FUNDACJA PANOPTYKON

REFORMA EUROPEJSKIEGO PRAWA O OCHRONIE DANYCH OSOBOWYCH

W związku z intensyfikacją prac legislacyjnych w Parlamencie Europejskim oraz Radzie Unii Europejskiej, przedstawiamy podsumowanie postulatów Fundacji Panoptykon, dotyczących projektu ogólnego rozporządzenia o ochronie danych osobowych[1]. Dokument zawiera ocenę projektu rozporządzenia w wersji przygotowanej przez Komisję Europejską oraz kierunku zmian, jaki wyłania się z prac w Radzie UE. W naszej opinii projekt Komisji Europejskiej powinien być traktowany jako punkt odniesienia dla dalszych prac legislacyjnych, a poprawki wnoszone przez Radę UE oraz Parlament Europejski nie powinny zmierzać do obniżenia zaproponowanego poziomu ochrony danych osobowych.

Z perspektywy obywateli, najważniejsze propozycje zawarte w projekcie to:

- szeroka, choć nadal elastyczna definicja danych osobowych i podmiotu danych, uwzględniająca rozwój technologii ułatwiającej łączenie danych i (wtórną) identyfikację (Art. 4.1);
- precyzyjna definicja i wysoki standard zgody na przetwarzanie danych osobowych, w szczególności wymóg pozyskiwania „wyraźnej" zgody (Art. 4.8, Art. 6.1a oraz Art. 7);
- wymóg maksymalnej ochrony prywatności w opcji „domyślnej" (*privacy by default;* Art. 23).

Projekt Komisji Europejskiej ma też słabe punkty, które – pod wpływem rozszerzającej interpretacji prawnej lub poprawek zmierzających do dalszego obniżenia standardu ochrony danych osobowych – mogą podważyć sens tej regulacji prawnej:

- bardzo szerokie wyjątki od ograniczeń przewidzianych dla środków stosowanych w oparciu o profilowanie (Art. 20);
- nieprecyzyjna i podatna na nadużycia klauzula „prawnie usprawiedliwionego interesu administratora", jako jedna z równorzędnych podstaw przetwarzania danych osobowych (Art. 6.1f).

Ocena najważniejszych propozycji zawartych w projekcie rozporządzenia o ochronie danych

Jeśli wierzyć badaniom, coraz więcej osób przyznaje, że nie czuje się bezpiecznie w warunkach ciągłego przepływu danych poza ich kontrolą i nie ma w tym zakresie zaufania do firm, z usług których korzysta. Obywatele wykazują większą potrzebę kontroli nad danymi osobowymi, a obecny model komercjalizacji informacji nie jest szeroko akceptowany[2].

W pełni podzielamy pogląd komisarz Viviane Reding, że czas najwyższy dostosować standardy ochrony prywatności do wyzwań, jakie stawia przed nami rozwój technologii. Nieprzystawalność wielu norm prawnych do realiów Internetu, jak również brak jednolitego standardu ochrony prywatności w Unii Europejskiej czynią to zadanie bardzo pilnym.

W naszej opinii projekt rozporządzenia przedstawiony przez komisarz Reding na początku ubiegłego roku zmierza do wzmocnienia standardów ochrony danych osobowych i ich dopasowania do obecnych praktyk rynkowych. Dlatego powinien być traktowany **jako punkt odniesienia dla dalszych prac legislacyjnych**. Poprawki wnoszone przez Radę Unii Europejskiej oraz Parlament Europejski w żadnym razie **nie powinny zmierzać do obniżenia poziomu ochrony zaproponowanego przez Komisję Europejską**. Jednocześnie, w kilku ważnych punktach projekt Komisji Europejskiej wymaga jednak wzmocnienia lub „uszczelnienia", tak aby cele reformy mogły zostać w pełni zrealizowane.

[1] Projekt rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), 2012/0011 (COD), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:PL:PDF.

[2] [2] Eurobarometr, *Attitudes on Data Protection and Electronic Identity in the European Union,* June 2011, http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_pl_en.pdf .

Poniżej omawiamy i oceniamy najważniejsze propozycje zawarte w projekcie rozporządzenia o ochronie danych osobowych, które albo stanowią fundament tej inicjatywy legislacyjnej, albo temu fundamentowi zagrażają.

(i) Definicja danych osobowych i podmiotu danych

Odpowiedni artykuł projektu: **Art. 4. 1.**

Co przewiduje projekt Komisji: „Dane osobowe" oznaczają każdą informację dotyczącą podmiotu danych, natomiast sam „podmiot danych" – każdą osobę, którą można (czyli: którą ktokolwiek na świecie może) zidentyfikować pośrednio lub bezpośrednio. To dobra, szeroka definicja, choć na kolejne 20 lat nawet ona może się okazać niewystarczająca. Definicja danych osobowych i podmiotu danych to fundamenty całego projektu. Od tego, jak szeroko zostaną one zakrojone, zależy zakres obowiązywania nowego prawa.

Kierunek zmian proponowany przez Radę UE: W wyniku dyskusji podczas spotkań grupy roboczej DAPIX definicja danych osobowych i podmiotu danych została połączona. Takie rozwiązanie nie wydaje się przejrzyste i utrudnia precyzyjne skonstruowanie obu definicji.

