STANOWISKO FUNDACJI PANOPTYKON W KONSULTACJACH „CAŁOŚCIOWEGO PODEJŚCIA DO KWESTII OCHRONY DANYCH OSOBOWYCH W UNII EUROPEJSKIEJ" (komunikat Komisji Europejskiej z 4 listopada 2010 r.)

1. Aksjologia: wspólny rynek nie powinien przesłaniać praw podstawowych

Swój komunikat „Całościowe podejście do kwestii ochrony danych osobowych Unii Europejskiej" Komisja Europejska rozpoczyna od stwierdzenia, że w Dyrektywie w sprawie ochrony danych z 1995 r. zapisano dwa z „najstarszych i równie podstawowych dążeń w procesie integracji europejskiej: z jednej strony jest to ochrona praw podstawowych i podstawowych wolności jednostek, w szczególności podstawowego prawa do ochrony danych, z drugiej zaś strony – realizacja rynku wewnętrznego – w tym przypadku swobodnego przepływu danych osobowych".

Zwracamy uwagę na ryzyko związane z postawieniem tych dwóch wartości na jednym poziomie. Implikacją takiego podejścia do aksjologii ochrony danych osobowych jest uznanie, że względy ekonomiczne mogą uzasadniać ograniczenie praw podstawowych, do których należy prawo do prywatności. Należy mieć na uwadze zasady zawarte w Europejskiej Konwencji Praw Człowieka (art. 8) oraz Traktacie o Unii Europejskiej (art. 6), zgodnie z którymi ograniczenia prawa do prywatności są dopuszczalne tylko o tyle, o ile są „konieczne w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób".

Nowe przepisy dotyczące ochrony danych osobowych w Unii Europejskiej powinny być tworzone w ścisłym związku z doktryną praw podstawowych. Dane osobowe to istotny element prywatności, a zatem zasady ich przetwarzania powinny odzwierciedlać ogólne zasady ochrony prywatności. Warto także, aby ewentualna nowa dyrektywa wprost odwoływała się do prywatności, jako jednej z podstawowych wartości, jakie podlegają ochronie prawa europejskiego i potraktowała zagadnienie ochrony danych osobowych jako element systemu ochrony prywatności.

2. Kompetencje organów ochrony danych osobowych (OOD)

Obserwacje praktycznych aspektów ochrony danych w Polsce skłaniają nas do wniosku, że kluczowe z punktu widzenia efektywności i spójności tego reżimu jest wzmocnienie kompetencji i pozycji systemowej OOD. Bez wsparcia silnego, niezależnego i działającego w sposób kompleksowy organu obywatele są pozostawieni w nierównej pozycji zarówno wobec potężnych graczy biznesowych, jak i instytucji państwowych gromadzących i przetwarzających ich dane.

Doświadczenie Polski pokazuje, że powierzenie parlamentom narodowym swobody w kształtowaniu kompetencji i charakteru OOD może prowadzić do ich ograniczenia ze względów politycznych. Na przykład w przypadku Polski z zakresu kompetencji kontrolnych OOD (Generalnego Inspektora Ochrony Danych Osobowych) zostały w zasadzie zupełnie wyłączone działania służb specjalnych, wymiaru sprawiedliwości i organów egzekwowania prawa (w tym związanie z ich działalnością transgraniczne systemy przetwarzania danych, takie jak SIS II czy EURODAC) oraz w dużym stopniu działania kościołów i związków wyznaniowych.

W naszej opinii niezbędna jest reforma w duchu artykułu 6 Traktatu o Unii Europejskiej, zgodnie z którym potrzebny jest „w pełni niezależny" organ powołany do ochrony danych. W świetle orzecznictwa ETS[1] standard ten obejmuje nie tylko niezależność instytucjonalną takiego organu (np. sposób dokonywania wyboru i odwołania), ale także zakres przyznanych mu kompetencji. Organ ochrony danych osobowych dla niezawisłego pełnienia swojej funkcji potrzebuje przede wszystkim realnego wpływu na działania podmiotów, które ma kontrolować.

