Filip Jasiński

Ochrona danych osobowych w porządku prawnym Unii Europejskiej

Kwartalnik Prawa Publicznego 3/3, 205-226

2003

KWARTALNIK PRAWA PUBLICZNEGO
ROK III • NR 3/2003 • UKSW – WARSZAWA • TNOiK – TORUŃ • ISSN 1642-9591

Filip Jasiński *

OCHRONA DANYCH OSOBOWYCH W PORZĄDKU PRAWNYM UNII EUROPEJSKIEJ

1. Wstęp

W ciągu ostatnich kilkudziesięciu lat nastąpił rewolucyjny wzrost ilości informacji przekazywanych między społeczeństwami na całym świecie, pojawiły się też nieznane do tej pory środki i metody gromadzenia danych oraz ich przetwarzania przede wszystkim w sposób elektroniczny. Wraz z postępującą globalizacją informacji, przyspieszeniem przesyłania ich na odległość, a także pojawianiem się zbiorów danych w wyspecjalizowanych dziedzinach aktywności społecznej, m.in. w administracji państwowej, opiece zdrowotnej, bankowości, podatkach, wymiarze sprawiedliwości, usługach ubezpieczeniowych, ewidencji ludności, badaniach naukowych, statystyce, marketingu i reklamie, zagadnienie ochrony danych osobowych nabrało szczególnego znaczenia, tworząc zarówno szanse, jak i zagrożenia społeczne. Informacje te stały się ponadto rzadkim towarem rynkowym[1], o który walczą m.in. wielcy producenci dóbr konsumpcyjnych, są też nimi zainteresowane agencje bezpieczeństwa wewnętrznego i wywiady wielu krajów.

---

* Dr Filip Jasiński – główny specjalista w Departamencie Polityki Integracyjnej Urzędu Komitetu Integracji Europejskiej. Tekst niniejszy przedstawia wyłącznie osobiste opinie autora i nie jest oficjalnym stanowiskiem Urzędu KIE. Autor składa podziękowania Panu Igorowi Kowalewskiemu z Departamentu Prawnego Biura Generalnego Inspektora Ochrony Danych Osobowych za cenne uwagi redakcyjne.

[1] Por. European Commission (red. Ch. Pounder, K. McLean), *IDA projects. A guide to data protection compliance; Final report. Annex to the Annual Report 1998 (XV D/5047/98) of the Working Party established by Article 29 of the Directive 95/46/EC*, Office for Official Publications of the European Commission, Luxembourg 1999, s. 114.

Prawie równocześnie z pojawieniem się znacznej liczby rozbudowanych baz danych i szybkim rozwojem komputerowych technik gromadzenia i przetwarzania informacji, nastąpiły istotne zmiany w krajowych rozwiązaniach prawnych, chroniące właścicieli informacji przed ich nielegalnym wykorzystywaniem, np. w celach handlowych – ochrona danych osobowych przyjęła zatem wyspecjalizowaną postać prawa do prywatności i intymności. Równocześnie nastąpiła ewolucja prawa dostępu do informacji i przejrzystości (transparencji) życia publicznego, swobody wypowiedzi i wyrażania poglądów, a także tzw. prawa do niewiedzy – np. odnośnie do określonych danych z pogranicza genetyki (wobec osób fizycznych), czy też ubezpieczeń (wobec osób prawnych)[2].

Bez istnienia baz danych zawierających informacje o wielu aspektach życia obywateli współczesne państwo w praktyce nie byłoby w stanie sprawnie funkcjonować. Konieczność zapewnienia im należytej ochrony – tak w wymiarze technicznym (informatycznym), jak i prawnym (na poziomie krajowym i międzynarodowym) – stała się kwestią często podnoszoną w debatach nt jakości działania służb administracyjnych poszczególnych państw, przede wszystkim z następujących powodów[3]:

— nieskuteczności tradycyjnych mechanizmów ochrony prywatności, które były możliwe do wykorzystania tylko na gruncie prawa karnego i prawa cywilnego; zdecydowano się wobec tego na położenie większego nacisku na niedopuszczanie do naruszenia, a mniejszego na usuwanie jego skutków;
— uznania przede wszystkim środków publicznoprawnych (administracyjno-prawnych) za podstawowy sposób ochrony, w tym wypadku o charakterze instytucjonalnym.

Ochrona prywatności i intymności stała się z czasem podstawowym warunkiem gwarantującym wolność i godność każdego człowieka oraz funkcjonowanie demokratycznego państwa prawa. Odnosić się do niej zaczęły, najpierw w formie aktów prawnie niewiążących, organizacje międzynarodowe, zarówno globalne (m.in. ONZ[4], UNESCO[5]), jak

[2] F. Jasiński, *Ochrona danych osobowych w Unii Europejskiej*, „Wspólnoty Europejskie. Biuletyn Informacyjny" nr 10(122), październik 2001, s. 53.

[3] M. Safjan, *Ochrona danych osobowych – granice autonomii informacyjnej* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 12.

[4] Por. art. 17 Pakty Praw Obywatelskich i Politycznych z 1966 r. oraz Wytyczne Zgromadzenia Ogólnego NZ w sprawie rozporządzania skomputeryzowanymi danymi osobowymi z 26.6.1985 r. – Rezolucja 45/95 Zgromadzenia Ogólnego NZ z 14.12.1990 r.

[5] Por. Uniwersalna Deklaracja UNESCO w sprawie Ludzkiego Genomu i Praw Człowieka z 11.11.1999 r.

i regionalne (Rada Europy, OECD[6], Światowe Stowarzyszenie Lekarskie[7]), a także pozarządowe (np. *Amnesty International*). Równolegle tworzeniem uregulowań dotyczących ochrony danych osobowych zaczęto zajmować się na krajowym gruncie legislacyjnym.

W niniejszym opracowaniu autor przybliża podstawy funkcjonowania rozwiązań prawnych w obszarze szeroko rozumianej ochrony danych osobowych w ramach przepisów prawa Unii Europejskiej, tj. w rozumieniu zarówno danych osobowych związanych z funkcjonowaniem unijnego I (w zakresie Rynku Wewnętrznego), jak i III filaru (współpracy policyjnej i sądowej w sprawach karnych). Wskazuje ponadto na istniejące w tym zakresie zobowiązania akcesyjne dla Polski w świetle przyszłorocznej przystąpienia do UE i przybliża główne problemy związane z dalszym rozwojem ochrony danych osobowych.

2. EUROPEJSKI MODEL OCHRONY DANYCH OSOBOWYCH

Podstawowy czynnik mający wpływ na kształt przepisów prawnych w krajach Europy Zachodniej po II wojnie światowej, czyli Europejska Konwencja o ochronie praw człowieka i podstawowych wolności zawarta 4.11.1950 r. pod auspicjami Rady Europy, nie odniosła się bezpośrednio do ochrony danych osobowych. W jej art. 8 wspomina się bowiem jedynie o „prawie do prywatności", w art. 10 o „swobodzie wypowiedzi", z kolei w art. 14 o „zakazie dyskryminacji". Jednak to właśnie mechanizmy ochrony prawnej wypracowane przez Radę Europy[8] z czasem przyczyniły się do ukształtowania międzynarodowych standardów prawnych w dziedzinie ochrony danych osobowych, począwszy od uchwały Zgromadzenia Parlamentarnego RE nr 509 z 1968 r. w sprawie ochrony praw człowieka na tle współczesnych przedsięwzięć naukowych i technicznych oraz uchwały nr 3 z 1971 r. w sprawie ochrony życia prywatnego w związku z rozwojem komputerowych technik gromadzenia danych osobowych.

---

[6] Por. Zalecenie Rady OECD dotyczące zasad ochrony prywatności i ponadgranicznego przepływu danych osobowych z 23.9.1980 r., COM(80)58 final, potwierdzone w Ottawie w 1999 r. na konferencji o handlu elektronicznym oraz Zalecenie Rady OECD dotyczące zasad ochrony systemów informatycznych z 12.3.1992 r., OCDE/GD(92)190.

[7] Por. Międzynarodowy Kodeks Etyki Lekarskiej z września 1948 r.

[8] Są to: 25 zalecenia i 3 uchwały Komitetu Ministrów RE oraz 6 zaleceń Zgromadzenia Parlamentarnego RE. W ramach Rady Europy działa ponadto Europejski Komitet Współpracy Prawnej zajmujący się m.in. zagadnieniem ochroną danych osobowych (fr. CDCJ).

Kultura prawna uwzględniająca coraz częściej podnoszone hasło ochrony danych osobowych zaczęła kształtować się faktycznie w latach 70-tych XX w., wpierw w państwach Europy Zachodniej, na co wpływ miało z jednej strony orzecznictwo Europejskiego Trybunału Praw Człowieka oraz Trybunału Sprawiedliwości Wspólnot Europejskich, jak i rosnące zainteresowanie obywateli domagających się uwzględnienia przysługujących im praw podstawowych w legislacjach krajowych. Utrwalenie europejskiego wzorca w tym zakresie nastąpiło ostatecznie wraz z przyjęciem 28 stycznia 1981 r. Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[9], którą do chwili obecnej podpisało 35, a ratyfikowało 30 z 45 krajów członkowskich Rady Europy, w tym wszystkie państwa członkowskie i przystępujące do Unii Europejskiej. Z punktu widzenia prawa międzynarodowego jest to pierwsza umowa międzynarodowa dotycząca przetwarzania danych osobowych[10] (weszła w życie 1 października 1985 r.), która pomimo oddziaływania wyłącznie w sferze publicznoprawnej, tj. bez wywoływania bezpośredniego skutku prawnego po stronie obywateli państwa-strony Konwencji, wskazuje na istniejący minimalny poziom ochrony danych osobowych. Jej ograniczoność wynika przede wszystkim z braku wystarczającego instrumentarium wymuszania na państwach-stronach faktycznego wdrażania zawartych w niej przepisów.

Ta regionalna umowa międzynarodowa sprawiła też, że Wspólnota Europejska (WE) zaczęła coraz częściej odnosić się do ochrony danych w swoich własnych działaniach legislacyjnych. Uchwały Parlamentu Europejskiego z lat 80-tych w sprawie praw pacjenta, technologii informacyjnych i inżynierii genetycznej nadały tempa pracom nad prawnie wiążącym *acquis communautaire*, obligującym państwa członkowskie WE do wprowadzenia w ich wewnętrznych porządkach prawnych, różniących się między sobą do tej pory w tym zakresie, odpowiedniego poziomu ochrony danych osobowych ich obywateli. Ochrona prywatności w coraz większym stopniu przestała być dostrzegana jedynie z punktu widzenia poufności komunikacji[11].

---

[9] Umowa ta, podpisana przez Polskę 21.4.1999 r. i ratyfikowana 23.5.2002 r., weszła w Polsce w życie 1.9.2002 r. (Dz. U. z 2002 r. Nr 3, poz. 25).

[10] J. Barta, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2001, s. 39.

[11] Por. m.in. sprawa 155/79, *AM & S Europe Limited v. Komisji* [1982] ECR 1575 oraz sprawa C-369/98 *Królowa v. Minister Rolnictwa*, [2000] ECR I-6751.

3. Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE

Elementy ochrony danych osobowych znajdują się w wielu obszarach działań Wspólnot Europejskich[12]. Jednak dopiero na początku lat 90-tych rozpoczęto prace nad właściwym *acquis* w tym zakresie – w komunikacie Komisji z 13.9.1990 r.[13] stwierdzono, że „różnorodność krajowych podejść i brak systemu ochrony na poziomie wspólnotowym są przeszkodą na drodze do utworzenia Wspólnego Rynku. W przypadku, gdy prawa podstawowe podmiotów danych, a w szczególności ich prawo do prywatności, nie są chronione na poziomie wspólnotowym, ponadgraniczny przepływ danych może być zahamowany". Komunikat odnosił się m.in. do akcesji Wspólnot do Konwencji nr 108 oraz zawierał projekty aktów prawnych dotyczących ochrony prywatności w kontekście publicznych cyfrowych sieci telekomunikacyjnych, telefonii komórkowej i bezpieczeństwa informacji.

Prace legislacyjne zakończyły się przyjęciem 24.10.1995 r. przez Parlament Europejski i Radę dyrektywy 95/46/WE[14] w sprawie ochrony osób w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych (wcześniej Komisja Europejska postulowała jedynie, aby kraje członkowskie ostatecznie ratyfikowały Konwencję nr 108 Rady Europy[15]). Państwom członkowskim pierwotnie dano trzy lata, czyli czas do 23 października 1998 r., na uchwalanie odpowiedniej legislacji wdrażającej nową dyrektywę w ich wewnętrznych porządkach prawnych, przy czym poważne opóźnienia w tym zakresie spowodowały wniesienie przez Komisję sprawy na mocy art. 226 TWE[16] przed Trybunał Sprawiedliwości przeciwko Francji, Irlandii, Luksem-

---

[12] Por. art. 43, 49 i 286 TWE oraz art. 6 TUE. W sprawie ochrony danych osobowych w I filarze UE por. http://www/europa.eu.int/comm/internal_market/privacy/index_fr.htm. Ochrona danych osobowych w ramach III filaru Unii Europejskiej opisana została w dalszej części tekstu.

[13] COM(90) 314 final.

[14] Dz. Urz. WE L 281 z 2.11.1995 r., s. 95. Podstawą traktatową dla przyjęcia tego aktu prawnego był art. 100a TWE (obecnie art. 95 TWE).

[15] J. Barta, R. Markiewicz, op. cit., s. 57.

[16] „Jeżeli Komisja uzna, że państwo członkowskie nie wypełniło zobowiązań przyjętych na podstawie niniejszego Traktatu, wydaje w tej sprawie umotywowaną opinię, umożliwiając uprzednio temu państwu przedstawienie swych uwag. Jeżeli odnośne państwo nie zastosuje się do powyższej opinii w terminie ustalonym przez Komisję, może ona skierować sprawę do Trybunału Sprawiedliwości".

burgowi, Niderlandom i Niemcom[17], co w efekcie przyspieszyło prace implementacyjne.

W chwili obecnej wszystkie państwa członkowskie Unii dysponują wewnętrznymi przepisami w zakresie ochrony danych osobowych, jednak pełne wdrożenie dyrektywy nie nastąpiło do tej pory we Francji, gdzie prace nad nowelizacją ustawy z 1978 r. trwają już czwarty rok (nie zrobiły tego ponadto 2 z 16 landów niemieckich). Warto przy tym zwrócić uwagę, że zdaniem Komisji Europejskiej istnieje możliwość bezpośredniego powołania się przez zainteresowane osoby na niektóre postanowienia dyrektywy w sporze przed sądami krajowymi, a także żądania przez nie odszkodowania przed tymi sądami od państwa ze względu na niedopełnienie obowiązku jej realizacji[18].

W preambule do dyrektywy zapisano, że „stworzenie i działanie rynku wewnętrznego, który zgodnie z art. 7a Traktatu (obecnie art. 14 TWE) ma służyć swobodnej wymianie towarów, osób, usług i kapitału, wymaga nie tylko swobodnego przepływu danych osobowych z jednego państwa członkowskiego do drugiego, ale również zapewnienia podstawowych praw poszczególnym jednostkom". To sformułowanie jest o tyle istotne, że podkreśla się w nim kluczowe znaczenie ochrony danych osobowych dla gospodarczych fundamentów istnienia Unii. Dyrektywa odzwierciedla faktycznie jedne z najważniejszych celów integracji europejskiej: utworzenie Rynku Wewnętrznego oraz ochronę praw i swobód obywatelskich[19].

Podstawowym celem dyrektywy 95/46/WE jest stworzenie jednolitego minimalnego poziomu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych zawartych w zbiorach, a także umożliwienie swobodnego przepływu tych danych między państwami członkowskimi Wspólnoty. W art. 2 dyrektywy „dane osobowe" (ang. *personal data*, fr. *données a caractere personnel*) definiuje się szeroko jako „wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby fizycznej", z kolei „przetwarzanie danych" (ang. *data processing*, fr. *traitement de données*), jako „każdą czynność lub szereg czynności wykonywanych na danych osobowych, bez względu na to, czy za pomocą środków automatycznych, czy nie, takich jak gromadze-

[17] W 2001 r. Niemcy i Holandia notyfikowały Komisji Europejskiej zmiany w swoich przepisach legislacyjnych. Trybunał wydał natomiast wyrok w sprawie Luksemburga (sprawa C-450/00 [2001] ECR I-7069). W kwestii interpretacji dyrektywy por. orzeczenie TS z 20.5.2003 r. w sprawie C-465/00, C-138/01 i C-139/01.

[18] J. Barta, R. Markiewicz, op. cit., s. 58 oraz IP/00/10 z 11.1.2000 r.

[19] Pierwszy raport z wdrażania dyrektywy o ochronie danych osobowych, COM(2003) 265 final, s. 4.

nie, rejestrowanie, porządkowanie, przechowywanie, dostosowywanie lub zmienianie, odzyskiwanie, konsultowanie, używanie, ujawnianie przez przekazywanie, rozpowszechnianie, bądź w inny sposób udostępnianie, wyrównywanie, łączenie, blokowanie, usuwanie lub niszczenie". Dyrektywa jest tutaj nieco bardziej precyzyjna od Konwencji nr 108, podaje bowiem, że „osobą dającą się zidentyfikować jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, szczególnie poprzez odniesienie się do numeru identyfikacyjnego lub innych wskaźników charakterystycznych dla jej fizycznej, fizjologicznej, umysłowej, gospodarczej, kulturowej lub społecznej tożsamości"[20]. Przepisy te odnoszą się do osób fizycznych, lecz zarówno Konwencja Rady Europy, jak i dyrektywa 95/46/WE przewidują możliwość objęcia ochroną danych również osób prawnych.

W preambule do dyrektywy 95/46/WE określono ją kwintesencją i umocnieniem zasad ujętych w Konwencji nr 108. Mając na celu zmniejszenie różnic prawnych między obydwoma dokumentami, 15 czerwca 1999 r. Komitet Ministrów Rady Europy przyjął poprawkę do Konwencji umożliwiającą przystąpienie do niej również Wspólnocie Europejskiej[21]. Ma to doprowadzić do większej homogeniczności systemów ochrony prywatności stosowanych przez Unię (na mocy dyrektywy) i przez Radę Europy (na podstawie Konwencji). Poprawka ta zyska moc prawnie wiążącą z chwilą zaakceptowania jej przez wszystkich dotychczasowych sygnatariuszy Konwencji nr 108.

W dyrektywie zamieszczono katalog głównych zasad chroniących interesy osób fizycznych, których dane podlegają przetwarzaniu Zalicza się do nich m.in.[22]:

— zakaz przetwarzania danych w celu innym, niż zostały one zebrane oraz w celu innym niż ten, który towarzyszył zgodzie osoby, której dane dotyczą (art. 6). Osoba, która wyraża zgodę na przetwarzanie swoich danych powinna być przez ich kontrolera powiadomiona o szczegółach związanych z tym procesem – danych kontrolera, celach przetwarzania, kategoriach odbiorcy danych, czy też możliwości ich ewentualnego korygowania (art. 10);
— istnienie możliwości wyrażenia sprzeciwu wobec obrotu danymi osobowymi, a także ich korekty, usunięcia lub zablokowania

[20] Por. A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, s. 24.

[21] http://www.legal.coe.int/dataprotection/Default.asp?fd=treaties&fn=Amend 108E.htm Polska zaakceptowała niniejszą poprawkę 23.10.2002 r.

[22] Por. Przewodnik Komisji Europejskiej pt. „Ochrona danych osobowych w Unii Europejskiej" z 15.5.2001 r. (http://europa.eu.int/comm/internal_market/en/dataprot/news/guide_en.pdf).

w przypadku, gdy uzyskane one zostały z naruszeniem postanowień dyrektywy (por. art. 7);
— zakaz zbierania określonych kategorii informacji w celu ich automatycznego przetwarzania, z wyjątkiem sytuacji, kiedy została na to wyrażona pisemna zgoda; jest to konieczne ze względu na prawo pracy (realizacja zobowiązań i uprawnień pracodawcy) lub w związku z ochroną istotnych interesów podmiotu danych lub innej osoby, gdy podmiot ten nie jest w stanie udzielić na to fizycznie lub prawnie takiej zgody (art. 8 par. 2). Sytuacja ta odnosi się np. do danych dotyczących pochodzenia rasowego lub etnicznego, przekonań religijnych lub filozoficznych, członkostwa w związkach zawodowych oraz kwestii zdrowia lub życia seksualnego (art. 8 ust. 1);
— gromadzenie danych dotyczących skazań kryminalnych wyłącznie w zbiorach danych o charakterze publicznym (art. 8 ust. 5);
— zobowiązanie państw członkowskich do ustanowienia odpowiedzialności cywilnej i karnej za naruszenie zawartych w dyrektywie przepisów. Katalog sankcji nie będzie natomiast narzucany odgórnie – winny one skutecznie zniechęcać do popełniania przestępstw (art. 24).

Obok norm określających minimalne standardy ochrony, dyrektywa wskazuje także na inne zagadnienia związane z tworzeniem „przyjaznego prawnego i instytucjonalnego środowiska" (por. punkt 8 preambuły), które mogą mieć istotny wpływ na zapewnienie porównywalnego we wszystkich państwach UE poziomu ochrony danych osobowych. Jedną z tych kwestii jest np. przekazywanie danych osobowych za granicę, o czym mówi rozdział IV dyrektywy. Z wyjątkiem sytuacji wymienionych w art. 26, państwa członkowskie winny podjąć odpowiednie kroki, aby przetwarzane dane osobiste mogły być przesyłane wyłącznie do państw, które zapewnią tym danym na ich terytorium odpowiedni poziom ochrony[23]. Tworzy się dzięki temu specjalny system wczesnego ostrzegania – kraje Piętnastki winny się powiadamiać nawzajem, jeśli uznają, że państwo docelowe nie zapewnia wystarczającego zakresu zabezpieczeń danych (art. 25 ust. 2). Formą nadania swoistego „certyfikatu bezpieczeństwa"[24] przepływowi danych było przyję-

[23] Por. Protokół Dodatkowy nr 179 do Konwencji nr 108 Rady Europy w sprawie organów kontrolnych i ponadgranicznego przekazywania danych z 8.11.2001 r. (Polska podpisała go 21.11.2002 r.).

[24] „Single Market News" nr 17, lipiec 1999, s. 26; oraz „Single Market News" nr 23, październik 2000, s. 20.

cie przez Komisję 26.7.2000 r. decyzji dotyczących wymiany ich ze Stanami Zjednoczonymi[25], Szwajcarią[26] i Węgrami[27].

Ponadto w decyzji Komisji 2000/497/WE z 15.6.2001 r.[28] określono standardowe klauzule kontraktowe dla transferu danych osobowych do państw trzecich, zgodnie z przepisami dyrektywy 95/46//WE[29]. W 1997 r. w badaniach przeprowadzonych przez Komisję Europejską postulowano utworzenie tzw. białej i czarnej listy, na których umieszczane mogłyby być kraje bezpieczne dla transferu danych oraz te, które nie gwarantują swoją praktyką i ustawodawstwem przestrzegania ochrony danych osobowych. Co istotne, często domniemuje się istnienie należytej ochrony w przypadku, kiedy państwo przeznaczenia jest stroną Konwencji nr 108 Rady Europy oraz skutecznie realizuje jej postanowienia. 20.12.2001 r. Komisja przyjęła decyzję w sprawie obrotu danymi z Kanadą[30], natomiast 30.6.2003 r. z Argentyną[31]. Pozytywna opinia wydana 13.6.2003 r. przez Grupę Roboczą ds. Art. 29 w odniesieniu do zgodności przepisów obowiązujących na wyspie Guernsey z *acquis* w zakresie ochrony danych osobowych pozwoli na przyjęcie wkrótce podobnej decyzji przez Komisję[32].

Dyrektywa odnosi się także do weryfikacji istnienia adekwatnej ochrony danych osobowych, jednakże nie przesądza o konkretnych procedurach w tym względzie. Należy monitorować przede wszystkim przekazywanie danych wrażliwych, danych potrzebnych do podejmowania decyzji istotnie związanych z ich podmiotem, danych mogących zagrozić reputacji jednostki lub spowodować wkroczenie w sferę jej życia prywatnego oraz w przypadku przekazywania znacznych ilości danych, jak np. w sektorze telekomunikacyjnym lub poprzez internet.

Ważnym przesłaniem sformułowanym w art. 9 dyrektywy 95/46/ /WE jest podkreślenie swobody wyrażania poglądów przez dziennikarzy i artystów, funkcjonującej jednakże tylko wtedy, gdy środki przez nich przedsiębrane, stanowiące wyjątki od części postanowień dyrektywy, wiążą prawo do prywatności z przepisami dotyczącymi wolności i wyrażania przekonań. Z kolei całościowe zawieszenie funkcjonowa-

[25] O.J. 2000, L 215/7; poprawiona O.J. 2001, L 115/14.
[26] O.J. 2000, L 215/1.
[27] O.J. 2000, L 215/4.
[28] O.J. 2001, L 181/19.
[29] „Single Market News" nr 27, lipiec 2001, s. 17.
[30] O.J. 2002, L 2/13. Por. wcześniejszą negatywną opinię Grupy Roboczej ds. Art. 29 z 26.1.2001 r. („Single Market News" nr 25, marzec 2001, s. 23).
[31] C(2003)1731 final. Dotychczas brak publikacji w Dz. Urz. UE.
[32] Opinia 5/2003, 10595/03/EN WP 79.

nia prawa do ochrony danych osobowych może być podjęte wyłącznie na podstawie właściwej wewnętrznej legislacji, jak np. podczas stanu wojennego (por. art. 13).

W rozdziałach VI i VII dyrektywy zamieszczono postanowienia odwołujące się do kolejnej podstawowej zasady współczesnego rozumienia ochrony danych osobowych – utworzenia i istnienia niezależnych organów państwowych spełniających funkcję kontrolną wobec administratorów baz danych. Tego typu instytucje, jak np. polski Generalny Inspektor Ochrony Danych Osobowych, pełnią niezwykle istotną rolę nie tylko z czysto prawnego punktu widzenia, jako skuteczna instancja odwoławcza, lecz także poprzez działalność propagującą świadomość społeczną w zakresie ochrony prywatności. W dyrektywie wspomina się o nich w rozdziale VI, tworząc jednocześnie niezależnie Grupę Roboczą ds. Art. 29 w sprawie ochrony osobistej w odniesieniu do przetwarzania danych personalnych (por. art. 29–30). Zadaniem tego organu doradczego jest monitorowanie wdrażania i stosowania dyrektywy 95/46/WE w krajach członkowskich UE i informowanie Komisji w przypadku stwierdzenia ewentualnych uchybień. Grupa opracowuje ponadto od 1997 r. dokumenty dyskusyjne (1), raporty roczne (4), dokumenty robocze (17), zalecenia (11) i wydaje opinie (37). W jej skład wchodzą przedstawiciele organów kontrolnych państw EOG oraz przedstawiciel Komisji Europejskiej, a także – od początku 2002 r., przedstawiciele organów kontrolnych z krajów kandydujących do członkostwa w UE, na mocy decyzji Grupy z 13.12.2001 r.[33] Znaczenie Grupy Roboczej ds. Art. 2 jest nie do przecenienia. Grupa dyskutuje bowiem te kwestie, które niejednokrotnie wyprzedzają o wiele miesięcy, a nawet lat regulacje prawnie wiążące przyjmowane na poziomie krajów członkowskich Unii, podnosi problematykę niezwykle aktualną, a często wręcz zbyt kontrowersyjną, aby spodziewać się jej szybkiego usankcjonowania w dokumentach o mocy prawnie wiążącej – np. przetwarzania tzw. danych biometrycznych[34], korzystania z danych osobowych w ramach nadzoru wideo[35], zrównoważonej walki z terroryzmem[36], ludzkiego genomu[37], czy też przetwarzania danych osobowych na internecie[38]. Obecnie w ramach specjalnej podgrupy roboczej dyskutuje się kwestię utworzenia ogólnoeuropejskiego rejestru administratorów danych.

[33] Decyzja 1/2001 WP 52, 5080/01.
[34] Dokument roboczy WP 80, MARKT/10595/03/EN z 1.8.2003 r.
[35] Dokument roboczy WP 67, MARKT/11750/03/EN z 25.11.2002 r.
[36] Opinia 10/2001 WP 53, MARKT 5404/01 z 14.12.2001 r.
[37] Opinia 6/2000 WP 34, DG MARKT 5062/00 z 13.7.2000 r.
[38] Dokument roboczy WP 16, DG MARKT 5013/99 z 23.2.1999 r.

Ponadto w art. 31 dyrektywy 95/46/WE mówi się o utworzeniu komitetu składającego się z przedstawicieli państw członkowskich, któremu przewodniczy reprezentant Komisji. Komitet ten wspomaga działania legislacyjne Komisji w odniesieniu do problematyki ochrony danych osobowych[39]. W jego pracach biorą udział przedstawiciele instytucji administracji rządowych krajów członkowskich właściwych w zakresie ochrony danych osobowych (chociaż w przypadku Austrii i Polski są to, podobnie jak w przypadku uczestników prac Grupy Roboczej Art. 29, szefowie niezależnych organów kontrolnych).

4. OCHRONA DANYCH OSOBOWYCH W SEKTORZE TELEKOMUNIKACYJNYM

Wspólnotowe podejście do ochrony danych osobowych i prywatności w sektorze telekomunikacyjnym ujęto w dyrektywie Parlamentu i Rady 97/66/WE z 15 grudnia 1997 r.[40], zmodyfikowanej w ramach tzw. pakietu telekomunikacyjnego w 2002 r.[41] Zasadnicze elementy tego podejścia zostały przeniesione z dyrektywy 95/46/WE, m.in. w celu zachowania spójności w ochronie danych osobowych w różnych przepisach acquis. Jak wskazano w dyrektywie 97/66/WE, celem legislatora wspólnotowego było dostosowanie rozwiązań z 1995 r. do szczegółowych reguł sektora telekomunikacyjnego. Z kolei nowa dyrektywa 2002/58/WE została wymuszona pojawieniem się rewolucyjnych zmian na rynku telekomunikacji zarówno w sferze prawnej, jak i – przede wszystkim – technologicznej. „Wprowadzane obecnie w publicznych sieciach komunikacyjnych nowe technologie cyfrowe powodują wzrost wymagań stawianych w zakresie ochrony danych osobowych i prywatności użytkowników", a „rozwój społeczeństwa informacyjnego charakteryzuje się wprowadzaniem nowych usług komunikacji elektronicznej" (pkt 5 preambuły do nowej dyrektywy). Państwa członkowskie Unii zostały zobowiązane do wdrożenia przepisów dyrektywy 2002/58/WE do końca października 2003 r.

Szczegółowe przepisy dyrektywy 2002/58/WE odnoszą się do kwestii dotyczących m.in. świadczenia publicznych usług w komunikacji

[39] Por. J. Barta, R. Markiewicz, op. cit., s. 65.

[40] Dz. Urz. WE L 24 z 30.1.1998 r., s. 1.

[41] Na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z 12.6.2002 r. w sprawie prywatności i komunikacji elektronicznej (O.J. 2002, L 201/37).

elektronicznej w publicznych sieciach komunikacyjnych na terytorium Wspólnot Europejskich (art. 3), stosowania odpowiedniego poziomu zabezpieczeń sieci gwarantującą poufność komunikacji, bilingów szczegółowych, spisów abonentów oraz marketingu bezpośredniego. Wprowadzono m.in. definicje danych dotyczących ruchu (ang. *traffic data*, fr. *données relatives au trafic*), danych dotyczących lokalizacji (ang. *location data*, fr. *données de localisation*), komunikatu, połączenia telefonicznego, usługi dodanej wartości (ang. *value added service*, fr. *service a valeur ajoutée*) oraz poczty elektronicznej. W art. 5 zabroniono „słuchania, nagrywania, przechowywania lub innych rodzajów przechwytywania informacji lub kontroli komunikacji i związanych z nią danych dotyczących ruchu przez osoby nie będące użytkownikiem, bez zgody użytkownika". Zobowiązano także dostarczycieli internetu do uzyskiwania wstępnej zgody użytkowników sieci na stosowania tzw. *cookies*, tj. ukrytych informacji internetowych niejako wiążących komputery internautów z konkretnymi witrynami w sieci, wymaga się ponadto zgody abonenta na otrzymywanie komercyjnej poczty elektronicznej i komercyjnych SMS-ów w ramach procedury *opt-in* (akceptacji wyrażanej przed uzyskaniem rzeczonych danych). Wyjątek w tym wypadku dotyczy sytuacji, gdy użytkownikowi oferuje się własne produkty lub usługi zbliżone do takich, które proponowano już wcześniej.

Wstępnie oceniając przyjęte rozwiązania legislacyjne dotyczące ochrony danych osobowych w sektorze telekomunikacyjnym należy wziąć pod uwagę kontekst polityczny, w jakim zostały one przyjęte. Debata nad modyfikacją przepisów dyrektywy 97/66/WE trwała już od pewnego czasu w ramach prac nad tzw. pakietem telekomunikacyjnym (ujmującym dodatkowo cztery inne akty prawne), gdy tragiczne wydarzenia 11.9.2001 r. skierowały ją na nowy tor, tj. relacji ochrony danych osobowych wobec działalności organów ścigania. Ostatecznie osiągnięty kompromis polega na zezwoleniu na przechowywanie danych (ang. *data retention*, fr. *conservation de données*) wówczas, gdy następuje to jedynie dla celów przeprowadzenia postępowania (art. 15 dyrektywy 2002/58/WE), chociaż co do zasady dane dotyczące ruchu na serwerach komputerowych powinny być usuwane lub trwale anonimizowane z chwilą ukończenia transmisji danych (w myśl art. 6) – ewentualne dłuższe przetwarzanie może być prowadzone wyłącznie dla potrzeb bilingu. Ograniczenia dotyczące „zabezpieczenia bezpieczeństwa narodowego (np. bezpieczeństwa państwa), obrony, bezpieczeństwa publicznego oraz zapobiegania, prowadzenia dochodzeń, wykrywania i ścigania przestępstw lub wykorzystywania bez zezwolenia systemów komunikacji elektronicznej" – stanowiące bardzo rozbudowany katalog potencjalnych działań organów ścigania – mogą być zastosowane wobec

zakresu praw i obowiązków określonych w art. 5, art. 6, art. 8 ust. 1–4 i art. 9. Co jest szczególnie ważne dla praktycznego stosowania tych ograniczeń, to brak ujęcia w dyrektywie zharmonizowanego limitu wskazującego jak długo dostarczyciele usług internetowych winni przechowywać dane oraz przepisów mówiących o podstawach żądania dostępu do tych danych (legislatorom krajowym pozostawiono swobodę działania w tym zakresie).

Zgodnie z powyższym, w ramach walki z terroryzmem realizowanej przez UE przede wszystkim na gruncie legislacyjnym – z dyskusyjnymi przy tym skutkami[42] – zagadnienie ochrony danych osobowych w obszarze telekomunikacji zostało częściowo podporządkowane priorytetom politycznym, a wpływ tego kroku na przestrzeganie praw podstawowych obywateli Unii Europejskiej będzie mógł być w pełni oceniony dopiero wówczas, gdy wszystkie państwa członkowskie wdrożą przepisy dyrektywy 2002/58/WE.

Warto w tym miejscu ponadto zaznaczyć, że zagadnienie prawnej ochrony baz danych, ujęte w dyrektywie Parlamentu i Rady 96/9/WE z 11.3.1996 r.[43], jest często mylnie wiązane z ochroną danych osobowych – z punktu widzenia przepisów wspólnotowych dyrektywa ta odnosi się bowiem do samych baz danych, a nie do ich zawartości, którymi faktycznie mogą być również dane osobowe[44].

5. Ochrona danych osobowych przetwarzanych przez instytucje wspólnotowe

Przyjęcie dyrektywy 95/46/WE, trwające przygotowania do przeniesienia jej wzorców do obszaru telekomunikacyjnego, a także wcześniejsze doświadczenia w zakresie ochrony danych osobowych m.in. w ramach Systemu Informacji Schengen (o czym dalej), doprowadziły z czasem do pojawienia się coraz wyraźniej podnoszonej potrzeby zagwarantowania prawa do prywatności na poziomie prawa pierwotnego UE. Podczas prac Konferencji Międzyrządowej '96, której efektem było przyjęcie 2.10.1997 r. Traktatu Amsterdamskiego, postanowiono, m.in. pod wyraźnym wpływem Rzecznika Praw Obywatelskich UE, aby od-

[42] Więcej: F. Jasiński, *Unia Europejska wobec terroryzmu*, „Sprawy Międzynarodowe" 2002, nr 3, s. 46.

[43] O.J. L 77/20.

[44] Autor nie odnosi się ponadto w niniejszym tekście do ochrony danych statystycznych w ramach *acquis*.

nieść się bezpośrednio do kwestii ochrony danych osobowych przetwarzanych w ramach instytucji wspólnotowych w Traktacie o utworzeniu Wspólnoty Europejskiej – dodano wówczas do niego nowy artykuł 213b (po zmianie numeracji artykułów jest to art. 286 TWE) w następującym brzmieniu:

„Począwszy od 1 stycznia 1999 r., akty wspólnotowe dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz swobodnego przepływu takich danych mają zastosowanie do instytucji oraz organów utworzonych niniejszym Traktatem lub na jego podstawie.

Przed datą wymienioną w ust. 1 Rada, podejmując działania zgodnie z procedurą określoną w art. 251, ustanowi niezależny organ kontrolny odpowiedzialny za nadzorowanie stosowania takich aktów wspólnotowych do instytucji i organów wspólnotowych oraz przyjmie wszelkie inne przepisy, jakie okażą się konieczne".

Część komentatorów uznała niniejszą zmianę traktatową za niewystarczającą, bowiem nie nakłada ona na kraje członkowskie dodatkowego zobowiązania traktatowego do ochrony danych osobowych swoich obywateli, wskazuje tylko na potrzebę przeniesienia istniejących standardów w tym względzie na poziom instytucji WE. Dyskusja nad przełożeniem tej zasady do wtórnego acquis trwała jednak niezwykle długo, poważnie opóźniając realizację zadania wskazanego w art. 286 TWE.

W rozporządzeniu Parlamentu Europejskiego i Rady (WE) 45/ /2001 z 18.12.2000 r. w sprawie ochrony osób w związku z przetwarzaniem danych osobowych przez instytucje i organy Wspólnoty oraz swobodnego przepływu takich danych[45] odniesiono się do znanego już od dłuższego czasu faktu, że również sama Komisja, Rada, Parlament i inne organy WE winny wierzytelnie realizować swoje cele w duchu ochrony danych osobowych. Nawoływał do tego wielokrotnie Rzecznik Praw Obywatelskich UE podkreślając, że niesłuszne jest ukrywanie przed obywatelami zbyt wielu kulisów działań legislacyjnych Wspólnot[46]. W rozporządzeniu skorzystano ze sprawdzonych już w dyrektywach rozwiązań legislacyjnych, przy czym najważniejsze z nich dotyczą w zasadzie instytucjonalnego wymiaru ochrony danych osobowych, tzn. obowiązku powołania w poszczególnych organach WE osób zajmujących się niniejszą problematyką (art. 24) oraz niezależnego Europejskiego

[45] O.J. 2001, L 8/1.

[46] Decyzja Rzecznika Praw Obywatelskich UE w sprawie skargi nr 916/2000/GG przeciwko Radzie z 16.7.2001 r. Więcej: F. Jasiński, R. Pelc, *Europejski Rzecznik Praw Obywatelskich*, „Służba Cywilna" nr 3, s. 55. Warto przy tym zaznaczyć, że 22.10.2002 r. Rzecznik wezwał Komisję do doprecyzowania dyrektywy 95/46/WE ta, aby nie stała ona na przeszkodzie realizacji zasady swobody dostępu do dokumentów (EO/02/25).

Inspektora Ochrony Danych Osobowych (rozdział V), którego głównym zadaniem będzie zapewnienie realizacji przepisów rozporządzenia w odniesieniu do funkcjonowania instytucji WE (do października 2003 r. nie udało się wybrać osoby na to stanowisko spośród wielu wskazanych kandydatów przede wszystkim w związku z daleko idącym upolitycznieniem debaty nad tą kwestią w Parlamencie Europejskim i w Radzie).

6. POZAWSPÓLNOTOWE STANDARDY UE W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

Z chronologicznego punktu widzenia, jeśli chodzi o kwestię rozwoju europejskich przepisów dotyczących ochrony danych osobowych, należałoby w zasadzie najpierw omówić funkcjonowanie odpowiednich przepisów dotyczących Systemu Informacji Schengen (SIS) i komputerowej bazy danych Europolu, czyli pozawspólnotowego obszaru unijnego *acquis* (III filaru UE – nota bene SIS, chociaż będący częścią porządku prawnego Schengen, pozostał nie włączony do I filaru UE, co nastąpiło wraz z wejściem w życie Traktatu Amsterdamskiego 1.5.1999 r.). Na wstępie należy także zaznaczyć, że strona unijna niejednokrotnie odnosiła się do treści zalecenia Komitetu Ministrów rady Europy R(87) 23 z 17.9.1987 r. w sprawie ochrony danych osobowych wykorzystywanych w sektorze policji, przy czym działo się tak często w sytuacjach, gdy państwa członkowskie Unii nie były w stanie uzgodnić między sobą własnych przepisów w tym zakresie[47].

System Informacyjny Schengen jest jednym z filarów Konwencji Wykonawczej z Schengen (KW)[48], na mocy której zniesiono między częścią państw członkowskich Unii wewnętrzną kontrolę graniczną. SIS służy wymianie informacji dotyczących m.in. osób przekraczających granice tych państw i ma głównie na celu „wychwytywanie" osób lub przedmiotów nieuprawnionych do pojawienia się na terytorium Schengen[49]. Zgodnie z art. 93 KW „zadaniem SIS jest (...) zapewnienie utrzymania porządku i bezpieczeństwa publicznego, w tym bezpieczeństwa państwa, a także umożliwienie stosowania postanowień dotyczących

[47] W zaleceniu uzgodniono m.in., że ochrona danych może być także rozszerzona na dane przetwarzane ręcznie.

[48] O.J. 2000, L 239/1.

[49] Por. A. Graś, *Porozumienie z Schengen – geneza i stan obecny* [w:] *Polska droga do Schengen. Opinie ekspertów*, Instytut Spraw Publicznych, Warszawa 2001, s. 33.

przepływu osób, zawartych w Konwencji, na terytorium Wysokich Umawiających się Stron za pomocą informacji przekazywanych w systemie". Dane zawarte w SIS wykorzystywane są podczas kontroli granicznej, policyjnej, celnej oraz podczas wydawania wiz i zezwoleń na pobyt w stosunku do obywateli krajów trzecich. Kontroli tej podlegają teoretycznie wszystkie osoby przekraczające granice zewnętrzne obszaru Schengen, chociaż ostateczna decyzja w tym zakresie należy do funkcjonariuszy służb granicznych. System zawiera informacje odnoszące się do osób (np. poszukiwanych, zaginionych lub podlegających niejawnemu nadzorowi) i przedmiotów (skradzionych pojazdów, broni, gotówki, dokumentów tożsamości i dokumentów in blanco). Mogą być wobec nich zastosowane takie środki, jak areszt w celu ekstradycji (art. 95 KW); odmowa wjazdu w stosunku do osób, które nie mają prawa do wjazdu na teren Schengen z powodu zagrożenia dla porządku publicznego i bezpieczeństwa wewnętrznego (art. 96 KW); zatrzymanie osób zaginionych, nieletnich oraz podlegających nakazowi sądowemu (art. 97 KW); zatrzymanie osób, świadków i podejrzanych, w celu złożenia wyjaśnień w procesie sądowym (art. 98 KW); prowadzenie nadzoru niejawnego (art. 99 KW); przechwycenie zaginionych lub skradzionych pojazdów samochodowych, broni, dokumentów i banknotów (art. 100 KW). Dane zawarte w Systemie podlegają ochronie (art. 102–118 KW), a bezpośredni i zastrzeżony dostęp do nich mają wyłącznie krajowe organy odpowiedzialne za kontrole graniczne oraz inne organy prowadzące kontrole policyjne i celne przeprowadzane wewnątrz kraju, jak również służby koordynujące te kontrole, i służby właściwe dla wydawania wiz oraz specjalizujące się w kwestiach dot. cudzoziemców (art. 101 KW). Należy przy tym zaznaczyć, że to kraje Schengen same definiują, jakie instytucje będą uczestniczyć w wymianie informacji.

Dane wprowadzane na mocy art. 94 ust. 3 KW zawierać mogą: nazwisko i imię, ewentualnie pseudonimy rejestrowane oddzielnie; znaki szczególne, obiektywne i niezmienne; pierwszą literę drugiego imienia; datę i miejsce urodzenia; płeć; obywatelstwo; informacja o tym, czy dana osoba jest uzbrojona; informację o tym, czy dana osoba stosuje przemoc; przyczynę zgłoszenia danej osoby oraz zalecany sposób postępowania. Każda osoba może domagać się informacji, czy dane dotyczące jej faktycznie znajdują się w SIS, dostępu do nich oraz domagania się ewentualnego ich sprostowania, usunięcia lub modyfikacji, również w drodze sądowej.

W formie rozbudowanego systemu informatycznego wspomagającego służby graniczne, celne, policyjne i sądowe państw Unii, SIS składa się z poszczególnych podsystemów krajowych, które tworzą specjalne „czarne listy" zawierające określone kategorie danych dotyczą-

cych osób, które należy aresztować w celu ich ekstradycji, obcokrajowców, którym odmówiono wstępu na terytorium Schengen, osób zaginionych, osób wzywanych przez oblicze sądu w związku z toczącym się postępowaniem karnym, a także osób inwigilowanych (por. Tytuł IV KW, art. 92–119 i Tytuł VI, art. 126–130 KW[50]). Osoby fizyczne mają ponadto prawo do zwracania się do swoich krajowych organów kontrolnych SIS nadzorujących bazy danych Systemu o ewentualne sprostowanie lub usunięcie danych nieprawdziwych, wnieść powództwo do sądu o odszkodowanie za straty poniesione w związku z niesłusznym umieszczeniem ich na liście SIS, a także zbadania, czy dane takie w ogóle znajdują się w krajowej bazie (art. 109–111 KW). Przyjęcie Konwencji Schengen nakłada obowiązek wyznaczenia niezależnego organu odpowiedzialnego za kontrolę rejestru działu krajowego Systemu oraz rozpoczęcia współpracy w ramach Wspólnego Organu Kontrolnego SIS (art. 114–115 KW). W ostatnich dniach września 2003 r. uruchomiona została po raz pierwszy strona internetowa Organu pod adresem http: //www.schengen-jsa.dataprotection.org.

Obecnie trwają prace nad opracowaniem drugiej generacji Systemu Informacji Schengen (SIS II), który wejdzie w życie około 2007 r.[51] Jak można się spodziewać, nowy System będzie nie tylko bardziej rozbudowany pod względem ilości użytkowników, lecz także zawierać będzie obszerniejszą liczbę danych, w tym – najprawdopodobniej – dane biometryczne. Wymaga to od legislatorów, którzy opracują ramy prawne dla SIS II, wzięcia pod uwagę potrzeby podwyższenia standardów ochrony danych osobowych.

Obok problematyki granicznej zagadnienie ochrony danych osobowych ujęto także we współpracy policyjnej. Utworzone 1 lipca 1999 r. Europejskie Biuro Policji[52] (Europol) odnosi się wyraźnie do ochrony danych osobowych zawartych w Systemach Komputerowych Europolu (TECS). Utworzony specjalnie w tym celu Wspólny Organ Kontrolny we współpracy z organami krajowymi, monitoruje wdrażanie postanowień Konwencji w zakresie ochrony danych osobowych. Trzeba podkreślić, że na 42 artykuły Konwencji o Europolu, aż 19 odnosi się bezpośrednio do kwestii zabezpieczania, limitowania dostępu oraz korzysta-

[50] Przepisy Tytułu VI KW odnoszą się do ochrony danych osobowych w ogóle, a nie tylko do osobnej kategorii traktowanej w ramach Tytułu IV KW. Por. przewodnik dla osób wnioskujących o dostęp do danych osobowych ujętych w SIS w poszczególnych krajach Schengen – http://escher.drt.garanteprivacy.it.

[51] Więcej: F. Jasiński, *Nie ma się czego bać. System Informacji Schengen*, „Rzeczpospolita" z 4.2.2003 r.

[52] O.J. 1995, C 316/2.

nia z zasobów bazy danych. Zasady wymiany danych osobowych między Biurem a państwami i organami trzecimi zostały określone w odrębnym akcie Rady z 12.3.1999 r.[53]

Równolegle z Konwencją o Europolu opracowano Konwencję o użytkowaniu technologii informatycznej dla celów celnych[54], która zawiera podobnie sformułowane przepisy odnoszące się do ochrony danych osobowych. Także w tym wypadku powołany został Wspólny Organ Kontrolny.

Wspomniane wyżej trzy Wspólne Organy Kontrolne powiązano instytucjonalnie na mocy decyzji Rady z 17.10.2000 r. w sprawie utworzenia Sekretariatu[55], który usprawnia realizację ich zadań, czyli wydawanie opinii w przypadku kolizji wprowadzonych do Systemu danych, wspieranie działalności krajowych organów kontrolnych, przygotowywanie projektów zmian prawnych mających na celu usprawnienie ochrony danych osobowych oraz interpretowane stosowania właściwych przepisów w tym względzie (w przeciągu 7 lat swojego istnienia Wspólny Organ Kontrolny SIS wydał 15 różnych opinii).

Jednakże ochrona danych osobowych nie ograniczyła się, jeśli chodzi o III filar UE, jedynie do trzech wyżej wymienionych Konwencji – znaczna część przepisów decyzji Rady 2002/187/JHA z 28.2.2002 r. w sprawie powołania *Eurojust* w celu wzmocnienia walki z poważną przestępczością[56] odnosi się do ochrony danych (zastosowane podejście zostało o tyle zmienione wobec standardów Schengen, iż zakres zbieranych danych osobowych został rozszerzony o nowe kategorie), podobnie jest w przypadku rozporządzenia Rady (WE) 2725/2000 z 11.12.2000 r. w sprawie systemu *Eurodac* dla porównywania odcisków palców osób ubiegających się o azyl w krajach Unii Europejskiej[57]. W obydwu przypadkach na uwagę zasługuje standardowe utworzenie Wspólnego Organu Kontrolnego, co jednak nie jest niestety podejściem przyjętym w odniesieniu do innych aktów prawnych przyjmowanych w ramach III filara UE. I tak, w decyzji Rady 2003/335/JHA z 8.5.2003 r. w sprawie śledzenia i karania ludobójstwa, zbrodni przeciwko ludzkości i zbrodni wojennych[58] mówi się niezwykle ogólnie o potrzebie przestrzegania „międzynarodowych i krajowych przepisów" dotyczących ochrony danych osobowych, jednakże bez bezpośredniego odwoływania się do

[53] O.J. 1999, C 88/1.
[54] O.J. 1995, C 316/34.
[55] O.J. 2000, L 271/1.
[56] O.J. 2002, L 63/1.
[57] O.J. 2000, L 316/1.
[58] O.J. 2003, L 118/12.

konkretnych aktów prawnych UE lub Rady Europy. Podobnie stało się w przypadku dyrektywy 2002/98/WE z 27.1.2003 r. w sprawie badania i testowania próbek krwi[59], gdzie odniesienie do ochrony danych osobowych jest niezwykle ogólne (art. 24). Podobnie ogólne sformułowania ujęto we wspólnotowych przepisach wizowych.

O wadze, jaką przywiązuje Unia do ochrony danych osobowych, świadczy ponadto umieszczenie jej w art. 8 Karty Praw Podstawowych UE uroczyście przyjętej podczas szczytu Rady Europejskiej w Nicei 8.12.2000 r.[60] Zapisano w niej m.in., iż „dane mogą być przetwarzane tylko w sposób rzetelny dla oznaczonych celów na podstawie zgody osoby zainteresowanej lub w uzasadnionych przypadkach określonych przez prawo"[61]. Karta, która obecnie nie ma jeszcze wiążącego prawnie charakteru, w istotny sposób wpływa na prace instytucji unijnych, tworząc wykładnię podstawowych praw i wolności Unii Europejskiej[62]. W wyniku wprowadzenia KPP do II części projektu Traktatu o Konstytucji dla Europy, opracowanego przez II Konwent Europejski i przedłożonego na szczycie Rady Europejskiej w Salonikach w czerwcu 2003 r., pojawiła się szansa, że ochrona danych osobowych – z chwilą ostatecznego zaakceptowania projektu nowego Traktatu przez państwa członkowskie UE w ramach rozpoczynającej się na początku października 2003 r. Konferencji Międzyrządowej – zyska dodatkowe odniesienie w prawie pierwotnym Unii Europejskiej.

7. Standardy ochrony danych osobowych w świetle członkostwa Polski w UE

Polska przygotowując się do członkostwa w Unii Europejskiej musiała wziąć pod uwagę zobowiązania nakładane na nią w związku z procesem dostosowawczym. Jednym z elementów tego procesu było podporządkowanie prac nad polską ustawą o ochronie danych osobowych

[59] O.J. 2003, L 33/30.

[60] Dz. Urz. WE C 364 z 18.12.2000 r. Więcej: F. Jasiński, *Karta Praw Podstawowych Unii Europejskiej*, Warszawa 2003, s. 192.

[61] Por. materiał wyjaśniający do projektu Karty – CHARTE 4473/00 CONVENT 73 z 11.10.2000 r.

[62] Por. C. Mik, *Karta Praw Podstawowych Unii Europejskie. Zagadnienia podstawowe*, [w:] *Traktat Nicejski*, red. A. Podraza, Lublin 2001 oraz F. Jasiński, *Nabycie mocy prawnie wiążącej przez Kartę Praw Podstawowych Unii Europejskiej – refleksje teoretyczne*, „Przegląd Prawa Europejskiego" 2003, nr 1.

z 29.8.1997 r.[63] wzorcom wypływającym ze wspólnotowego *acquis* oraz Konwencji nr 108. Kilkakrotne nowelizowanie ustawy (obecnie trwa kolejne – 23.9.2003 r. Rada Ministrów przyjęła projekt ustawy o zmianie ustawy) wynikało z toczących się dwustronnych rozmów z przedstawicielami Komisji Europejskiej. Problematyka ochrony danych osobowych podnoszona była zarówno w ramach rozdziałów negocjacyjnych 3. „Swoboda świadczenia usług", jak i rozdziale 24. „Sprawiedliwości i spraw wewnętrznych". Najczęściej podnoszone zarzuty wobec strony polskiej dotyczyły domniemanego braku kontroli wstępnej w polskiej procedurze zgłaszania zbiorów do rejestracji, ograniczonego włączenia do polskiej ustawy definicji użytych w dyrektywie 95/46/WE, dostosowania zakresu przedmiotowego i podmiotowego ustawy oraz zapewnienia swobody przepływu danych w państwach członkowskich Europejskiego Obszaru Gospodarczego. Ponadto właśnie dzięki naciskom strony wspólnotowej Polska ostatecznie stała się stroną Konwencji nr 108.

Skuteczne wypełnianie zadań przez polskiego Generalnego Inspektora Ochrony Danych Osobowych (GIODO, którym w Polsce od 1996 r., już drugą kadencję jest dr Ewa Kulesza) było niejednokrotnie pozytywnie oceniane przez stronę wspólnotową[64], w tym podczas ostatniej misji przeglądowej (ang. *peer review*), która miała miejsce w maju 2002 r. w Warszawie, i która oceniała instytucjonalny wymiar ochrony danych osobowych w Polsce, czyli funkcjonowanie Biura GIODO. Z kolei Raporcie Okresowym Komisji Europejskiej o postępach Polski na drodze do członkostwa z 9.10.2002 r.[65] wskazano, że Generalny Inspektor winien otrzymać „silniejsze uprawnienia administracyjne, aby zapewnić lepsze wdrożenie przepisów dotyczących ochrony danych". Przedstawiciele Biura GIODO aktywnie uczestniczą w pracach Grupy Roboczej Art. 29 i Komitetu Art. 31 Komisji Europejskiej, a także prowadzą szkolenia dla pracowników administracji publicznej i sektora prywatnego z zakresu problematyki ochrony danych osobowych.

---

[63] Dz. U. z 1997 r., Nr 133, poz. 883, z późn. zm.; por.: *Preparing the implementation of the Community personal data protection system in Poland* [w:] *Enlargement of the European Union*, Mediolan 2002; więcej: R. Szałowski, *Prawna ochrona informacji niejawnych i danych osobowych*, Warszawa 2000; *R. Markiewicz, J. Barta*, Ochrona danych osobowych. Poradnik, Kraków 2002; M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice. Wolność informacji, prawo dostępu do informacji publicznej, ochrona danych osobowych*, Wrocław 2002 oraz G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003.

[64] Por. E. Kulesza, *Pozycja i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych w świetle ustawy o ochronie danych osobowych. Uwagi de lega lata i de lega ferenda*, „Przegląd Sejmowy" 1999, nr 6, s. 9; więcej: www.giodo.gov.pl.

[65] COM(2002) 700 final.

***

Ochrona danych osobowych jest zagadnieniem, które rzeczywiście pojawia się w unijnej agendzie coraz częściej – nie tylko w kontekście zbliżającego się rozszerzenia Unii, lecz także odnośnie do problematyki zwalczania tzw. cyber-przestępczości[66], terroryzmu, przejrzystości działań instytucji wspólnotowych, dalszego rozwoju technologicznego (w tym multimedialnego) odnośnie do przetwarzania danych osobowych, czy też kontaktów państw unijnych z krajami trzecimi[67]. Poważne wyzwania stojące zarówno przed legislatorami działającymi na poziomie unijnym, jak i prawnikami w jej obecnych oraz przyszłych państwach członkowskich, to m.in. odpowiedź na pytanie, czy dyrektywa 95/46/WE winna ulec zmianie, a jeśli tak, to w jakim kierunku powinny pójść ewentualne zmiany. Zdaniem autora na obecnym etapie wdrażania *acquis* w obszarze ochrony danych osobowych wszelkie działania ukierunkowane na zdjęcie części ciążących na administratorach danych zadań związanych z obowiązkiem ich ochrony, i zmierzające do nowelizacji – a de facto osłabienia roli – dyrektywy 95/46/WE należy traktować z daleko idącą ostrożnością tym bardziej, że w przeciągu ośmiu lat od przyjęcia poziom implementacji jej przepisów w krajowych porządkach prawnych pozostawia jeszcze wiele do życzenia. Natomiast zbliżające się rozszerzenie Unii o nowe kraje członkowskie na pewno nie poprawi statystyk w tym zakresie[68]. Jak stwierdzono w I raporcie z wdrażania dyrektywy, doświadczenia w jej stosowaniu w dalszym ciągu są jeszcze ograniczone, natomiast badanie opinii publicznej przeprowadzone przez Dyrekcję Generalną Komisji Europejskiej ds. Rynku Wewnętrznego wykazało, że aż 81% badanych osób fizycznych i prawnych uznało swoją wiedzę o ochronie danych osobowych za niewystarczającą i słabą. We wspomnianym raporcie pojawiła się ponadto uwaga, że wraz z przyjęciem przepisów o ochronie danych

[66] „Single Market News" nr 17, maj 2001.

[67] Do tej pory nie został jeszcze zażegnany spór między Komisją Europejską a Stanami Zjednoczonymi w sprawie przetwarzania przez amerykańskie organy ścigania danych dotyczących pasażerów linii lotniczych, por. SPEECH/03/396 z 9.9.2003 r. Por. R. Kraemer, M. Pokrzycki, *Ochrona danych osobowych w instytucjach finansowych z amerykańskiej perspektywy*, „Transformacje prawa prywatnego" 2001, nr 4, s. 73.

[68] Jedynie Turcja nie wprowadziła dotychczas w swojej legislacji przepisów o ochronie danych osobowych, lecz poziom faktycznego wdrażania ich w pozostałych krajach przystępujących i kandydujących jest niezwykle zróżnicowany.

osobowych we wszystkich krajach członkowskich UE, strona wspólnotowa winna była rozpocząć przygotowania do tzw. drugiej fazy implementacji, czyli przyjrzenia się innym aktom prawnym WE i oceny, czy w związku z koniecznością zapewnienia odpowiedniego wdrażania dyrektywy 95/46/WE nie powinno się też dokonać zmian w innych aktach *acquis*.

Skuteczna realizacja idei ochrony danych osobowych może być odpowiednio realizowana jedynie wówczas, jeśli będzie ona stosowana równie skutecznie w odniesieniu do danych przetwarzanych np. w celach medycznych lub marketingowych, jak i wobec danych, które mogą być przetwarzane przez służby policyjne lub wywiadowcze. Nie powinno się bowiem dopuścić do sytuacji, w której prywatność będzie nagminnie naruszana właśnie w imię ochrony swobód obywatelskich. Nie oznacza to jednak przy tym, że organy ścigania winny być całkowicie pozbawione dostępu, realizowanego zgodnie z odpowiednimi przepisami, do danych osobowych, lecz że dostęp taki musi mieć zakres ściśle określony ramami prawnymi oraz ma podlegać skutecznemu nadzorowi ze strony utworzonych tym celu organów kontrolnych. Tylko takie zabezpieczenia mogą zagwarantować rzeczywistą realizację zasady ochrony danych osobowych w demokratycznych państwach prawnych.

Wreszcie, sprawne funkcjonowanie systemu ochrony danych osobowych na poziomie europejskim będzie mogło być realizowane wyłącznie w sytuacji, gdy istnieć będzie jednocześnie swoista przeciwwaga pod postacią zagwarantowania obywatelom UE swobody wyrażania myśli, sumienia i wyznania (por. art. 10 KPP) oraz wypowiedzi[69] i informacji[70], w tym mediów[71] (por. art. 11 KPP).

---

[69] Por. m.in. sprawy połączone 43/82 i 63/82 *VBVB i VBBB v. Komisja*[1984] ECR 9 i 62 oraz sprawa 34/79, *Regina v. M. D. Henn i J. F. E. Darby* [1979] ECR 3795.

[70] Więcej: D. Curtin, *Citizens' fundamental right of access to EU information: an evolving digital passepartout?*, „Common Market Law Review" 2000, nr 37, s. 7; R. W. Davis, *Public access to Community documents: A fundamental human right?*, „European Integration Online Papers" 1999, nr 8, http://eiop.or.at/eiop/texte/1999-008a.htm; M. Broberg, *Access to documents: a general principle of Community law?*, „European Law Review" nr 27/2002, s. 194.

[71] Por. uchwały PE w sprawie praw człowieka i wolności prasy oraz w sprawie poufności dziennikarskich źródeł informacji.