CEPS Background Briefing

Przygotowania do wyborów do Parlamentu Europejskiego

Kształtowanie debaty o polityce ochrony danych osobowych

Elspeth Guild, Sergio Carrera i Alejandro Eggenschwiler

Wiele obszarów polityki Unijnej będzie przedmiotem kluczowych debat i dyskusji w trakcie kampanii przed wyborami do Parlamentu Europejskiego w dniach 4-7 czerwca 2009. Pomimo iż tematyka i waga przywiązywana do poszczególnych zagadnień będzie się różniła między krajami członkowskimi, zagadnienia, które w ciągu ostatnich 10 lat weszły w zakres polityki i prawa obszaru wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej zasługują na kompetentne i spójne potraktowanie. Polityki te dotyczą bowiem prawa każdej osoby do wolności i bezpieczeństwa w poszerzonej Europie.

Ninijesza nota informacyjna skupia się na polityce ochrony danych osobowych. Po zarysowaniu obecnego stanu polityki UE i kroków które podjęte zostaną w tym zakresie w niedalekiej przyszłości, document ten odnosi się do kluczowych ograniczeń i zagadnień dotyczących tej poliyki. Sekcja końcowa podkreśla główne problemy oraz przedstawia rekomendacje na kolejnych pięć lat.

Niniejsza nota informacyjna jest jedną z czterech zajmujących się odpowiednio imigracją, azylem, ochroną granic i ochroną danych osobowych. Cztery dokumenty są częścią projektu: "Kształtowanie debaty o imigracji: Przygotowania do wyborów do Parlamentu Europejskiego 4-7 czerwca" wspieranego przez Barrow Cadbury Trust – niezależną fundację charytatywną, która finansuje i promuje przedsięwzięcia poświęcone sprawiedliwości społecznej (dodatkowe informacje na http://www.bctrust.org.uk). Celem wszystkich not informacyjnych jest kształtowanie debaty na często kontrowersyjne i techniczne dla partii politycznych tematy w momencie gdy przygotowują się one do wyborów do Parlamentu Europejskiego i kontaktują się z wyborcami.

Espeth Guild jest profesorem w Centrum Prawa Migracyjnego na Uniwersytecie Radboud w Nijmegen (w Holandii) oraz starszym analitykiem sekcji spraw wewnętrznych i sprawiedliwości w Centrum Studiów Polityki Europejskiej (CEPS). Sergio Carrera jest analitykiem w CEPS. Alejandro Eggenschwiler jest młodszym asystentem w CEPS.

Autorzy pragną podziękować Patrykowi Pawlakowi z Europejskiego Instytutu Uniwersyteckiego we Florencji za przetłumaczenie niniejszej noty informacyjnej na język polski.

1. Obecne ramy prawne ochrony danych osobowych w UE

Prawo do ochrony danych osobowych w UE opiera się na szeregu aktów prawnych, zarówno międzynarodowych jak i europejskich (pełna lista aktów przyjętych w dziedzinie ochrony danych znajduje się w Aneksie 1). Podstawowym dokumentem w tym zakresie jest dyrektywa o ochronie danych osobowych z 1995 roku.1 Ustanawia ona ogólne zasady jakimi powinny się kierować państwa członkowskie, aby zagwarantować prawa jednostek do prywatności a jednocześnie umożliwić swobodny przepływ danych. Dyrektywa stosowana jest do operacji takich jak zbieranie, przechowywanie, ujawnianie i rozpowszechnianie danych osobowych przy użyciu srodków automatycznych (bazy elektroniczne) lub nieautomatycznych (tradycyjne systemy rejestracji). Daje ona podmiotowi danych zestaw praw, włącznie z prawem do bycia informowanym w jakis sposób dane te są przetwarzane; prawo do korekty, usunięcia lub zablokowania danych, które były przetwarzane w sposób niezgodny z prawem; oraz prawo do wstąpienia na drogę sądową w przypadku naruszenia praw wynikających z przetwarzania danych osobowych. Odnosząc się do zagrożeń dla ochrony danych osobowych wynikających z rozwoju nowych technologii, dyrektywa wzmocniona została kolejnymi dwoma instrumentami dotyczącymi prywatności w sektorze telekomunikacji2 i komunikacji elektronicznej.3 Głównym zadaniem tych dwóch dokumentów jest zagwarantowanie poufności komunikacji poprzez zabronienie nieupoważnionego podsłuchiwania, nagrywania, przechowywania czy stosowania innych form przechwycania lub nadzoru.

