Anastazja Gajda

OCHRONA DANYCH OSOBOWYCH I KIERUNKI ZMIAN W TEJ DZIEDZINIE W PRAWIE UNII EUROPEJSKIEJ

Wprowadzenie[1]

Gromadzenie, przetwarzanie i przekazywanie danych osobowych w istotny sposób wpływa na podstawowe prawa jednostki. Dlatego prawo do ochrony danych osobowych jest jednym z podstawowych warunków gwarantujących wolność i godność każdego człowieka. Dane osobowe obejmują wszelkie informacje dotyczące konkretnej osoby fizycznej o ustalonej tożsamości, którą można zidentyfikować. Cechą wyróżniającą dane osobowe od innych informacji dotyczących osób jest brak anonimowości[2]. Dane osobowe stanowią element życia prywatnego. Prawo do ich ochrony jest stosunkowo nowym w treści prawem podmiotowym, które przysługuje jednostce na równi z innymi prawami podstawowymi.

W opracowaniu przedstawiam obowiązujące rozwiązania prawne, które służą zapewnieniu skutecznej ochrony danych osobowych w Unii Europejskiej. Istotny wpływ na ich kształt wywarł Traktat z Lizbony (dalej: TL)[3]. Chcąc pokazać specyfikę tych uregulowań, nie sposób nie odnieść się do innych aktów prawnych tworzonych w ramach systemu prawnego Rady Europy, które w znaczący sposób wpłynęły na obecny kształt regulacji w UE.

Ponadto omawiam podstawowe założenia nowej reformy w zakresie ochrony danych osobowych przedstawione przez Komisję Europejską w styczniu 2012 r. Propozycje zmiany unijnego prawa dotyczącego ochrony danych osobowych pod wieloma względami cechuje rewolucyjny charakter. Nowe prawo będzie miało wpływ

---

[1] Stan prawny regulacji omawianych w opracowaniu datowany jest na 1 października 2013 r.

[2] A.M. Dereń, *Ochrona danych osobowych. Omówienie przepisów ustawy*, Bydgoszcz 1998, z. 77/98, s. 9.

[3] Zob. Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13 grudnia 2007, DzUrz. UE 2007 C 306/1. W sposób znaczący zmienił dwa dotychczasowe traktaty, tj. Traktat o Unii Europejskiej (dalej: TUE) oraz Traktat ustawiający Wspólnotę Europejską (dalej: TWE), przy czym ten ostatni od 1 grudnia 2009 r. zwany jest Traktatem o funkcjonowaniu Unii Europejskiej (dalej: TfUE). Wersje skonsolidowane traktatów zob. DzUrz. UE 2012 C 326/1.

na prawo polskie. Propozycje obejmują zarówno przetwarzanie danych osobowych w sektorze prywatnym, jak i przez podmioty publiczne w związku z egzekwowaniem prawa. Reforma ma zagwarantować obywatelom Unii poszanowanie prywatności, o którą coraz trudniej w cyfrowym świecie, oraz doprowadzić do harmonizacji zasad ochrony prywatności w obszarze dawnego trzeciego filaru UE, tj. w ramach współpracy policyjnej i sądowej w sprawach karnych.

1. Ochrona danych osobowych w systemie prawnym Rady Europy

Pierwsze kroki zmierzające do zapewnienia europejskiej ochrony danych osobowych zostały poczynione przez Radę Europy[4]. Ta międzynarodowa organizacja zajmuje się przede wszystkim ochroną praw człowieka. Instrumentem prawnym, który się do takiej ochrony przyczynia, jest Europejska konwencja o ochronie praw człowieka i podstawowych wolności (dalej: EKPCz), podpisana w Rzymie 4 listopada 1950 r.[5] EKPCz w swoich postanowieniach nie odnosi się jednak bezpośrednio do ochrony danych osobowych. W jej art. 8 znalazło się jednak prawo każdej osoby do ochrony własnego życia prywatnego i rodzinnego[6]. Nie dopuszcza się jakiejkolwiek ingerencji władzy publicznej w korzystanie z tego prawa. W artykule 10 jest z kolei mowa o wolności wyrażania opinii. Artykuł 14 wprowadza zakaz dyskryminacji[7].

Od wczesnych lat 70. XX w. coraz częściej podnoszono w Europie sprawę ochrony danych osobowych. Było to związane m.in. z burzliwym rozwojem technologii informacyjnych i komunikacyjnych, którym towarzyszyło wzrastające przekonanie o konieczności istnienia prawnych i technicznych środków dla ochrony prywatności danych osobowych[8]. W 1968 r. Komitet Ministrów Rady Europy rozpoczął prace zmierzające do przyjęcia kompleksowego aktu prawnego odnoszącego się do ochrony danych w państwach członkowskich. Ich rezultatem było przyjęcie przez Radę Europy w 1981 r. Konwencji nr 108 o ochronie osób w związku z automatycznym

[4] Rada Europy powstała 5 maja 1949 r. Na ten temat zob. W. Czapliński, A. Wyrozumska, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, wyd. 2, Warszawa 2004, s. 383 i n.

[5] Tekst zob. DzU 1993, nr 61, poz. 284 z późn. zm.

[6] Zob. S.M. Krajnik, *Prawo do poszanowania prywatności w systemie Europejskiej Konwencji Praw Człowieka*, w: *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowska, Toruń 2008, s. 177–188.

[7] Zob. też J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. 2, Warszawa 2011, s. 37–45.

[8] G. Pearce, N. Platten, *Achieving Personal Data Protection in the European Union*, „Journal of Common Market Studies" 1998, Vol. 36, No. 4, s. 531.

przetwarzaniem danych osobowych (dalej: Konwencja nr 108)[9]. Była to pierwsza umowa międzynarodowa w Europie o przetwarzaniu danych osobowych oraz zawierająca minimalne standardy ich ochrony[10]. Stanowiła znaczący krok w rozwoju prawa dotyczącego tej problematyki nie tylko w systemach wewnętrznych państw–stron tej Konwencji nr 108, ale także w prawie wspólnotowym/unijnym. W 2001 r. został przyjęty Protokół dodatkowy[11] do Konwencji nr 108 o organach nadzoru i transgranicznego przepływu danych. Ustanawia on dodatkowe materialne i formalne warunki dla właściwego przetwarzania danych osobowych. Wszystkie państwa członkowskie UE są stronami Konwencji nr 108, ale nie wszystkie są stronami Protokołu dodatkowego.

Podstawowym celem Konwencji nr 108 jest „zapewnienie każdej osobie fizycznej, bez względu na narodowość lub miejsce zamieszkania, poszanowanie jej praw i podstawowych wolności [...], a w szczególności jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych"[12] (por. art. 1). W preambule do Konwencji nr 108 podkreślono, że „pożądane jest rozszerzenie zakresu ochrony praw podstawowych i wolności każdej osoby, a w szczególności prawa do poszanowania prywatności, biorąc pod uwagę stale rosnący przepływ przez granice danych osobowych, podlegających automatycznemu przetwarzaniu". Jednocześnie strony Konwencji nr 108 „potwierdziły swoje zaangażowanie na rzecz wolności przepływu informacji, bez względu na granice" oraz uznały „konieczność pogodzenia podstawowych wartości, takich jak poszanowanie prywatności i swobody przepływu informacji między ludźmi".

Najważniejsze problemy związane z ochroną danych osobowych w Konwencji nr 108 można sklasyfikować w następujący sposób[13]:

- wymogi co do jakości przetwarzanych informacji,
- dopuszczalność przetwarzania szczególnych kategorii danych,
- prawa osób, których dane dotyczą,
- kwestia bezpieczeństwa danych.

---

[9] Konwencja nr 108 została sporządzona w Strasburgu dnia 28 stycznia 1981 r. Weszła w życie 1 października 1985 r. Tekst zob. European Treaty Series – No. 108 oraz DzU 2003, nr 3, poz. 25.

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

[11] Zob. Additional protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, sporządzony w Strasburgu 8 listopada 2001 r. Tekst zob. European Treaty Series – No. 181 oraz DzU 2005, nr 11, poz. 1.

[12] Zgodnie z art. 2 pkt a) Konwencji nr 108 przez dane osobowe należy rozumieć każdą informację dotyczącą osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować.

[13] D. Mednis, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, „Państwo i Prawo" 1997, z. 6, s. 37.

Konwencja nr 108 w art. 5 wskazuje ogólne wymogi dotyczące jakości przetwarzanych danych osobowych. Informacje te powinny być pozyskiwane i przetwarzane w sposób rzetelny i zgodny z prawem. Zakres gromadzonych i używanych danych powinien odpowiadać określonym celom. Ponadto dane powinny być dokładne i aktualne. Należy je przechowywać w formie pozwalającej na identyfikację osób tylko przez taki okres, który jest niezbędny do celów, dla których zostały one zebrane.

Przetwarzanie szczególnych kategorii danych osobowych, tj. danych ujawniających pochodzenie rasowe, poglądy polityczne, przekonania religijne, dotyczące stanu zdrowia lub życia seksualnego[14], jest dozwolone tylko wtedy, gdy prawo wewnętrzne przewiduje odpowiednie gwarancje dla prywatności jednostek. Konwencja nr 108 nie precyzuje jednak, na czym konkretnie te gwarancje miałyby polegać (por. art. 6).

Każdej osobie zapewnia się prawo do informacji o zbiorze, w którym są przechowywane dotyczące jej dane. Osoba ta może otrzymywać – w rozsądnych odstępach czasu i bez zbędnej zwłoki oraz kosztów – informacje o tych danych i ich treści (tzw. prawo dostępu). Przysługuje jej także prawo do sprostowania błędnych danych oraz domagania się ich usunięcia, jeśli są przetwarzane niezgodnie z prawem. Ma ona również możliwość odwołania się w razie nieprzestrzegania powyższych praw (por. art. 8).

Konwencja nr 108 zobowiązuje także sygnatariuszy do przyjęcia odpowiednich zabezpieczeń przed przypadkowym i nieuprawnionym zniszczeniem danych osobowych, ich utratą, zmianą, upublicznieniem lub dostępem (por. art. 7). Wyznacza jednak jedynie minimalny standard ochronny i w żadnym razie nie stoi na przeszkodzie przyznaniu z mocy przepisów prawa wewnętrznego ochrony szerszej niż ta, która wynika z jej postanowień (por. art. 11).

Zasady przetwarzania danych osobowych określone w Konwencji nr 108 stosuje się ogólnie do przetwarzania danych zarówno w sektorze prywatnym, jak i publicznym. Taka regulacja okazała się jednak niewystarczająca. Zaistniała potrzeba przystosowania tych zasad do specyficznych wymogów poszczególnych sektorów. To „sektorowe ujęcie" ochrony danych osobowych doprowadziło do przyjęcia przez Komitet Ministrów i Zgromadzenie Parlamentarne Rady Europy wielu zaleceń i rekomendacji[15]. Akty te rozwijają przepisy Konwencji nr 108, precyzują jej wymagania oraz

[14] Są to tzw. dane wrażliwe.

[15] Należą do nich m.in.: Zalecenie nr R (87) 15 o ochronie danych osobowych wykorzystywanych w sektorze policji z 17 września 1987 r., Zalecenie nr R (81) 1 dotyczące automatycznych banków danych medycznych z 23 stycznia 1981 r., Zalecenie nr R (83) 10 o ochronie danych osobowych wykorzystywanych do celów naukowych i badań statystycznych z 23 września 1983 r., Zalecenie nr R (85) 20 o ochronie danych osobowych wykorzystywanych dla celów marketingu bezpośredniego z 25 października 1985 r. oraz Zalecenie nr R (86) 1 o ochronie danych osobowych wykorzystywanych dla celów ubezpieczenia społecznego

wprowadzają dodatkowe warunki przetwarzania danych osobowych odnoszących się do policji, zatrudnienia, telekomunikacji, marketingu bezpośredniego czy danych medycznych.

