Uwagi do strategii poprawy skuteczności unijnych przepisów dotyczących ochrony danych osobowych, przedstawionej przez Komisję Europejską

przygotowane przez

Stowarzyszenie „Naukowe Centrum Prawno-Informatyczne”

Warszawa, styczeń 2011

SPIS TREŚCI:

I. ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH

1) Dr Wojciech Wiewiórowski

Niezwykle istotna jest kwestia tego, aby w sytuacjach, w których jest ona potrzebna, zgoda na przetwarzanie danych osobowych była udzielana świadomie i w pełni dobrowolnie. Powoływanie się na zgodę powinno następować tylko jeżeli ta zgoda jest w pełni dobrowolna. „Dobrowolność" zgody może mieć miejsce tylko w przypadku istnienia rynku konkurencyjnego. Jeżeli konkretna osoba nie ma wyboru, np. zgoda jest potrzebna do realizacja zadania publicznego to mamy *de facto* przymus a nie dobrowolną zgodę.

Kolejną ważną kwestią jest zagadnienie zgody na przetwarzanie danych osobowych osoby małoletniej. W tej materii konieczna jest harmonizacja. Nie ma aktualnie w Unii Europejskiej regulacji ujednolicającej wiek, do którego jest się osobą małoletnią. Należy przy tym pamiętać, iż obecnie znaczącą część użytkowników Internetu, którzy zgadzają się na przetwarzanie ich danych, stanowią osoby małoletnie.

2) Dr hab. Paweł Fajgielski

Zgoda na przetwarzanie danych osobowych ma być zgodą osoby poinformowanej, posiadającej wiedzę o tym, co będzie się z jej danymi dziać. Czasami sposób przedstawienia informacji dotyczących przetwarzania danych uniemożliwia zapoznanie się z nimi np. poprzez objętość dokumentu czy też konstrukcję strony internetowej.

Ponadto należy ujednolicić wymogi dotyczące zgody na przetwarzanie danych osobowych w poszczególnych państwach członkowskich Unii Europejskiej – obecnie są one zróżnicowane, co uniemożliwia wypracowanie wspólnych rozwiązań w tej materii.

Prawo do bycia zapomnianym powinno być wprowadzone tylko wtedy, jeżeli będzie możliwe do wyegzekwowania. W innym wypadku będą to martwe przepisy.

3) Mecenas Xawery Konarski

Doprecyzowania w dyrektywie wymaga zagadnienie udzielania zgody na przetwarzanie danych osobowych przez kogoś innego niż podmiot danych osobowych. Zgodnie z obecnym stanem prawnym wspomniana zgoda może być udzielana nie tylko przez

podmiot danych, ale także przez osobę trzecią. Istnieją sytuacje, na przykład w sprawach pracowniczych, w których możliwość wyrażenia zgody na przetwarzanie danych, przez osobę trzecią, może mieć niezwykle istotne znaczenie.

4) **Dr Paweł Barta**

Materią, którą powinna regulować dyrektywa jest także kwestia odwołania zgody małoletniego. Wokół tej kwestii powstaje wiele pytań, na przykład: kto może cofnąć zgodę na przetwarzanie danych osobowych małoletniego?

Kolejnym zagadnieniem, które warto poruszyć, jest kwestia zagwarantowania osobom, których dane dotyczą uzyskania pełnej informacji o przysługujących im uprawnieniach.

5) **Dyr. Monika Krasińska**

Możliwość uzyskania przez osobę, której dane dotyczą podstawowych informacji dotyczących przetwarzania jej danych osobowych jest istotna także dlatego, iż prawo złożenia sprzeciwu co do procesu przetwarzania jej danych osobowych, o którym nie ma ona pojęcia jest *de facto* iluzją.

6) **Dr hab. Grażyna Szpor, prof. UKSW**

Należy poświęcić uwagę także kwestii trudności z wycofaniem zgody na przetwarzanie danych osobowych. Formalności, które należy spełnić, aby zgodę wycofać nie powinny być rażąco bardziej skomplikowane niż formalności niezbędne do tego, aby zgodę na przetwarzanie danych osobowych wyrazić.

7) **Dr Arwid Mednis**

Dyrektywa powinna jednoznacznie przesądzać kwestię odwoływalności zgody na przetwarzanie danych osobowych, a także warunki (czas załatwienia sprawy, koszty) i skutki odwołania zgody (obowiązek zaprzestania przetwarzania danych dla celów objętych zgodą).