Prywatność i zasady ochrony danych osobowych są również nakreślone w Europejskiej Konwencji Ochrony Praw Człowieka i Praw Podstawowych (art. 8) i Konwencji 108, które zostały przyjęte przez Radę Europy, oraz w Karcie Praw Podstawowych Unii Europejskiej (art. 7 i 8).4 Należy również podkreślić, że w UE istnieją instytucje Europejskiego Inspektora Danych Osobowych (EDPS)5 oraz Grupa robocza art. 29 do spraw danych osobowych,6 które założone zostały jako niezależne ciała o kompetencjach nadzorczych i doradczych. Zwłaszcza EDPS ma za zadanie zapewnić, by instytucje i organy UE postępowały z danymi osobowymi w sposób zgodny z pawem i doradza im odnośnie nowych propozycji aktów prawnych lub wszelkich innych zagadnień mających wpływ na ochronę danych. EDPS współpracuje także z krajowymi organami zajmującymi się ochroną danych osobowych w celu promowania jednolitego poziomu ochrony danych w UE (lista wybranych opinii EDPS znajduje się w Aneksie).7 Z kolei grupa robocza jest platformą dla współpracy między przedstawicielami krajowych organów zajmujących się ochroną danych, EDPS oraz Komisją Europejską.8

Powyższe ramy prawne stosowane są jedynie do tych polityk obszaru wolności, bezpieczeństwa i sprawiedliwości (AFSJ) któreznajdują się w pierwszym filarze, tzn. w Tytule IV TWE (wizy, azyl i imigracja). Zagadnienia ochrony danych osobowych mogą także pojawić się w tych obszarach AFSJ które regulowane są w ramach treciego filaru, tzn. Tytulu VI TUE (współpraca policyjna i sądownicza). Regulowane są one na mocy niedawno przyjętej decyzji ramowej 2008/977/JHA w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych.9 Podział ten jest konsekwencją międzyfilarowej struktury AFSJ. Grozi on obniżeniem standardów i podważa spójność ochrony danych osobowych w UE, zwłaszcza w świetle faktu, że decyzja ramowa nie jest stosowana do przetwarzania danych osobowych dotyczących, między innymi, danych krajowych, danych wymienianych między państwami członkowskimi i państwami trzecimi oraz danych przetwarzanych przez Europol, Eurojust, System Informacji Schengen (SIS) oraz System Informacji Celnej (CIS).

2. Tematy i zagadnienia polityki ochrony danych osobowych

Obszar wolności, bezpieczeństwa i sprawiedliwości jest w znacznym stopniu kierowany przekonaniem, że technologia stanowi rozwiązanie dla każdego zagrożenia. Nie bierze się pod uwagę faktu, że technologia może także prowadzić do większego zagrożenia dla korzystania z praw podstawowych i swobód obywatelskich, zwłaszcza jeśli chodzi o prawo do ochrony danych osobowych, które zostało określone w art. 8 Karty Praw Podstawowych. Do tej pory, UE stworzyła szereg baz danych i systemów wymiany informacji, które obejmują między innymi:10

- EURODAC: baza danych zawierająca odciski palców wszystkich osób starających się o azyl i osób zatrzymanych w trakcie nielegalnego przekraczania zewnętrznej granicy UE. Przed końcem roku 2007, EURODAC zgromadził 1,086,246 zestawów odcisków palców, a w trakcie pierwszych pięciu lat działalności kosztował UE €8.1 miliona. Po spadku w latach 2005 i 2006 statystyki EURODAC pokazują, że w roku 2007 nastąpił 19% wzrost (197,284 w porównianiu do 165,958 w 2006) w ilości transakcji dotyczących danych o osobach ubiegających się o azyl. Liczba osób zatrzymanych w trakcie nielegalnego przekraczania granic spadła w 2007 o 8% do poziomu 38,173.11

- System Informacji Schengen (SIS): baza danych używana przez władze państw należących do strefy Schengen do wymiany danych o niektórych kategoriach osób i dóbr.