Problem ochrony danych osobowych został także zauważony przez Radę Europy przy okazji podjętej próby regulacji biomedycyny w Europejskiej konwencji bioetycznej z 4 kwietnia 1997 r.[16] Zgodnie z jej art. 1 przedmiotem i celem tego aktu prawnego jest ochrona godności i tożsamości osoby ludzkiej oraz gwarancja poszanowania integralności, a także innych praw podstawowych i wolności każdej osoby bez dyskryminacji wobec zastosowań biologii i medycyny. W art. 10 tej konwencji wyraźnie zapewniono, że każda osoba ma prawo do poszanowania życia prywatnego w zakresie informacji o jej zdrowiu. Przy czym należy uszanować życzenia jednostek, które nie chcą być w ten sposób informowane. Jednocześnie w art. 10 ust. 3 tej konwencji zapisano, że w przypadkach wyjątkowych prawo może wprowadzić – w interesie pacjenta – ograniczenia w korzystaniu z praw poznania wszelkich zebranych informacji o swoim zdrowiu.

W zasadzie wszystkie istniejące w UE akty prawne dotyczące ochrony danych osobowych odwołują się do postanowień zawartych zarówno w Konwencji nr 108, jak i w Zaleceniu nr R (87) 15[17].

2. Ochrona danych osobowych w prawie Unii Europejskiej przed wejściem w życie Traktatu z Lizbony

Do czasu wejścia w życie Traktatu z Lizbony[18] struktura UE była trójfilarowa. I filar tej struktury stanowiły Wspólnoty Europejskie, funkcjonujące zgodnie z prawem wspólnotowym. II filar obejmował Wspólną Politykę Zagraniczną i Bezpieczeństwa (WPZiB), w ramach której współpraca nie wykraczała poza tradycyjną współpracę międzynarodową regulowaną przez prawo międzynarodowe publiczne.

---

z 23 stycznia 1986 r. Teksty tych zaleceń zob. oficjalna strona internetowa Rady Europy http://www.coe.int. Polski przekład zob. T. Jasudowicz, *Ochrona danych osobowych, standardy europejskie. Zbiór materiałów*, Toruń 1998.

[16] Zob. Convention for Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine, European Treaty Series 164.

[17] Zalecenie nie ma jednak w przeciwieństwie do Konwencji nr 108 mocy prawnie wiążącej. Nie oznacza to jednak, że nie wywiera wpływu na praktyczny aspekt jego stosowania i tworzenia prawa pod jego wpływem.

[18] Traktat z Lizbony wszedł w życie 1 grudnia 2009 r.

III filar UE, czyli współpraca policyjna i sądowa w sprawach karnych również mieściła się w ramach tradycyjnej współpracy międzyrządowej.

W efekcie istnienia struktury filarowej UE przetwarzanie danych osobowych w poszczególnych filarach było zróżnicowane. Inaczej wyglądało ono w ramach I filaru, a inaczej w dwóch pozostałych. Nie było podstawy prawnej, która umożliwiałaby przyjęcie w ramach III filaru UE stosownych przepisów ogólnych w zakresie ochrony danych osobowych, mogących mieć zastosowanie m.in. do przetwarzania takich danych na poziomie krajowym[19].

Przez długi czas Wspólnoty Europejskie (potem UE) nie zajmowały się problemem odrębnej regulacji dotyczącej ochrony danych osobowych. Komisja Europejska postulowała jedynie, by państwa członkowskie UE ratyfikowały do końca 1982 r. Konwencję nr 108[20]. Dopiero na początku lat 90. rozpoczęły się prace nad właściwym *acquis* w tym zakresie[21]. Dnia 13 września 1990 r. Komisja Europejska[22] przedstawiła swój komunikat dotyczący ochrony danych osobowych. Stwierdziła w nim, że różnorodność krajowych podejść i brak systemu ochrony na poziomie wspólnotowym stanowią barierę dla utworzenia Wspólnego Rynku. Jeśli prawa podstawowe podmiotu danych (w szczególności jego prawo do prywatności) nie są chronione na poziomie wspólnotowym, to ponadgraniczny przepływ danych może być zahamowany. Komunikat odnosił się m.in. do przystąpienia Wspólnot do Konwencji nr 108 oraz zawierał projekty aktów prawnych dotyczących prywatności w kontekście publicznych cyfrowych sieci telekomunikacyjnych, telefonii komórkowej i bezpieczeństwa informacji. Spowodowane to było rangą problematyki ochrony danych osobowych oraz istnienia w tej dziedzinie znacznych rozbieżności w uregulowaniach prawnych występujących w państwach członkowskich UE.

Prace legislacyjne zakończyły się przyjęciem 24 października 1995 r. Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (dalej: Dyrektywa 95/46/WE)[23]. Sama dyrektywa, choć jej podstawowym celem jest zagwarantowanie przepływu danych osobowych, przewiduje w art. 1 ust. 1, że

---

[19] Zob. A. Grzelak, *Projekt ochrony danych osobowych w sprawach karnych w UE – kolejny krok na drodze do społeczeństwa nadzorowanego?*, „Europejski Przegląd Sądowy" 2012, nr 11, s. 20 i n.; S. Nouwt, *Towards a Common Approach to Data Protection: A Critical Analysis of Data Protection Perpectives of the Council of Europe and European Union*, w: *Reinventing Data Protection*, red. S. Gurwith et al., Berlin 2009, s. 275 i n.

[20] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. 4, Kraków 2007, s. 83.

[21] F. Jasiński, *Ochrona danych osobowych w porządku prawnym Unii Europejskiej*, „Kwartalnik Prawa Publicznego" 2003, nr 3, s. 208–209.

[22] Proposal for a European Parliament and Council Directive concerning the Protection of Individuals in relation to the processing of personal data, COM(90) 314 final.

[23] DzUrz. WE 1995 L 281/95.

„państwa członkowskie zobowiązują się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych". Poszczególne motywy Dyrektywy 95/46/WE, zwłaszcza motyw 10 i 11, wyrażają również ten wymóg[24]. Potwierdził to także wyrok Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE) z 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01 Österreichischer Rundfunk, stwierdzając, że choć celem Dyrektywy 95/46/WE jest zapewnienie swobodnego przepływu danych, to w znaczącym zakresie stoi ona również na straży praw podstawowych[25]. Teza ta została następnie potwierdzona w wyroku Trybunału Sprawiedliwości UE z 6 listopada 2003 r. w sprawie C-101/01 Postępowanie karne przeciwko B. Lindqvist, poprzez stwierdzenie, że Dyrektywa 95/46/WE ma za zadanie sprzyjać swobodnemu przepływowi danych, jednocześnie zapewniając wysoki poziom ochrony praw i interesów osób, których te dane dotyczą[26].

W artykule 2 lit. a Dyrektywy 95/46/WE „dane osobowe" definiuje się szeroko jako „wszelkie informacje dotyczące zidentyfikowanej lub dającej się zidentyfikować osoby fizycznej". Z kolei „osoba możliwa do zidentyfikowania" to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. Definicja ta nie zawiera katalogu informacji, które można uznać za dane osobowe.

Pojęcie danych osobowych nie było także, samo w sobie, przedmiotem wątpliwości rozstrzyganych przez TSUE. Jednak w kilku przypadkach uznał on za stosowne potwierdzić, że sprawa dotyczy danych o charakterze osobowym. W tym celu Trybunał Sprawiedliwości dokonywał stosownej analizy informacji, o które chodziło w danej sprawie pod kątem ich „osobowego" charakteru. O tym, czy mamy do

[24] Motyw 10 Dyrektywy 95/46/WE stanowi, że „celem krajowych przepisów prawa dotyczących przetwarzania danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności, które zostało uznane zarówno w art. 8 Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności oraz w zasadach ogólnych prawa wspólnotowego; z tego powodu zbliżanie przepisów prawa nie powinno wpłynąć na zmniejszenie ochrony, jaką gwarantują, lecz przeciwnie, musi dążyć do zapewnienia jak najwyższego stopnia ochrony we Wspólnocie". Z motywu 11 wynika, że „zasady ochrony praw i wolności jednostek, szczególnie prawa do prywatności, które zawarte są w niniejszej dyrektywie, utrwalają i umacniają zasady wyrażone w Konwencji Rady Europy z dnia 28 stycznia 1981 r. w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych".

[25] Zb. Orz. 2003, s. I-04989, pkt 70.

[26] Zb. Orz. 2003, s. I-12971, pkt 96. Zob. także podobnie np. wyrok TSUE z 16 grudnia 2008 r. w sprawie C-524/06 Heinz Huber przeciwko Bundesrepublik Deutschland, Zb. Orz. 2008, s. I-9705, pkt 47 oraz wyrok TSUE z 24 listopada 2011 r. w sprawach połączonych C-468/10 i C-469/10 Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado, niepubl., pkt 25.

czynienia z danymi osobowymi, decyduje zatem nie tyle ich treść, co okoliczność pozwalająca je łatwo powiązać z konkretną osobą (wskazać ją)[27]. Za dane osobowe Trybunał uznał więc następujące kategorie informacji:

- nazwisko osoby w połączeniu z jej numerem telefonu lub informacjami dotyczącymi jej warunków pracy czy sposobów spędzania przez nią wolnego czasu[28],
- nazwiska osób i ich roczne dochody[29],
- dane dotyczące dochodu z tytułu działalności zarobkowej i z kapitału oraz dane dotyczące majątków osób fizycznych[30],
- imię, nazwisko, data i miejsce urodzenia, narodowość, stan cywilny, płeć, historia wjazdów na terytorium danego państwa i opuszczania tego terytorium, status pobytu, szczegóły odnoszące się do kolejnych paszportów, historia wpisów meldunkowych, oznaczenie urzędów i służb, które dane przekazały[31].

Zgodnie z art. 3 ust. 1 przepisy Dyrektywy 95/46/WE stosuje się do przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych. „»Przetwarzanie danych osobowych« oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie" (por. art. 2 lit. b). Nigdy nie budziło wątpliwości to, że przetwarzaniem danych osobowych jest każda czynność dokonana na danych osobowych. Jednak zastosowanie przepisów Dyrektywy 95/46/WE zależy również od sposobu wykorzystania danych – jeśli przetwarzanie nie jest choćby w części zautomatyzowane, to Dyrektywa 95/46/WE ma zastosowanie tylko wówczas, gdy dane są lub mają stanowić część zbioru danych.

Dlatego w wyroku TSUE Postępowanie karne przeciwko B. Lindqvist Trybunał Sprawiedliwości uznał, że operację polegającą na zamieszczaniu danych osobowych

---

[27] Zob. A. Mednis, *Dyrektywa 95/46 w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej – wybrane zagadnienia*, w: *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. A. Mednis, Warszawa 2013, s. 130 i n.

[28] Zob. wyrok TSUE z 6 listopada 2003 r. w sprawie C-101/01 Postępowanie karne przeciwko B. Lindqvist, Zb. Orz. 2003, s. I-12971.

[29] Zob. wyrok TSUE z 20 maja 2003 r. w sprawach połączonych C-465/00, C-138/01 i C-139/01 Österreichischer Rundfunk, Zb. Orz. 2003, s. I-04989.

[30] Zob. wyrok TSUE z 16 grudnia 2008 r. w sprawie C-73/07 Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy, Zb. Orz. 2008, s. I-09831.

