FUNDACJA PANOPTYKON

REFORMA EUROPEJSKIEGO PRAWA O OCHRONIE DANYCH OSOBOWYCH

Najważniejsze problemy do rozwiązania na etapie trilogu

W związku z przyjęciem przez Radę Unii Europejskiej tzw. ogólnego podejścia (*general approach*) w sprawie projektu ogólnego rozporządzenia o ochronie danych osobowych i rozpoczęciem trilogu (negocjacji politycznych między Radą, Komisją i Parlamentem Europejskim), przedstawiamy podsumowanie postulatów Fundacji Panoptykon dotyczących procedowanego projektu.

Ogólne podejście wypracowane w Radzie UE w wielu aspektach należy ocenić pozytywnie. W szczególności na poparcie zasługują propozycje:

i. wzmocnienia pozycji organów odpowiedzialnych za ochronę danych osobowych;

ii. odpowiednio wysokich sankcji administracyjnych za naruszenie prawa;

iii. utrzymanie szerokiego zakresu terytorialnego, zapewniającego stosowanie nowego prawa wobec firm zagranicznych (bez względu na ich siedzibę czy miejsce przetwarzania danych);

iv. zabezpieczenia niektórych praw osób, których dane są przetwarzane, w postaci prawa do informacji oraz prawa do przeniesienia i usunięcia danych;

v. ścisłej współpracy organów ochrony danych osobowych, uwzględniającej zarówno interesy administratorów danych (tzw. obsługa w jednym miejscu), jak i interesy podmiotów danych, które powinny być reprezentowane przez najbliższy im terytorialnie organ (rozbudowany mechanizm konsultowania decyzji).

Niestety, efektem prac Rady UE są również propozycje w niebezpieczny sposób obniżające standard ochrony danych osobowych wyznaczony przez Komisję i Parlament Europejski lub wręcz standard obowiązujący na mocy Dyrektywy 95/46/WE. W niniejszym opracowaniu zwracamy uwagę na szczególnie problematyczne kwestie i wskazujemy potrzebę powrotu do wcześniej przyjętych rozwiązań lub wprowadzenia zmian gwarantujących wyższy poziom ochrony praw i interesów podmiotów danych.

(i) Ograniczenia stosowania nowego prawa wobec organów państwowych i UE

Odpowiednie artykuły projektu: a**rt. 2, art. 21**

Zmiany zaproponowane przez Radę UE:

Wyłączenie instytucji unijnych spod nowego standardu przetwarzania danych oraz pozostawienie państwom członkowskim swobody w kształtowaniu zasad ochrony danych w przypadku, gdy ich przetwarzanie ma związek z bezpieczeństwem narodowym, obronnością, bezpieczeństwem publicznym, interesem ekonomicznym lub fiskalnym, zdrowiem publicznym, opieką społeczną czy „innym ważnym interesem publicznym".

Postulaty Fundacji Panoptykon:

- Ograniczenie wyłączeń od stosowania rozporządzenia o ochronie danych osobowych w relacji obywatel-państwo jedynie do przetwarzania danych w związku z zapobieganiem przestępstwom, ich wykrywaniem, prowadzeniem dochodzeń, ściganiem i wymierzaniem kar.
- Powrót do propozycji Parlamentu Europejskiego przewidującej objęcie rozporządzeniem o ochronie danych osobowych również instytucji unijnych.

Uzasadnienie:

Proponowane rozwiązanie może prowadzić do nieuzasadnionego obniżenia standardu ochrony danych w sektorze publicznym, na co zwraca uwagę Grupa Robocza Art. 29 w dokumencie „Kluczowe tematy z pespektywy trilogu"[1]. Wprowadzenie nadmiernie elastycznych zasad w odniesieniu do niezdefiniowanej grupy instytucji publicznych i nieprecyzyjnie określonych rodzajów działań (kategoria działań związanych z bezpieczeństwem publicznym czy „innym ważnym interesem publicznym" jest niezwykle szeroka) może przyczynić się do spadku zaufania obywateli do całego systemu ochrony danych. Ponadto może to skutkować utrudnieniami w harmonizacji przepisów o ochronie danych na poziomie Unii Europejskiej, ponieważ państwa członkowskie będą mogły sięgać po szeroką gamę wyłączeń, odmiennie kształtując przepisy dotyczące przetwarzania danych w wielu sferach życia publicznego. Podobny skutek, w postaci osłabienia fundamentów nowego reżimu i stworzenie niepewności co do obowiązującego prawa, może mieć całkowite wyłączenie instytucji unijnych, które przetwarzają nie tylko dane swoich pracowników, ale coraz częściej także dane osobowe obywateli i rezydentów UE.

