybkiego rozwoju nowych technologii wkraczających do każdej dziedziny codziennego życia i aktywności każdego z nas. Profilowanie, biometria, monitoring wizyjny, Internet rzeczy, wykorzystywanie technologii identyfikacji radiowej (RFID), Big Data, to tylko przykładowe obszary wymagające przedyskutowania i odpowiedniego uregulowania.

W tym kontekście niezwykle istotne jest też wzmożenie działań edukacyjnych w zakresie prawa i zasad ochrony danych, w celu podnoszenia świadomości i wiedzy zarówno osób, których dane dotyczą, jak i podmiotów przetwarzających dane. Realizacji tego celu służą m.in. konferencje i spotkania organizowane z okazji obchodów X Dnia Ochrony Danych Osobowych, podczas których część z wymienionych zagadnień będzie dyskutowana. W tym roku, dzięki włączeniu się w obchody Dnia uczelni wyższych, z którymi GIODO ma zawarte porozumienia o współpracy, możliwa jest realizacja bardzo bogatego programu, z którym można zapoznać się na stronie internetowej GIODO – www.giodo.gov.pl.