Postulaty Fundacji Panoptykon:

- Poszerzenie definicji podmiotu danych o **kryterium wyróżnienia (*single out*)**.
- Zachowanie zaproponowanego przez Komisję Europejską **kryterium ograniczającego** definicję danych osobowych: „by means reasonably likely to be used by the controller or by any other natural or legal person".
- **Zachowanie** obydwu **rozdzielnych** definicji – podmiotu danych oraz danych osobowych.

Uzasadnienie:

Coraz częściej, szczególnie w Internecie, identyfikacja osoby nie jest już potrzebna do tego, żeby móc **w istotny sposób ingerować w jej prywatność** – wystarczy właśnie możliwość „wyróżnienia" jej z grona pozostałych użytkowników, np. na podstawie unikatowego profilu generowanego na podstawie cyfrowego śladu, nawet jeśli nie jest on połączony z żadnym trwałym ani tymczasowym identyfikatorem. Z taką sytuacją mamy do czynienia za każdym razem, kiedy profilowanie i oddziaływanie na decyzje użytkownika jest oparte o informacje zawarte w pliku *cookie* lub pozyskiwane na podstawie innych technik śledzenia. Na tej podstawie można z powodzeniem dopasować np. reklamę grającą na emocjach do wrażliwego na te emocje dziecka czy ofertę zakupu środków na odchudzanie do nastolatki cierpiącej na anoreksję.

Prawo powinno uwzględniać fakt, że nieuchronnie będą się pojawiać **nowe środki techniczne umożliwiające identyfikację** osób, a zatem informacje, które ze względu na to kryterium nie mogły być uznane za dane osobowe kilka lat temu, będą mogły uzyskać taki status w **niedalekiej przyszłości**. Łatwość łączenia danych i wtórnej identyfikacji osób na tej podstawie potwierdzają badania naukowe[3].

Wraz ze pojawianiem się nowych możliwości identyfikacji osób, powinien zwiększać się również zakres obowiązywania standardów ochrony danych. Definicja zaproponowana przez Komisję Europejską zapewnia taką elastyczność, a jednocześnie zawiera zdroworozsądkowe ograniczenie w postaci kryterium prawdopodobieństwa, że środki umożliwiające identyfikację zostaną użyte przez administratora danych lub inną osobę (fizyczną albo prawną). To kryterium ograniczające nawiązuje do kryterium „nadmiernej trudności", jakie obecnie przewiduje polskie prawo. W tym sensie trudno uznać propozycję Komisji za rewolucyjną czy nadmiernie poszerzającą definicję danych osobowych.

[3] Zgodnie z badaniem przeprowadzonym przez prof. Latanyę Sweeney (Uniwersytet Harvarda), by zidentyfikować 87,5 % Amerykanów wystarczy tylko, by podmiot znał tylko kod pocztowy osoby, jej płeć oraz datę urodzin. Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population* (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4, 2000).

Podobne stanowisko zajmowała Grupa Robocza Art. 29[4].

(ii) Dane spseudonimizowane

Odpowiedni artykuł rozporządzenia: projekt komisji nie zawiera propozycji dotyczących danych spseudonimizowanych.

Kierunek zmian proponowany przez Radę UE: Podczas prac w grupie roboczej DAPIX do projektu rozporządzenia włączono definicję danych spseudonimizowanych. Jest ona zawarta w art. 4.2a.

Postulaty Fundacji Panoptykon:

- **Nie sprzeciwiamy się** samemu wprowadzeniu do projektu rozporządzenia definicji danych spseudonimizowanych. Domagamy się jednak jej doprecyzowania, aby uniknąć wątpliwości interpretacyjnych.
- Postulujemy wprowadzenie przepisów gwarantujących, że dodatkowe informacje, umożliwiające identyfikację, będą przechowywane nie tylko w **odrębnym zbiorze**, ale także będą zabezpieczone przy pomocy **niezależnych środków organizacyjnych i technicznych**.
- Kategorycznie sprzeciwiamy się poprawkom zmierzającym do wyłączenia danych spseudonimizowanych spod reżimu ochrony danych osobowych lub obniżenia standardu ochrony w stosunku do tej kategorii danych osobowych.
- Dopuszczamy natomiast wyłączenia od niektórych obowiązków wobec podmiotu danych, o ile ich realizacja bez pełnej i bezpośredniej identyfikacji nie jest możliwa.

Uzasadnienie:

Dodanie definicji danych spesudoninimizowanych nie może być traktowane jako „przyczółek" do stworzenia odrębnych zasad przetwarzania tego typu danych. Nie może być wątpliwości co do tego, że dane spseudonimizowane wchodzą w zakres definicji danych osobowych, ponieważ są to po prostu dane umożliwiające pośrednią identyfikację (przy założeniu, że identyfikacja jest możliwa bez nadmiernych trudności czy nieproporcjonalnych środków). Potwierdza to nie tylko analiza autorytetów prawnych w dziedzinie danych osobowych, ale również liczne przykłady pokazujące, w jak łatwy sposób można odbudować połączenie pomiędzy danymi spseudonimizowanymi, a danymi bezpośrednio identyfikującymi daną osobę.