(ii) Definicja danych osobowych i dane pseudonimiczne

Odpowiednie artykuły projektu: **Art. 4. 1.; 4.3b**

Zmiany zaproponowane przez Radę UE:

Projekt Parlamentu Europejskiego, w preambule do rozporządzenia, która ma wpływ na interpretację całego aktu prawnego, wprowadzał bardzo istotne kryterium wyodrębnienia (*single out*) podmiotu danych, odwołujące się do sytuacji, w których bezpośrednia identyfikacja podmiotu danych nie jest możliwa lub potrzebna, podczas gdy administrator danych ma możliwość ustalenia, że przetwarza dane tej, a nie innej osoby. Propozycja Rady UE nie uwzględnia tego typu sytuacji, tym samym usztywniając definicję danych osobowych i ograniczając zakres stosowania projektowanego rozporządzenia.

Projekt przyjęty przez Radę wprowadza również kategorię „danych pseudonimicznych", których wykorzystywanie może wiązać się z wprowadzeniem dodatkowych odstępstw od ogólnych zasad ochrony danych lub wyłączeniem niektórych praw podmiotów danych.

Postulaty Fundacji Panoptykon:

- Poszerzenie definicji danych osobowych o kryterium wyodrębnienia podmiotu danych (*single out*).
- Usunięcie z projektu rozporządzenia definicji danych pseudonimicznych lub zapewnienie, że w żadnym kontekście ich przetwarzanie nie będzie się wiązało z niższym poziomem ochrony (w szczególności w kontekście przetwarzania danych w oparciu o uzasadniony interes administratora).

Uzasadnienie:

Definicja danych osobowych i podmiotu danych to fundamenty całego projektu. Od tego, jak szeroko zostaną one zakrojone, zależy zakres obowiązywania nowego prawa. Jest niezwykle ważne, by przyjęta definicja uwzględniała realia przetwarzania danych osobowych i możliwości, jakie daje rozwój technologii. Coraz częściej, szczególnie w Internecie, **identyfikacja osoby nie jest już potrzebna do tego, żeby móc w istotny sposób ingerować w jej prywatność** – wystarczy możliwość „wyodrębnienia" jej z grona pozostałych użytkowników, np. na podstawie unikatowego profilu, jaki można wygenerować dzięki cyfrowym śladom, 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.

[1] Grupa robocza Art. 29, Kluczowe tematy z perspektywy trilogu, http://www.giodo.gov.pl/plik/id_p/9537/j/pl/.

W tym kontekście ograniczenie definicji danych osobowych do informacji, które dotyczą osoby zidentyfikowanej lub możliwej do zidentyfikowania, to bardzo krótkowzroczne podejście. Podobne stanowisko zajęła Grupa Robocza Art. 29[2], która poparła uwzględnienie możliwości wyodrębnienia jako sposobu identyfikacji osoby, której dane dotyczą, wśród motywów wyjaśniających rozporządzenia. Jednocześnie Grupa zwróciła uwagę, że treść motywu powinna zostać tak sformułowana, żeby jej interpretacja obejmowała numery identyfikacyjne, dane lokalizacyjne, identyfikatory online lub inne szczególne czynniki.

W odniesieniu do nowej kategorii danych – danych pseudonimicznych – Grupa Robocza Art. 29 zwróciła uwagę, że jej wprowadzenie może prowadzić do nieporozumień i stanowić wytrych do stosowania szczególnych odstępstw od standardu ochrony danych osobowych. Ponieważ w istocie są to dane osobowe, które w sposób pośredni (przy wykorzystaniu dodatkowych informacji) mogą zostać powiązane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą, wyodrębnianie ich z pomocą niezależnej definicji jest niepotrzebne, a wręcz może prowadzić do problemów interpretacyjnych. Sam proces pseudonimizacji powinien być traktowany wyłącznie jako system minimalizacji danych i zapewniania ich bezpieczeństwa.