[31] Zob. wyrok TSUE z 16 grudnia 2008 r. w sprawie C-524/06 H. Huber przeciwko Bundesrepublik Deutschland, Zb. Orz. 2008, s. I-09705.

na stronie internetowej należy uznać za przetwarzanie danych osobowych w rozumieniu art. 3 ust. 1 Dyrektywy 95/46/WE. Co do „zautomatyzowanego" charakteru przetwarzania TSUE stwierdził, że zamieszczenie danych osobowych na stronie internetowej wymagało, według stosowanych procedur technicznych i informatycznych, załadowania tej strony na serwer oraz przeprowadzenia niezbędnych operacji, które uczynią tę stronę dostępną dla osób, które mają połączenie z internetem. Operacje te są zatem – w opinii TSUE – realizowane, przynajmniej częściowo, w sposób zautomatyzowany.

Natomiast w wyroku TSUE z 16 grudnia 2008 r. w sprawie C-73/07 Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy[32] Trybunał uznał, że przetwarzaniem danych będzie: gromadzenie danych osobowych w oparciu o dokumenty urzędowe, opublikowanie ich w formie obszernej listy, udostępnianie ich w formie płyty CD-ROM na potrzeby wykorzystania do celów komercyjnych, przetworzenie ich na potrzeby serwisu SMS, w którego ramach po wysłaniu krótkiej wiadomości tekstowej zawierającej imię, nazwisko i miejsce zamieszkania konkretnej osoby pod konkretny numer użytkownik telefonu komórkowego może uzyskać dane dotyczące konkretnej osoby.

Państwa członkowskie UE zostały zobowiązane do zapewnienia rzetelnego i legalnego przetwarzania danych osobowych. Powinny być one gromadzone do określonych, jednoznacznych i legalnych celów oraz niepoddawane dalszemu przetwarzaniu w sposób niezgodny z tymi celami. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie jest uważane za niezgodne z przepisami, pod warunkiem ustanowienia przez państwa członkowskie odpowiednich środków zabezpieczających, ponadto adekwatne, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone. Dane te powinny być prawidłowe oraz w razie konieczności aktualizowane. Należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane. Dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których zostały zgromadzone lub dla których są dalej przetwarzane. Państwa członkowskie ustanowią odpowiednie środki zabezpieczające dla danych przechowywanych przez dłuższe okresy dla potrzeb historycznych, statystycznych i naukowych. Obowiązek przestrzegania tych zasad Dyrektywa 95/46/WE nakłada na administratora danych (por. art. 6 ust. 1 i 2).

[32] Zb. Orz. 2008, s. I-09831.

Dyrektywa 95/46/WE wprowadza także katalog minimalnych praw służących osobom, których dane są zbierane. Naruszenie tych uprawnień może być dochodzone na drodze sądowej. Gdy przewidziana jest zgoda osoby na działania dotyczące jej danych, jest ona uzależniona od uprzedniego dostarczenia tej osobie oznaczonych w Dyrektywie 95/46/WE informacji o administratorze, o zbiorze danych, jego charakterze i celu, a także informacji w sprawie dobrowolności udostępnienia danych (por. art. 10 i 11). Osoby, których dane osobowe są zbierane, powinny być informowane co najmniej o: przeznaczeniu danego zbioru danych, obligatoryjnym lub dobrowolnym charakterze odpowiedzi na pytania kwestionariusza, konsekwencjach braku odpowiedzi, możliwości wglądu i korekty danych dotyczących danej osoby oraz odbiorcach i nadzorującym zbiór danych. Istotne jest także, że Dyrektywa 95/46/WE zakazuje zasadniczo przetwarzania danych w innym celu niż ten, dla którego zostały zebrane, i w innym celu niż ten, który towarzyszył zgodzie ze strony osoby, której dane dotyczą. Przetwarzanie danych osobowych pomimo braku zgody osoby, której dane dotyczą, jest dopuszczalne tylko w ściśle określonych sytuacjach (por. art. 7 Dyrektywy 95/46/WE).

Przepisy Dyrektywy 95/46/WE zawierają także wyraźne postanowienia dotyczące zakazu zbierania w celu automatycznego przetwarzania określonych kategorii informacji, chyba że zainteresowany podmiot wyraził w formie pisemnej zgodę na takie postępowania (por. art. 8). Do informacji objętych tych zakazem (tzw. danych wrażliwych) zaliczono dane dotyczące pochodzenia etnicznego lub rasowego, poglądów politycznych, przekonań religijnych i politycznych, członkostwa w związkach zawodowych oraz informacje dotyczące zdrowia i życia seksualnego. Natomiast jeżeli chodzi o dane dotyczące skazań kryminalnych, to mogą być one gromadzone jedynie w zbiorach danych o charakterze publicznym (por. art. 8 ust. 5).

Każda osoba, której dane znajdują się w zbiorze danych, ma prawo do informacji o istnieniu takiego zbioru, jego głównych celach oraz adresie prowadzącego dany zbiór (por. art. 12 Dyrektywy 95/46/WE). Ponadto każdy zainteresowany powinien mieć prawo do uzyskania, w rozsądnym czasie oraz bez nadmiernego opóźnienia i kosztów, informacji o tym, czy dane dotyczące jego osoby znajdują się w zbiorze danych – w razie odpowiedzi pozytywnej przysługiwać mu powinno prawo do uzyskania tych danych w formie umożliwiającej do zapoznania się z nimi.

Uprawniony może także domagać się korekt, usunięcia lub zablokowania tych danych dotyczących go, które uzyskane zostały z naruszeniem przepisów Dyrektywy 95/46/WE. Może się również domagać identycznych czynności od osób trzecich, którym takie dane zostały przekazane. Uprawnienia osoby, której dane dotyczą, do dostępu i korekty lub wycofania danych mogą zostać ustawowo w poszczególnych państwach członkowskich wyłączone lub ograniczone w przypadkach podyktowanych

m.in. następującymi względami: bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego, działań prewencyjnych, prowadzonych czynności dochodzeniowo-śledczych i prokuratorskich w sprawach karnych lub w sprawach o naruszenie zasad etyki w zawodach podlegających regulacji, ważnego interesu ekonomicznego lub finansowego państwa członkowskiego UE (wraz z kwestiami pieniężnymi, budżetowymi i podatkowymi) oraz funkcji kontrolnych, inspekcyjnych i regulacyjnych (por. art. 13 Dyrektywy 95/46/WE).

Osoba, której dane dotyczą, może także wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych, zebranych w warunkach, gdy było to niezbędne do wykonywania określonych prawem zadań realizowanych dla dobra publicznego lub gdy było to niezbędne do wypełnienia usprawiedliwionych celów administratorów danych (jeśli administrator danych zamierza je przetwarzać w celach marketingowych) lub wobec przekazania danych osobowych innemu administratorowi danych (por. art. 14 Dyrektywy 95/46/WE).

W tekście Dyrektywy 95/46/WE uregulowano także kwestie dotyczące poufności i bezpieczeństwa przetwarzanych danych (art. 16–17), obowiązków administratora danych (art. 18–21), odpowiedzialności za wyrządzenie szkody wskutek niezgodnej z prawem operacji przetwarzania danych (art. 22–24), przekazywania danych osobowych do państw trzecich (art. 25–26), problemu kodeksów postępowania w zakresie przetwarzania danych osobowych (art. 27), uprawnienia organu nadzorczego i grupy roboczej do spraw ochrony osób fizycznych w zakresie przetwarzania danych (art. 28–30) oraz kwestie wspólnotowych środków wykonawczych (art. 31)[33].

Warto też wyraźnie zaznaczyć, że z mocy postanowień Dyrektywy 95/46/WE wyłączono obszary nieobjęte ówczesnym prawem wspólnotowym, tj. WPZiB oraz współpracę policyjną i sądową w sprawach karnych (por. art. 3 ust. 2).

Poza Dyrektywą 95/46/WE, która ma charakter ogólny, istnieje cały szereg sektorowych aktów prawnych odnoszących się do ochrony danych osobowych. Wspólnotowe podejście do ochrony danych osobowych i prywatności w sektorze telekomunikacyjnym pierwotnie ujęto w Dyrektywie 97/66/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 1997 r. dotyczącej przetwarzania danych osobowych oraz

[33] Szeroko na temat Dyrektywy 95/46/WE zob. m.in.: N.N. Gomes de Andrade, *Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights*, w: *Privacy and Identity*, red. S. Fischer-Hübner et al., International Federation for Information Processing 2011, s. 90 i n.; S. Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, „Iowa Law Review" 1995, No. 3, s. 445–469; M.T. Tinnefeld, *Ochrona danych – kamień węgielny budowy Europy. Wprowadzenie*, w: *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999, s. 33 i n.; P. Fajgielski, *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno-prawne*, Lublin 2008, s. 75 i n. oraz M. Andenas, S. Zleptnig, *Surveillance and Data Protection: Regulatory Approaches in the EU and Member States*, „European Business Law Review" 2003, Issue 6, s. 771 i n.

ochrony prywatności w sektorze telekomunikacyjnym[34]. Precyzuje ona i uzupełnia zasady zawarte w Dyrektywie 95/46/WE. Jednak gwałtowny rozwój techniczny w tym obszarze oraz konieczność uwzględnienia go w regulacjach prawnych doprowadziły do zastąpienia Dyrektywy 97/66/WE nową Dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze komunikacji elektronicznej[35]. Znalazły się w niej szczegółowe uregulowania dotyczące m.in. świadczenia usług publicznych w komunikacji elektronicznej w ramach publicznych sieci komunikacyjnych, stosowania odpowiedniego poziomu zabezpieczeń sieci gwarantujących poufność informacji, szczegółowych bilingów, spisów abonentów oraz marketingu bezpośredniego[36].

Odrębnej regulacji prawnej poddana została tematyka ochrony danych osobowych przetwarzanych przez instytucje i organy wspólnotowe. W prawie pierwotnym podstawowe znaczenie miała w tym zakresie treść art. 286 TWE[37]. Artykuł ten nie nałożył na państwa członkowskie zobowiązania traktatowego do ochrony danych osobowych swoich obywateli, ale wskazał jedynie na potrzebę przeniesienia istniejących standardów w tym względzie na poziom instytucji WE.

Natomiast w prawie wtórnym podstawowe znaczenie w tym zakresie mają: Rozporządzenie (WE) 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych [dalej:

---

[34] DzUrz. WE 1998 L 24/1.

[35] Dz.Urz. WE 2002 L 201/37.

[36] Dyrektywa 2002/58/WE została częściowa zmieniona z mocy Dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, DzUrz. UE 2006 L 105/54. Jej podstawowym założeniem jest zbliżenie przepisów państw członkowskich UE w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego. Na uwagę zasługuje także Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, DzUrz. UE 2009 L 337/11.

[37] Art. 286 TWE stanowił: „1. Począwszy od 1 stycznia 1999 roku, akty wspólnotowe dotyczące ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych oraz swobodnego przepływu tych danych mają zastosowanie do instytucji i organów ustanowionych niniejszym Traktatem lub na jego podstawie.

2. Przed nadejściem daty określonej w ustępie 1 Rada, stanowiąc zgodnie z procedura określoną w artykule 251, ustanawia niezależny organ kontrolny odpowiedzialny za nadzorowanie stosowania tych aktów wspólnotowych do instytucji i organów wspólnotowych oraz, w odpowiednim przypadku, przyjmuje wszelkie inne właściwe przepisy". Artykuł ten został wprowadzony do TWE przez Traktat z Amsterdamu.

Rozporządzenie (WE) 45/2001][38] oraz Decyzja Rady z dnia 13 września 2004 r. ustanawiająca reguły wykonawcze dotyczące rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[39]. Powyższe akty prawne stanowią konkretyzację dyrektyw odnoszących się do ochrony danych (zarówno Dyrektywy 95/46/WE, jak i dyrektyw telekomunikacyjnych). Uwzględniają specyfikę przetwarzania danych przez instytucje i organy wspólnotowe. Oprócz przepisów natury ogólnej, odnoszących się m.in. do zasad i podstaw dopuszczalności przetwarzania danych przez wspomniane instytucje i organy, zawierają one cały szereg postanowień odnoszących się do kwestii szczegółowych. Należą do nich m.in. zasady przekazywania danych w stosunkach wewnętrznych i zewnętrznych, wstępnej kontroli przetwarzania danych oraz ochrony danych w kontekście wewnętrznych sieci telekomunikacyjnych.