II. ADMINISTRATORZY BEZPIECZEŃSTWA INFORMACJI

1) **Dr Paweł Litwiński**

Dyrektywa powinna wzmocnić pozycję Administratora Bezpieczeństwa Informacji. Administrator Bezpieczeństwa Informacji powinien być instytucją obowiązkową, a jego obecność mogłaby dawać administratorowi danych pewne specjalne uprawnienia, na przykład pozwalać na rezygnację z obowiązku rejestracji zbiorów danych zwykłych czy też dawać możliwości scedowania na ABI procedury uprzedniej kontroli przy rejestracji zbiorów danych drażliwych.

2) **Dr Grzegorz Sibiga**

Należy oddzielić urzędnika do spraw ochrony danych osobowych od procedury notyfikacji. Obecnie wspomniany urzędnik jest „przypisany" do procedury notyfikacji i do procedury kontroli wstępnej. Należałoby stworzyć samodzielną regulację prawną dla ww. urzędnika. Regulacja tego typu doprowadziłaby do wzmocnienia efektywności kontroli przestrzegania przepisów o ochronie danych osobowych. Obecnie organy krajowe nie są w stanie skontrolować w całości tego, w jaki sposób przetwarzane są dane osobowe.

Wspomniany urzędnik powinien być niezależny od administratora danych osobowych. W tym miejscu powstaje pytanie jak to zagwarantować.

3) **Dr Arwid Mednis**

Pozycja urzędnika do spraw ochrony danych osobowych powinna ulec wzmocnieniu. Dyrektywa powinna przewidywać obowiązek jego powołania, a także podstawowe kompetencje. Powołanie urzędnika mogłoby wiązać się z przejęciem przez niego niektórych kompetencji organu ochrony danych a tym samym ograniczeniem niektórych obowiązków administratora wobec organu ochrony danych. Warto rozważyć rozwiązanie, zgodnie z którym urzędnik prowadziłby rejestr danych zwykłych, a notyfikacja do organu ochrony danych osobowych dotyczyłaby wyłącznie danych sensytywnych. Jednocześnie status urzędnika powinien mu gwarantować niezależność od administratora danych.

III. RETENCJA DANYCH TELEKOMUNIKACYJNYCH

1) **Prof. dr hab. Andrzej Adamski**

Traktat Lizboński przewiduje jednolity tryb legislacji w postaci dyrektyw, znosząc dotychczasowe ograniczenia, które wynikały z trójfilarowej struktury Unii Europejskiej.

Poprawiona dyrektywa ramowa dotycząca retencji danych telekomunikacyjnych powinna być bardziej kompleksowa i regulować nie tylko zachowania operatorów telekomunikacyjnych, tj. dostawców usług świadczonych publicznie, ale także zachowania „konsumentów" tych danych: organów ścigania i wymiaru sprawiedliwości. Krokiem w dobrą stronę byłoby dodanie do grupy podmiotów, których zachowania są regulowane, także służb specjalnych.

Ponadto, w znowelizowanej dyrektywie, konieczne jest określenie pewnych zasad, wynikających głównie z orzecznictwa Europejskiego Trybunału Praw Człowieka, dotyczących ochrony praw i wolności obywatelskich. Zasady te byłyby przeciwwagą dla naruszeń wyżej wymienionych praw i wolności koniecznych ze względu na interes państwa oraz wymiar sprawiedliwości. Chodzi tu, między innymi, o udostępnianie danych telekomunikacyjnych na potrzeby prowadzenia dochodzeń w sprawach dotyczących poważnych przestępstw.

Istotną jest także kwestia tzw. autonomii informacyjnej – obywatel w każdym wypadku powinien zostać poinformowany, iż jego dane były/są przetwarzanie.

2) **Redaktor Piotr Waglowski**

Retencja danych nie powinna być dokonywana na koszt przedsiębiorcy. Dobrym pomysłem wydaje się być wprowadzenie opłaty od rekordu dotyczącego konkretnej osoby a udostępnianego przez przedsiębiorcę odpowiednim organom/służbom na podstawie przepisów prawa. Byłby to swoisty „filtr ekonomiczny", racjonalizujący korzystanie przez odpowiednie służby/organy z przechowywanych przez przedsiębiorców danych.

3) **Katarzyna Szymielewicz**

Konieczne jest poddanie działalności organów egzekwowania prawa i wymiaru sprawiedliwości tym samym zasadom ochrony danych osobowych i prywatności w ogóle. Na tym tle na szczególną uwagę zasługuje problem blankietowej retencji danych – instrumentu, który stanowi najbardziej inwazyjny środek inwigilacji społeczeństwa w prawie europejskim. Obecnie istniejące przepisy w zakresie retencji danych (Dyrektywa 2006/24/WE) nakładają na państwa obowiązek retencji danych telekomunikacyjnych, a jednocześnie nie określają granic, które gwarantowałyby poszanowanie podstawowych praw jednostki.