W szczególności Grupa Robocza Art. 29 krytykuje możliwość dopuszczenia niższego standardu ochrony danych pseudonimowych przy przetwarzaniu w oparciu o uzasadniony interes administratora: „Wykorzystywanie danych pseudonimowych jako sposobu zapewnienia gwarancji do zapewnienia rzetelnego przetwarzania danych osobowych może odgrywać rolę w określeniu, czy podstawa prawna w zakresie uzasadnionego interesu może być legalnie wykorzystana. Nadal jest to jednak tylko jeden czynnik spośród wielu a test równowagi zawsze wymaga, aby oceniać również cel przetwarzania"[3].

(iii) Nieprecyzyjna definicja zgody na przetwarzanie danych osobowych

Odpowiedni artykuł projektu: **art. 4 (8)**

Zmiany zaproponowane przez Radę UE:

Przyjęta propozycja dopuszcza zgodę niewyrażoną wprost (*explicit*), która wynika – czy też może zostać wyinterpretowana – z innego zachowania podmiotu danych, np. wejścia na stronę internetową lub rozpoczęcia korzystania z usługi. Takie podejście otwiera drogę do nadużywania konstrukcji zgody i zaciemniania sposobu, w jaki dane są zbierane, a następnie wykorzystywane.

Postulaty Fundacji Panoptykon:

- **Rekomendujemy powrót do definicji zgody zaproponowanej przez Komisję Europejską**, w szczególności wprowadzenie wymogu pozyskiwania wyraźnej i świadomej zgody podmiotu danych oraz podkreślenie jej dobrowolnego charakteru.

Uzasadnienie:

Zgoda podmiotu danych stanowi jedną z sześciu zaproponowanych przez Komisję Europejską 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 taka sytuacja występuje jedynie wówczas, gdy potrzeba przetwarzania danych nie wynika z umowy ani przepisów prawa. Z tego względu oraz ze względu na istotę tego oświadczenia woli, zgoda w każdych okolicznościach powinna być wyraźna, dobrowolna, odnosząca się do konkretnego celu oraz zakresu przetwarzania danych (*specific*) i oparta na rzetelnej informacji (świadoma). W praktyce administratorzy danych nie powinni mieć możliwości przetwarzania danych w oparciu o „domyślnie

[2] 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.
[3] Kluczowe tematy z perspektywy trilogu, *op.cit.*

zaznaczone pola" (*pre-ticked boxes*) ani do domniemywania zgody w oparciu o inne zachowania podmiotów danych.

Propozycja wypracowana przez Radzę UE stanowi 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[4]. Grupa Robocza art. 29 potwierdziła swoje stanowisko w zakresie elementów definicji zgody w dokumencie przygotowanym na potrzeby trilogu, wskazując, że zgoda podmiotu danych musi być świadoma, udzielana na określony cel, dobrowolna i wyraźna[5].

(iv) Odejście od zasady ograniczenia celem przetwarzania danych

Odpowiednie artykuły projektu: **Art. 6.2 i 6.4**

Zmiany zaproponowane przez Radę UE:

Projekt przyjęty przez Radę przewiduje możliwość zmiany celu przetwarzania danych w oparciu o tzw. uzasadniony interes administratora lub „strony trzeciej" (np. innej firmy, z którą administrator współpracuje). Możliwe ma być również praktycznie nieograniczone dalsze przetwarzanie danych w celach historycznych, statystycznych i naukowych, przy czym projekt nie definiuje, jak rozumieć te nieprecyzyjne określenia (np. czy badania prowadzone przez firmę można uznać za cel naukowy).

Postulaty Fundacji Panoptykon:

- Postulujemy wykreślenie Art. 6.4.
- Postulujemy doprecyzowanie pojęć dotyczących badań w celach historycznych, naukowych i statystycznych.
- Przetwarzanie (czy to pierwotne, czy dalsze) do celów badań historycznych, statystycznych i naukowych powinno zawsze być oparte na jednej z podstaw prawnych wymienionych w art. 6.1 lub, w przypadku danych sensytywnych, spełniać wymogi z artykułu 9.2.

Uzasadnienie:

[4] "(...) 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.