Na uwagę zasługuje także utworzenie na mocy postanowień Rozporządzenia 45/2001 niezależnego organu nadzorczego, tj. Europejskiego Inspektora Ochrony Danych Osobowych (EIOD)[40]. Do jego zadań należy m.in. zapewnienie skutecznej realizacji przepisów Rozporządzenia 45/2001 w odniesieniu do funkcjonowania instytucji i organów wspólnotowych oraz odpowiedzialność za zapewnienie, że podstawowe prawa i wolności osób fizycznych (w szczególności prawo do prywatności) są respektowane przez te instytucje i organy przy przekazywaniu danych osobowych.

Przetwarzanie danych osobowych w ramach I filaru UE zostało więc objęte spójnymi regulacjami, wynikającymi przede wszystkim z Dyrektywy 95/46/WE. Od momentu jej przyjęcia w 1995 r. ukształtowało się prawodawstwo oraz instytucje i orzecznictwo TSUE dotyczące ochrony danych osobowych w UE[41]. Natomiast w przypadku dawnego III filaru rozwój prawodawstwa następował w odwrotnej kolejności[42]. Najpierw pojawiły się regulacje szczegółowe dotyczące ochrony danych osobowych, zawarte w różnych aktach prawnych tworzonych w ramach współpracy policyjnej i sądowej w sprawach karnych[43]. Akty te różnią się zarówno zakresem

[38] DzUrz. WE 2001 L 8/1.

[39] DzUrz. UE 2004 L 296/16.

[40] Szeroko na ten temat EIOD zob. H. Hijmans, *The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority*, „Common Market Law Review" 2006, Vol. 43, s. 1313–1342.

[41] A. Grzelak, op.cit., s. 21.

[42] Zob. na ten temat m.in.: A. Gajda, *Ochrona danych osobowych w III filarze Unii Europejskiej*, „Studia i Prace Kolegium Ekonomiczno-Społecznego SGH" 2008, z.n. 15, s. 423–453; H. Maroń, *Ochrona danych osobowych w III filarze Unii Europejskiej*, w: *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowski, Toruń 2008, s. 133–140.

[43] Szczegółowy wykaz aktów prawnych tworzonych w ramach III filaru, gdzie znajdują się postanowienia związane z ochroną danych osobowych, zob. Commission Staff Working Paper, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection

gwarantowanej ochrony, jak i możliwością realnego wpływu jednostek na sam proces przetwarzania dotyczących ich informacji. Ponadto różne poziomy ochrony danych osobowych oraz brak wspólnych zasad dostępu do informacji powoduje, że nawet minimalne standardy ochrony danych osobowych mogą nie być przestrzegane.

Dopiero 27 listopada 2008 r. przyjęto Decyzję ramową Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (dalej: Decyzja ramowa 2008/977/WSiSW)[44]. Ten akt prawny ma zapewnić wysoki poziom ochrony podstawowych praw i wolności osób fizycznych, a zwłaszcza ich prawa do prywatności, gdy przetwarzane są dane osobowe w ramach współpracy policyjnej i sądowej w sprawach karnych. Gwarantuje też wysoki poziom bezpieczeństwa publicznego (por. art. 1 ust. 1 Decyzji ramowej 2008/977/WSiSW).

Zgodnie z Decyzją ramową 2008/977/WSiSW państwa członkowskie UE chronią prawa podstawowe i wolności osób fizycznych, zwłaszcza ich prawo do prywatności, gdy w celu zapobiegania przestępstwom, wykrywania przestępstw, ich ścigania i karania oraz wykonywania sankcji karnych dane osobowe są przekazywane lub udostępniane:

- między państwami członkowskimi lub też zostały już przez nie sobie nawzajem przekazane lub udostępnione,
- przez państwa członkowskie organom lub systemom informacyjnym utworzonym na podstawie dawnego tytułu VI TUE lub też zostały już przez nie przekazane lub udostępnione,
- właściwym organom państw członkowskich przez organy lub systemy informacyjne utworzone na podstawie TUE lub dawnego TWE lub też zostały już przez nie przekazane lub udostępnione (por. art. 1 ust. 2).

Decyzja ramowa 2008/977/WSiSW ma zatem ograniczony zakres zastosowania, gdyż dotyczy tylko transgranicznego przetwarzania danych. Oznacza to, że przetwarzanie danych osobowych, które nie było przedmiotem wymiany informacji, nie jest obecnie objęte przepisami unijnymi dotyczącymi takiego przetwarzania i przestrzegania praw podstawowych w zakresie ochrony danych. W niektórych przypadkach stwarza to praktyczne utrudnienia dla policji i innych organów, dla których może nie być oczywiste, czy przetwarzanie danych będzie czysto krajowe, czy transgraniczne.

---

of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25.1.2012, SEC(2012) 72 final, annex 3.

[44] DzUrz. UE 2008 L 350/60. Decyzja ramowa 2008/977/WSiSW weszła w życie 19 stycznia 2009 r.

Decyzja ramowa 2008/977/WSiSW przyjmuje zasady legalności, proporcjonalności i celowości (por. art. 3). Reguluje także korygowanie i usuwanie danych oraz blokowanie do nich dostępu (por. art. 4–5). Dane wrażliwe, czyli takie dane osobowe, które ujawniają pochodzenie rasowe i etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe albo przynależność do związków zawodowych, oraz dane osobowe dotyczące stanu zdrowia i seksualności wolno przetwarzać tylko wtedy, gdy jest to bezwzględnie konieczne i gdy prawo krajowe przewiduje stosowne gwarancje (por. art. 6).

Decyzja ramowa 2008/977/WSiSW wprowadza wymagane mechanizmy ochronne oraz gwarantuje, że różnice w poziomie ochrony danych osobowych w poszczególnych państwach nie będą utrudniać wymiany istotnych informacji w oparciu o zasadę wzajemnego uznawania. Dlatego przyjęte w niej regulacje dotyczą ogólnych zasad zgodnego z prawem przetwarzania danych (takich jak przekazywanie i udostępnianie danych osobowych właściwym organom innych państw członkowskich oraz ich dalsze przetwarzanie), poufności i bezpieczeństwa w odniesieniu do przetwarzania, praw podmiotu danych osobowych, a także przysługujących mu środków prawnych. Decyzja ramowa 2008/977/WSiSW dopuszcza też transfer danych osobowych wyłącznie do tych krajów trzecich i organów międzynarodowych, które zapewniają odpowiedni poziom ochrony[45].

Decyzja ramowa 2008/977/WSiSW nawiązuje w swoich postanowieniach do Dyrektywy 95/46/WE, ale jednocześnie uwzględnia szczególne potrzeby w zakresie współpracy policyjnej i sądowej w sprawach karnych oraz w świetle zasady proporcjonalności. W wielu przypadkach ten akt prawny bezpośrednio odnosi się także do Konwencji nr 108, a Zalecenie nr R (87) 15 zostało wzięte pod uwagę w celu transponowania jego głównych zasad do wiążących prawnie przepisów na poziomie Unii[46].

---

[45] Zob. na temat Decyzji ramowej m.in. A. Lach, *Ochrona danych osobowych w ramach współpracy policyjnej i sądowej*, w: *Europejskie prawo karne*, red. A. Grzelak, M. Królikowski, A. Sakowicz, Warszawa 2012, s. 390–395; F. Boehm, *Information Sharing and Data Protection in Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Berlin 2012, s. 114 i n.; P. de Hert, C. Riehle, *Data Protection in the Area of Freedom Security and Justice. A Short Introduction and Many Questions Left Unanswered*, „ERA Forum" 2011, No. 11, s. 162 i n.; M. McGinley, *Data Protection Standard of the European Union: Rights vs. Effectiveness?*, w: *The Europeanization of Control. Venues and Outcomes of the EU Justice and Home Affairs Cooperation*, red. P. Bendel et al., Berlin 2011, s. 223 i n.

[46] Zalecenie postuluje przestrzeganie 8 zasad, które odnoszą się do gromadzenia, rejestrowania, wykorzystywania oraz dostępu i bezpieczeństwa danych. Państwa mogą rozszerzać zasady w nim zawarte na dane dotyczące ugrupowań, stowarzyszeń, fundacji, spółek, korporacji bądź jakichkolwiek innych organizacji grupujących – bezpośrednio lub pośrednio – osoby fizyczne, mające lub niemające osobowości prawnej.

3. Ochrona danych osobowych w prawie Unii Europejskiej po wejściu w życie Traktatu z Lizbony

Z mocy postanowień Traktatu z Lizbony dokonanych zostało wiele istotnych zmian zmierzających do zapewnienia skutecznej i spójnej ochrony praw podstawowych jednostki w UE. System filarowy UE został zastąpiony jednolitym reżimem prawnym UE jako organizacji międzynarodowej. Unia uzyskała osobowość prawną. Karcie Praw Podstawowych Unii Europejskiej[47] (dalej: KPP) przyznano charakter prawnie wiążący. Ponadto z mocy z art. 6 ust. 3 TUE wprowadzono podstawę prawną umożliwiającą przystąpienie UE do EKPCz[48]. Zmiany te wpływają m.in. na zwiększenie efektywności i legitymacji demokratycznej UE oraz na poprawę skuteczności jej działań.

Te zmiany miały także istotne znaczenie i wpływ na kwestie związane z ochroną danych osobowych w UE. Traktat z Lizbony wprowadził fundamentalne zmiany w systemie ochrony danych osobowych w UE[49]. Dzięki zniesieniu struktury trójfilarowej ustanowiono jedną wspólną podstawę dla ochrony danych osobowych. Standard ochrony danych osobowych wyznacza obecnie art. 16 TfUE stanowiący:

„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".

Artykuł 16 TfUE nie tylko ustanawia indywidualne prawo podmiotu danych do ochrony jego danych osobowych, ale także zobowiązuje PE i Radę do zapewnienia

---

[47] KPP została pierwotnie proklamowana w Nicei 7 grudnia 2000 r. wspólnie przez Komisję Europejską, Radę i Parlament Europejski oraz podpisana przez przedstawicieli tych instytucji. Początkowo nie miała jednak mocy prawnie wiążącej. Dopiero wejście w życie Traktatu z Lizbony spowodowało, że moc prawna KPP uległa zasadniczej zmianie i obecnie ma status prawa pierwotnego. Pierwotna wersja KPP została poddana redakcji i KPP została ponownie uchwalona przez Komisję Europejską, Radę i Parlament Europejski, tekst zob. DzUrz. UE 2012 C 326/391.

[48] Szeroko na temat akcesji UE do EKPCz zob. A. Gajda, *Przystąpienie Unii Europejskiej do Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności*, „Kwartalnik Kolegium Ekonomiczno-Społecznego Studia i Prace" 2013, nr 1 (13), s. 11–35.

[49] H. Hijmans, A. Scirocco, *Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?*, „Common Market Law Review" 2009, Vol. 46, s. 1514 i n.

ochrony danych osobowych we wszystkich obszarach działania UE. Artykuł ten jest głównym źródłem ochrony danych osobowych w UE[50]. Ma zasięg ogólny i zastosowanie do przetwarzania danych osobowych w sektorze prywatnym i publicznym, w tym w ramach współpracy policyjnej i sądowej w sprawach karnych oraz przez instytucje, organy i jednostki organizacyjne UE. Przestrzeganie zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu takich danych podlega kontroli niezależnego organu, jakim jest Europejski Inspektor Ochrony Danych Osobowych.

Artykuł 16 ust. 1 TfUE jest bezpośrednio skuteczny. Dzięki temu staje się podstawą uprawnień osób fizycznych w zakresie ochrony ich danych osobowych. Bezpośrednio skuteczna norma traktatowa chroni osoby fizyczne także w sytuacjach, kiedy nie mogą one korzystać z ochrony gwarantowanej przez akty prawa wtórnego. Ponadto z brzmienia art. 16 ust. 2 TfUE wyraźnie wynika, że zasady ochrony danych osobowych określone w treści aktów prawa wtórnego będą miały zastosowanie zarówno w odniesieniu do danych osób fizycznych przetwarzanych przez instytucje, organy i jednostki organizacyjne Unii, jak i danych osobowych przetwarzanych przez państwa członkowskie w takim zakresie, w jakim działania te będą służyć stosowaniu prawa Unii[51].

Pomimo kompleksowego charakteru art. 16 TfUE, który obejmuje całe prawo unijne, jeden ważny obszar jest wyłączony z jego zastosowania, tj. przetwarzanie danych osobowych w państwach członkowskich w sprawach należących do dawnego II filaru UE (WPZiB). Warto wskazać, że w treści art. 16 ust. 2 TFUE *in fine* przyjęto, że zasady przyjęte w art. 16 pozostają bez uszczerbku dla zasad szczególnych określonych w art. 39 TUE. Zgodnie z art. 39 TUE na zasadzie odstępstwa od art. 16 ust. 2 Rada może przyjąć decyzję określającą zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania WPZiB. Artykuł 39 TUE został skonstruowany jako odstępstwo od art. 16 ust. 2. Największą różnicą w porównaniu z art. 16 TfUE jest to, że PE jest wyłączony z procesu decyzyjnego w tym zakresie[52]. Czyli ochrona danych osobowych w ramach WPZiB odbywa się w oparciu o inną podstawę traktatową i na innych zasadach. To niewątpliwie stanowi o braku spójności systemowych w ramach prawa UE.

---

[50] H. Hijmans, *Recent Developments in Data Protection at European Union Level*, „ERA Forum" 2010, Vol. 11, s. 220.

[51] Zob. J. Sobczak, *Artykuł 8: komentarz*, w: *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2013, s. 296.

[52] Zob. też A. Scirocco, *The Lisbon Treaty and the Protection of Personal Data in the European Union*, „Dataprotectionreview.eu" 2008, No. 5.

W odniesieniu do zagadnień wchodzących w zakres dawnego III filaru UE konsekwencje wejście w życie Traktatu z Lizbony są także dość skomplikowane. Traktat z Lizbony wprawdzie położył kres istnieniu struktury trójfilarowej, ale nie spowodował, że Dyrektywa nr 95/46/WE będzie miała automatyczne zastosowanie do współpracy policyjnej i sądowej w sprawach karnych. W dalszym ciągu te dziedziny są wyłączone, zgodnie z art. 3 ust. 2 tej dyrektywy.

Należy także wskazać na dwie ważne deklaracje dołączone do Aktu końcowego Konferencji międzyrządowej, która przyjęła do TL. W Deklaracji nr 20[53] Konferencja oświadcza, że w każdym przypadku, w którym na podstawie art. 16 TfUE mają zostać przyjęte zasady dotyczące ochrony danych osobowych mogących mieć bezpośredni wpływ na bezpieczeństwo narodowe, powinno to być należycie wzięte pod uwagę. Jednocześnie wskazuje się na aktualnie obowiązujące prawodawstwo w tym zakresie, w szczególności na Dyrektywę nr 95/46/WE.

W Deklaracji nr 21[54] Konferencja wskazuje, że ze względu na szczególny charakter współpracy policyjnej i sądowej w sprawach karnych konieczne może się okazać wprowadzenie zasad szczególnych dotyczących ochrony danych osobowych, zapewnianej na podstawie art. 16 TfUE. Deklaracja ta wzywa zatem do przyjęcia specyficznych zasad w tym obszarze.

Warto przypomnieć, że deklaracje wprawdzie nie mają mocy prawnie wiążącej, ale mają dużą siłę polityczną i mogą mieć wpływ na interpretację postanowień traktatowych dotyczących ochrony danych osobowych i na dalszy rozwój instrumentów prawnych w tej dziedzinie.

Jak wskazano powyżej, KPP uzyskała z mocy Traktatu z Lizbony charakter prawnie wiążący. Nie jest wprawdzie częścią traktatów stanowiących podstawę Unii, ale art. 6 ust. 1 TUE wyraźnie stanowi, że KPP „ma taką samą moc prawną jak Traktaty"[55]. Postanowienia dotyczące ochrony danych osobowych zawarte są w art. 8 KPP Ochrona danych osobowych, który stanowi:

„1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.

2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.

3. Przestrzeganie tych zasad podlega kontroli niezależnego organu".

---

[53] Deklaracja nr 20 odnosząca się do art. 16 Traktatu o funkcjonowaniu Unii Europejskiej.

[54] Deklaracja nr 21 w sprawie ochrony danych osobowych w dziedzinie współpracy sądowej w sprawach karnych i współpracy policyjnej.

[55] F. Donati, *Article 8 – Protection of Personal Data*, w: *Human Rights in Europe. Commentary on the Charter of Fundamental Rights of the European Union*, red. W.B. Moch, Durham 2010, s. 53 i n.

Treść art. 8 KPP oparta jest – jak wynika z objaśnień Sekretariatu Konwencji redagującej KPP – na tekście art. 16 TFUE, Dyrektywie 95/46/WE, art. 8 EKPCz oraz Konwencji nr 108. Jednocześnie stwierdza się tam dość lakonicznie, że Dyrektywa 95/46/WE i Rozporządzenie (WE) 45/2001 „zawierają warunki i ograniczenia stosowane w wykonywaniu prawa do ochrony danych osobowych".

Prawo do ochrony danych osobowych jest także ściśle związane z prawem do poszanowania życia prywatnego ustanowionym w art. 7 KPP[56]. Dane osobowe są generalnie chronione w zakresie normy chroniącej życie prywatne i rodzinne. Zgodnie z orzecznictwem Trybunału Sprawiedliwości UE poszanowanie życia prywatnego w kontekście przetwarzania danych osobowych, uznane w art. 7 i 8 KPP, odnosi się do wszelkiej informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[57]. Związek między prywatnością a ochroną danych został również odzwierciedlony w motywach 10–12 oraz w art. 1 ust. 1 Dyrektywy 95/46/WE. Artykuł 7 KPP jest zasadniczo tożsamy z art. 8 EKPCz i dlatego musi być należycie wzięty pod uwagę przy dokonywaniu wykładni stosownych przepisów tej dyrektywy, która wymaga od państw członkowskich szczególnie prawa do prywatności[58].

KPP ma zastosowanie do instytucji, organów i jednostek organizacyjnych Unii (przy poszanowaniu zasady pomocniczości) oraz do państw członkowskich w takim zakresie, w jakim stosują one prawo Unii (por. art. 51 ust. 1). Dlatego ochrona danych osobowych jest uznawana za prawo podstawowe w całej Unii, niezależnie od istnienia dawnej struktury trójfilarowej UE. Potwierdził to TSUE w wyroku z dnia 29 stycznia 2008 r. w sprawie C-275/06 Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU[59].

Artykuł 8 KPP potwierdza szeroki zasięg tego prawa, które musi być przestrzegane we wszystkich obszarach działania UE i podlega kontroli niezależnych organów. TSUE w wyroku z 9 listopada 2010 r. w sprawach połączonych C-92/09 i C-93/09 V. i M. Schecke, H. Eifert przeciwko Land Hessen[60] uznał, że prawo do ochrony danych osobowych nie stanowi jednak prerogatywy o charakterze absolutnym i powinno być oceniane w świetle jego funkcji społecznej[61]. Artykuł 8 ust. 2 KPP zezwala tym

[56] Art. 7 KPP Poszanowanie życia prywatnego i rodzinnego stanowi: „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się".

[57] Zob. wyrok TSUE z 9 listopada 2010 r. w sprawach połączonych C-92/09 i C-93/09 V. i M. Schecke, H. Eifert przeciwko Land Hessen, Zb. Orz. 2010, s. I-11063, pkt 52.

[58] Zob. Opinia Rzecznika Generalnego N. Jääskinena przedstawiona w dniu 25 czerwca 2013 r. w sprawie C-131/12 Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mario Costeja González.

[59] Zb. Orz. 2008, s. I-00271, pkt 63.

[60] Zb. Orz. 2010, s. I-11063, pkt 48.

[61] Zob. podobnie wyrok TSUE z 12 czerwca 2003 r. w sprawie C-112/00 E. Schmidberger, Internationale Transporte und Planzüge przeciwko Republice Austrii, Zb. Orz. 2003, s. I-5659, pkt 80 i przytoczone

samym na przetwarzanie danych osobowych, jeżeli spełnione są określone warunki. W tym względzie postanowienie to przewiduje, że dane osobowe „muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą”[62].

Ponadto należy także pamiętać, że art. 52 ust. 1 KPP dopuszcza wprowadzenie ograniczeń w wykonywaniu praw takich jak prawa ustanowione w jej art. 7 i 8, o ile przewidziane są one ustawą, szanują istotę tych praw i wolności i z zastrzeżeniem zasady proporcjonalności są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

Z artykułu 52 ust. 3 KPP wynika, że w takim zakresie, w jakim zawiera ona prawa, które odpowiadają prawom zagwarantowanym w EKPCz, ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję. Artykuł 53 KPP dodaje w tym kontekście, że żadne z jej postanowień nie może być interpretowane jako ograniczające lub naruszające prawa uznane w szczególności w EKPCz. W związku z tym, że art. 8 EKPCz również obejmuje zagadnienia dotyczące ochrony danych osobowych, to zgodnie z art. 52 ust. 3 KPP orzecznictwo Europejskiego Trybunału Praw Człowieka (ETPC)[63] w przedmiocie art. 8 EKPCz ma znaczenie zarówno dla art. 7, jak i 8 KPP. W tych warunkach należy uznać, z jednej strony, że poszanowanie życia prywatnego w kontekście przetwarzania danych osobowych, uznane w art. 7 i 8 KPP, odnosi się do wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a z drugiej strony, że ograniczenia prawa do ochrony danych osobowych mogą być uzasadnione, jeżeli odpowiadają tym, które są tolerowane w ramach art. 8 EKPCz.

Warto także wskazać, że art. 8 KPP koresponduje z treścią art. 16 ust. 1 TfUE. Jednak żaden z tych artykułów nie definiuje pojęcia „dane osobowe”. Należy je zatem pojmować zgodnie z definicją zawartą w art. 2 lit. a Dyrektywy 95/46/WE. Dwa praktycznie identyczne przepisy – art. 16 ust. 1 TfUE i art. 8 KPP – znalazły się w dwóch różnych aktach prawa pierwotnego UE. Artykuł 16 ust. 1 TfUE stanowi jednak rozwinięcie i uzupełnienie art. 8 KPP.

---

tam orzecznictwo.

[62] Zob. też ciekawie G.G. Fuster, R. Gellert, *The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right*, „International Review of Law, Computers & Technology” 2012, Vol. 26, No. 1, s. 74 i n.

[63] Z art. 8 EKPCz orzecznictwo ETPC wyprowadza standard nie tylko ochrony tożsamości (imienia, nazwiska, tożsamości rodzinnej, płciowej, orientacji seksualnej), prywatności, lecz także potrzebę ochrony rozmaitych danych osobowych, zarówno o charakterze jawnym, jak i danych, których gromadzenie służy ochronie bezpieczeństwa państwa, wskazując na konieczność uregulowania zasad udostępniania tych danych podmiotom trzecim, zob. J. Sobczak, op.cit., s. 295.

4. Reforma przepisów o ochronie danych osobowych w Unii Europejskiej

4.1. Powody zmian w zakresie ochrony danych osobowych

Dyrektywa 95/46/WE stanowiła kamień milowy w dziejach ochrony danych osobowych w UE. Jej postanowienia służą urzeczywistnianiu dwu bardzo istotnych celów. Po pierwsze, gwarantują ochronę praw podstawowych jednostki, w szczególności podstawowego prawa do ochrony danych osobowych. Po drugie, realizują założenia rynku wewnętrznego – w tym przypadku swobodnego przepływu danych osobowych pomiędzy państwami członkowskimi UE. Te cele w dalszym ciągu są aktualne, podobnie jak zasady zawarte w tym akcie prawnym.

Jednak od przyjęcia Dyrektywy 95/46/WE minęło już 18 lat. Następujący w tym czasie szybki rozwój technologiczny i globalizacja doprowadziły do głębokich przemian w otaczającym nas świecie. Przyniosło to nowe wyzwania dla skutecznej ochrony danych osobowych. Dzisiejsze technologie umożliwiają jednostkom łatwe dzielenie się informacjami na temat ich zachowania i preferencji oraz publiczne udostępnianie tych informacji w skali globalnej. Sieci społecznościowe z setkami milionów użytkowników rozsianych po całym świecie stanowią chyba najbardziej ewidentny, choć nie jedyny przykład tego zjawiska. Również tzw. przetwarzanie w chmurze[64] stanowi duże wyzwanie dla ochrony danych osobowych. Wiąże się to bowiem z utratą przez jednostkę kontroli nad poufnymi informacjami w sytuacji, w której przechowują one te dane, korzystając z programów zainstalowanych na urządzeniach osób trzecich.

Ponadto metody gromadzenia danych osobowych stały się coraz bardziej wyrafinowane i trudniej wykrywalne. Użycie zaawansowanych narzędzi umożliwia podmiotom gospodarczym skuteczniejsze dobranie strategii przyjmowanej wobec poszczególnych jednostek poprzez monitorowanie ich zachowania w sieci. Także organy publiczne wykorzystują coraz większą ilość danych osobowych do różnych celów (np. ustalenie miejsca pobytu osoby fizycznej w przypadku epidemii choroby zakaźnej, zapobieganie terroryzmowi i przestępczości, zarządzanie systemami zabezpieczenia społecznego).

---

[64] Ang. *cloud computing* oznacza przetwarzanie dokonywane w internecie za pomocą oprogramowania, dzielonych zasobów i informacji znajdujących się na zewnętrznych serwerach („w chmurze"). Szeroko na ten temat zob. *Internet. Cloud Computing. Przetwarzanie w chmurach*, red. G. Szpor, Warszawa 2013 oraz B.J.A. Schellekens, *The European Data Protection Reform in the Light of Cloud Computing*, Tilburg 2012 [materiał w posiadaniu autorki].

Należy zdawać sobie sprawę, że próby rozwiązywania problemów z zakresu ochrony danych osobowych w sieci jedynie na płaszczyźnie technicznej lub wyłącznie w zakresie regulacji normatywnej nie przynoszą oczekiwanych rezultatów. Tylko ścisłe współdziałanie w tych dziedzinach może pozwolić na wypracowanie skutecznych mechanizmów ochrony danych osobowych w globalnej sieci[65]. Rodzi się pytanie, czy obowiązujące obecnie unijne przepisy w zakresie ochrony danych osobowych mogą w dalszym ciągu stanowić pełną i skuteczną odpowiedź na te wyzwania? Dlatego Komisja Europejska zainicjowała przegląd obowiązujących ram prawnych w UE, rozpoczynając od konferencji na wysokim szczeblu w maju 2009 r., po której nastąpiły konsultacje publiczne prowadzone do końca 2009 r.[66] W związku z tym przygotowano również szereg analiz[67].

Dokonane w nich ustalenia pokazały, że podstawowe zasady zawarte w Dyrektywie 95/46/WE są nadal aktualne i że ta technologiczna neutralność powinna być zachowana. Równocześnie jednak zidentyfikowano szereg kwestii wiążących się z konkretnymi wyzwaniami. Wszystkie one zostały zawarte w komunikacie KE z 4 listopada 2010 r. Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej[68]. Wyzwania te w ocenie KE obejmują:

- reakcję na oddziaływanie nowych technologii,
- poprawę sytuacji w zakresie aspektów ochrony danych związanych z rynkiem wewnętrznym,
- reakcję na globalizację oraz poprawę międzynarodowego przekazywania danych,
- zapewnienie lepszych rozwiązań instytucjonalnych w celu skutecznego egzekwowania przepisów o ochronie danych,
- zwiększenie spójności ram prawnych w zakresie ochrony danych.

---

[65] K. Celarek, *Prawo informatyczne a ochrona danych osobowych – szczególna rola administracji w procesie rozwoju społeczeństwa zinformatyzowanego*, w: *Jakość wobec wyzwań i zagrożeń XXI wieku*, red. N. Majchrzak, A. Zduniak, Poznań 2010, s. 227.

[66] Zob. odpowiedzi na konsultacje publiczne KE dostępne na stronie internetowej: http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm. Zob. też: European Commission, *Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data*, Brussels, 4 November 2010.

[67] Zob. np. analizę dotycząca korzyści gospodarczych związanych z technologiami służącymi wzmocnieniu ochrony prywatności, *Study on the economic benefits of privacy enhancing technologies*, London Economic, July 2010, dostępną na stronie internetowej: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf oraz analizę porównawczą różnych strategii w zakresie nowych wyzwań w ochronie prywatności, w szczególności w świetle postępu technologicznego, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*, 20.01.2010, dostępną na stronie internetowej: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

[68] KOM(2010) 609 wersja ostateczna.

Zasadnicze cele nowego, całościowego podejścia do ochrony danych osobowych w UE obejmują przede wszystkim: wzmocnienie praw osób fizycznych[69], poprawę wymiaru związanego z rynkiem wewnętrznym[70], zmianę przepisów o ochronie danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych, globalny wymiar ochrony danych[71] oraz zapewnienie lepszych rozwiązań instytucjonalnych w celu skuteczniejszego egzekwowania przepisów o ochronie danych osobowych.

Jednocześnie Komisja Europejska w swoim komunikacie zobowiązała się do przygotowania i przedstawienia w 2011 r. nowych przepisów zmierzających do zmiany istniejących ram prawnych w zakresie ochrony danych osobowych. Miałyby one również zapewnić skuteczniejszą ochronę danych osób fizycznych w ramach wszystkich polityk UE, w tym egzekwowania prawa i zapobiegania przestępczości. Równocześnie Komisja Europejska zapewniła o dalszych działaniach o charakterze nielegislacyjnym, takich jak zachęcanie do samoregulacji oraz badanie możliwości wprowadzenia unijnych certyfikatów prywatności. W dalszej kolejności Komisja Europejska będzie także oceniać, czy konieczne jest dostosowanie innych instrumentów prawnych dotyczących ochrony danych osobowych do nowych, ogólnych ram prawnych. Dotyczyć to ma w pierwszej kolejności Rozporządzenia (WE) 45/2001, a na dalszym etapie także innych instrumentów prawnych o charakterze sektorowym.

Między wrześniem a grudniem 2011 r. Komisja Europejska prowadziła rozszerzony dialog z działającymi w UE krajowymi organami ochrony danych i z Europejskim Inspektorem Ochrony Danych Osobowych. Celem tych rozmów było przeanalizowanie możliwości wprowadzenia bardziej spójnej regulacji dotyczącej ochrony danych osobowych w UE. Rozmowy te pokazały, że zarówno obywatele Unii, jak i przedsiębiorcy chcą, by Komisja Europejska w sposób kompleksowy zreformowała unijne przepisy o ochronie danych osobowych[72].

---

[69] Chodzi przede wszystkim o zagwarantowanie odpowiedniej ochrony we wszystkich okolicznościach, zwiększenie przejrzystości wobec osób, których dane dotyczą, poprawę kontroli nad własnymi danymi, pogłębienie świadomości społeczeństwa, zapewnienie świadomej i dobrowolnej zgody, ochronę danych szczególnie chronionych oraz zapewnienie większej skuteczności sankcji i środków zaradczych.

[70] Wiąże się to m.in. ze zwiększeniem pewności prawnej oraz zapewnieniem równych szans administratorom danych, zmniejszeniem obciążeń administracyjnych oraz wzmocnieniem odpowiedzialności administratorów danych.

[71] Ten aspekt dotyczy uproszczenia przepisów odnoszących się do międzynarodowych transferów danych oraz propagowania uniwersalnych zasad ochrony osób fizycznych w zakresie przetwarzania danych osobowych.

[72] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku, KOM(2012) 9 wersja ostateczna, Bruksela, 25 stycznia 2012 r.

Dnia 25 stycznia 2012 r. Komisja Europejska przedstawiła długo oczekiwaną propozycję zmiany unijnego prawa dotyczącego ochrony danych osobowych, obejmującą przetwarzanie danych w sektorze prywatnym i przez podmioty publiczne w związku z egzekwowaniem prawa. Komisja Europejska zaproponowała, by nowe ramy prawne obejmowały:

1) rozporządzenie (zastępujące Dyrektywę 95/46/WE) ustanawiające ogólne unijne przepisy w zakresie ochrony danych osobowych (dalej: Projekt rozporządzenia)[73],
2) dyrektywę (zastępującą Decyzje ramową 2008/977/WSiSW) określającą przepisy o ochronie danych osobowych przetwarzanych do celów zapobiegania przestępstwom, wykrywania ich, prowadzenia dochodzeń w ich sprawie i ścigania ich oraz powiązanych działań sądowych (dalej: Projekt dyrektywy)[74].

Podstawę prawną przyjęcia obu projektów stanowi art. 16 ust. 2 TfUE. Projekty Komisji Europejskiej zmierzają do aktualizacji i unowocześnienia zasad zawartych w Dyrektywie 95/46/WE. W sposób szczególny mają one na celu zwiększenie praw osób fizycznych, wzmocnienie rynku wewnętrznego UE, zapewnienie wysokiego poziomu ochrony danych we wszystkich obszarach, w tym w ramach współpracy policyjnej i sądowej w sprawach karnych, zapewnienie właściwego egzekwowania przepisów oraz wprowadzenie ogólnoświatowych norm ochrony danych osobowych.

Przedstawione propozycje mają także zagwarantować obywatelom Unii poszanowanie prywatności, o które coraz trudniej w cyfrowym świecie. Służą również umożliwieniu każdej osobie większej kontroli nad jej danymi osobowymi, ułatwiają dostęp i zwiększają jakość otrzymywanych informacji na temat tego, co dzieje się z danymi danej osoby po podjęciu przez nią decyzji o ich udostępnieniu. Celem zmian jest więc zapewnienie ochrony danych osobowych – niezależnie od miejsca ich przesyłania lub przechowywania – nawet poza UE (często może to mieć miejsce w internecie).

[73] Zob. Wniosek rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), KOM(2012) 11 wersja ostateczna, Bruksela, 25 stycznia 2012 r.

[74] Wniosek dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, KOM(2012) 10 wersja ostateczna, Bruksela, 25 stycznia 2012 r.

4.2. Projekt rozporządzenia – najważniejsze założenia i nowe propozycje[75]

Projekt rozporządzenia stawia sobie dwa cele. Po pierwsze, poprawę wymiaru rynku wewnętrznego oraz ułatwienie swobodnego przepływu danych osobowych. Po drugie, zagwarantowanie poszanowania podstawowego prawa do ochrony danych osobowych na terytorium UE[76]. Ten nowy akt prawny zastąpiłby Dyrektywę 95/46/WE i obowiązywałby bezpośrednio w państwach członkowskich UE bez potrzeby implementacji jego postanowień do wewnętrznych porządków prawnych tych państw. W efekcie nastąpiłaby pełna harmonizacja prawa materialnego w ramach UE i swobodnego przepływu danych osobowych.

Projekt rozporządzenia składa się z 91 artykułów i jest podzielony na 11 rozdziałów[77]. Wśród najistotniejszych zmian zaproponowanych w Projekcie rozporządzenia znalazły się te, które bardzo mocno wzmacniają prawa podmiotu danych[78]:

- redefiniowanie zgody podmiotu danych na przetwarzanie danych osobowych jako świadomego i wyraźnego oświadczenia woli złożonego w jakiejkolwiek formie, a zatem całkowita rezygnacja z wymogu formy pisemnej (por. art. 1 pkt 8);
- precyzyjniejsze określenie podstawy do przetwarzania danych (por. art. 6);
- wyłączenie zgody podmiotu danych jako podstawy prawnej przetwarzania w sytuacji poważnej nierówności między podmiotem danych a administratorem (np. w stosunkach pomiędzy pracodawca i pracownikiem, por. art. 7 ust. 4);
- uregulowanie przetwarzania danych osobowych dzieci w wieku poniżej lat 13 (por. art. 8);

---

[75] Autorka nie analizuje szczegółowo wszystkich postanowień Projektu rozporządzenia. Podstawowym celem jest ukazanie najważniejszych zmian, które ten akt proponuje.

[76] Zob. też ciekawie K. Irion, G. Luchetta, *Online Personal Data Processing and EU data Protection Reform. Report of the CEPS Digital Forum*, April 2013, s. 63 i n., www.ceps.eu

[77] Rozdział I – Przepisy ogólne; rozdział II – Zasady; rozdział III – Prawa podmiotu danych; rozdział IV – Administrator i podmiot przetwarzający; rozdział V – Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych; rozdział VI – Niezależne organy nadzorcze; rozdział VII – Współpraca i zgodność; rozdział VIII – Środki ochrony prawnej, odpowiedzialność i sankcje; rozdział IX – Przepisy dotyczące szczególnych sytuacji przetwarzania danych; rozdział X – Akty delegowane i akty wykonawcze; rozdział XI – Przepisy końcowe.

[78] Zgodnie z art. 4 pkt 1 Projektu rozporządzenia „podmiot danych oznacza zidentyfikowaną osobę fizyczną lub osobę fizyczną, którą można zidentyfikować, bezpośrednio lub pośrednio, za pomocą wszelkich środków, które z rozsądnym prawdopodobieństwem mogą być użyte przez administratora lub inną osobę fizyczną bądź prawną, szczególnie przez odniesienie do numeru identyfikacyjnego, danych dotyczących lokalizacji, identyfikatora online lub przynajmniej jednego czynnika charakterystycznego dla fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby".

- zdefiniowanie „danych genetycznych”[79] i włączenie ich do katalogu tzw. danych wrażliwych o szczególnym reżimie przetwarzania (por. art. 9 ust. 1);
- wprowadzenie bądź zmiana na korzyść podmiotu danych uprawnienia do dostępu do swoich danych, ich poprawiania, usuwania i przenoszenia oraz prawa do wniesienia sprzeciwu (por. art. 15, 16, 18 i 19);
- uregulowanie „prawa do bycia zapomnianym” (prawa żądania usunięcia danych przez administratora), z zastrzeżeniem kompetencji Komisji Europejskiej do doprecyzowania zakresu i technicznych aspektów usuwania (por. art. 17);
- uregulowanie stosowania tzw. środków opartych na profilowaniu, tj. środków wywołujących skutki prawne względem osoby fizycznej lub istotnie wpływających na tę osobę, a opartych wyłącznie na automatycznym przetwarzaniu danych mających służyć ocenie niektórych aspektów osobistych tej osoby fizycznej lub też analizie bądź przewidzeniu zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności lub zachowania tej osoby fizycznej (por. art. 20).

W Projekcie rozporządzenia zawarto także rozwiązania, które nakładają dodatkowe obowiązki na administratorów danych[80] oraz zmierzają do ułatwienia im wykonywania obowiązków. Do najważniejszych propozycji dotyczących administratorów należą:

- usankcjonowanie instytucji współadministratorów (por. art. 24);
- nałożenie obowiązków podawania przejrzystych oraz łatwo dostępnych i zrozumiałych informacji oraz zapewnienia procedur i mechanizmów ułatwiających podmiotowi danych wykonywanie przysługujących mu praw (por. art. 11–12);
- wprowadzenie obowiązku zgłoszenia faktu naruszenia ochrony danych osobowych organowi nadzorczemu (por. art. 31);
- wprowadzenie obowiązku powiadomienia podmiotu danych o naruszeniu ochrony jego danych osobowych (por. art. 32);
- wprowadzenie obowiązku przeprowadzenia oceny skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych, jeżeli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych

[79] „Dane genetyczne oznaczają wszelkie dane dowolnego rodzaju dotyczące charakterystycznych cech osoby fizycznej, odziedziczonych lub nabytych na etapie wczesnego rozwoju prenatalnego”, por. art. 4 pkt 10 Projektu rozporządzenia.

[80] Przez administratora danych w rozumieniu Projektu rozporządzenia rozumie się „osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który samodzielnie lub wspólnie z innymi organami ustala cele, warunki i sposoby przetwarzania danych osobowych; w przypadkach, w których cele, warunki i sposoby ustalane są prawem Unii lub państwa członkowskiego, administrator lub szczególne kryteria jego wyznaczania mogą zostać określone w prawie Unii lub państwa członkowskiego”, por. art. 4 pkt 5.

z racji swego charakteru, zakresu lub celów, a w razie stwierdzenia wysokiego ryzyka – skonsultowanie i uzgodnienie z organem nadzoru wyboru i zastosowania środków służących złagodzeniu tego ryzyka (por. art. 33–34);
- administratorzy, zatrudniający więcej niż 250 osób lub będący podmiotem publicznym, przy czym ich główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych, będą mieli obowiązek wyznaczenia w przedsiębiorstwie inspektora ochrony danych (por. art. 35);
- przyjęto zasadę „punktu kompleksowej obsługi" – gdy administrator lub podmiot przetwarzający ustanowieni są na terytorium UE i prowadzą działalność w więcej niż jednym państwie członkowskim, to organ nadzorczy miejsca ich głównej siedziby jest odpowiedzialny za nadzór nad ich działalnością we wszystkich państwach członkowskich (por. art. 51 ust. 2).

Projekt rozporządzenia wprowadza także nowe, szczegółowe regulacje w zakresie przetwarzania danych dotyczących zdrowia, w kontekście zatrudnienia oraz do celów dokumentacji, statystyki i badań naukowych (por. art. 81–83). Na nowo skonstruowano zasady przekazywania danych osobowych do krajów trzecich, z aktywną rolą Komisji Europejskiej, która wydawać ma decyzje dotyczące spełniania przez państwa trzecie odpowiedniego poziomu ochrony, publikowane w Dzienniku Urzędowym Unii Europejskiej i uprawniające do przekazania danych do tych państw bez osobnego zezwolenia (por. art. 41).

Projekt rozporządzenia zobowiązuje państwa członkowskie do ustanowienia organów nadzorczych, rozszerzając zakres powierzonych im zadań o wzajemną współpracę i współpracę z Komisją Europejską oraz określa warunki ich niezależności (por. rozdział VI). Ustanawia też niezależne ciało w postaci Europejskiej Rady Ochrony Danych, w której skład wchodzą szefowie organów nadzorczych wszystkich państw członkowskich oraz Europejski Inspektor Ochrony Danych. Europejska Rada Ochrony Danych zastępuje Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych powołaną na mocy art. 29 Dyrektywy 95/46/WE (por. rozdział VII).

Powagę zagadnień ochrony danych osobowych niewątpliwie wzmocnić mają także bardzo wysokie kary administracyjne przewidziane w projekcie jako sankcje z tytułu naruszeń zasad ochrony danych osobowych. Górna wysokość kar – za najcięższe co do gatunku naruszenia – sięga 1 mln euro lub w przypadku przedsiębiorstwa 2% jego rocznego światowego obrotu (por. art. 79).

Prace nad ostatecznym kształtem Projektu rozporządzenia trwają. Trudno przewidzieć, kiedy się zakończą. Komisarz UE ds. sprawiedliwości, praw podstawowych i obywatelstwa V. Reding zaapelowała o przyspieszenie prac nad tym projektem.

Chciałaby, aby na październikowym szczycie UE, poświęconym m.in. Europejskiej Agendzie Cyfrowej, szefowie rządów i państw zadeklarowali przyspieszenie prac nad projektem rozporządzenia dotyczącego ochrony danych osobowych, tak aby zakończyły się one przed wyborami do Parlamentu Europejskiego w maju 2014 r.[81]

Obecnie Projekt rozporządzenia znajduje się w Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego. Posłowie spierają się o kompromisowe poprawki dotyczące m.in. profilowania danych osobowych, ich definiowania, a także definicji zgody. Do głosowania, które pierwotnie zostało zaplanowane na czerwiec 2014 r., dojdzie najprawdopodobniej dopiero w październiku br.

Równolegle trwają prace nad reformą w Radzie Unii Europejskiej. Zakończona w czerwcu prezydencja irlandzka poświęciła bardzo dużo uwagi ochronie danych i znacznie przyspieszyła ten proces. Podkreślały to wszystkie delegacje na czerwcowym posiedzeniu Rady Unii Europejskiej ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych[82].

4.3. Projekt dyrektywy – najważniejsze założenia i nowe propozycje

Celem Projektu dyrektywy jest stworzenie spójnych ram ochrony danych osobowych przetwarzanych w państwach członkowskich UE w ramach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, zagwarantowanie wysokiego poziomu ochrony takich danych oraz ułatwienie wymiany danych osobowych między państwami członkowskimi UE[83]. Ten nowy akt prawny ma zastąpić Decyzję ramową 2008/977/WSiSW. Zakres zastosowania tej decyzji ramowej jest bowiem ograniczony tylko do transgranicznego przetwarzania danych. Natomiast rozwiązania zawarte w Projekcie dyrektywy mają jednolicie odnosić się zarówno do transgranicznego, jak i wewnątrzkrajowego przetwarzania danych (por. art. 2). Ma to służyć osiągnięciu spójnego i wysokiego poziomu ochrony danych osobowych we wszystkich państwach członkowskich, dzięki czemu organy tych państw – przekonane, że w innym państwie członkowskim poziom ochrony danych jest równie wysoki – będą bardziej niż dzisiaj skłonne przekazywać dane za granicę.

---

[81] Podaję za: *Reding chce przyspieszenia prac nad ochroną danych osobowych w UE*, www.euractiv.pl, dostęp 17.07.2013.

[82] Zob. Council of the European Union, Press Release 3244th Council Meeting Justice and Home Affairs, Luxembourg, 6–7 June 2013, doc. 10461/13.

[83] Zob. szeroko na temat Projektu dyrektywy: A. Grzelak, op.cit., s. 20 i n.

Projekt dyrektywy składa się z 64 artykułów i jest podzielony na 10 rozdziałów[84]. Do najważniejszych zmian w tej propozycji należy:

- określenie ogólnych zasad dotyczących przetwarzania danych osobowych, w tym podkreślenie znaczenie zasady minimalizmu (por. art. 4);
- zróżnicowanie poszczególnych kategorii osób, których dotyczą przetwarzane dane osobowe (wprowadza się kategorie: podejrzany, skazany, ofiara, świadek, osoba, która nie należy do żadnej z wyżej wymienionych kategorii, por. art. 5), co jest potrzebne z jednej strony dla ochrony tych osób, z drugiej zaś – dla pełnego wykorzystania tych danych[85];
- rozróżnienie między danymi osobowymi opartymi na faktach i ocenach oraz według stopnia ich dokładności i wiarygodności (por. art. 6);
- przetwarzanie danych genetycznych i biometrycznych (por. art. 8);
- wprowadzenie jednolitego systemu oceny, czy państwo trzecie lub instytucja międzynarodowa, którym mają być przekazane dane osobowe, zapewniają odpowiedni poziom ochrony tych danych (por. art. 33–38);
- poddanie przetwarzania danych osobowych w omawianych dziedzinach kontroli organu nadzorczego (por. art. 39–49).

Projekt dyrektywy przewiduje rozwiązania będące krokiem naprzód w porównaniu z regulacjami zawartymi w Decyzji ramowej 2008/977/WSiSW. Należy jednak pamiętać, że ten projektowany akt prawny nie stworzy jednolitych ram ochrony danych osobowych w dziedzinie współpracy policyjnej i sądowej w sprawach karnych. Projekt dyrektywy nie narusza bowiem wcześniej przyjętych szczególnych aktów prawnych w tej dziedzinie. Jedną z podstawowych wątpliwości w kontekście Projektu dyrektywy jest pytanie o to, w jakim stopniu projekt ten stanie się standardem, jeśli chodzi o ochronę danych w dziedzinie współpracy policyjnej i sądowej, i jaka będzie jego relacja względem istniejących licznych szczególnych instrumentów prawnych.

Projekt dyrektywy będzie przedmiotem jeszcze długotrwałych prac. Należy więc mieć świadomość, że ostateczny kształt dyrektywy może odbiegać nawet dość znacząco od pierwotnego tekstu przedłożonego przez Komisję Europejską.

---

[84] Rozdział I – Przepisy ogólne; rozdział II – Zasady; rozdział III – Prawa podmiotu danych; rozdział IV – Administrator i podmiot przetwarzający; rozdział V – Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych; rozdział VI – Niezależne organy nadzorcze; rozdział VII – Współpraca; rozdział VIII – Środki ochrony prawnej, odpowiedzialność i sankcje; rozdział IX – Akty delegowane i wykonawcze; rozdział X – Postanowienia końcowe.

[85] Jest to nowy przepis, którego nie ma w Dyrektywie 95/46/WE, ani w Decyzji ramowej 2008/977/WSiSW. Inspirację dla niego stanowi Zalecenie nr R (87) 1. Podobne przepisy istnieją już w odniesieniu do Europolu (por. art. 14 Decyzji o ustanowieniu Europolu 2009/371/WSiSW) oraz Eurojustu (por. art. 15 Decyzji ustanawiającej Eurojust 2009/426/WSiSW).

Wnioski

Problem danych osobowych w Unii Europejskiej ma charakter fundamentalny, przede wszystkim z uwagi na „wrażliwość" tych informacji oraz poważne konsekwencje związane z ewentualnym przejęciem ich przez osoby niepożądane. Ochrona danych osobowych jest postrzegana w UE jako podstawowe prawo jednostki (por. art. 8 KPP). Aby skutecznie zagwarantować to prawo, potrzebne są jasne i konsekwentne przepisy w zakresie ochrony danych osobowych.

Unia Europejska przywiązuje dużą wagę do należytej ochrony danych osobowych. Jednak obowiązujący stan prawny w omawianej dziedzinie jest skomplikowany i po części stanowi rezultat dotychczasowej trójfilarowej struktury UE, istniejącej do wejścia w życie Traktatu z Lizbony. Przetwarzanie danych osobowych w dawnym I filarze UE zasadniczo objęło czynności dokonywane przez jednostki prywatne w ramach prowadzonej przez nie działalności. Podstawowym – ale nie jedynym – aktem prawnym, na mocy którego państwa członkowskie zobowiązały się chronić podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do prywatności, jest cały czas obowiązująca Dyrektywa 95/46/WE.

Celem Dyrektywy 95/46/WE jest zapewnienie równorzędnego poziomu ochrony danych osobowych w całej UE. Jednak w przepisach obowiązujących w państwach członkowskich UE nadal istnieją duże rozbieżności w tej dziedzinie. Biorąc pod uwagę brak harmonizacji krajowych przepisów dotyczących ochrony danych osobowych i różne uprawnienia krajowych organów ds. ochrony danych, osobom fizycznym w niektórych państwach członkowskich trudniej jest egzekwować swoje prawa niż w innych, zwłaszcza w kontekście usług internetowych.

W ramach dawnego III filaru UE nie było podstawy prawnej, która umożliwiałaby przyjęcie stosownych przepisów ogólnych w zakresie ochrony danych osobowych. Przyjmowane akty prawne miały wyłącznie charakter szczególny i dotyczyły jednej instytucji albo wybranych form przetwarzania danych, zwłaszcza transgranicznego przepływu danych. Przyjęta w 2008 r. Decyzja ramowa 2008/977/WSiSW ma ograniczony zakres przedmiotowy zastosowania i posiada różne luki, co powoduje poczucie niepewności prawnej u osób fizycznych i organów egzekwujących prawo oraz prowadzi do praktycznych trudności w jej prawidłowym wdrażaniu. Ponadto ten akt prawny przewiduje szereg możliwości odstąpienia od ogólnych zasad ochrony danych osobowych na szczeblu krajowym, co niewątpliwie nie prowadzi do ich ujednolicenia.

Wejście w życie Traktatu z Lizbony i wprowadzenie nowej podstawy prawnej (por. art. 16 TfUE) umożliwia ustanowienie kompleksowych ram ochrony danych

osobowych w UE. W aktualnym stanie prawnym możliwe jest bowiem objęcie zrewidowanymi unijnymi ramami ochrony danych zarówno transgranicznego, jak i krajowego przetwarzania danych osobowych. To z pewnością przyczyniłoby się do ograniczenia różnic między systemami prawnymi w państwach członkowskich i przyniosłoby ogólne korzyści w zakresie ochrony danych osobowych. Mogłoby też przyczynić się do sprawniejszej wymiany informacji między organami policyjnymi i sądowymi państw członkowskich UE, a przez to poprawić współpracę w zakresie zwalczania przestępczości w Europie.

Szybki rozwój technologiczny przyniósł nowe wyzwania w zakresie ochrony danych osobowych. Niezwykle wzrosła też skala wymiany i zbierania danych osobowych. Nowe technologie umożliwiają zarówno przedsiębiorstwom prywatnym, jak i organom publicznym wykorzystywanie danych osobowych do wykonywania powierzonych im zadań na niespotykaną dotąd skalę. Osoby fizyczne coraz częściej udostępniają dane osobowe publicznie i globalnie. Te technologie całkowicie zmieniły gospodarkę i życie społeczne.

Dlatego nadszedł czas, by stworzyć silniejsze i bardziej spójne ramy ochrony danych osobowych w UE. Komisja Europejska w styczniu 2012 r. zaproponowała Projekt rozporządzenia i Projekt dyrektywy. Podstawowym celem tych nowych aktów prawnych jest wzmocnienie praw, zapewnienie osobom fizycznym skutecznych środków gwarantujących, że będą one w pełni informowane o tym, co dzieje się z ich danymi osobowymi i umożliwiających im skuteczniejsze korzystanie z przysługujących im praw.

Reforma zasad ochrony danych jest absolutnie konieczna. Aktualnie obowiązujące przepisy o ochronie danych zostały uchwalone 18 lat temu i nie przystają już do rzeczywistości społeczeństwa informacyjnego. Nie ma wątpliwości co do tego, że obecny system ochrony danych osobowych jest rozdrobniony, nieskuteczny i przestarzały. W tym kontekście kierunek zmian zaproponowany przez Komisję Europejską należy ocenić bardzo pozytywnie. Szczególnie istotne, z punktu widzenia praw i interesów jednostek, są te propozycje, które zmierzają do zaostrzenia wymogów dotyczących zgody na przetwarzanie danych osobowych, zmiany zasad stosowania prawa UE w stosunku do krajów trzecich, uregulowanie problematyki charakterystycznej dla usług internetowych (profilowania, „prawa do bycia zapomnianym", możliwości przenoszenia danych między serwisami) oraz zwiększenie roli organów ochrony danych osobowych, w tym nadanie im wyraźnego uprawnienia do stosowania sankcji administracyjnych[86].

[86] Zob. Fundacja Panoptykon, *Wielka reforma danych osobowych. Dlaczego jest ważna i co w tym pakiecie warto jeszcze poprawić*, www.panoptykon.org

Jednocześnie w zaproponowanych przez Komisję Europejską projektach pojawiają się liczne wyłączenia, luki prawne i problemy definicyjne, które będą musiały być uwzględnione w dalszym procesie zmierzającym do ich przyjęcia. Poważne wątpliwości dotyczą m.in. anonimizacji danych i jej ograniczeń, definicji profilowania, nierozwiązanego problemu wykorzystywania danych osobowych zbieranych (pierwotnie) w celach komercyjnych oraz dla celów bezpieczeństwa publicznego, a także szerokie uprawnienia Komisji Europejskiej do wydawania aktów quasi-legislacyjnych.

Personal data protection law and its reform in the EU

The paper concentrates on the protection of personal data in the European Union. The paper presents a comprehensive reform of the data protection framework, proposed by the European Commission in January 2012, including a policy Communication setting out the Commission's objectives and two legislative proposals: a regulation setting out a general EU framework for data protection and a directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. Both proposals concern the question of ensuring effective protection of fundamental rights. The analysis of the proposed legislation shows nevertheless that in this shape they do not lead to consistency and uniformity of the entire system of personal data protection in the EU. Significant differences in both proposals concern including different subject matter and material scope, effective protection of fundamental rights and the establishment of the hierarchy of the existing legal acts in this area.

Keywords: European Union, personal data, protection, fundamental rights, reform of the data protection legal framework, proposal for a regulation, proposal for a directive

La loi sur la protection des données personnelles et sa réforme dans l'UE

L'article se concentre sur la protection des données personnelles dans l'Union européenne. La législation actuelle et les objectifs de la réforme dans ce domaine proposée par la Commission européenne en janvier 2012 sont discutés. Il y a deux propositions législatives: la première proposition établit un cadre général de l'UE pour la protection des données et la seconde proposition est une directive sur la protection des données à caractère personnel traitées à des fins de prévention,

de détection, d'enquête ou de poursuite des infractions pénales et des activités judiciaires connexes. Les deux propositions se réfèrent à la question de savoir d'assurer la protection effective des droits fondamentaux. L'analyse de ces propositions législatives montre que, dans cette forme, elles ne conduisent pas à la cohérence et l'uniformité de l'ensemble du système de protection des données personnelles dans l'UE. Des différences significatives dans les deux projets compennent entre autres: les solutions et les conséquences juridiques.

Mots-clés: l'Union européenne, les données personnelles, la protection, les droits fondamentaux, la réforme du cadre juridique de la protection des données, la proposition de règlement, la proposition de directive

Система защиты персональных данных в Европейском союзе и ее реформа

Предметом данного исследования является защита персональных данных в Европейском союзе. В статье представлена, предложенная Европейской комиссией в январе 2012 года, комплексная реформа системы защиты персональных данных, включая изложение целей Комиссии и два законодательных акта: постановление об общих рамках защиты персональных данных в ЕС и директиву о защите персональных данных при обработке в целях профилактики, выявления, расследования или судебного преследования уголовных преступлений и связанных с ними судебных мероприятий. Оба предложения относятся к вопросу обеспечения эффективной защиты основных прав. Однако, анализ предлагаемых законопроектов показывает, что в этом виде они не приводят к однородности и целостности всей системы защиты персональных данных в ЕС. Значительные различия в обоих предложениях касаются тематики и материальной сферы, эффективной защиты основных прав и установления иерархии существующих правовых актов в этой области.

Ключевые слова: европейский союз, персональные данные, защита, основные права, реформа системы защиты персональных данных, проект постановления, проект директивы