W tym celu należy rozważyć wprowadzenie lub wzmocnienie następujących gwarancji niezależności i odpowiedniego zakresu kompetencji organów ochrony danych osobowych (OOD) na gruncie prawa europejskiego:

i. Poszerzenie funkcji OOD w kierunku utworzenia swoistego rzecznika prawa do prywatności w warunkach społeczeństwa informacyjnego i nadanie im odpowiednich uprawnień kontrolnych.

ii. Nadanie OOD możliwości nakładania kar finansowych za niektóre naruszenia przepisów o ochronie danych osobowych bezpośrednio na podmioty będące administratorami danych.

iii. Poddanie kontroli OOD działań organów egzekwowania prawa, wymiaru sprawiedliwości i służb specjalnych w zakresie zgodności ich działań z podstawowymi zasadami przetwarzania danych osobowych, ze szczególnym uwzględnieniem baz danych tworzonych na potrzeby wzmocnionej międzynarodowej współpracy policyjnej i w sprawach bezpieczeństwa.

iv. Stworzenie minimalnych instytucjonalnych gwarancji niezawisłości tych organów, obejmujące: ścisłe ograniczenia odwoływalności osoby pełniącej tę funkcję, transparentną procedurę wyborczą; wybór dokonywany przy udziale różnych i równoważących swój wpływ organów władzy państwowej; ustalenie minimalnych merytorycznych wymogów dla kandydatów, zabezpieczenie budżetu i aparatu wykonawczego adekwatnego do pełnionych zadań.

3. Rozciągnięcie zasad ochrony danych osobowych na działania w sferze wymiaru sprawiedliwości, współpracy sądowej i bezpieczeństwa

Zgadzamy się w pełni ze stwierdzeniem Komisji Europejskiej, że konieczne jest poddanie działalności organów egzekwowania prawa i wymiaru sprawiedliwości ogólnym zasadom ochrony danych osobowych. Brak jasno określonych reguł chroniących prywatność obywateli w odniesieniu do tych organów skutkuje nadużyciami i powoduje systemową dysfunkcję. Jest też – w naszej ocenie – niezgodny z zasadą rządów prawa. Przykład funkcjonowania służb specjalnych w Polsce jest tego dobitnym dowodem. Brak kontroli niezależnych, zewnętrznych organów nad celami i zakresem przetwarzania danych oraz brak gwarancji poszanowania praw

[1] Sprawa nr C-518/07.

jednostki, takich jak prawo do informacji o przetwarzaniu czy korekty własnych danych, doprowadził do systemowego problemu z poszanowaniem ogólnych zasad przetwarzania danych, takich jak celowość i proporcjonalność. Zasady wyrażone w dyrektywie o ochronie danych osobowych muszą być skutecznie stosowane do wszystkich obszarów, należących wcześniej do tzw. trzeciego filaru.

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 tejże 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 (zamknięty katalog).

Kolejny palący problem to zagwarantowanie poszanowania prawa do prywatności w obszarze zwiększonej współpracy policyjnej i bezpieczeństwa, w tym, w odniesieniu do transgranicznych systemów przetwarzania danych osobowych (SIS II, EURODAC, VIS) oraz wymiany danych z krajami trzecimi, w szczególności USA (np. danych z systemu SWIFT czy PNR).

Unia Europejska powinna w tym obszarze zapewnić najwyższy poziom ochrony danych, jaki jest przyjmowany w konstytucji któregokolwiek z państw członkowskich oraz europejskich instrumentach ochrony praw człowieka. Jako podstawa w tym zakresie może posłużyć Zalecenie Rady Europy w sprawie wykorzystania danych osobowych w sektorze policji. Kluczowe zasady, jakie muszą być uwzględnione w procesie dostosowania zasad funkcjonowania mechanizmów międzynarodowej współpracy do wymogów ochrony danych to: kategoryczny zakaz wtórnego przekazywania danych do państw trzecich, ścisłe przestrzegania zasad celowości i proporcjonalności, zakaz hurtowego przekazywania danych oraz konieczność wprowadzenia niezależnego audytu.

