

Świat orwellowski chce naszych danych

Musimy wypracować rozsądny kompromis między korzyściami, jakie wiążą się ze stosowaniem nowoczesnych technologii, a zapewnieniem nam prawa do prywatności.

Rozmowa z dr Edytą Bielak-Jomaa, Generalnym Inspektorem Ochrony Danych Osobowych (GIODO)

Problematyka dotycząca ochrony danych osobowych narasta lawinowo i wymaga wyjątkowej aktywności GIO-DO. Co było dla Pani najważniejszym wyzwaniem tuż po objęciu stanowiska w ubiegłym roku?

Jednym z generalnych stojących przede mną wyzwań było i jest takie działanie, by kierowany przeze mnie urząd postrzegany był przede wszystkim jako organ działający w interesie obrony praw obywateli. Chciałabym, by Polacy mieli poczucie, że jest ktoś, kto stoi na straży ich praw do prywatności i ochrony danych osobowych. Biorąc pod uwagę fakt, jak wiele jest podmiotów, które chciałyby zawładnąć naszymi danymi, musi być organ, który będzie się temu przyglądać i, gdy zajdzie potrzeba, powie: dość. Inaczej znajdziemy się w świecie orwellowskim. Kolejne wyzwania wynikają z rozwoju nowych technologii. Gromadzenie danych, ich łączenie, profilowanie – to wszystko stanowi bardzo duże wyzwanie zarówno dla użytkowników, jak i dla organu, jakim jest GIO-DO. Wymaga to z jednej strony bardzo dużej wiedzy, a z drugiej otwartości na dyskusję i wymianę doświadczeń. Musimy bowiem wypracować rozsądny kompromis między korzyściami, jakie wiążą się ze stosowaniem nowoczesnych technologii, a zapewnieniem nam prawa do prywatności. To trudne, ale jednocześnie konieczne. Do tego potrzebna jest jednak wiedza, dlatego edukacja to kolejne z wyzwań. Przed nami przede

wszystkim konieczność zmiany mentalnego podejścia do ochrony danych, która ma się stać jednym z fundamentów budowania zaufania obywatela do państwa i klienta do firmy. W tym kontekście ważną kwestią jest też odpowiednie ukształtowanie praktyki działania administratorów bezpieczeństwa informacji (ABI), których rola i pozycja od stycznia 2015 r. uległy znacznemu wzmocnieniu. Jako osoby dysponujące odpowiednią wiedzą, mają być wsparciem dla administratora danych, lecz zależy mi na tym, by stały się również ważną częścią całego systemu ochrony danych osobowych. Kolejne wyzwania dotyczą już kwestii szczegółowych, sektorowych, takich jak np. profilowanie, biometria, monitoring wizyjny, Internet rzeczy, wykorzystywanie technologii identyfikacji radiowej (RFID), Big Data. To tylko przykładowe obszary wymagające przedyskutowania i odpowiedniego uregulowania.

W tej chwili uruchamiany jest program 500+. Wiadomo już, że będzie możliwość składania wniosków za pomocą banku. Jest to duże ułatwienie dla obywateli, ale czy wykorzystanie prywatnych mechanizmów identyfikacji elektronicznej w sektorze publicznym na pewno będzie bezpieczne z punktu widzenia ochrony danych osobowych?

Rozwiązanie polegające na możliwości składania wniosków o ustalenie prawa do świadczenia wychowawczego za

pomocą systemu teleinformatycznego banków krajowych świadczących usługi drogą elektroniczną nie było przedmiotem konsultacji z Generalnym Inspektorem Ochrony Danych Osobowych, podobnie jak i inne przepisy ustawy o pomocy państwa w wychowywaniu dzieci. Organ z własnej inicjatywy zgłosił jednak obszerne uwagi do projektu ustawy zarówno na etapie prac rządowych, jak i parlamentarnych, przestrzegając przed zagrożeniami związanymi z przyjęciem przepisów w zaproponowanej wersji. Uwagi te nie zostały jednak uwzględnione. Odnosząc się natomiast do przepisu art. 13 ust. 5 pkt 3 ustawy, to wskazać należy, że został do niej wprowadzony na końcowym etapie prac legislacyjnych, również bez konsultacji z GIO-DO, co uniemożliwiło organowi szersze odniesienie się do zagadnienia. Tymczasem wprowadzona regulacja niesie za sobą szereg ryzyk dla ochrony prywatności i danych osobowych jednostek. Po pierwsze, zakłada przeniesienie zadań organów państwa na podmioty prywatne, co jest rozwiązaniem dotąd niespotykanym i naruszającym podstawowe zasady podziału kompetencji. Po drugie, nie jest jasne, kto w takim przypadku miałby być administratorem danych ani jak dokładnie miałyby wyglądać procedura postępowania z danymi zgromadzonymi przez banki. Szczególnie niepokojąca jest możliwość dalszego wykorzystania zebranych informacji – zwłaszcza że wnioski zawierać będą również tzw. dane szcze-



Edyta Bielak-Jomaa jest absolwentką Wydziału Prawa i Administracji Uniwersytetu Łódzkiego (WPiA UŁ). W 2003 r. uzyskała stopień doktora nauk prawnych i została zatrudniona w Katedrze Prawa Pracy WPiA UŁ na stanowisku adiunkta. Do kwietnia 2015 r., czyli do czasu powołania na stanowisko Generalnego Inspektora Ochrony Danych Osobowych, pełniła funkcję kierownika Podyplomowych Studiów Ochrony Danych Osobowych WPiA UŁ (od 2012 r.) oraz kierownika Centrum Ochrony Danych Osobowych i Zarządzania Informacją (od 2013 r.).

gólnie chronione, które mogą zostać użyte np. do profilowania osób, których dane dotyczą. Nawet te skrótowo przedstawione wątpliwości i zagrożenia pozwalają stwierdzić, iż komentowane rozwiązanie nie może zostać zaakceptowane przez Generalnego Inspektora Ochrony Danych Osobowych i jest kolejnym negatywnym aspektem przyjętej regulacji.

Sporo kontrowersji odnośnie do kwestii prywatności wywołała też nowelizacja ustawy o policji. Jakie jest stanowisko GIODO w sprawie pobierania przez służby specjalne danych telekomunikacyjnych, internetowych i pocztowych oraz prowadzenia kontroli operacyjnej?

GIODO od dawna zwracał uwagę na problemy związane z dostępem do danych telekomunikacyjnych, zabiegając o takie wdrożenie tzw. dyrektywy retencyjnej, które zapewni odpowiednią ochronę naszej prywatności. Stąd kwestia ta była m.in. tematem przewodnim Dnia Ochrony Danych Osobowych w 2011 r., a w 2014 r. stała się przedmiotem debaty w Senacie, której GIODO był współorganizatorem. Jako organ ds. ochrony danych osobowych swoje stanowisko w kwestii retencji danych telekomu-

nikacyjnych prezentowaliśmy również podczas obrad Trybunału Konstytucyjnego, aktywnie uczestniczyliśmy też we wszystkich pracach legislacyjnych dotyczących tej tematyki. Przy formułowaniu uwag do projektów aktów prawnych, które były przedmiotem prac parlamentarnych jesienią 2015 r. oraz na początku 2016 r., GIODO odnosił się m.in. do dwóch bardzo ważnych wyroków – Trybunału Sprawiedliwości Unii Europejskiej z 8 kwietnia 2014 r., stwierdzającego nieważność tzw. dyrektywy retencyjnej (2006/24), oraz

internetowych. Przyjęty 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, kontrola ta powinna być uprzednia i niezależna. Ponadto przyjęta forma kontroli nie gwarantuje w sposób realny przestrzegania zasad niezbędności, adekwatności i celowości, a przede wszystkim nie blokuje możliwości pozyskiwania danych nawet wtedy, gdy miałyby 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 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 nie-

W 2015 r. do ABI skierowaliśmy 13 wystąpień o dokonanie sprawdzenia, z czego 12 dotyczyło banków.

Trybunału Konstytucyjnego z 30 lipca 2014 r. Zawarte w nich zalecenia i wskazówki nie zostały jednak wdrożone w uchwalonych przepisach. Zatem przedstawiane w toku prac parlamentarnych uwagi GIODO, które są dostępne na naszej stronie internetowej, pozostają aktualne. Zastrzeżenia organ ds. ochrony danych osobowych zgłaszał również do formy kontroli nad pozyskiwaniem przez policję i służby specjalne danych telekomunikacyjnych, pocztowych lub

zwłocznemu komisijnemu 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. Przepisy nie przewidują też dopełniania obowiązku informacyjnego wobec osób, których dane zostały pozyskane przez policję i służby, co budzi zastrzeżenia GODO. Ma to szczególne znaczenie w odniesieniu do osób, wobec których nie zapadł wyrok lub którym nie zostały oficjalnie postawione zarzuty, jak również w stosunku do osób trzecich, których kontrola operacyjna czy pozyskanie danych bezpośrednio nie dotyczyły, bowiem osoby te nie będą miały świadomości, że jakiegokolwiek działania wobec nich zostały podjęte.

Ważnym wydarzeniem organizowanym przez GODO jest Dzień Ochrony Danych Osobowych. W tym roku tematem przewodnim było coraz istotniejsze zagadnienie Big Data.

Rozwój nowych technologii i globalizacja niewątpliwie spowodowały, że skala pozyskiwania, gromadzenia i wymiany informacji, w tym danych osobowych, osiągnęła niebotyczne rozmiary. Doskonałone 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 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 trafniejszych decyzji w sferze zarządzania. Mam świadomość, że 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

Po wejściu w życie unijnego rozporządzenia o ochronie danych osobowych wszystkie instytucje publiczne będą musiały mieć w swoich strukturach DPO.

prywatności i właściwej ochrony danych osobowych. Uważam, że jest to jedno z poważnych wyzwań, jakie stoją przed organami ochrony danych osobowych, w tym GODO. 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.

Czy od strony praktycznej będzie wkrótce możliwe zapewnienie ochrony danych osobowych przetwarzanych w tak gigantycznej skali?

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. Pomocne w skutecznej ochronie naszej prywatności i danych osobowych mogą być rozwiązania, jakie przewidywane są w unijnym rozporządzeniu dotyczącym ochrony danych osobowych, którego formalne uchwalenie przez Radę i Parlament Europejski ma nastąpić w pierwszej połowie 2016 r. W omawianej kwestii 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 zobowiązani będą 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.

Od ponad roku obowiązują nowe zasady regulujące powoływanie i pełnienie funkcji Administratora Bezpieczeństwa Informacji. Jak Pani zdaniem zmiany te wpłynęły na stopień ochrony danych osobowych, szczególnie w placówkach publicznych?

Wprawdzie od wprowadzenia zmian dotyczących roli i pozycji ABL minął ponad rok, to na bardzo szczegółowe podsumowanie dotyczące funkcjonowania ABL w sferze publicznej jest jeszcze za wcześnie. Cieszy mnie jednak fakt, że podmioty z tego sektora decydują się na powoływanie takich osób, które działają wedle nowych zasad. Spośród ponad 16 tysięcy ABL zgłoszonych do rejestracji GODO, większość to osoby z szeroko rozumianej administracji publicznej. Dla przykładu: szkoły podstawowe zgłosiły około 1500 ABL, policja – ponad 100, sądy – 173, prokuratury – 129, gminy – 1200. Można powiedzieć, że około dwóch trzecich zgłoszeń dotyczy sektora

publicznego, a jedna trzecia – biznesu. I to mimo że prywatnych firm jest więcej niż instytucji publicznych. Jednak to, jak działają w praktyce, czy dzięki ich powołaniu ochrona danych osobowych w danej placówce bądź instytucji uległa poprawie, będzie można ocenić po zapoznaniu się z efektami ich pracy, np. podczas kontroli czy sprawdeń realizowanych na zlecenie GIODO.

Ustawa umożliwi GIODO zlecenie ABI kontroli przetwarzania danych osobowych w podmiocie. Czy korzystali Państwo z tego przepisu?

W 2015 r. do ABI skierowaliśmy 13 wystąpień o dokonanie sprawdzenia, z czego 12 dotyczyło banków. Zakresem sprawdzeń objęto zabezpieczenie danych osobowych. Jak dotąd nie ma większych problemów z terminowym wywiązywaniem się tych podmiotów ze złożeniem sprawozdania. A co do ich jakości, to trudno ją ocenić, jesteśmy bowiem na razie na etapie dokonywania analizy przesłanego materiału. W tym roku do ABI również zamierzamy kierować wystąpienia o dokonanie sprawdzeń. Poza tymi doraźnymi, realizowanymi w związku ze skargami złożonymi do GIODO, zgłaszaniem zbiorów do rejestracji czy wnioskami innych organów, planujemy działania systemowe w tym zakresie. Z wnioskami o dokonanie sprawdzeń zamierzamy wystąpić do ABI z takich sektorów, jak banki, towarzystwa ubezpieczeniowe oraz gminy. W przypadku pierwszej grupy najbardziej będzie nas interesowała polityka w zakresie rozpatrywania sprzeciwów klientów wobec przetwarzania danych osobowych w celach marketingowych. W przypadku drugiej grupy zależy nam na sprawdzeniu, w jaki sposób przetwarzane są dane o stanie zdrowia w związku z oferowanymi przez te podmioty ubezpieczeniami zdrowotnymi. Natomiast w przypadku gmin chcemy skoncentrować się na realizowanym przez te podmioty obowiązku informacyjnym, który nie zawsze bywa wypełniany.

Fundamentalnym wydarzeniem będzie w tym roku uchwalenie przez Radę i Parlament Europejski unijnego rozporządzenia o ochronie danych

osobowych. Jakie czekają nas zmiany po jego wejściu w życie?

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 uzmystowienia 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

lach statystycznych i naukowych. Niezbędne też będzie wprowadzenie nowych uregulowań proceduralnych określających m.in. status i kompetencje organu ds. ochrony danych osobowych. 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 niejedyne rozwiązanie, które ma temu służyć. Projekt unijnego rozporządzenia przewiduje też większą odpowiedzialność i rozliczalność podmiotów przetwarzających dane osobowe, zobowiązując je m.in. do zgłaszania poważnych naruszeń ochrony danych osobowych krajowemu organowi nadzorcemu tak szybko, jak tylko jest to możliwe. Wyposaża również osoby, których dane dotyczą, w prawo do uzyskania odszkodowania. Dla podmiotów z sektora publicznego istotny może być zaś obowiązek zatrudnienia inspektora ochrony danych (Data Protection Officer, DPO). Taką funkcję pełni obecnie administrator bezpieczeństwa informacji – jednak jego powołanie jest dobrowolne. Po wejściu w życie unijnego rozporządzenia

Mam świadomość, że 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.

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 ce-

wszystkie instytucje publiczne będą musiały mieć w swoich strukturach DPO, a w przypadku firm prywatnych będzie to zależało od charakteru przetwarzanych danych oraz ich ilości.

Rozmawiał Eryk Chilmon