KANCELARIA SENATU
Przedstawiciel Kancelarii Senatu
przy Unii Europejskiej

Bruksela, dnia 2 lutego 2013 r.

**Sprawozdanie nr 10/2013**

# Sprawozdanie ze spotkania Koła Polskiego z dr Wojciechem Wiewiórowskim, Generalnym Inspektorem Ochrony Danych Osobowych

**Bruksela, 22 stycznia 2012 r.**

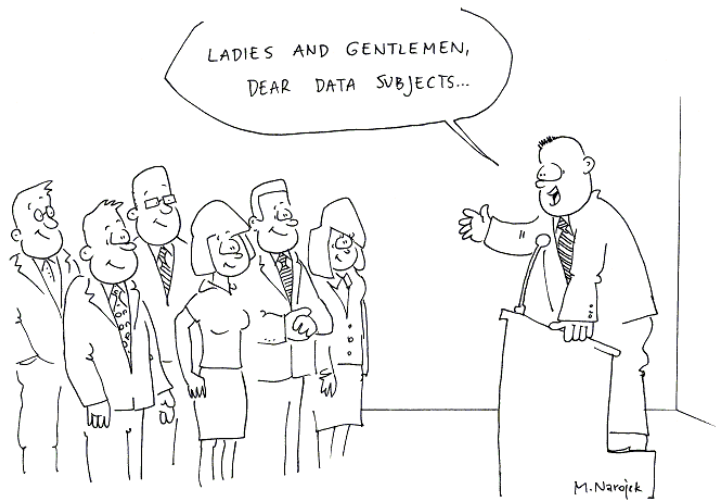
W dniu 22 stycznia w Brukseli odbyło się spotkanie Koła Polskiego (polskich posłów do PE) z dr **Wojciechem Wiewiórowskim**, Generalnym Inspektorem Ochrony Danych Osobowych. Pretekstem do spotkania był VII Europejski Dzień Ochrony Danych. Tematem spotkania była dyskusja na temat aktualnych problemów dotyczących ochrony danych osobowych.

Rok 2012 był okresem prac nad reformą prawa ochrony danych osobowych Unii Europejskiej, w których Parlament Europejski odrywa niezwykle istotną rolę. Projekty aktów legislacyjnych dotyczących nowych ram prawnych ochrony danych osobowych są przedmiotem intensywnych prac wielu komisji parlamentarnych, w tym Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Komisji Prawnej, Komisji Rynku Wewnętrznego i Ochrony Konsumentów oraz Komisji Przemysłu, Badań Naukowe i Energii. Jednocześnie pojawiło się wiele nowych tematów, które mogą mieć wpływ na przyszłość ochrony danych osobowych, takich jak nowa infrastruktura cyfrowych usług publicznych, nowelizacja ram prawnych badań klinicznych w Unii Europejskiej, europejska strategia wobec chmury (Cloud Computing), a także nowe projekty budzące kontrowersje i liczne pytania, jak np. projekt INDECT.

Lista zagadnień, które zostały omówione podczas spotkania, obejmowała:

- Stan prac nad zmianą ram prawnych ochrony danych osobowych w Unii Europejskiej
- Europejska strategia wobec chmury (Cloud Computing)
- Nowelizacja ram prawnych podpisów elektronicznych w UE – propozycja rozporządzenia

- Nowelizacja ram prawnych badań klinicznych w UE – propozycja rozporządzenia
- Projekt INDECT




Dr **Wojciech Wiewiórowski** rozpoczął swoje wystąpienie od stwierdzenia, że wszyscy jesteśmy podmiotami danych osobowych. Uświadomił zgromadzonym, że nawet tak prosta czynność, jak synchronizacja IPADa z komputerem, może oznaczać, że udostępniamy nasze dane każdemu serwisantowi samochodu.

## 1. Stan prac nad zmianą ram prawnych ochrony danych osobowych w Unii Europejskiej

Generalny Inspektor przypomniał, że w **art. 47. i 51. Konstytucja Rzeczpospolitej Polskiej** odnosi się do ochrony danych osobowych. Art. 47 stanowi, że: „Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym".

Z kolei w art. 51. Konstytucja stanowi, że:

1. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
2. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
3. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.

4. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.
5. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

Traktatową podstawę do ochrony danych osobowych stanowi **art. 16 Traktatu o funkcjonowaniu UE**. Stanowi on, co następuje:

1. Każda osoba ma prawo do ochrony danych osobowych jej dotyczących.
2. Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów.

Zasady przyjęte na podstawie niniejszego artykułu pozostają bez uszczerbku dla zasad szczególnych przewidzianych w **artykule 39 Traktatu o Unii Europejskiej**.

Dr Wiewiórowski odniósł się również do kwestii zmian prawnych w ochronie danych osobowych na poziomie europejskim, a co za tym idzie również w Polsce. Komisja Europejska opublikowała komunikat pt. **„Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej”.** Obecnie w Parlamencie Europejskim i Radzie prowadzone są prace nad dwoma dokumentami:

- Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych COM(2012) 11 z 25 stycznia 2012 r.

http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_pl.pdf

- Projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych COM(2012) 10 z 25 stycznia 2012 r.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:PL:PDF

Główny Inspektor podkreślił, że w Parlamencie Europejskim te dwa ww. projekty są traktowane jako pakiet i rozpatrywane razem, co zapowiedziały wszystkie frakcje parlamentarne. Rada z kolei stoi na stanowisku, że mogą dyskutować o rozporządzeniu, natomiast dyrektywa dotycząca policji, sądów, postępowań karnych, itp. - nie jest w kompetencji Unii Europejskiej.

Dr **Wiewiórowski** stwierdził, że niezależnie od tego, cokolwiek zostanie uchwalone w dyrektywie będzie i tak lepsze niż to, co mamy obecnie w Polsce, bowiem nie ma niezależnej kontroli danych policji, służby, prokuratury. Tak więc zapisy dyrektywy będą korzystniejsze dla Polski w porównaniu z obecną sytuacją i brakiem jakiejkolwiek kontroli.

W Radzie Europejskiej ww. projektami zajmuje się Grupa robocza Rady UE ds. Wymiany Informacji i Ochrony Danych, na której Polskę reprezentują:

- **Ministerstwo Administracji i Cyfryzacji** (cały pakiet) i/lub
  **Ministerstwo Spraw Wewnętrznych** (dyrektywa) oraz
  **Stałe Przedstawicielstwo RP przy UE**
- **Eksperci uczestniczący w Grupie:**
  Biuro Generalnego Inspektora Ochrony Danych Osobowych

**Stanowisko Polski uzgadniają:** Ministerstwo Gospodarki, Ministerstwo Sprawiedliwości, Ministerstwo Zdrowia, Główny Urząd Statystyczny, Urząd Komunikacji Elektronicznej oraz Ministerstwo Spraw Zagranicznych
**Instrukcję przyjmuje** natomiast Komitet Rady Ministrów ds. UE.
Dr Wiewiórowski podkreślił, że na razie koordynacja prac po stronie rządowej jest niezła.

Nad projektami pracuje również komisja LIBE Parlamentu Europejskiego. **Sprawozdawcami PE są:**

- **Jan Phillipp Albrecht** (Zieloni, Niemcy) – rozporządzenie
- **Dimitrios Droutsas** (Socjaliści S&D, Grecja) – dyrektywa

Przebieg prac nad rozporządzeniem w PE wygląda następująco:

- Wrzesień 2012: Wymiana poglądów nt. rozporządzenia w komisji LIBE
- 9-10 października 2012 - Komitet Międzyparlamentarny Parlamentu Europejskiego i parlamentów krajowych (Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych LIBE)

- Październik 2012: Prezentacja szczegółowego dok. roboczego nt. rozporządzenia (WD 2)
- Październik /listopad 2012: Czytanie w komisji LIBE
- Listopad 2012: Prezentacja projektu sprawozdania
- Grudzień 2012: Termin wnoszenia poprawek
- Koniec stycznia/luty 2013: Dyskusja nt. poprawek w Komisji LIBE
- Luty 2013: Dyskusja nt. opinii innych komisji
- Marzec/kwiecień 2013: Orientacyjne głosowanie w LIBE
- Lato 2013 (?) Trylog z Radą i Komisją
- Początek 2014 (?): Głosowanie na sesji plenarnej

**Dr** Wiewiórowski podkreślił, że jeśli do 2014 r. pakiet nie zostanie uchwalony – to nie będzie uchwalony przez następne 10 lat. To od posłów PE zależy, jak będzie wyglądała ochrona prywatności w UE przez kolejne 10 lat.