4. Problem regulacji monitoringu wizyjnego

Komisja Europejska w swoim komunikacie nie uwzględniła, istotnej dla ochrony prywatności obywateli, kwestii regulacji monitoringu wizyjnego. Narzędzie to jest stosowane coraz powszechniej w rozmaitych celach zarówno przez podmioty publiczne, jak i prywatne. Choć kraje Unii Europejskiej różnią się od siebie pod względem skali i sposobu wykorzystania monitoringu, można powiedzieć, że staje się on elementem codziennego życia jednostek i w coraz bardziej inwazyjny sposób wkracza w ich prywatność. Co więcej, ciągłym zmianom podlegają organizacyjne i technologiczne możliwości związane z wykorzystaniem monitoringu. Budowane są coraz większe i bardziej zintegrowane systemy, pojawiają się bardziej zaawansowane możliwości łączenia i wymiany informacji, a wzrost jakości nagrań zwiększa możliwości identyfikacji osób. Testowane i wprowadzane są takie funkcjonalności jak rozpoznawanie twarzy czy automatyczne wykrywanie zagrożeń. Oczywiście nadal wiele

systemów monitoringu charakteryzuje się niskim poziomem technologicznego zaawansowania, jednak ciągły rozwój tego narzędzia i związany z tym spadek cen, a także lobbing firm z sektora bezpieczeństwa z pewnością będzie prowadził do upowszechniania się bardziej zaawansowanych rozwiązań.

Poszczególne państwa Unii Europejskiej różnią się 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 niektórych przypadkach regulacje dotyczą wszystkich podmiotów korzystających z tego narzędzia, w innych przede wszystkim podmiotów publicznych, w większości jednak brakuje kompleksowej regulacji prawnej działania monitoringu. Oznacza to, że poziom ochrony praw osób, które są za jego pomocą poddawane kontroli, jest w poszczególnych krajach Unii Europejskiej bardzo różny, a przy tym w większości przypadków zdecydowanie niewystarczający.

Przykład Polski jest w tym wypadku bardzo pouczający. Obowiązuje szereg aktów prawnych bezpośrednio bądź pośrednio odnoszących się do monitoringu wizyjnego, jednak mają one w większości przypadków charakter fragmentaryczny i bardzo powierzchowny. W praktyce większość przypadków wykorzystywania monitoringu wymyka się regulacji prawnej. Ma to związek m.in. z powstałą na gruncie polskiego prawa kontrowersją, czy do danych zebranych za pomocą monitoringu należy stosować ustawę o ochronie danych osobowych (uodo). Analiza ustawowej definicji danych osobowych prowadzi wprawdzie do wniosku, że – przynajmniej w sporej części przypadków – jest to jak najbardziej możliwe, jeszcze bardziej stanowczo w tej sprawie wypowiada się Grupa Robocza Art. 29[2], jednak polska praktyka idzie w przeciwnym kierunku.

Podstawowe zasady przetwarzania danych osobowych sformułowane uodo rzadko wprowadzane są w życie przez podmioty korzystające z monitoringu wizyjnego. Obywatele nie mogą mieć pewności, że monitoring wykorzystywany jest w sposób celowy i adekwatny, nie wiedzą zazwyczaj, w jaki sposób przetwarzane są dane pozyskiwane za jego pomocą (jak są zabezpieczone, jak długo przechowywane, kto ma do nich dostęp, do jakich celów mogą być wykorzystane), zazwyczaj nie są nawet informowani o tym, że znajdują się w przestrzeni, która podlega monitoringowi. Ze szczególnym nasileniem problemy te występują w przypadku wykorzystywania monitoringu przez podmioty prywatne, ale również w przypadku podmiotów publicznych niedostateczna szczegółowość regulacji prowadzi do sytuacji, w której prawo do prywatności nie jest w wystarczający sposób zabezpieczone.

Wobec rozbieżności regulacji prawnych dotyczących monitoringu wizyjnego w poszczególnych krajach Unii Europejskiej oraz niedostatecznego poziomu ochrony praw i wolności jednostek postulujemy zmniejszenie stanu niepewności prawnej i przyjęcie pewnych zasadniczych rozwiązań na poziomie wspólnotowym. Uważamy, że prawo Unii Europejskiej powinno przewidywać pewien minimalny standard ochrony danych osób podlegających monitoringowi,