1 Directive 95/46/EC on the protection of individuals regard to the processing of personal data and the free movement of such data (OJ 1995 L 281/31).

2 Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24/1).

3 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201/37), amended by Directive 2006/24/EC (OJ 2006 L 105/54).

4 OJ 2000 C 364/1.

5 Art. 41 of Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8/1).

6 Art. 29 of Directive 95/46/EC.

7 http://www.edps.europa.eu/EDPSWEB

8 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

9 Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350/60).

10 Pełen przegląd baz danych UE i systemów wymiany informacji znaleźć można na przykład w: F. Geyer (2008), "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice", CHALLENGE Research Paper No. 9, May 2008, Centre for European Policy Studies.

11 European Commission, Communication, Annual Report on the activities of EURODAC Central Unit in 2007, COM(2009) 13, 26.1.2009, Brussels.

W pierwszej kolejności była ona wykorzystywana jako baza danych o obywatelach państw trzecich którym odmówiono wjazdu na terytorium UE, a następnie przekształcona w SIS z włączeniem państw członkowskich wstępujących do UE w 2004. Planowane jest przekształcenie SIS w bazę danych drugiego pokolenia SIS II, która będzie miała nowe zdolności i informacje.12

- System Informacji Wizowej (VIS): będzie zawierał dane osób ubiegających się o wizy na pobyt krótki w UE;

- Dodatkowo, jako część "Pakietu granicznego" z 2008 roku, Komisja Europejska zaproponowała utworzenie trzech nowych baz danych na dużą skalę: system ewidencji wjazdów/wyjazdów rejestrujący ruch pewnych kategorii obywateli państw trzecich; system automatycznej kontroli granicznej, który na podstawie technologii biometrycznej pozwoli na automatyczną weryfikację tożsamości osoby podróżującej będącej lub nie obywatelem UE; 3) elektroniczny system zezwoleń na podróż (ESTA) który nakładał będzie na podróżnych obowiązek przekazania pewnej ilości danych w celu ich sprawdzenia jeszcze przed wyjazdem (więcej szczegółów znajduje się w nocie informacyjnej na temat ochrony granic).

Zawartość tych przepisów i sposób w jaki narzędzia te są wykorzystywane budzi szereg wątpliwości.

Po pierwsze, naznaczanie danych (ang. data mining) jest jednym z najbardziej wrażliwych zagadnień w debacie o ochronie danych osobowych. Skutki przeszukiwania baz danych przez organy ścigania mogą być problematyczne w zależności od tego jak są one wykonywane. Na przykład, nie każdego dane są we wszystkich bazach danych, co oznacza że podejrzenie pada przeważnie na tych, którzy odpowiadają określonemu przez władze profilowi i którzy są już w bazie danych. Różne rodzaje przeszukiwań poruszają różne problemy. Pojedyncze lub wielokrotne przeszukiwania dotyczące konkretnej osoby należą do najbardziej rozpowszechnionych. Większe wątpliwości budzą przeszukiwania w oparciu o profil, kiedy to agenci organów ścigania nie wiedzą kogo konkretnie szukają. Używanie danych zebranych dla celów handlowych w celach ścigania może również powodować problemy. Aby uniknąć ryzyka niepotrzebnej szkody, dane osobowe zebrane w celach ścigania muszą być bezbłędne. Problemy zaczynają się gdy oryginalne dane są integrowane z bardziej aktualnymi informacjami, zazwyczaj kiedy osoba zwraca na siebie uwagę władz, co tworzy kompletnie arbitralny wizerunek danej osoby. Poza tym, informacje o osobach zebrane w celu poprawy bezpieczeństwa muszą być adekwatne i proporcjonalne, ponieważ masowe zbieranie danych nie gwarantuje większego bezpieczeństwa i jest pogwałceniem praw jednostki do prywatności.