Dlatego niezbędne są daleko idące zmiany w Dyrektywie, przede wszystkim: (i) skrócenie maksymalnego okresu zatrzymywania danych do przedziału między 3 a 6 miesięcy, w zależności od rodzaju danych; (ii) ograniczenie zakresu gromadzonych danych do

informacji, które są standardowo zbierane przez operatorów telekomunikacyjnych na potrzeby komercyjne; (iii) określenie ścisłych reguł dostępu do zatrzymywanych danych, przy zapewnieniu kontroli sędziego lub prokuratora; (iv) ścisłe określenie celów, w których zatrzymywane dane mogą być wykorzystywane i ich ograniczenie do walki z najcięższymi przestępstwami (potrzebny jest przynajmniej ich zamknięty katalog).

IV. PRAWO DO BYCIA ZAPOMNIANYM

1) Dr hab. Irena Lipowicz, prof. UKSW

Prawo osoby do spowodowania skutecznego i trwałego usunięcia jej danych osobowych nie jest obdarzane należytą uwagą. Brak mechanizmów kontrolowania daty "przydatności do spożycia" danych powoduje bezkarne wykorzystywanie danych od dawna niepotrzebnych do przetwarzania w zgodnych z prawem celach przez organy państwowe, pracodawców, podmioty gospodarcze.

Nawet w przypadku sprawców przestępstw dojrzałe systemy prawne przewodują zatarcie skazania, tymczasem nierozważny czyn lub wypowiedź młodej osoby mogą rzutować na jej życie zawodowe, prywatne czy np. karierę polityczną po 20 - 30 latach. Współczesna globalizacja przetwarzania i wielkie portale społecznościowe czynią niezbędnymi regulacje ponadnarodowe (w tym unijne) i są dowodem na internacjonalizację prawa administracyjnego.

2) Dr Arwid Mednis

Prawo do bycia zapomnianym tj. prawo osoby do spowodowania usunięcia jej danych oraz zaprzestania ich przetwarzania, jeżeli przestały być potrzebne do zgodnych z prawem celów, powinno służyć osobom fizycznym w szczególności w przypadkach umieszczenia ich danych w sieci (np. na portalach społecznościowych).

W praktyce jednak regulacja prawna tego zagadnienia może okazać się trudna do sformułowania, jak również niemożliwa do wyegzekwowania. Być może należałoby rozważyć wprowadzenie przepisów zachęcających do poszukiwania rozwiązań technicznych pozwalających np. na określenie „daty ważności" informacji umieszczanych w sieci, a także zachęcających do edukacji o skutkach umieszczania danych w Internecie.

V. PRAWO WŁAŚCIWE I JURYSDYKCJA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

1) Dr Marek Świerczyński, Mecenas Radosław Nożykowski

Mając na uwadze obecnie obowiązujące uregulowanie art. 4 dyrektywy 95/46/EC oraz opinię 8/2010 z 16 grudnia 2010 r. grupy roboczej ds. ochrony danych osobowych utworzonej na podstawie art. 29 ww. dyrektywy, przedstawiamy następujące stanowisko w sprawie prawa właściwego i jurysdykcji w zakresie ochrony danych osobowych:

a) nowe formy działalności obejmującej przetwarzanie danych osobowych (m.in. *cloud computing,* serwisy społecznościowe, usługi geolokacyjne) powodują potrzebę ponownego rozważenia regulacji kolizyjnych dotyczących stosowania przepisów z zakresu danych osobowych. Przy poszukiwaniu właściwych łączników warto uwzględnić toczącą się obecnie dyskusję dotyczącą prawa właściwego dla ochrony dóbr osobistych i prywatności w kontekście rozporządzenia Rzym II o prawie właściwym dla zobowiązań pozaumownych. Zasadne jest spójne uregulowanie tej kwestii, tak aby podobne łączniki były stosowane w przypadku publiczno i prywatnoprawnej ochrony prywatności (w tym danych osobowych);
b) w związku z powyższym celowe jest utrzymanie preferencji łączników personalnych i zmniejszenie znaczenia kryteriów dotyczących umiejscowienia środków technicznych (np. serwerów). Za celowe uważamy utrzymanie jako podstawowego łącznika siedzibę administratora danych osobowych/procesora. Nie jest naszym zdaniem trafne stosowanie łącznika personalnego dotyczącego osoby, której dane są przetwarzane, nawet w drodze wyjątku czy w formie kwalifikowanej (np. w połączeniu z regułą przewidywalności zastosowania takiego prawa przez administratora danych osobowych). Prowadziłoby to bowiem do dystrybutywnego albo kumulatywnego stosowania praw właściwych, z wszystkimi negatywnymi skutkami, które z tym się wiążą – za wyjątkiem określonym poniżej;
c) w przypadku przetwarzania danych osobowych przez administratorów/procesorów z siedzibą w UE/EOG łącznikiem powinna być siedziba jednego z tych podmiotów. Powinna ona być rozumiana w sposób spójny z siedzibą usługodawcy w rozumieniu dyrektywy o handlu elektronicznym 2000/31/WE (zasada państwa pochodzenia). Powinno to zostać jednak (aby uniknąć „forum shopping") połączone z dalszą harmonizacją reguł dotyczących ochrony danych osobowych poprzez zastąpienie