Dla przykładu w 2006 r. amerykański serwis Netflix (strona umożliwiająca wypożyczanie filmów on-line) upublicznił informacje o tym, jakie filmy ogląda i jak je ocenia ponad 500 tys. użytkowników tego serwisu. Z zestawienia tego usunięto wszystkie informacje umożliwiające bezpośrednie zidentyfikowanie poszczególnych osób (np. nazwę użytkownika), przydzielając jedocześnie poszczególnym osobom numery (anonimizacja) – stąd było wiadomo, że np. użytkownik 1345 przydzielił poszczególnemu filmowi 5 gwiazdek. Naukowcy z Uniwersytetu Teksańskiego Arvind Narayanan i Vital Shmatikov, udowodnili, że osoba z zewnątrz, mając tak niewiele informacji jak indywidualny numer może w 84% przypadków dokonać bezbłędnej identyfikacji poszczególnych użytkowników serwisu[5].

Wyłączenie danych spseudonimizowanych spod reżimu ochrony danych osobowych, **stanowi zagrożenie dla spójności całego systemu**. Taki pogląd jest również wyrażany w oficjalnych stanowiskach przez Europejskiego Inspektora Ochrony Danych Osobowych[6] oraz Grupę Roboczą Art. 29[7]. Autorzy rozporządzenia

[4] Opinia Grupy Roboczej Art. 29 ds. ochrony danych nr 4/2007 w sprawie koncepcji danych osobowych z dnia 20 czerwca 2007 r., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.
[5] Arvind Narayanan, Vitaly Shmatikov, How to Break the Anonymity of the Netflix Prize Dataset, ARVIX, 2006, http://arxiv.org/abs/cs/0610105v1.
[6] Dodatkowy komentarz Europejskiego Inspektora Ochrony Danych w sprawie reformy ochrony danych z dnia 15 marca 2013 r., http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

powinni dążyć do stworzenia **spójnego systemu ochrony prawnej**, bez szerokich wyłączeń i odrębnych reżimów, które z zasady powodują trudności interpretacyjne i otwierają pole do nadużyć.

(iii) Definicja i warunki udzielenia zgody na przetwarzanie danych

Odpowiednie artykuły projektu rozporządzenia: **Art. 4 ,8, Art. 6.1 a oraz Art. 7**

Co przewiduje projekt Komisji: Jedną z sześciu podstaw przetwarzania danych jest zgoda osoby, której one dotyczą. Zgodnie z projektem Reding taka zgoda musi być wyraźna – nie można jej domniemywać z naszego zachowania, bo w praktyce otwierałoby to drogę do oczywistych nadużyć. Z kolei ciężar udowodnienia zgody podmiotu danych na przetwarzanie spoczywa na administratorze.

Kierunek zmian proponowany przez Radę UE: W ostatnich propozycjach wymóg pozyskiwania zgody „wyraźnej" (*explicit*) zostaje zastąpiony przez mniej precyzyjne kryterium „jednoznaczności" (*unambiguous*). Jest to powrót do niższego standardu ochrony prawnej, jaki przewiduje aktualnie obowiązująca dyrektywa 95/46/WE.

Postulaty Fundacji Panoptykon:

- **W pełni akceptujemy definicję zgody zaproponowaną przez Komisję Europejską**, w szczególności wprowadzenie wymogu pozyskiwania wyraźnej zgody oraz podkreślenie jej dobrowolnego charakteru.
- Sprzeciwiamy się wszelkim poprawkom, które obniżałyby standard wymagany dla uznania oświadczenia woli podmiotu danych za zgodę na przetwarzanie danych osobowych, w szczególności rezygnacji z wymogu pozyskiwania **wyraźnej zgody** na przetwarzanie danych osobowych oraz z ograniczenia, zgodnie z którym **zgoda pozyskana w sytuacji istotnej nierównowagi stron nie może zostać uznana za dobrowolną**.
- Ponieważ jest to istotna, niezależna podstawa przetwarzania danych osobowych, zgoda w każdych okolicznościach musi być wyraźna, dobrowolna, szczegółowo odnosząca się do konkretnego celu oraz zakresu przetwarzania danych i oparta na rzetelnej informacji.
- W praktyce administratorzy danych nie powinni mieć możliwości przetwarzania danych w oparciu o „domyślnie zaznaczone pola" (*pre-ticked boxes*), ani do domniemywania zgody w oparciu o inne zachowania podmiotów danych.

Uzasadnienie:

Krytyka definicji zgody zaproponowanej przez Komisję Europejską ze strony niektórych środowisk biznesowych pomija fundamentalny fakt, że zgoda podmiotu danych stanowi jedną z sześciu niezależnych podstaw przetwarzania danych osobowych. Ta konkretna podstawa ma na celu zagwarantowanie autonomii informacyjnej podmiotu danych w sytuacji, gdy to właśnie od jego decyzji zależy możliwość przetwarzania danych. Należy pamiętać, że jest to sytuacja szczególna, występująca wówczas, gdy potrzeba przetwarzania danych nie wynika z umowy ani przepisów prawa.