[5] Kluczowe tematy z perspektywy trilogu, *op.cit.*

Zasada ograniczenia celem, dla którego przetwarzane dane zostały pierwotnie zebrane, ma fundamentalne znaczenie dla ochrony praw osoby, której dane dotyczą. Zgadzając się na przetwarzanie danych w określonym celu (np. badawczym) lub decydując na przekazanie danych w ramach konkretnej umowy (np. kredytu), osoba, której dane dotyczą, ma prawo oczekiwać, że nie zostaną one wykorzystane w innych celach, np. na potrzeby profilowanej reklamy czy przekazane innej firmie w ramach umowy o współpracy. Samo poinformowanie podmiotu danych o fakcie zmiany podstawy i celu przetwarzania nie rozwiązuje tego problemu, ponieważ nie zabezpiecza autonomii informacyjnej (dane są faktycznie w posiadaniu administratora i będą wykorzystywane). Propozycja Rady UE stoi w sprzeczności z zasadą ograniczenia celem, dla którego przetwarzane dane zostały zebrane, i jako taka podważa fundamenty nowego rozporządzenia. Takie stanowisko zajmuje również Grupa Robocza Art. 29[6].

(v) Rozszerzenie uzasadnionego interesu administratora na podmioty trzecie

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

Zmiana zaproponowana przez Radę UE:

Rozszerzenie klauzuli prawnie usprawiedliwionego interesu administratora danych na „podmioty trzecie" (*third parties*).

Postulaty Fundacji Panoptykon:

- Wykreślenie „podmiotów trzecich" z art. 6.1f.
- Doprecyzowanie, że korzystanie z tej podstawy prawnej przez administratora danych powinno być dopuszczalne tylko wówczas, gdy nie ma on faktycznej możliwości skorzystania z innej podstawy prawnej.

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 nieprzejrzyste z perspektywy osób, których dane dotyczą, prowadząc do **erozji zaufania** między podmiotem danych i ich administratorem[7]. 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. W oparciu o 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.

---

[6] Kluczowe tematy z perspektywy trilogu, *op.cit.*

[7] 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.

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

(vi) Możliwość zbierania większej ilości danych niż to konieczne

Odpowiedni artykuł projektu: **art. 5.1c**

Zmiany zaproponowane przez Radę UE:

W miejsce ugruntowanego w doktrynie ochrony danych osobowych pojęcia „danych niezbędnych do realizacji celu", Rada UE proponuje nowe pojęcie „nienadmiarowego przetwarzania danych" (*non-excessive data processing*). Z projektu usunięto również wymóg, że dane osobowe mogą być przetwarzane wyłącznie wtedy, gdy danego celu nie można zrealizować przy użyciu informacji, która nie ma takiego charakteru.

Postulaty Fundacji Panoptykon:

- Przywrócenie brzmienia art. 5.1c z propozycji Komisji Europejskiej lub Parlamentu Europejskiego uwzględniającej w pełnym kształcie zasadę ograniczenia zbierania danych do niezbędnego minimum.

Uzasadnienie:

Zasada ograniczenia zbierania danych do niezbędnego minimum jest jednym z fundamentów reżimu ochrony danych osobowych. Ani prywatne, ani publiczne podmioty nie powinny pozyskiwać danych „na wszelki wypadek", czyli zbierać informacji, których podstawa i cel przetwarzania danych nie uzasadnia (np. bank nie powinien pytać klienta o stan zdrowia, a ubezpieczyciel – o stan rachunku oszczędnościowego). Propozycja Rady UE podważa tę zasadę, odchodząc od twardego zakazu przetwarzania danych, które nie są niezbędne. Koncepcja „nienadmiarowego przetwarzania danych" nie ma oparcia w doktrynie i jest otwarta na zbyt swobodne interpretacje, stanowiąc niebezpieczne otwarcie na zbieranie wszystkiego, co dany podmiot uzna za uzasadnione.

(vii) Transfer danych poza granice UE niemal bez ograniczeń

Odpowiednie artykuły projektu: **art. 40-45**

Zmiany zaproponowane przez Radę UE:

Propozycja Rady UE przewiduje bardzo szerokie podstawy dla transferu danych poza granice UE, w tym dopuszcza również odstępstwa od ogólnych zasad transferu danych dla firm, które wykażą „uzasadniony interes" w takim działaniu. Rada UE nie zdecydowała się również na wprowadzenie (za przykładem Parlamentu Europejskiego) obowiązku odmowy udostępniania przetwarzanych danych organom z państw spoza UE, o ile umowa międzynarodowa nie przewiduje odpowiednich gwarancji, oraz obowiązku powiadomienia europejskich organów o fakcie udostępnienia danych.

Postulaty Fundacji Panoptykon:

- Wyłączenia zawarte w art. 44 powinny zostać istotnie ograniczone, w szczególności usunięta powinna zostać możliwość transferu danych w oparciu o uzasadniony interes administratora. W przypadku, gdyby okazało się to niemożliwe, konieczną zmianą jest wprowadzenie zastrzeżenia, że art. 44.1h może być stosowany jedynie wyjątkowo i tylko w odniesieniu do nie masowego, nie powtarzającego się i nie zorganizowanego przekazywania danych.

- Wprowadzenie obowiązku odmowy udostępniania przetwarzanych danych organom z państw spoza UE, o ile umowa międzynarodowa nie przewiduje odpowiednich gwarancji, oraz obowiązku powiadomienia europejskich organów o fakcie udostępnienia danych.

Uzasadnienie:

Jak pokazują 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.

Rozwiązania zaproponowane przez Radę UE nie gwarantują, że po przyjęciu rozporządzenia wzrośnie standard ochrony danych Europejczyków przetwarzanych przez międzynarodowe korporacje – a przecież jest to jeden z podstawowych celów realizowanej reformy. 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).

Idąc za rekomendacją Grupy Roboczej Art. 29 Parlament Europejski zaproponował usunięcie paragrafu h art. 44.1, pozwalającego na dokonywanie transferów do państw spoza UE ze względu na uzasadniony interes administratora. Zdaniem Grupy art. 44.1h ostatecznie może być utrzymany, o ile będzie stosowany jedynie wyjątkowo i tylko w odniesieniu do nie masowego, nie powtarzającego się i nie zorganizowanego przekazywania danych[8].

W świetle doniesień o skali wykorzystywania danych Europejczyków przez służby wywiadowcze innych krajów, w szczególności USA, administratorzy powinni mieć obowiązek odmowy udostępniania danych organom z państw spoza 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.

(viii) Brak dostatecznych gwarancji ochrony praw podmiotu danych w sytuacji profilowania

Odpowiednie artykuły projektu: **Art. 4.12a i art. 20**

Zmiany zaproponowane przez Radę UE:

Propozycja Rady UE utrzymuje ograniczenia dotyczące podejmowania decyzji dotyczących podmiotów danych w oparciu o profilowanie („środków opartych na profilowaniu"), nie przewiduje jednak dodatkowych gwarancji prawnych w sytuacji samego poddania profilowaniu. Zgodnie z definicją profilowania propozycja Rady UE ogranicza też stosowanie tych szczególnych przepisów jedynie do w pełni zautomatyzowanych procesów.

Postulaty Fundacji Panoptykon:

- Poszerzenie definicji profilowania o procesy, które nie opierają się wyłącznie na automatycznym przetwarzaniu danych.
- 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,

[8] Kluczowe tematy z perspektywy trilogu, *op.cit.*

jak również prawa do wyjaśnienia ostatecznej decyzji i wyrażenia sprzeciwu wobec tworzenia i wykorzystania profilów.

- Doprecyzowanie celów, jakim może służyć profilowanie zgodnie z rekomendacją Grupy roboczej Art. 29.

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. 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[9]. 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. Na te ryzyka zwraca uwagę również Grupa Robocza Art. 29 w swojej opinii do projektu rozporządzenia[10].

Z powyższych względów niezbędna jest szczelna regulacja, która – nie zakazując takich praktyk –zapewni odpowiednie gwarancje w każdym przypadku zastosowania środków opartych o profilowanie oraz dodatkowe standardy dotyczące samego profilowania. Zgodnie z rekomendacjami Grupy roboczej Art. 29, art. 20 projektu powinien zostać zmodyfikowany poprzez dodanie przepisów dotyczących celów, dla których profile mogą być tworzone oraz wykorzystywane oraz szczególnych obowiązków administratorów do poinformowania osoby, której dane dotyczą[11]. Gwarancje zwiększające przejrzystość i zabezpieczające prawa podmiotów danych są niezbędne nie tylko w kontekście decyzji podejmowanych w oparciu o profilowanie, ale również w odniesieniu do samego procesu. Zaproponowane przez Radę UE podejście, traktujące profilowanie jak każde inne działanie na danych, sankcjonuje niebezpieczny trend, zgodnie z którym predykcyjne profilowanie klientów przez firmy czy kandydatów do pracy przez rekrutujących staje się standardem.

[9] 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.

[10] 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.

[11] Kluczowe tematy z perspektywy trilogu, *op.cit.*