istniejącej dyrektywy rozporządzeniem. W przypadku przetwarzania danych osobowych poza UE/EOG kryterium lokalizacji danych nie powinno mieć znaczenia. Zasadne jest natomiast uwzględnienie kryterium nakierowania (również na podobieństwo propozycji dotyczących ochrony prywatności w kontekście reguł kolizyjnych ppm). Rozwiązaniem problemu ustalenia prawa właściwego dla administratorów/procesorów spoza UE/EOG byłby obowiązek (w przypadku powiązania działalności obejmującej przetwarzanie danych osobowych z terenem UE/EOG) powołania przedstawiciela administratora na terenie UE/EOG (jako przykład takiej regulacji można podać tzw. przedstawiciela prawnego sponsora badań klinicznych pochodzącego spoza UE/EOG). W takim wypadku prawem właściwym dla ochrony danych osobowych byłoby prawo państwa, w którym znajduje się siedziba tego przedstawiciela. W przypadku gdyby taki przedstawiciel nie został ustanowiony konieczne jest przyjęcie innego „tymczasowego" łącznika. Łącznikiem takim musiałby być albo łącznik umiejscowienia środków technicznych (co nie jest najtrafniejszym rozwiązaniem) albo łącznik państwa, w związku z którym dane są przetwarzane (łącznik miejsca faktycznego prowadzenia działalności – np. prowadzenia sklepu internetowego nastawionego na sprzedaż na danym terytorium);

d) przyjęcie przez grupę roboczą opinii 8/2010 o prawie właściwym samo w sobie stanowi działanie bardzo wartościowe dla doprecyzowania obecnie obowiązujących regulacji z zakresu ochrony danych osobowych w państwach UE/EOG. Ma to również istotne znaczenie dla prawidłowej interpretacji art. 3 polskiej ustawy o ochronie danych osobowych, który implementuje art. 4 dyrektywy 95/46/WE;
e) w zakresie jurysdykcji rozważyć należy możliwość stosowania obcego prawa administracyjnego przez krajowe organy zajmujące się ochroną danych osobowych. Stanowiłoby to wyjątek od generalnego zakazu stosowania obcych regulacji prawa publicznego przez organy administracyjne. Służyłoby jednak sprawniejszej ochronie danych osobowych na terenie UE/EOG.

VI. MONITORING WIZYJNY

1) Małgorzata Szumańska

Poszczególne państwa Unii Europejskiej różnią się wyraźnie od siebie, jeśli chodzi o zakres i sposób prawnej regulacji wykorzystywania monitoringu wizyjnego. W niektórych

kwestia ta została podjęta w ustawach dotyczących ochrony danych osobowych, w innych obowiązują odrębne akty prawne regulujące to zagadnienie. W wielu – tak jak w Polsce – regulacja jest bardzo fragmentaryczna i powierzchowna, co skutkuje brakiem realnej kontroli zarówno nad tym, czy monitoring wykorzystywany jest w sposób celowy i adekwatny, jak i nad tym, w jaki sposób przetwarzane są dane pozyskiwane za pomocą monitoringu.

W tej sytuacji słuszne wydaje się przyjęcie pewnych zasadniczych rozstrzygnięć na poziomie europejskim. Niestety problem wyzwań związanych z dynamicznym rozwojem monitoringu nie pojawił się w komunikacie Komisji Europejskiej. Postulujemy, by ten temat został włączony do prac nad nową dyrektywą. Uważamy, że dokument ten powinien jasno odnosić się do tematu monitoringu wizyjnego i precyzować, kiedy dane zbierane za jego pomocą należy uważać za dane osobowe, a także przewidywać pewien minimalny standard ochrony danych osób podlegających monitoringowi (przy założeniu, że poszczególne państwa członkowskie będą mogły realizować dalej idącą ochronę).

VII. PRYWATNOŚĆ W SIECI

1) Dr hab. Grażyna Szpor, prof. UKSW

Podstawą dla wytyczania nowych celów kompleksowej ochrony danych osobowych w prawie europejskim powinna być pogłębiona refleksja nad zachodzącą od wydania dyrektywy z 1995 roku ewolucją: wartości chronionych prawem europejskim związanym z ochroną danych, celów regulacji ochrony danych i ich hierarchii a także relacji między ochroną prywatności a ochroną danych osobowych. W minionym piętnastoleciu prawo ochrony danych osobowych stało się prawem odrębnym od prawa ochrony prywatności a rozwój Internetu, w tym portali społecznościowych, nie pozwala już koncentrować się na relacjach między prawami i wolnościami jednostki a swobodą przepływu danych obrocie gospodarczym na rynku wewnętrznym. Istotą nowych zagrożeń jest ograniczenie autonomii informacyjnej jednostki związane z utratą kontroli nad przechowywanymi przez nią danymi, monitorowaniem jej zachowań i próbami sterowania tymi zachowaniami. Rozumienie informacji jako dobra zmniejszającego niepewność i autonomii informacyjnej jako samodecydowania o zmniejszaniu niepewności może być pomocne przy weryfikacji dotychczasowej siatki pojęciowej.

2) **Dorota Głowacka**

Jednym z istotnych celów nowych przepisów o ochronie danych osobowych powinno być przystosowanie już obowiązujących reguł do nowych okoliczności związanych z rozwojem nowych technologii, w tym komunikacji internetowej. Kluczowe znaczenie ma wzmocnienie przejrzystości i kontroli nad przetwarzaniem danych w Internecie.

Niezbędne wydaje się wypracowanie nowej siatki pojęć odpowiadającej nowym podmiotom i ich rolom oraz nowym zjawiskom, które pojawiają się w społeczeństwie informacyjnym. W świetle rozwoju tzw. sieci 2.0, która umożliwia umieszczanie i modyfikowanie treści *online* przez użytkownika Internetu (np. w ramach portalu społecznościowego, w którym sam użytkownik zarządza swoim profilem i może przetwarzać dane innych osób), dotychczasowy podział ról na „administratora danych" i „osobę, której dane dotyczą" nie znajduje zastosowania.

Należy zapobiegać wykorzystywaniu przez prywatnych usługodawców internetowych istniejących luk w prawie w celu uniknięcia realizacji obowiązków wynikających z przepisów o ochronie danych osobowych. Taki stan rzeczy pozbawia należytej ochrony użytkowników prowadzonych przez nich serwisów.

Niezbędna jest redefinicja pojęcia „danych osobowych". Obecnie obowiązująca definicja, która pozwala na elastyczną interpretację tego terminu, doprowadziła do bardzo zróżnicowanej wykładni w państwach członkowskich, zapewniając jednocześnie nierówny poziom ochrony w UE. Warto chociażby rozstrzygnąć na poziomie unijnym, w jakich okolicznościach najczęściej budzące wątpliwości dane takie jak: adres IP, dane geolokalizacyjne, czy historia przeglądanych stron internetowych powinny być uznawane za dane osobowe. Innym zagadnieniem wzbudzającym istotne wątpliwości są warunki dla realizacji przesłanki uzyskania zgody na przetwarzanie danych osobowych. W przypadku wielu serwisów gromadzących dane o użytkownikach (podobnie, jak w przypadku niektórych regulacji krajowych, np. Wielkiej Brytanii) zgoda ta może być dorozumiana, a w praktyce często wyrażana w sposób nieświadomy.

Trudnym problemem, który należy rozwiązać jest także zagadnienie jurysdykcji nad serwisami internetowymi prowadzonymi przez usługodawców z krajów trzecich, oferujących swoje usługi obywatelom UE. Obecnie nie są oni związani zasadami ochrony danych osobowych w UE, co wpływa na mniejszą przejrzystość procesu przetwarzania danych i brak kontroli nad sposobem ich przechowywania oraz ograniczoną możliwość dochodzenia swoich praw przez obywateli UE w stosunku do tych podmiotów. Warunkiem skuteczności nowych

regulacji będzie skuteczne narzucenie ich przestrzegania przez podmioty spoza UE oraz realna możliwość pociągnięcia ich do ewentualnej odpowiedzialności.