Opinia Polskiego Towarzystwa Informatycznego dotycząca

„projektu Stanowiska Rządu do dokumentu ***COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: A comprehensive approach on personal data protection in the European Union COM(2010) 609***."

1. Uwagi ogólne.

Przesłany do zaopiniowania projekt stanowiska generalnie popiera dokument Unii Europejskiej „w zakresie propozycji określenia ram dotyczących ochrony danych osobowych w Unii Europejskiej do nowych wyzwań w zakresie ochrony danych osobowych, związanych przede wszystkim z szybkim rozwojem technologicznym i globalizacją, które doprowadziły do głębokich przemian w świecie".

Nie ulega wątpliwości, że takie stanowisko Polskiego Rządu jest w zakresie deklaratywnym słuszne, problem ochrony danych osobowych, szczególnie w zakresie ich przetwarzania poza obszarem UE zaczyna być coraz poważniejszy, a w większości przypadków wymyka się spod kontroli.

Pozostaje jednak wątpliwość o charakterze zasadniczym, jakie konkretne działania mogą podjąć kraje UE, aby ten proceder ukrócić „u źródła" czyli tam, gdzie na terenie UE takie dane są nagminnie zbierane.

Podobnie jest z danymi zbieranymi przez przeróżne „służby" pod pozorem zapewnienia bezpieczeństwa. Kasowanie tych danych i kontrola prawomocności ich wykorzystywania jest równie ważnym problemem jak poruszony w stanowisku problem likwidowania naszych własnych danych z portali społecznościowych, czyli prawa do „bycia zapomnianym". Wiąże się z tym kwestia wykorzystywania tych danych w zupełnie innym celach niż zakładały to osoby korzystające z forów, np. do weryfikacji pracowników przez działy kadr. Nieopatrznie wypowiedziane zdanie połączone z danymi osobowymi może po kilku latach skutkować utratą miejsca pracy, lub szansy na zawodową karierę. To nie są problemy teoretyczne, lecz już istniejąca praktyka działania.

Biorąc pod uwagę postęp technologiczny warto zauważyć, iż dalsze poszerzanie katalogu danych „wrażliwych" i nakładanie na administratorów danych osobowych nowych obowiązków pod rygorem odpowiedzialności karnej może nie przynieść oczekiwanych rezultatów. Oczywiście, można będzie tych administratorów i ich pracodawców karać, ale będą oni mieli coraz mniejsze faktyczne możliwości wywiązywania się z obowiązków nakładanych nowymi przepisami. Trzeba też uwzględnić coraz większe koszty po stronie budowy systemów informatycznych mających zapewnić taką kontrolę.

W tej sytuacji warto zaproponować, w stanowisku rządowym, poważną dyskusję nad kompletnym minimalnym katalogiem danych wrażliwych, które będzie się rzeczywiście na terenie całej UE chronić za pomocą takich samych środków prawnych, przy stosowaniu podobnych rozwiązań technicznych.

2. Propozycje szczegółowe które proponujemy umieścić w uzasadnieniu stanowiska Rządu.

- Nowe regulacje powinny uwzględniać wzmocnienie prawnej ochrony obywateli w przypadku, gdy bezprawnie wykorzystano dane wrażliwe (osobowe) w celu wyrządzenia szkody, krzywdy bądź naruszenia dobrego imienia właściciela tych danych. Ochrona ta powinna być skuteczna

niezależnie od tego, czy czynu dopuści się organ władzy publicznej, podmiot gospodarczy czy osoba fizyczna.

- GIODO lub Rzecznik Praw Obywatelskich powinni otrzymać uprawnienia do występowania z oskarżeniem z urzędu w przypadkach bezprawnego wykorzystywania danych wrażliwych na skalę masową.
- Należy nadać GIODO kompetencje do kontrolowania służb specjalnych wykorzystujących dane osobowe (także osób z innych krajów UE). Uprawnienia te miałyby dotyczyć sposobu przechowywania danych i wywiązywania się z obowiązku ich niszczenia po upływie określonego w prawie okresu czasu.
- W sytuacji braku rzeczywistej kontroli nad danymi osobowymi obywateli UE poza jej obszarem, należy zaproponować wprowadzenie zakazu ich przechowywania poza obszarem UE. W tym zakresie powinny być wprowadzone wysokie kary finansowe dla firm i instytucji łamiących te zasady. Jedynym wyjątkiem od tej zasady może być sytuacja, w której obywatel UE wyraża dobrowolnie zgodę na przechowywanie swych danych osobowych poza obszarem UE. Zgoda ta nie może być jednak na właścicielu danych "wymuszona" pod rygorem nieudostępniania mu usług o charakterze powszechnym, lub zakazem dostępu do treści publicznych.
- Dane obywateli UE zbierane w związku z ich pobytem za granicą, szczególnie przy wykorzystywaniu biometrycznych dokumentów podróży i wiz biometrycznych, muszą być na podstawie umowy pomiędzy UE i tymi krajami chronione przez te kraje (z poszanowaniem zasady wzajemności). Ich wykorzystanie do innych celów powinno (w poważnych sytuacjach) skutkować pozywaniem tych krajów przez UE przed właściwe, przewidziane w umowach, sądy. Wszystkie kraje UE powinny być w tym zakresie chronione jednakowo, niedopuszczalne byłoby różnicowanie tych zasad w zależności od tego, o który kraj UE chodzi.
- Warto rozważyć podjęcie inicjatywy, w postaci poważnych eksperckich analiz, związanej ze zmianą organizacji sieci internetowej na obszarze UE. Celem takiego działania powinno być zwiększenie niezawodności funkcjonowania Internetu na obszarze UE w sytuacjach globalnych konfliktów i ataków cyberterrorystycznych, a także zapewnienie skutecznych mechanizmów zachowania prywatności i ochrony wrażliwych danych osobowych użytkowników Internetu. Takie działanie mogłoby dać rzeczywiste korzyści w utrudnianiu wycieku danych osobowych obywateli UE z systemów informatycznych jej krajów.