W przypadku usług internetowych powszechną praktyką jest przetwarzanie danych osobowych w oparciu o **domniemaną zgodę** (np. ze względu na sam fakt wejścia na stronę lub skorzystania z usługi). Badania prowadzone zarówno w Europie, jak i USA wykazały jednak, że takie domniemanie nie ma oparcia w rzeczywistym poziomie świadomości użytkowników[8].

---

[7] Dodatkowa opinia Grupy Roboczej art. 29 ds. ochrony danych, nr 08/2012 w sprawie reformy ochrony danych z dnia 5 października 2012 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf .

[8] Por. np. Big Brother Watch, „Nine in ten people haven't read Google's new privacy policy", http://www.bigbrotherwatch.org.uk/home/2012/02/ten-people-havent-read-googles.html; Rebecca Smithers, "Terms and conditions: not reading the small print can mean big problems", The Guardian, http://www.guardian.co.uk/money/2011/may/11/terms-conditions-small-print-big-problems.

Propozycje zgłaszane w Radzie UE stanowią powrót do siatki pojęciowej z aktualnie obowiązującej dyrektywy o ochronie danych osobowych. Praktyka jej stosowania pokazała, że kryterium „jednoznaczności" jest podatne na interpretację rozszerzającą. W efekcie nie można dziś mówić o spójnym i konsekwentnym stosowaniu przepisów definiujących pojęcie zgody. W oparciu o koncepcję „jednoznacznej" zgody rozwinęły się takie praktyki, jak umieszczanie klauzuli zgody w ogólnych warunkach i regulaminach oraz domniemywanie zgody z różnych zachowań użytkownika, pod warunkiem poinformowania go o konsekwencjach (np. wejścia na stronę czy skorzystania z serwisu). Utrzymanie tej koncepcji w nowym rozporządzeniu będzie jednoznaczne z zaakceptowaniem praktyk, które w żaden sposób nie gwarantują autonomii informacyjnej podmiotów danych.

Zgodnie z opinią Grupy Roboczej Art. 29, zagwarantowanie w rozporządzeniu, że zgoda musi być wyraźna, jest niezbędne do zapewnienia podmiotom danych możliwości korzystania z ich praw. Ponieważ jest to jedna z samodzielnych przesłanek przetwarzania danych osobowych, rozporządzenie musi gwarantować odpowiedni standard dla oświadczenia woli o tak doniosłych skutkach. Tę opinię podziela również Europejski Inspektor Ochrony Danych Osobowych[9].

Kryterium dobrowolności wyrażonej zgody oznacza, że **użytkownik musi mieć możliwość realnego wyboru co do tego, czy wyrazić zgodę na przetwarzanie danych**. Taka możliwość nie istnieje w sytuacji istotnej nierównowagi pomiędzy administratorem a podmiotem danych, np. w relacji pracodawcy z pracownikami lub w warunkach monopolu lub dominacji rynkowej (gdy administrator danych ma monopolistyczną pozycję na rynku i oferuje usługi, których nikt inny nie oferuje).

(iv) Ograniczenia dla środków stosowanych w oparciu o profilowanie

Odpowiedni artykuł projektu rozporządzenia: **Art. 20**

Co przewiduje projekt Komisji: Projekt komisarz Reding przewiduje **regulację środków (np. decyzji) opartych na profilowaniu, wobec których formułuje kilka ograniczeń**. Np. przyznaje osobie, która jest poddawana takim środkom, prawo do uzyskania „ludzkiej interwencji", jeśli nie zgadza się z podjętą decyzją. **Zaproponowana regulacja ma bardzo łagodny charakter: nie ma w niej mowy o zakazie profilowania, a przewidziane wyłączenia mają szeroki zakres**.

Kierunek zmian proponowany przez Radę UE: Pojawiała się propozycja dodania w projekcie rozporządzenia definicji profilowania (Art. 4.12a). W przypadku środków opartych o profilowanie proponuje się uzależnienie zakresu stosowania projektowanych przepisów od tego, jaki skutek wywiera środek oparty na profilowaniu i czy jest to skutek „negatywny" (*measures adversly affecting data subject)*.

Postulaty Fundacji Panoptykon:

- Utrzymanie **jednolitych reguł dotyczących środków opartych na profilowaniu bez względu na to, jaki wpływ wywierają** na podmiot danych. W naszej opinii uzależnianie zakresu regulacji prawnej od tak subiektywnego kryterium podważa sens tej regulacji.
- **Doprecyzowanie** definicji profilowania oraz **poszerzenie** jej o procesy, które nie opierają się wyłącznie na **automatycznym przetwarzaniu danych**.