[2] Patrz np. Opinia 4/2007 w sprawie pojęcia danych osobowych: „administratorzy często twierdzą, że do zidentyfikowania dojdzie tylko w przypadku niewielkiej części zgromadzonych materiałów i że w związku z tym, zanim takie zidentyfikowanie nastąpi, nie przetwarza się danych osobowych. Jednakże jako że celem nadzoru wideo jest zidentyfikowanie osób występujących na obrazie wideo w każdym przypadku, gdy administrator stwierdza taką potrzebę, należy uznać cały proces za przetwarzanie danych dotyczących osób możliwych do zidentyfikowania, nawet jeżeli niektóre zarejestrowane osoby nie są możliwe do zidentyfikowania w praktyce".

przy założeniu, że poszczególne państwa członkowskie będą mogły realizować dalej idącą ochronę. Dlatego postulujemy włączenie tematu monitoringu do prac nad nową dyrektywą. Z ostatecznego brzmienia tego dokumentu powinien wypływać jasny wniosek, że dane gromadzone za pomocą monitoringu wizyjnego podlegają reżimowi ochrony danych osobowych. To powinno zapewniać pewien minimalny standard ochrony, a jednocześnie może stać się bodźcem dla niektórych państw członkowskich do bardziej poważnego zajęcia się problemem regulacji funkcjonowania monitoringu.

5. Ochrona prywatności w warunkach Web 2.0

Kluczowe znaczenie dla ochrony danych osobowych w kontekście rozwoju komunikacji internetowej ma wzmocnienie przejrzystości i kontroli nad przetwarzaniem danych w różnego rodzaju serwisach społecznościowych, gdzie dostarczycielem treści jest ich użytkownik.

Główną bolączką serwisów społecznościowych jest to brak poprawnego informowania użytkownika o sposobie przetwarzania danych, które wprowadza do systemu. 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 za „zgodę" uważana jest akceptacja zasad funkcjonowania serwisu wyrażana w sposób nieświadomy.

Prawo europejskie powinno narzucić serwisom społecznościowym obowiązek wprowadzania wysokich standardów ochrony prywatności jako ustawień domyślnych, w tym wymogu wyrażenia przez użytkownika świadomej zgody na udostępnianie danych poszczególnym kategoriom użytkowników. Jest to tym bardziej uzasadnione, że portale społecznościowe umożliwiają wprowadzanie przez użytkowników nie tylko danych osobowych ich samych, ale i osób trzecich. Mimo że z zasady treść umieszczana w takich serwisach jest przeznaczona dla określonej grupy „znajomych" (co może stwarzać wrażenie, że informacje są przetwarzane jedynie w celach osobistych w ramach pewnej grupy osób), w rzeczywistości jest ona otwarta na właściwie niekontrolowany dostęp i możliwość wykorzystywania w każdym celu, również komercyjnym. Warto, by przyjęta na poziomie europejskim regulacja dawała jasny sygnał, że umieszczanie danych osobowych w sieci stanowi działanie, z którym wiążą się określone konsekwencje prawne.

Wracając do obowiązków portali społecznościowych, warto podkreślić, że wysokie standardy ochrony danych osobowych, do których muszą dostosować się europejskie portale społecznościowe działają na konkurencyjnym rynku z serwisami spoza Unii Europejskiej, które warunków tych przestrzegać obecnie nie muszą. Wynika z tego, że wprowadzając w Europie wyższe standardy ochrony danych, działamy na niekorzyść naszych przedsiębiorców. Rozwiązaniem tego problemu byłoby poddanie temu samemu reżimowi ochrony danych wszystkich podmiotów działających na europejskim rynku, niezależnie od ich siedziby.

6. Problem jurysdykcji w sferze usług świadczonych drogą elektroniczną

Trudnym problemem, który należy rozwiązać jest także zagadnienie jurysdykcji nad usługami świadczonymi drogą elektroniczną przez podmioty z krajów trzecich, które swoją ofertę kierują do obywateli Unii Europejskiej. Obecnie nie są oni związani zasadami ochrony danych osobowych w Unii Europejskiej, co wpływa na mniejszą przejrzystość procesu przetwarzania

danych i brak kontroli nad sposobem ich przechowywania oraz ograniczoną możliwość dochodzenia praw przez obywateli Unii Europejskiej w stosunku do tych podmiotów.