Innym kluczowym zagadnieniem jest zapewnienie by dostęp do danych wrażliwych był ściśle ograniczony do osób dla których jest on niezbędny. Dostęp do baz danych UE zależy od instrumentu na podstawie którego konkretna baza danych została ustanowiona. Na przykład, dostęp do bazy EURODAC jest ograniczony do urzędników którzy sprawdzają, czy osoba aplikująca o azyl starała się wcześniej o azyl w innym kraju (lub wjechala w sposób nieregularny). Jednakże poczyniono również kroki w kierunku poszerzenia tego dostępu dla innych przedstawicieli organów ścigania. Jakość agencji zbierających, przetwarzających i wymieniających dane, jak również konsekwencje umożliwienia dostępu do europejskich baz danych władzom państw trzecich muszą być ostrożnie przeanalizowane. Pomoże to zapewnić że dane osobowe obywateli są traktowane w sposób adekwatny i zgodny z prawem.

W końcu, osoby muszą być odpowiednio chronione przed konsekwencjami zgromadzenia błędnych danych lub niedbałej wymiany danych i muszą być odpowiednio poinformowane o swych prawach w tym zakresie. Według badań opinii publicznej przeprowadzonych przez Eurobarometer w 2008 roku13 większość obywateli UE (64%) obawia się o ochronę danych osobowych, ale jedynie jedna czwarta z nich (27%) jest świadoma praw jakie posiada w przypadku nieprawidłowego obchodzenia się z ich danymi. Mniej niż jedna trzecia (29%) wie, że dane wrażliwe, czyli na przykład o rasie czy pochodzeniu etnicznym, podlegają specjalnej ochronie prawnej.

Zatem prawa jednostek oraz efektywna informacja o tych prawach muszą być zaadresowane jako kolejne kluczowe zagadnienie w debacie o ochronie danych osobowych. Przyczyni się to do wyeliminowania sprzeczności które obecnie osłabiają ramy prawne UE dotyczące ochrony danych, zwłaszcza jeśli chodzi o ich aplikację w zakresie AFSJ. Stopień ochrony istniejący na poziomie UE jest nadal daleki od bycia jednolitym jako że prawa podmiotów zależą w znacznym stopniu od konkretnej bazy danych a przepaść między standardami zagwarnatowymi w poszczególnych obszarach należących odpowiednio do pierwszego i trzeciego filaru jest wciąż znaczna.

3. Przyszłe wyzwania i rekomendacje

Rozwój unijnej polityki ochrony danych osobowych może stanąć w przyszłości przed następującymi wyzwaniami.

Po pierwsze, zasady ochrony prywatności muszą być wbudowane w programy które obsługują bazy danych i systemy informatyczne. Programy te powinny zawierać funkcję automatycznego kasowania danych pod koniec dozwolonego okresu; zapobiegać wszelkim nieautoryzwanym próbom dostępu do danych oraz kopiowania obrazów na ekranie; zabronić zbyt wielu przeszukiwań baz danych z wyjątkiem za posiadaniem nakazu sadowego.

Po drugie, bazy danych nie powinny być tworzone bez wcześniejszej analizy oceny ich wpływu dokonanej przez obiektywne i niezależne organizacje. Jakakolwiek strategia UE odnośnie wymiany danych musi zaczynać się od ewaluacji i spisu istniejących polityk, narzędzi i struktur instytucjonalnych zaangażowancyh w wymianę danych w dziedzinie bezpieczeństwa na poziomie unijnym. Jakakolwiek nowa baza danych powinna być stworzona, a następnie używana, wyłącznie do celów zgodnych z prawem, unikać niejasnych i otwartych definicji oraz bezcelowego zbierania danych.