[9] "(...) the EDPS stresses that the concept of explicit consent as currently defined in the Commission proposal (in particular Articles 4(8), 6(1)(a) and 7) should be maintained. It provides for some flexibility as to its manner of expression (by a statement or a clear affirmative action) and builds on the requirement of 'unambiguous' consent which constitutes an essential element of the overall balance of data protection since 1995. EU data protection authorities have consistently interpreted the requirement of Article 7(a) of Directive 95/46/EC, in relation to Article 2(h), that the consent be 'unambiguous' as meaning that such consent needed to be 'explicit'10 (so that, for instance, a lack of action or silence cannot be considered as unambiguous). Consequently, the EDPS recommends that amendments such as ITRE AM 83, IMCO AM 63, and proposed LIBE AM 757, 758, 760, 764-766 etc. be rejected". Dodatkowy komentarz Europejskiego Inspektora Ochrony Danych w sprawie reformy ochrony danych z dnia 15 marca 2013 r., http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

- **Ograniczenie możliwości wykorzystywania danych wrażliwych** w procesie profilowania, aby zmniejszyć ryzyko dyskryminacji.
- **Zagwarantowanie podmiotom danych prawa do informacji** o tym, czy podlegają profilowaniu, jaka logika stoi za zastosowanym algorytmem oraz do jakich kategorii ich dane zostały zakwalifikowane, jak również prawa do wyjaśnienia ostatecznej decyzji. Te gwarancje pomogą ograniczyć brak przejrzystości, który podważa zaufanie do podmiotów przetwarzających dane, zwłaszcza w kontekście usług online.

Uzasadnienie:

Profilowanie, czyli zbieranie i automatyczne przetwarzanie informacji na nasz temat po to, żeby zbudować pewne założenia na temat naszej osobowości i przyszłych zachowań, wiąże się z wieloma ryzykami. Najważniejsze to **ryzyko dyskryminacji**, **wykluczenia i utrwalenia społecznych stereotypów**.

Profilowanie opiera się na korelacjach statystycznych, a zatem z zasady jest obarczone istotnym marginesem błędu. Z perspektywy podmiotu przetwarzającego dane ten margines może być nieznaczny, jednak z perspektywy osoby, która się w nim mieści, taki błąd ma zasadnicze znaczenie – **może prowadzić do dyskryminacji na tle rasowym, wykluczenia z dostępu do istotnej usługi, dyskryminacji cenowej, naruszenia prywatności i innych negatywnych skutków**[10].

Z punktu widzenia podmiotu danych **znaczenie ma nie tylko nie tylko stworzenie indywidualnego profilu, ale już samo zakwalifikowanie go do określonej grupy**. Z perspektywy autonomii informacyjnej podmiotu danych istotne jest to, że administrator wie na pewno, że podmiot danych należy do określonej kategorii (np. osób homoseksualnych, osób z nadwagą, osób po rozwodzie etc.) i jest w stanie tę wiedzę wykorzystać. Dlatego obok kryterium identyfikowalności **potrzebujemy wprowadzenia kryterium *singling out*, przynajmniej w przepisach dotyczących profilowania**.

Utworzone profile mogą być trudne lub wręcz niemożliwe do zweryfikowania, ponieważ opierają się na złożonych i dynamicznych algorytmach. Algorytmy wykorzystywane w tym procesie często są kwalifikowane jako tajemnica handlowa, wobec czego osoby poddane profilowaniu nie mają dostępu do informacji na ich temat. W tym kontekście duże znaczenie mają **gwarancje zwiększające transparentność** środków opartych na profilowaniu z perspektywy podmiotu danych.

Z uwagi na te immanentne ryzyka niezbędna jest szczelna regulacja, która – nie zakazując takich praktyk – zapewni odpowiednie gwarancje w każdym przypadku zastosowania środków opartych o profilowanie. Dlatego stanowczo sprzeciwiamy się uzależnieniu zakresu projektowanej regulacji od tego, jaki skutek wywiera środek oparty na profilowaniu („istotny" lub „negatywny"). Taka konstrukcja uzależnia standard ochrony danych od oceny i dobrej woli administratorów danych, tworząc istotny wyłom w rozporządzeniu.

Podobne zastrzeżenia i uwagi zgłaszała także Grupa Robocza Art. 29 w swojej opinii do projektu rozporządzenia[11].

(v) *Privacy by default* – maksymalna ochrona prywatności w opcji „domyślnej"

Odpowiedni artykuł projektu rozporządzenia: **Art. 23**

[10] Np.: Dominic Basulto, "Is social profiling discrimination?", The Washington Post, http://www.washingtonpost.com/blogs/innovations/post/is-social-profiling-the-new-racism/2012/05/03/gIQAXQQDzT_blog.html; Herb Weisbaum, "Google ads may be racially biased, professor says", NBC News, http://www.nbcnews.com/business/google-ads-may-be-racially-biased-professor-says-1C8369538; Raport Agencji Praw Podstawowych Unii Europejskiej, "Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide", http://fra.europa.eu/sites/default/files/fra_uploads/1133-Guide-ethnic-profiling_EN.pdf; Jakub Mikians, László Gyarmati, Vijay Erramilli, Nikolaos Laoutaris, "Detecting price and search discrimination on the Internet, HotNets-XI Proceedings of the 11th ACM Workshop on Hot Topics in Networks", http://www.tid.es/es/Lists/Scientific_Publications/Attachments/251/hotnets2012_pd_cr.pdf.