Przykładowo, w najpopularniejszym obecnie portalu społecznościowym na świecie, aktywni użytkownicy z Europy są obecnie na drugim miejscu (zaraz po Stanach Zjednoczonych), jeśli chodzi o reprezentację wśród klientów tych usług, podczas gdy wymogi dotyczące ochrony danych osobowych bazują na prawie amerykańskim, które jest w tym zakresie o wiele łagodniejsze niż obowiązujące w Europie. Warunkiem skuteczności nowych regulacji będzie objęcie podmiotów spoza Unii Europejskiej obowiązkiem przestrzegania „europejskich kryteriów" oraz wprowadzenie realnej możliwości pociągnięcia ich do ewentualnej odpowiedzialności prawnej za naruszanie obowiązujących standardów. Obecnie przedstawiciele portalu twierdzą, że (np. w odniesieniu do Polski) nie ma możliwości pozywania ich w kraju zamieszkania zagranicznego odbiorcy ich usług, ani poddawania serwisu kontroli jakiegokolwiek zagranicznego organu ochrony danych osobowych. Warto przy tej okazji odnieść się do przykładu Kanady, która uznała, że ma prawo do sprawowania jurysdykcji nad Facebookiem, ponieważ jedna trzecia obywateli tego państwa ma na tym serwisie utworzone profile. Kanadyjczycy uznali, że skoro firma ma swoje biuro w Kanadzie oraz tak ogromną liczbę użytkowników zamieszkałych na jej terytorium, istnieje tzw. istotny związek *(ang. substantial connection)*, który pozwala Kanadzie na objęcie serwisu kanadyjską jurysdykcją.

Za przyjęciem podobnej konstrukcji w Unii Europejskiej przemawia również europejskie prawo konsumenckie, zgodnie z którym konsument może pozwać dostawcę w państwie swojego zamieszkania, jeśli pozwany kieruje działalność handlową lub zawodową do państwa członkowskiego, w którym konsument ma miejsce zamieszkania, a umowa z konsumentem została zawarta w ramach tej działalności. Zastosowanie – jako łącznika przy ustalaniu jurysdykcji – miejsca zwyczajnego pobytu konsumenta jest w pełni uzasadnione, ponieważ prawo państwa, w którym konsument ma miejsce zwyczajnego pobytu, jest mu najlepiej znane oraz umożliwia spełnienie oczekiwań konsumenta co do jego zastosowania, a także zapewnia występowanie przed własnym sądem w przypadku zaistnienia sporu.

7. Dane biometryczne jako dane szczególnie chronione

Kwestią, która nie pojawia się w komunikacie Komisji Europejskiej, jest zagadnienie ochrony danych biometrycznych, które – jak się wydaje – należy uregulować choćby na poziomie definicji. Obecnie obowiązująca Dyrektywa (95/46/WE) wyróżnia szczególną kategorię danych (art. 8), które przynajmniej co do zasady powinny być objęte dalej idącą ochroną. Ich wyjątkowość polega na tym, że dotyczą one bezpośrednio sfer należących do prywatności czy nawet intymności, a poza tym ich wykorzystanie może wiązać się zagrożeniem podejmowania decyzji o dyskryminującym charakterze[3].

Należy przemyśleć rozszerzenie tej kategorii i objęcie nią przynajmniej wybranej części danych biometrycznych (Komisja Europejska w swoim komunikacie wymienia *expressis verbis* jedynie kod genetyczny[4]). Dane biometryczne wykorzystywane są przez rozmaite podmioty coraz bardziej powszechnie, również w sytuacjach, w których stosowanie takich środków wydaje się zbyt inwazyjne i nieadekwatne do założonego celu. Nie wszystkie dane biometryczne zwiększają

[3] Por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, LEX, 2007, wyd. IV.
[4] W polskiej ustawie o ochronie danych osobowych jest już obecnie włączony do grupy danych szczególnie chronionych.

bezpośrednio zagrożenie dyskryminacją, ale ich wykorzystywanie stanowi szczególną ingerencję cielesność, a co za tym idzie prywatność obywateli i dlatego nie powinny być one wykorzystywane w sposób rutynowy. W związku z tym postulujemy: zdefiniowanie danych biometrycznych na potrzeby projektowanej dyrektywy oraz podjęcie decyzji, które z nich – jeśli nie wszystkie – powinny być objęte szczególną ochroną i czy ta ochrona powinna realizować się poprzez włączenie do kategorii danych wrażliwych.