



**WOJCIECH
WIEWIÓROWSKI,**

generalny inspektor
ochrony danych
osobowych:

*Nie ma szczególnych
przepisów
odnoszących się do
big data i trudno się
ich spodziewać.
Przecież dzisiejsze
big data za kilka lat
może być nazywane
small data.*

Nowelizacje przepisów
uwzględniają
big data

big data big data big data

BIG DATA

– Czy w obowiązującym prawie funkcjonują już przepisy dotyczące dużych zbiorów danych przetwarzanych w systemach IT (big data)?

Pojęcie big data jest obecnie bardzo popularne, ale nie jest nowe. Wszystkie przepisy dotyczące ochrony danych osobowych, które pojawiły się w polskim prawie w latach 70. XX wieku, odnoszą się do zasobów, których nie jesteśmy w stanie „ogarnąć” działaniami człowieka i musimy do tego wykorzystywać procesy zautomatyzowane – dziś określamy takie procesy zbiorczym pojęciem big data. Jednak big data dziś i big data sprzed 40 lat to dwie różne rzeczywistości, zwłaszcza pod względem ilości przetwarzanych danych i stosowanych przy tym technologii. Niemniej przepisy dotyczące zasad przetwarzania danych od dość dawna są takie same. Na razie nie ma szczególnych przepisów odnoszących się do big data i trudno się ich spodziewać, zwłaszcza gdy weźmiemy pod uwagę, że to, co dziś nazywamy big data, za kilka lat może być nazywane small data, bo znaczenie źródłowego pojęcia istotnie się zmienia.

– Czy to oznacza, że ustawodawcy krajowy i unijny (europejski) nie zamierzają stworzyć nowych przepisów regulujących trend big data?

Rozwiązania proponowane w tzw. ogólnym rozporządzeniu o ochronie danych, będącym głównym aktem w ramach reformy regulacji ochrony danych osobowych w Unii Europejskiej, uwzględniają tendencje wzrostu ilości danych osobowych, które są przetwarzane. Wprawdzie trudno oczekiwać regulacji prawnych ściśle dedykowanych fenomenowi big data, ale w pracach nad nowymi unijnymi przepisami dotyczącymi ochrony danych osobowych kwestie związane z big data są brane pod uwagę.

– Czy dane pokazujące aktywność poszczególnych osób w korzystaniu z kart płatniczych podlegają ochronie prawa?

Oczywiście. Wszystkie dane, które można powiązać z konkretną osobą są danymi osobowymi podlegającymi ochronie prawnej. Podlegają jej też dane odzwierciedlające kto, gdzie i w jaki sposób korzystał z karty płatniczej. Często tego rodzaju dane są anonimizowane, by poddać je analizie bez powiązania ich z osobami. W trendzie big data nieraz do-

chodzi jednak do odwrotnego procesu – analiza coraz większej liczby danych dotyczącej anonimowej osoby może w końcu spowodować pojawienie się chęci jej zdeanonimizowania. Wprawdzie gdy płacimy kartą kredytową lub debetową sklep nie zbiera informacji, które można by uznać za dane osobowe, bo po wykonaniu takiej operacji zna tylko ostatnie 4 cyfry numeru karty. Gdy jednak informację tę uzupełnimy o kod pocztowy właściciela karty, wówczas blisko już do identyfikacji osoby.

– W dobie hostowanej korespondencji e-mailowej i mediów społecznościowych człowiek zostawia wirtualnej rzeczywistości (skrzynki e-mailowe, wpisy w social mediach, dane z billingów korzystania z telefonu mobilnego i przeglądania stron WWW, itp.) coraz więcej śladów. Czy praktyka skrzętnego zbierania tych śladów, analizowania ich i wyciągania stąd wniosków przydatnych do działalności komercyjnej nie jest sprzeczna z prawem?

To zależy, o których konkretnie danych, spośród wszystkich wymienionych w pytaniu, mówimy i jaki poziom ich analizy oraz przetwarzania wchodzi w grę. Treść korespondencji przesyłanej e-mailem, w tym zawarte w niej dane, jest objęta tajemnicą korespondencji chronioną przepisami art. 49 Konstytucji RP, ale też art. 267 Kodeksu karnego. Ktoś kto hostuje naszą korespondencję nie ma prawa przeglądania jej treści. Natomiast statystyki odzwierciedlające aktywność korespondencyjną użytkownika skrzynki e-mailowej podlegają ochronie jako dane osobowe. Inaczej sytuacja przedstawia się, gdy korzystamy z otwartych serwisów informacyjnych czy serwisów społecznościowych. Tutaj nasze dane osobowe są często ujawnione publicznie. Dlatego nie podlegają pełnej ochronie przysługującej danym osobowym. Jeśli jednak dane te są pozyskiwane i wykorzystywane do innych celów niż ten, dla którego zostały ujawnione, to podmiot, który w ten sposób je przetwarza, zobowiązany jest do dopełnienia tzw. obowiązku informacyjnego wynikającego z ustawy o ochronie danych osobowych. Będzie więc mógł przetwarzać dane osobowe pozyskane z sieci pod warunkiem, że dana osoba zostanie o tym fakcie powiadomiona i się na to zgodzi. Istotnym problemem jest w tym przypadku to, do jakiego zakresu informacji o osobie ma dostęp podmiot analizujący dane, np. analiza lo-

kalizacji telefonu komórkowego może pokazać, że anonimowy użytkownik podróżował po kraju czy był za granicą oraz jakie trasy przemierzył; zestawienie ich z danymi z bazy rezerwacyjnej może doprowadzić do identyfikacji osoby, a wtedy pojawiają się dane chronione prawem.

Łączenie danych objętych tajemnicą telekomunikacyjną z danymi objętymi tajemnicą bankową jest bezprawne, chyba że dokonują tego organy ścigania w ramach konkretnego prowadzonego postępowania.

– Firmy oferują konsumentom i przedsiębiorstwom usługi IT świadczone z chmur obliczeniowych, czyli wielkich centrów danych, dostępnych on-line, które często znajdują się poza granicami kraju. Czy fakt przetwarzania danych pochodzących z Polski w zagranicznym centrum danych oznacza, że należy się z nimi obchodzić zgodnie z polskimi przepisami?

Z pewnością tak, ale to nie oznacza, że za granicą nie można przetwarzać danych pochodzących z Polski, w tym danych osobowych. Przecież także jednostki administracji publicznej przetwarzają dane w chmurach (cloud computing), np. dane zawarte w Biuletynach Informacji Publicznej (BIP). Mogą w tym celu wykorzystywać serwery znajdujące się za granicą, w każdym państwie na świecie, gdyż już wcześniej zdecydowały, że jest to „informacja publiczna” i może być ona przetwarzana przez każdego. Jeśli jednak dane z zasobów administracji publicznej należą do innej kategorii, to mogą być przetwarzane na serwerach zlokalizowanych w Polsce lub w jednym z krajów należących do Unii Europejskiej, Europejskiego Obszaru Gospodarczego, bądź tzw. krajów zapewniających adekwatny poziom ochrony danych osobowych. Problem powstaje, gdy takie dane trafiają do chmur zlokalizowanych w krajach innych niż wymienione. Podobnie jest z informacjami niejawnymi – te powinny być przechowywane jedynie w Polsce.

W 2013 roku, w związku ze wzrostem popularności przetwarzania danych w chmurach (cloud) GIODO opublikował Dekalog Chmuroloba, w którym radzi, co należy wziąć pod uwagę, gdy decydujemy się na przetwarzanie danych w chmurach obliczeniowych.

Rozmawiał Krzysztof Polak