[11] Opinia Grupy Roboczej art. 29 ds. ochrony danych, nr 01/2012 w sprawie reformy ochrony danych z dnia 23 Marca 2012 r., http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

Co przewiduje projekt Komisji: Komisarz Reding proponuje **zmianę paradygmatu w relacji klient – usługodawca** z „domyślnego śledzenia" na „domyślne gwarancje prywatności" (*privacy by default*). Zgodnie z tym modelem już w momencie, w którym zaczynamy korzystać z danego serwisu czy usługi, powinniśmy mieć zapewnioną maksymalną ochronę prywatności. Projekt nakłada na administratora danych obowiązek zapewnienia, by domyślnie były przetwarzane tylko te dane, które są niezbędne dla realizacji konkretnego, zakładanego celu (zarówno jeśli chodzi o ilość danych, jak i czas ich przetwarzania). W szczególności administrator danych powinien zapewnić, że w opcji domyślnej dane osobowe nie będą udostępniane nieograniczonej liczbie osób.

Kierunek zmian proponowany przez Radę UE: Dyskutowane propozycje przewidują ograniczenie obowiązku zapewnienia, że w opcji domyślnej dane osobowe nie są udostępniane nieograniczonej liczbie osób, poprzez dodanie frazy *without human intervention*. Pojawia się też propozycja zastąpienia odniesienia do *state of art* przy wdrażaniu przez administratora danych odpowiednich środków technicznych odniesieniem do dostępnych technologii (*available technology*), bez zdefiniowania tego pojęcia.

Postulaty Fundacji Panoptykon:

- Propozycja Komisji zmierza w bardzo dobrym kierunku i wymaga zachowania – w szczególności jeżeli chodzi o wyraźny obowiązek zapewnienia, że w opcji domyślnej dane osobowe nie będą udostępniane nieograniczonej liczbie osób.
- Jednocześnie proponujemy **doprecyzowanie definicji** ochrony prywatności w opcji „domyślnej" oraz jej ujednolicenie z definicją ochrony prywatności w fazie projektowania (*privacy by design*) **poprzez odwołanie do środków technicznych i organizacyjnych**, jakie powinien zapewnić administrator danych dla zrealizowania tego obowiązku.

Uzasadnienie:

Zasada ochrony prywatności w opcji „domyślnej" zmierza do ochrony podmiotów danych również w sytuacji niezrozumienia lub braku kontroli sposobu, w jaki ich dane są przetwarzane, szczególnie w kontekście technologii. U źródeł tej zasady jest założenie, że funkcje danego produktu lub usługi, które potencjalnie mogą zagrażać prywatności, są na starcie ograniczone do tego, co absolutnie konieczne. W tym modelu decyzja o poszerzeniu możliwości przetwarzania danych należy wyłącznie do podmiotu danych[12].

Tym samym zasada *privacy by default* zabezpiecza dane osobowe przed eksploatacją przez samego usługodawcę. Nie chodzi przy tym o zakaz przetwarzania danych, ale o uszanowanie podstawowych zasad, takich jak proporcjonalność i adekwatność tego, co jest na nasz temat zbierane do tego, co jest nam oferowane.

Ryzyko udostępnienia danych nieograniczonej liczbie odbiorców i związanych z nim nieodwracalnych konsekwencji istnieje nie tylko w przypadku automatycznego przetwarzania danych (tj. „bez ludzkiej interwencji"). Do takiego ujawnienia może np. dojść w wyniku decyzji pracownika upoważnionego do przetwarzania danych lub samego administratora danych. Dlatego Art. 23 powinien zezwalać na to jedynie w przypadku świadomej decyzji samego podmiotu danych.

(vi) Prawnie usprawiedliwiony interes administratora

Odpowiedni artykuł rozporządzenia: **Art. 6.1 f**

Co przewiduje projekt Komisji: W projekcie rozporządzenia przewidziano sześć podstaw przetwarzania danych, wśród nich tzw. prawnie usprawiedliwiony interes administratora. Ta podstawa dopuszcza przetwarzanie danych osobowych bez zgody podmiotu danych w przypadku, gdy w opinii administratora jego prawnie usprawiedliwiony interes przeważa nad interesem lub fundamentalnymi prawami podmiotu danych.

[12] Dodatkowy komentarz Europejskiego Inspektora Ochrony Danych w sprawie reformy ochrony danych z dnia 15 marca 2013 r., http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-03-15_Comments_dp_package_EN.pdf.

Kierunek zmian proponowany przez Radę UE: Wśród ostatnich propozycji pojawia się możliwość rozszerzenia klauzuli prawnie usprawiedliwionego interesu administratora danych na „podmioty trzecie" (*third parties*) lub innych administratorów, którym dane są udostępniane.