Pojawiają się dwa rodzaje wątpliwości dotyczących rozporządzenia i dyrektywy:

- fundamentalne – czy można uchwalać rozporządzenie w zakresie ochrony danych osobowych (Wielka Brytania)
- szczegółowe (np. jak usankcjonować prawo do bycia zapomnianym - trudne zagadnienie)

## 2. Europejska strategia wobec chmury (Cloud Computing)

Kolejną kwestią, omówioną przez Głównego Inspektora Danych Osobowych było tzw. przetwarzanie w chmurze, czyli *cloud computing*.

Definicja przetwarzania w chmurze przygotowana przez *National Institute of Standards and Technology* (NIST)[1] zwraca uwagę na możliwości nieograniczonego zarządzania przestrzenią, wygodnego dostępu na żądanie do konfigurowalnej i współdzielonej puli zasobów obliczeniowych (np. sieci, serwerów, pamięci masowej, aplikacji i usług), które mogą być dostarczane szybko i wymagają minimalnego wysiłku w kwestii zarządzania i interakcji z

[1] "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics**,** three service models, and four deployment models." National Institute of Standards and Technology (NIST), Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011, Page 3.

usługodawcą. Jednocześnie NIST podkreśla, że przetwarzanie w chmurze nie jest nową technologią. NIST definiuje również pięć głównych cech chmur oraz ich trzy modele usługowe i pięć modeli wdrożeniowych

Pięć głównych cech chmurowego modelu przetwarzania to:

- *On-demand self-service* – klienci chmury powinni mieć możliwość skorzystania z usług w chmurze (np. obliczeniowych, pamięci i zasobów pamięci masowej), używając mechanizmu samoobsługi (np. portal internetowy), tak żeby nabywanie usług nie wymagało interwencji przez usługodawcę chmury,

- *Broad network access* – chmura powinna być dostępna z każdego miejsca (jeśli wymagane) na różnych urządzeniach, takich jak: smartfony, tablety, laptopy, komputery stacjonarne oraz na wszystkich innych typach czytników, istniejących obecnie lub w przyszłości,

- *Resource pooling* – chmury powinny udostępniać pule współdzielonych zasobów, które wykorzystywane są przez klientów chmury. Zasoby, takie jak: moc obliczeniowa, pamięć, sieć i dysk, przydzielone są do klientów korzystających z usług udostępnionej, wspólnej puli. Zasoby pobierane są z aktualnej lokalizacji, a klienci nie są świadomi lokalizacji tych zasobów,

- *Rapid elasticity* - chmury powinny zapewnić szybkie zastrzeganie i uwolnienie zasobów ze względu na zapotrzebowanie usług w chmurze. Powinno to odbywać się automatycznie, bez konieczności ingerencji człowieka. Ponadto, odbiorcy usługi chmury powinni odnosić wrażenie, że istnieje nieograniczona pula zasobów – usługa jest w stanie spełnić wymagania dla dowolnego scenariusza w przypadku użycia,

- *Metered Services* – model chmury, określany jako „*pay-as-you-go*", powinien czasem umożliwiać ładowanie usług konsumenta chmury w oparciu o rzeczywiste wykorzystanie zasobów chmury. Wykorzystanie zasobów jest monitorowane, zgłaszane i kontrolowane przez dostarczyciela usług chmurowych i politykę serwisu, które zapewniają przejrzystość rozliczeń, zarówno z dostarczycielem usług chmurowych, jak i z konsumentem usług.

Dr Wiewiórowski zwrócił uwagę na następujące problemy dotyczące przetwarzania w chmurze:

- Uczestnicy gry rynkowej oraz ich konsultanci nie mają fachowej i praktycznej wiedzy, brak im również doświadczenia w kontakcie z chmurą;
- Nierówność w zakresie wiedzy i doświadczenia;
- Brak wspólnej rozwiniętej i utrwalonej terminologii;
- Zastosowane dotąd rozwiązania technologiczne nie są wystarczająco sprawdzone;
- Ogromna ilość gromadzonych i przetwarzanych danych;
- Transgraniczność i globalizacja rozwiązań;
- Brak transparentności przetwarzania danych, procedur i praktyk po stronie procesora, w szczególności brak wiedzy od podwykonawcach procesów i ich procedurach;
- Brak transparentności ogranicza możliwość przeprowadzenia analizy ryzyk;
- Brak transparentności ogranicza możliwość kontroli przetwarzania;
- Dostarczyciele usług chmurowych są pod presją zwrotu kosztów inwestycji;
- Użytkownicy chmur są pod presją zmniejszania kosztów
- Niskie ceny są powiązane z akceptacją umów adhezyjnych.
- Błędy wynikające zazwyczaj z braku zrozumienia, trudności komunikacyjnych i niejasnych klauzul umownych;
- Incydenty bezpieczeństwa informacji takie jak naruszenie tajemnic prawnie chronionych, integralności i dostępności danych (w tym danych osobowych);
- Przesyłanie danych osobowych do tzw. państw trzecich nie zapewniających odpowiedniego poziomu ochrony;
- Łamanie prawa i zasad ochrony danych osobowych;
- Administrator danych osobowych narażony jest na nieznane mu zagrożenia;
- Administrator danych osobowych akceptuje standardowe klauzule w umowach dostarczonych przez dostarczyciela usług chmurowych włączają w to sytuacje, gdy procesor może zmieniać sposób przetwarzania danych;
- Dostarczyciele usług chmurowych i ich podwykonawcy używają danych osobowych dostarczonych przez użytkownika do innych celów bez wiedzy administratora danych osobowych;
- Rozliczalność i odpowiedzialność rozmywa się w łańcuchu podwykonawców;
- Brak możliwości kontroli dokonywanej przez administratora danych osobowych lub jego przedstawiciela;
- Organy ochrony danych nie mają możliwości dokonywania inspekcji systemów chmurowych.

Dr Wiewiórowski odniósł się także do komunikatu Komisji Europejskiej **Wykorzystanie potencjału chmury obliczeniowej w Europie z 27 września 2012 r.** COM(2012) 529 final

Komisja Europejska podejmie trzy konkretne działania sprzyjające przyjęciu chmury obliczeniowej:

(1) Działanie 1: uporządkowanie dużej ilości różnych norm;
(2) Działanie 2: bezpieczne i uczciwe warunki umowne
(3) Działanie 3: utworzenie Europejskiego partnerstwa na rzecz chmur obliczeniowych w celu wspierania innowacji i wzrostu przez sektor publiczny.

## 3. Nowelizacja ram prawnych badań klinicznych w UE – propozycja rozporządzenia

Badań klinicznych dotyczy projekt z dnia 17.7.2012 r. COM(2012) 369 final – **Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE**. Projekt rozporządzenia UE o badaniach klinicznych odnosi się do kwestii danych osobowych w rozdziale V, dotyczącym ochrony uczestników i świadomej zgody. Odsyła on do aktów prawnych dotyczących danych osobowych.

Ponadto w odniesieniu do ochrony danych osobowych zastosowanie mają przepisy dyrektywy 95/46/WE9 i rozporządzenia (WE) nr 45/200110.

W bazie danych UE nie będą gromadzone żadne dane osobowe uczestników biorących udział w badaniu.

Ważne jest, by dane osobowe badaczy, które mogą być gromadzone w bazie danych UE, przechowywane były zgodnie z wyjątkiem przewidzianym w art. 17 ust. 3 lit. b) wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (ogólne rozporządzenie o ochronie danych). W razie wykrycia przypadków niewłaściwego prowadzenia badań klinicznych ważne byłoby na przykład zidentyfikowanie wszystkich badań klinicznych, w które zaangażowani byli ci sami badacze, nawet kilka lat po zakończeniu tych badań klinicznych.

## 4. Nowelizacja ram prawnych podpisów elektronicznych w UE – propozycja rozporządzenia

Ostatnią kwestią, którą omówił dr Wiewiórowski były podpisy elektroniczne, których dotyczy **Rozporządzenie dotyczące identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym**. Rozporządzenie to zastąpi ustawę o podpisie elektronicznym.

Na koniec swojego przemówienia dr Wiewiórowski odniósł się do kwestii tzw. smart-grid – inteligentnych liczników energetycznych. Przy pomocy takich liczników, można ustalić nie tylko wielkość zużycia energii, ale również, na jakie godziny przypadają szczyty zużycia energii. Jeśli ustawimy liczniki na poszczególnych obwodach w domu i sekundowy okres ustawiania danych, wówczas można nawet stwierdzić, jaki program w danym momencie oglądany jest w telewizji, ale również, czy ktoś w danym momencie przebywa w domu.

## 5. Projekt INDECT

Następnie głos zabrał profesor **Andrzej Dziach** z Akademii Górniczo-Hutniczej w Krakowie, koordynator projektu INDECT, który prowadzi badania naukowe w obszarze bezpieczeństwa i prywatności. Podkreślił, że bezpieczeństwo i prywatność to wzajemnie uzupełniające się obszary. INDECT jest projektem naukowo-badawczym, przyznanym do realizacji AGH w Krakowie. Jest to duże wyróżnienie i świadczy o sukcesie nauki polskiej, bowiem jest to największy projekt europejski koordynowany przez uczelnię wyższą.

Projekt zyskał opinię kontrowersyjnego, z uwagi na wprowadzenie domniemanego totalnego monitoringu i obserwacji, itp. Zastrzeżenia były nawet tak daleko idące, że projekt miał zakładać monitoring przez satelity, pola elektromagnetyczne, czy też czytać w myślach ludzi, itp. Projekt stał się popularny a to ciąży. Podkreślił, że projekt nie ma nic wspólnego z orwellowskim systemem inwigilacji, ale ma pomagać policji w łapaniu przestępców.

Projekt zajmuje się ochroną prywatności i ochroną danych osobowych poprzez rozwijanie technologii kryptografii kwantowej i znaków wodnych, które są w stanie zabezpieczyć dane na dyskach twardych. W konsekwencji żadne haker nie ma szans dostania się do nich.

Jeśli chodzi o monitoring, to projekt jest oparty na filozofii monitoringu zagrożeń. Badaczy interesuje, gdy pojawia się zagrożenie, np. ktoś wyciąga nóż, pistolet, itp. Wtedy zapala się

światełko na monitorze a operator decyduje, czy sytuacja jest zagrożeniem, czy zabawą np. w czasie juwenaliów. Nie jest prowadzony monitoring w sposób ciągły, ale tylko obserwacja tych zdarzeń, które mogą stanowić zagrożenie dla ludzi. Nosi on nazwę 'black box monitoring' – monitoring zagrożeń. Monitoring koncentruje się na dwóch obszarach: dziecięcej pornografii i sprzedaży organów ludzkich, co jest związane z przestępczością. Projekt jest oceniany bardzo wysoko. Ochrona prywatności to podstawowe prawo człowieka i projekt respektuje to prawo.

Podsumowując, cele systemu to m.in. ochrona danych oraz wykrywanie niebezpiecznych narzędzi poprzez kamery monitoringu czy lokalizowanie w sieci źródeł pornografii dziecięcej.

Na koniec prof. Dziach podał przykład nowoczesnych smartfonów i poinformował, że od 5 miesięcy istnieje oprogramowanie, które wysyła informacje o posiadaczu tego smartfona automatycznie, nawet w trybie uśpionym. To jest rozwiązanie komercyjne. Kolejny przykład ingerencji w prywatność to rozwiązania przyjęte przez google i facebook. Informacje tam gromadzone przekazywane są do serwerów amerykańskich. Czy takie gromadzenie danych przez Amerykanów w jednym miejscu nie jest ingerencją w prywatność?

Prof. Dziach podziękował posłom Kowalowi i Kurskiemu za trzeźwy, życzliwy głos w PE, tłumaczący, czym jest ten projekt.

Prof. **Jan Derkacz** z AGH dodał, że w projekcie zakrywane są wrażliwe części obrazu, np. numery rejestracyjne, twarz, itp. Klucz kryptograficzny pozwala na odtworzenie danych. Warto tego typu rozwiązania wziąć pod uwagę. W ramach badań oczywiście przestrzegane są regulacje i normy etyczne. Przy projekcji istnieje rada etyki – Ethics Board. Ma miejsce współpraca z GIODO, z instytucjami pozarządowymi (Panoptykon). Jeśli chodzi o uczestników badań, to są oni informowani, czego dotyczą badania, w których biorą udział i wyrażają świadomą zgodę na udział w tych badaniach. W każdym momencie mogą się z nich wycofać.

## 6. Debata

Poseł **Rafał Trzaskowski** (EPP, Polska) powiedział, że najważniejsze jest zachowanie w pracach nad ochroną danych osobowych równowagi między ochroną danych i dążeniem do ograniczenia negatywnego wpływu tej ochrony na możliwości wykorzystania modeli biznesowych, bowiem gospodarka internetowa jest ważna i prorozwojowa. Zapisy Komisji Europejskiej wprowadzają w błąd, stosując pojęcia takie, jak np. prawo do zapomnienia, czy próba wpływania na profilowanie, bowiem stworzyły wrażenie, że można wymazać ślady swojej obecności w internecie. W Polsce zawarto porozumienie między Lewiatanem a Fundacją Panoptykon. W tym względzie Europa jest daleko za nami. Podkreślił jednak, że pojawia się zagrożenie, które może mieć podobne konsekwencje do debaty nad ACTA, bowiem przestaniemy mówić o konkretach, a skoncentrujemy się na tym, kto jest za ochroną internautów, a kto przeciw. Niektóre siły polityczne będą próbowały to wykorzystać – w tym kierunku idą propozycje Zielonych. Ważne jest umożliwienie biznesowi rozwijania modeli biznesowych. Trzeba jasno określić takie kwestie, jak dostęp, definicje, kwestie profilowania i ustalić, co jest korzystne i niezbędne w badaniach naukowych a co niekorzystne i dyskryminujące. Dla przykładu, należy jasno określić definicję odbiorców danych i uzasadnionego interesu administratora (np. zapobieganie przestępstwom popełnianym na szkody administratora). Konieczny jest dialog między rządem, GIODO, biznesem i NGOsami.

Dr **Wiewiórowski** powiedział, że w kontekście definicji odbiorców danych w ostatnim czasie nastąpiło zbliżenie stanowisk GIODO z Lewiatanem i Polskim Stowarzyszeniem Marketingu. GIODO i inne organizacje są w stanie tę definicję zaakceptować. Jeśli chodzi o profilowanie, to najważniejsze jest, by osoba podlegająca profilowaniu była o tym poinformowana.

**Katarzyna Szymilewicz,** prezes Fundacji Panoptykon, podkreśliła, że konieczna jest aktualizacja regulacji w zakresie ochrony danych osobowych, bowiem technologia wyprzedziła obowiązujące prawo. Wykonano ogromną pracę nad projektem, jednak nie można dopuścić do kompromisów idących zbyt daleko. W kontekście prawa do prywatności, ważne jest przygotowanie regulacji, które powinny tego prawa bronić. Swobodny przepływ informacji nie może pójść tak daleko, aby prywatność przestała istnieć w Polsce. Istnieje przyzwolenie na odbieranie prawa do prywatności z pewnych względów. W tym kontekście pojawia się jednak parę rzeczy niepokojących, dlatego tak ważne jest określenie definicji, zakresu stosowania przyjmowanych regulacji, co znaczyć ma zgoda, podmiot danych, itp. Wynik prac w komisji IMCO PE nad projektem rozporządzenia jest bardzo trzeźwiący, żeby nie powiedzieć alarmujący: posłowie zamiast bronić praw obywateli-konsumentów wybrali

ochronę interesów biznesu i postawili na swobodny przepływ danych. Jeśli ta tendencja się utrzyma, "wielka reforma" będzie gwoździem do trumny prywatności w cyfrowym świecie. Definicja zgody w obecnym prawie jest bardzo dobra – niektórzy posłowie chcą ją jednak poluźnić. Zgoda ma znaczyć to, co intuicyjnie rozumiemy pod tym pojęciem. W odniesieniu do uzasadnionego interesu administratora danych, praktyka kilkunastu lat pokazała, że przepis ten bywa nadużywany. Firmy korzystają z niego i dane są przekazywane kontrahentom. Jeśli zostanie w takim kształcie, jak proponuje KE, będzie miała miejsce „dramatyczna niespójność". Z kolei definicja prawa do zapomnienia idzie zbyt daleko. To samo dotyczy profilowania – na te tematy konieczny jest dialog.

Poseł **Tadeusz Zwiefka** (EPP, Polska) uspokoił dr Wiewiórowskiego stwierdzając, że w PE nie obowiązuje zasada kosza w przypadku końca kadencji a data wyborów nie jest datą graniczną na przyjęcie przepisów.

Posłanka **Lidia Geringer der Oedenberg** (S&D, Polska) spytała, czy na stronie GIODO pojawi się instrukcja, jak dać się zapomnieć w internecie. Odniosła się w tym względzie do przykładu modelu skandynawskiego. Spytała również, jaki będzie ciąg dalszy projektu INDECT - jak zostanie wdrożony w życie.

Poseł **Piotr Borys** (EPP, Polska) spytał, na ile kwestie dotyczące INDECTu będą wdrażane w przestrzeni publicznej a na ile będą wykorzystywane w sposób komercyjny.

Dr **Wiewiórowski** odpowiedział, że nie jest w stanie zrealizować projektu o prawie do bycia zapomnianym, jak to ma miejsce w projekcie skandynawskim realizowanym w Norwegii. Na norweskiej stronie internetowej jest instrukcja, w jaki sposób usuwać dane z serwisów, ale również pomagają w tym sami pracownicy biura GIODO w Norwegii. Zatrudniono dwóch pracowników z grantu. W krótkim czasie wpłynęło 1470 wniosków o pomoc w usuwaniu treści w internecie. GIODO nie jest w stanie obsłużyć takiej ilości wniosków w ramach swojego biura. Interactive Advertising Bureau (IAB) – stowarzyszenie pracodawców internetowych było chętne, ale ich chęć ostatnio przycichła. Jest to jedno z działań do zrealizowania w 2013. Dr Wiewiórowski przyznał, że nie wierzy w procedury KE, ale wierzy w zaproponowaną ideę. Do realizacji tego projektu potrzebny byłby osobny departament skargowy, na co nie ma w tej chwili środków.

Odnosząc się do dyrektywy i kwestii przetwarzania danych przez policję i służby, dr Wiewiórowski przyznał, że dostęp do danych służb i policji oraz kontrola nad danymi

gromadzonymi przez służby stanowi poważny problem na poziomie PE. Dania, Wielka Brytania i Niemcy twierdzą z kolei, że to jest bezpieczeństwo publiczne (nie narodowe) i sobie z tym świetnie dają sami radę. W Polsce potrzebny jest niezależny organ, nie wewnętrzny jak ABW, czy CBA, ale taki, który z zewnątrz będzie się tym kwestiom przyglądał. Do takiego organu powinna wpływać skarga a on powinien ją zbadać – takiego systemu w Polsce nie ma. Wspiera ideę tego, by dyrektywa została uchwalona również w zakresie bezpieczeństwa publicznego.

Organy nadzoru są w wielu krajach różnie zorganizowane i mają różne uprawnienia. Dla przykładu, węgierski odpowiednik GIODO ma prawo do zmieniania procedur tajności. W Wielkiej Brytanii powołano inny organ niż GIODO - niezależnie powoływany, zajmuje się tymi kwestiami, nie podlega premierowi a parlamentowi. Organy te mają inne umiejętności niż GIODO. Dr Wiewiórowski przyznał, że nie byłby w stanie osobiście skontrolować bazy policyjnej.

Odnośnie projektu INDECT, GIODO nie zgadza się ze wszystkimi działaniami prowadzonymi w ramach tego projektu. Istnienie projektu i podejmowane działania pokazały dwa duże problemy, co jest winą kształtu badań naukowych. Po pierwsze – prowadzone są badania naukowe, które mają doprowadzić do określonego rezultatu, ale nie ma oceny, jak będzie wykorzystany ten efekt - czy w policji, czy będę to efekty skomercjalizowane. Nie ma oceny wpływu tego projektu na prywatność. Druga kwestia – GIODO kwestionuje sposób prowadzenia badań na uniwersytetach w Polsce. Z prac komisji etycznej nie wynika, że wszyscy uczestnicy badań są poinformowani o przysługujących im prawach. Monitoring prowadzony był w miejscach, gdzie byli studenci i pracownicy naukowi, którzy o tym nie wiedzieli. Naukowcy w Polsce albo nie znają kodeksów własnych uczelni, albo uczelnie nie mają tych kodeksów.

Prof. **Dziach** powiedział, że problem produktu i jego zastosowalności to problem rzeka. Dla przykładu - grafen to wynalazek epokowy, służący do produkcji monitorów, które będzie można zwijać, ale można go też wykorzystać do celów militarnych. Czy to znaczy, że nie mają się tym zajmować? Projekt INDECT jest w nieznacznej części elementem badań z zakresu Security - bezpieczeństwo. Jest to projekt realizowany w ramach VII programu ramowego, który obejmuje ponad 200 projektów. Część projektów jest bardziej wrażliwych niż INDECT, dotyczących badań związanych z przetwarzaniem danych osobowych. INDECT nie należy do nich.

Projekt INDECT zakłada stworzenie szybkich algorytmów w watermarkingu (znaki wodne) – do tej pory ich nie znano. Zakłada m.in. zabezpieczenie przed programami w smartfonach służącymi do inwigilacji. 90% projektu to ochrona danych i tworzenie prototypów w tym obszarze – algorytm kryptografii kwantowej do ochrony danych. Kolejne zadanie to zastosowanie wyszukiwarki twardych dysków w celu poszukiwania elementów dziecięcej pornografii - jest to prototyp. Wyszukiwane są ukryte informacje z treściami zakazanymi - obecnie trwa to kilka minut. W ramach projektu stworzono również prototyp urządzenia wykrywającego porzucony bagaż na lotnisku oraz prototyp zakrywania wrażliwych elementów, tj. twarz i tablica rejestracyjna.

Prof. **Derkacz** podkreślił, że zadaniem członków komisji etycznej jest wykrywanie zagrożeń dla prywatności i ochrona kwestii etycznych. Zaznaczył jednak, że analiza obrazu może dotyczyć kwestii bezpieczeństwa, ale może być także stosowana w analizie obrazu medycznego. Przyznał, że czasem trudno pewne dziedziny badań oddzielić od siebie.

Na koniec dr **Wiewiórowski** poinformował, że tzw. grupa berlińska przygotowuje opracowanie dotyczące prywatności w smartfonach. W lutym przedstawione zostanie opracowanie dla czterech rodzajów oprogramowania. Nawoływał również do sprawdzania swoich rachunków telefonicznych, w szczególności podczas wyjazdów zagranicznych.

**Opracowała:**
**Dr Magdalena Skulimowska**[2]

[2] Na podstawie dyskusji podczas spotkania Koła Polskiego i prezentacji dr Wojciecha Wiewiórowskiego, przedstawionej podczas spotkania.