Po trzecie, systemy zbierania danych nie powinny ujawniać danych wrażliwych dotyczących pochodznia etnicznego, religii i innych aspektów zakazanych na podstawie unijnego prawa o niedyskryminacji. Ukryte kryteria wskazujące na etniczne i religijne cechy, takie jak miejsce urodzenia rodziców lub osoby czy wcześniejsza narodowość powinny być zakazane.

12 Report from the Commission on the Development of the Second Generation Schengen Information System (SIS II) Progress Report – July 2008 – December 2008, COM(2009) 133, 24.3.2009, **Brussels.**

13 The Gallup Organisation (2008), "Data Protection in the European Union. Citizens'perceptions", Eurobarometer, strona 5.

ANEKS

Środki przyjęte

1. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ 1995 L 281/31).
2. Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24/1).
3. Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8/1).
4. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201/37).
5. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105/54).
6. Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350/60).

Opinie przyjęte przez Europejskiego Inspektora Ochrony Danych w 2009 r.
Nadzór

1. Opinion of 29 April 2009 on a notification for prior checking on Voice Logging at the Joint Research Centre Institute for Energy (JRC-IE) in Petten (Case 2008-014).
2. Avis du 1er avril 2009 sur la notification d'un contrôle préable à propos du dossier "Exercice annuel de retraite anticipée sans réduction des droits à pension" (Dossier 2008-719).
3. Avis du 30 mars 2009 sur la notification d'un contrôle préalable concernant le dossier "stagiaires structurels" (Dossier 2008-760).
4. Avis du 25 mars 2009 sur la notification d'un contrôle préalable à propos du dossier "traitement des demandes de levée de l'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission" (Dossier 2008-645).
5. Avis du 23 mars 2009 sur la notification de contrôle préalable à propos de la gestion des informations transmises par l'OLAF dans le cadre du Memorandum of Understanding (Dossier 2009-011).
6. Avis du 10 mars 2009 sur la notification d'un contrôle préalable à propos du dossier Procédure de fin de stage (Dossier 2008-720).
7. Opinion of 26 February 2009 on a notification for prior checking regarding ETF - Flexitime procedure (Case 2008-697).
8. Avis du 23 février 2009 sur la notification d'un contrôle préalable à propos du dossier "Groupe de réintégration et de réorientation professionnelle" (Dossier 2008-746).
9. Opinion of 20 February 2009 on a notification for prior checking regarding the engagement and use of temporary agents (Case 2008-315).
10. Opinion of 18 February 2009 on a notification for prior checking on the procedure for early retirement without reduction of pension rights (Case 2008-748).
11. Opinion of 9 February 2009 on a notification for prior checking regarding "ART: Audit Reconciliation Tool" (Case 2008-239).
12. Avis du 26 janvier 2009 sur la notification de contrôlé préalable à propos du dossier "Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme" (Dossier 2008-440).
13. Opinion of 21 January 2009 on a notification for prior checking on the assessment of staff's capacity to work in a third language before first promotion (Case 2008-690).
14. Opinion of 21 January 2009 on a notification for prior checking concerning the report on probation period (Case 2008-604)
15. Opinion of 16 January 2009 on a notification for prior checking on the management of Central and Local Training SYSLOG Formation (Case 2008-481).
16. Avis du 16 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "Procédure relative aux commissions d'invalidité" (Dossier 2008-626).
17. Avis du 15 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "gestion et facturation de la crèche du Secrétariat Général du Conseil" (Dossier 2007-441).
18. Avis du 9 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "Exercice annuel de retraite anticipée sans réductions des droits à pension" (Dossier 2008-552).

Opinie przyjęte przez Grupę roboczą art. 29 do spraw danych osobowych w 2008 r.

1. Opinion 3/2008 of the Article 29 Working Party on the World Anti-Doping Code draft International Standard for the Protection of Privacy.
2. Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 2008.
3. Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive).
4. Opinion 1/2008 on data protection issues related to search engines.