Postulaty Fundacji Panoptykon:

- **Proponujemy lepsze zdefiniowanie** prawnie usprawiedliwionego interesu administratora danych i obwarowanie tej podstawy przetwarzania danych **dodatkowymi gwarancjami**.
- W szczególności, proponujemy wprowadzenie zasady, że z tej podstawy prawnej można skorzystać jedynie wtedy, gdy przetwarzanie danych w oparciu o pozostałe podstawy prawne jest niemożliwe lub nadmiernie utrudnione oraz tylko wówczas, gdy uzasadnia to relacja umowna lub „racjonalne oczekiwania" (*reasonable expectations*) podmiotu danych.
- Postulujemy zachowanie propozycji Komisji Europejskiej, która **ogranicza możliwość wykorzystywania tej podstawy prawnej do pierwotnego administratora danych.** Dopuszczamy jednak wyłączenie w sytuacji, gdy relacja umowna lub „racjonalne oczekiwania" (*reasonable expectations*) podmiotu danych uzasadniają przekazanie danych „podmiotom trzecim" (*third parties)*.

Uzasadnienie:

Pojęcie „prawnie usprawiedliwionego interesu administratora" jest **niejasne, zakłada uznaniowość** i pozostawia **duże pole do interpretacji**. Art. 6.1f zakłada **dobrą wolę administratora**, który sam ma decydować o tym, czy dane mogą być przetwarzane (bez zgody osoby, której dotyczą), podczas gdy **nie powinien być on sędzią we własnej sprawie**.

Stosowanie tej przesłanki sprawia, że **przetwarzanie danych staje się nietransparentne** z perspektywy osób, których dane dotyczą, prowadząc do **erozji zaufania** między podmiotem danych i ich administratorem[13].

Ponadto, interpretacja tej klauzuli może się różnić w poszczególnych państwach członkowskich, podważając tym samym sens harmonizacji i wprowadzając niepewność co do zakresu i legalności niektórych form przetwarzania danych.

Obserwacja istniejących praktyk rynkowych każe przyjąć, że w przypadku, gdy w grę wchodzi masowe przetwarzanie danych, **interes użytkowników zawsze przegra z interesem administratora**. W toku stosowania i interpretowania dyrektywy 95/46/WE klauzula „prawnie usprawiedliwionego interesu" stała się standardowym uzasadnieniem dla przetwarzania danych wykraczającego poza to, co konieczne dla realizacji umowy lub obowiązków wynikających z przepisów prawa.

Przykładem takiej praktyki (skrytykowanej przez europejskich inspektorów ochrony danych osobowych) może być niedawna **zmiana polityki prywatności firmy Google**, zakładająca integrację danych przetwarzanych w związku z różnymi usługami świadczonymi przez tę firmę. Również **w oparciu tę podstawę prawną funkcjonują rozbudowane ekosystemy marketingu bezpośredniego**, gdzie osoby, których dane są przetwarzane i łączone w rozbudowane profile, nie mają nad tym procesem żadnej kontroli, a często nawet wiedzy o wszystkich zaangażowanych podmiotach.

Za szczególnie niepożądaną i niebezpieczną uważamy konstrukcję umożliwiającą wykorzystywanie tej podstawy prawnej przez podmioty trzecie. Takie podejście w zasadzie **przekreśla zasadę autonomii informacyjnej oraz celowości przetwarzania danych**. Osoba, której dane dotyczą, nie ma bowiem żadnej

[13] Przykłady nadużyć i bardzo szerokiego wykorzystania uzasadnionego interesu są liczne: (a) Google przetwarza większość danych użytkowników w oparciu o uzasadniony interes. Polityka prywatności tej firmy wskazuje, że gromadzi ona szeroki zakres danych o osobie. Kontrowersyjna decyzja korporacji o utworzeniu jednej polityki prywatności dla wszystkich swoich serwisów doprowadziła do wszczęcia postępowań przeciwko Google, przez organy ochrony danych osobowych z sześciu krajach Unii Europejskiej (http://www.rp.pl/artykul/995952.html); (b) Linkedin: Wraz z zainstalowaniem aplikacji na urządzeniach mobilnych, dającej w zamyśle dostęp do kalendarza spotkań, aplikacja zaczęła zbierać wszystkie dane znajdujące się w urządzeniu. Firma jako podstawę dla takiego stanu rzeczy wskazała, uzasadniony interes.

realnej kontroli nad tym, przez kogo, w jakim zakresie i w jakim celu jej dane są przetwarzane przez kolejnych administratorów.

Ze względu na te zagrożenia zasada wyrażona w artykule 6.1f powinna zostać sformułowana tak wąsko, jak to tylko możliwe. Pierwotnie ta podstawa przetwarzania danych była z resztą pomyślana, jako wyjątek i do tego założenia należy powrócić.

(vii) Transfery danych do państw trzecich lub organizacji międzynarodowych

Odpowiednie artykuły rozporządzenia: **Art. 40-45**

Co przewiduje projekt Komisji: Projekt rozporządzenia przewiduje dwie podstawowe sytuacje w których możliwe jest przekazanie danych do państw trzecich: wydanie przez Komisję Europejską decyzji stwierdzającej odpowiedni poziom ochrony danych albo istnienie tzw. odpowiednich gwarancji (appropriate *safeguards*) Niestety, od tych dwóch zasad istnieją liczne wyjątki, niekorzystne z perspektywy podmiotów danych.

Kierunek zmian proponowany przez Radę UE: Ostatnie propozycje dyskutowane w ramach grupy DAPIX zmierzają do odebrania Komisji możliwości podjęcia samoistnej decyzji o braku odpowiedniego poziomu ochrony danych w kraju trzecim. Komisja Europejska będzie jedynie mogła zrewidować wydaną już, pozytywną decyzję. Proponowane jest również usunięcie z art. 42 wymogu zawarcia gwarancji ochrony danych w prawnie wiążącym instrumencie. W przypadku wyłączeń z art. 44 propozycje grupy DAPIX zmierzają do uszczegółowienia pojęć „uzasadnionego interesu" oraz „interesu publicznego".

Postulaty Fundacji Panoptykon:

- Komisja Europejska powinna mieć możliwość wydania zarówno decyzji stwierdzającej odpowiedni poziom ochrony danych, jak i jej brak. Istotne jest także stworzenie mechanizmu umożliwiającego rewizję podjętej decyzji. Postulujemy także dodanie do tej procedury obowiązku zasięgnięcia opinii Europejskiej Rady Ochrony Danych Osobowych.
- Uważamy, że gwarancje będące podstawą transferu danych powinny znajdować się we wiążącym instrumencie prawnym.
- Postulujemy wprowadzenie przynajmniej minimalnej gwarancji chroniącej administratorów danych przed koniecznością udostępnienia danych osobowych organom państw trzecich, które nie mają odpowiednich porozumień międzynarodowych z UE, a tym samym nie mogą zagwarantować odpowiedniego standardu ochrony praw podmiotów danych.
- Uważamy, że wyłączenia zawarte w art. 44 powinny zostać istotnie ograniczone. Proponujemy, by skorzystanie z nich było dopuszczalne tylko w przypadku transferów o incydentalnym charakterze. Proponujemy również wykreślenie z katalogu wyłączeń uzasadnionego interesu administratora oraz przesłanki interesu publicznego.

Uzasadnienie:

Przekazywanie danych do krajów trzecich jest tematem politycznie drażliwym. Rozporządzenie próbuje pogodzić dwa cele, które mogą stać w konflikcie: ochronę danych oraz ułatwienie transferu danych do krajów trzecich, które nie mogą zapewnić odpowiedniego poziomu ich ochrony. Jak pokazują choćby kontrowersje związane z programem *Safe Harbour*, państwa trzecie nie zawsze zapewniają Europejczykom odpowiedni standard ochrony danych osobowych. Dlatego prawo europejskie powinno przewidywać silniejsze, niż dotychczas gwarancje poszanowania minimalnych standardów w tym zakresie.

Możliwość wydania decyzji stwierdzającej brak odpowiedniego poziomu ochrony danych stanowi polityczne narzędzie w rękach Komisji, które może być wykorzystane do wywarcia nacisku na kraje trzecie. Z drugiej strony, z uwagi na polityczny wymiar przekazywania danych osobowych poza granice UE, decyzja o uznaniu zagranicznych gwarancji prawnych za adekwatne nie powinna być pozostawiona do oceny samej Komisji

Europejskiej. Stąd propozycja włączenia obowiązkowej oceny Europejskiej Rady Ochrony Danych Osobowych.

Przewidziane w art. 44 wyłączenia od reguły, zgodnie z którą wymagana jest decyzja stwierdzająca odpowiedni poziom ochrony danych lub odpowiednie gwarancje (appropriate *safeguards*), stanowią bardzo niebezpieczny i niezrozumiały wyłom w europejskim standardzie ochrony danych osobowych. Szczególnie dotyczy to możliwości transferu danych na podstawie uzasadnionego interesu administratora lub przesłanki interesu publicznego. Trudno logicznie uzasadnić, dlaczego transfer danych do kraju trzeciego, który **nie** gwarantuje odpowiedniego poziomu ochrony danych osobowych, miałby być dopuszczalny w oparciu o te same przesłanki, które uzasadniają przetwarzanie danych w ramach UE (przy bardzo wysokich gwarancjach prawnych). Dlatego postulujemy ograniczenie zakresu stosowania art. 44 do transferów, które nie mają charakteru *„massive, frequent or structural"*[14]. Administratorzy danych skuszeni możliwością oparcia się o odstępstwa, mogą nie chcieć zapewniać odpowiednich gwarancji ochrony danych.

W świetle doniesień o skali wykorzystywania danych Europejczyków przez służby wywiadowcze innych krajów, w szczególności USA, niezbędny wydaje się również powrót do pierwotnego brzemienia art. 42, zaproponowanego przez Komisję w grudniu 2012 r. Administratorzy powinni mieć prawo do odmowy udostępniania danych organom z państw poza UE, o ile umowa międzynarodowa nie przewiduje odpowiednich gwarancji, oraz obowiązek powiadomienia europejskich organów o fakcie udostępnienia danych. Wprowadzenie takiego przepisu nie rozwiąże problemu konfliktu norm prawnych, z którym będzie musiał zmierzyć się administrator danych (zobowiązany jednocześnie do stosowania obcego prawa), ale da UE lepszą pozycję w negocjacjach na poziomie międzynarodowym oraz zwiększy transparentność transferów.

[14] Pogląd taki wyraża także Grupa Robocza Art. 29 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf .