Rozdział I. Dane osobowe – zagadnienia ogólne

1. Geneza prawnej ochrony danych osobowych

Ochrona prawna danych osobowych jest ideą, której źródeł upatrywać należy w rozwoju i upowszechnianiu się nowych technologii, za pomocą których dokonywano przetwarzania informacji, w tym informacji o osobie[1]. Zastąpienie tradycyjnych metod gromadzenia informacji przez skomputeryzowane mechanizmy przetwarzania danych oraz wzrastająca liczba elektronicznych baz danych tworzonych nie tylko przez instytucje publiczne, ale także przez podmioty prywatne stwarzały niebezpieczeństwo niekontrolowanego obiegu zarówno samej wiadomości, jak i jej treści zawierającej dane osobowe jednostki. Informacja o osobie uzyskała przymiot pewnego rodzaju produktu o wartości ekonomicznej, a niejednokrotnie była wykorzystywana do celów mogących naruszyć interesy osobiste podmiotu, na temat którego była ona gromadzona[2]. Cywilnoprawne środki ochrony przewidziane w krajowych ustawodawstwach okazały się niewystarczające i nieefektywne[3] dla rozwiązywania konfliktu między wartością ekonomiczną, jaką niosły ze sobą dane osobowe, a ochroną dóbr osobistych jednostek, których te dane osobowe dotyczyły. Uczynienie z baz danych zawierających dane osobowe swoistego rodzaju produktu będącego przedmiotem obrotu niosło potencjalne ryzyko masowego charakteru naruszeń. Wskazywano, że brak kontroli jedsnostki nad przetwarzaniem jej danych osobowych ogranicza szanse na samookreślenie oraz informacyjnej autoprezentacji, co w konsekwencji może naruszyć jej prawo do wizerunku własnego życia, a także demobilizować obywateli do aktyw-

[1] *M. Safjan*, Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym, PiP 2002, Nr 6, s. 3.

[2] *A. Bierć*, Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne, [w:] *M. Wyrzykowski* (red.), Ochrona danych osobowych, Warszawa 1999, s. 111.

[3] *G. Szpor*, Publicznoprawna ochrona danych osobowych, PUG 1999, Nr 12, s. 2.

nego uczestnictwa w życiu społecznym[4]. Istniało przy tym ryzyko koncentracji w jednym zbiorze informacji o jednostce poprzez łączenie poszczególnych danych z różnych baz.

Zagrożenia związane z cyfrowym przetwarzaniem danych były już podnoszone w latach 50. XX w., to zagadnienie to nabrało jednak szczególnego znaczenia dopiero pod koniec lat 60. XX w., kiedy to rozpoczęto prace nad stworzeniem aktów prawnych związanych z utworzeniem ogólnokrajowych komputerowych banków informacji[5]. Podjęcie prac nad skonstruowaniem instrumentów prawnych umożliwiających funkcjonowanie banków danych stanowiło impuls do wystąpienia w 1968 r. przez Zgromadzenie Parlamentarne Rady Europy do Komitetu Ministrów z zaleceniem Nr 509 o dokonanie oceny ochrony praw człowieka na tle współczesnych przedsięwzięć naukowych i technicznych. Powołana przez Komitet Ministrów grupa ekspertów uznała, że ówczesne rozwiązania prawne w sposób niewystarczający zapewniają ochronę interesów i praw jednostki w obliczu zagrożeń powstających ze strony zautomatyzowanych banków danych[6]. Efektem tych prac było podjęcie przez Komitet Ministrów Rady Europy w 1973 r. rezolucji Nr 22(73) o ochronie prywatności jednostek w związku z funkcjonowaniem elektronicznych banków danych w sektorze prywatnym oraz w 1974 r. rezolucji Nr 29(74) dotyczącej ochrony prywatności w związku z działaniem takich banków w sektorze publicznym[7]. W rezolucjach tych sformułowano zasady: uzyskiwania, gromadzenia, wykorzystywania, udostępniania informacji, określenia celu pozyskiwania informacji, zastosowania środków ostrożności zapobiegających niewłaściwemu bądź podstępnemu wykorzystaniu informacji oraz usuwania informacji uzyskanych w sposób bezprawny lub nieaktualnych. Z uwagi na niewiążący charakter powyższych aktów wezwano państwa członkowskie Rady Europy do stworzenia na poziomie ogólnokrajowym środków prawnych zmierzających do ochrony danych osobowych. Powyższe dokumenty w swych założeniach miały więc spowodować mobilizację krajów człon-

[4] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych. Komentarz, Warszawa 2011, s. 25–26.

[5] *L. Kański*, Prawo do prywatności, nienaruszalności mieszkania i tajemnicy korespondencji, [w:] *R. Wieruszewski* (red.), Prawa człowieka. Model prawny, Wrocław 1991, s. 329–366.

[6] *S. Szmak*, Europejskie standardy w zakresie ochrony danych osobowych – zarys problemu, [w:] *G. Goździewicz* (red.), Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych, Toruń 2008, s. 167.

[7] *T. Banyś*, *E. Bielak-Jomaa*, *M. Kuba*, *J. Łuczak*, Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków, Warszawa 2016, s. 13.

Kup książkę

kowskich do wprowadzenia w swych ustawodawstwach niezbędnych mechanizmów realizujących zasady podane w powyższych aktach[8].

W obliczu niebezpieczeństwa związanego ze swobodnym i nieograniczonym przepływem informacji rolą państwa było utworzenie i ukształtowanie takiego systemu prawnego, który umożliwiłby prawnie reglamentowaną ingerencję w szeroko rozumianą prywatność jednostki przy zapewnieniu jej możliwości decydowania o sposobie korzystania z informacji oraz zapewnił nieskrępowany rozwój usług i rynków telekomunikacyjnych[9]. Zagrożenie autonomii informacyjnej jednostki związane z niekontrolowanym zasięgiem przetwarzania informacji stanowiło asumpt do stworzenia w systemach ustrojodawczych mechanizmów i instytucji zmierzających do ochrony danych osobowych[10].

W drugiej połowie XX w. zaczęły pojawiać się na świecie pierwsze akty prawne fragmentarycznie regulujące problematykę ochrony danych osobowych[11]. Unormowania ochrony danych osobowych odnosiły się tylko do wybranych dziedzin życia, np. posługiwania się informacjami udzielanymi w celu uzyskania kredytu[12]. Za pierwszą na świecie kompleksową regulację o ochronie danych osobowych uważa się przyjętą 7.12.1970 r. przez parlament niemieckiego kraju związkowego Hesji ustawę o ochronie danych osobowych[13]. Natomiast na szczeblu państwowym pierwszą ustawą o ochronie danych osobowych była uchwalona w 1973 r. ustawa szwedzka[14]. Podobny akt prawny został w 1977 r. przyjęty w Niemczech na poziomie federalnym[15]. W tej samej dekadzie powstały ustawy o ochronie danych osobowych m.in. we Francji, Danii, Norwegii i Luksemburgu. W latach 80. i 90. XX w. problematykę tę uregulo-

[8] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych..., s. 54.

[9] *N. Brieskorn*, Ochrona danych osobowych a zagrożenia prywatności, [w:] *M. Wyrzykowski* (red.), Ochrona danych osobowych..., s. 208–210.

[10] *J. Borecka*, Geneza prawnej ochrony danych osobowych i pojęcie danych osobowych, ZNIAA im. Jana Długosza w Częstochowie 2006, s. 6–13.

[11] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych..., 2011, s. 25.

[12] Przykładowo, w Stanach Zjednoczonych w 1970 r. uchwalono ustawę *The Fair Credit Reporting Act* dotyczącą gospodarki kredytowej. Regulacja ta miała zapobiec praktykom nadużywania przez sektor prywatny danych osobowych kredytobiorców poprzez przyznanie im prawa do określonych roszczeń w przypadku wykorzystania ich danych osobowych niezgodnie z celem ich udzielenia.

[13] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych..., s. 25.

[14] Zob. szerzej: *G. González Fuster*, The Emergence of Personal Data Protection as a Fundamental Right of the EU, Springer International Publishing 2014, s. 21, 56–71, gdzie autorka omawia poszczególne ustawy krajowe.

[15] *A. Mrózek*, Zachodnioniemiecka ustawa o ochronie danych osobowych w warunkach automatycznego przetwarzania, SP 1978, Nr 1, s. 175.

Kup książkę

wały również m.in. Austria, Islandia, Finlandia, Węgry, Wielka Brytania. Na poziomie konstytucyjnym ochrona danych osobowych została pierwszy raz uregulowana w 1976 r. w Portugali, a następnie w 1978 r. w Austrii, a kolejno w 1978 r. w Hiszpanii. Kompleksowa ochrona danych osobowych w Polsce została przyjęta – zarówno na poziomie konstytucyjnym, jak i ustawowym – w 1997 r. Unormowania prawne odnoszące się bezpośrednio do ochrony danych osobowych w latach 90. XX w. stały się standardem w państwach europejskich.

W systemach prawnych na poziomie ustawowym można wyodrębnić zasadniczo dwa modele ochrony danych osobowych[16]. Pierwszy model, tzw. licencyjny, uzależnia przetwarzanie danych osobowych i tworzenie banków danych od spełnienia określonych przez ustawodawcę warunków. Model ten zakłada utworzenie specjalnego organu państwowego, któremu przysługują uprawnienia kontrolne oraz decyzyjne odnoszące się do udzielania zezwoleń na zakładanie banków danych[17]. Przyjęta w ustawodawstwie polskim konstrukcja prawna ochrony danych osobowych wpisuje się, co do zasady, w powyższy model. Natomiast drugi model, tzw. aprobacyjny, opiera się na akceptacji jednostki na przetwarzanie jej danych osobowych, poza wyraźnie wskazanymi w ustawie przypadkami określającymi warunki, tryb i podmiot uprawniony do przetwarzania danych osobowych. Istnieją również rozwiązania łączące w sobie elementy obu wspomnianych konstrukcji[18].

Ze szczególną sytuacją prawną mamy do czynienia w ustawodawstwie Stanów Zjednoczonych Ameryki Północnej. W systemie prawnym tego państwa nie ma jednolitego aktu prawnego regulującego całościowo materię związaną z ochroną danych osobowych[19]. Kwestie prawne odnoszące się do tej problematyki normowane są jedynie przez przepisy sektorowe, które uzupełniane są przez normy samoregulujące, przyjmowane w drodze umów lub powszechnej aprobaty[20]. Ponadto w państwie tym nie ma niezależnego organu państwo-

[16] *A. Siostrzonek*, Dane osobowe gromadzone w bazach danych i ich ochrona w prawie polskim, Rej. 1999, Nr 9, s. 274–275.

[17] Taki model został przyjęty w ustawodawstwie szwedzkim, austriackim i niemieckim.

[18] Rozwiązania prawne łączące elementy obydwu modeli występują np. we Francji, w Norwegii i Danii. Szerzej na ten temat zob. *A. Mrózek*, Ustawowe prawo ochrony danych. Analiza prawnoporównawcza, Toruń 1981, s. 91.

[19] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych..., s. 31.

[20] *F.H. Cate*, The Changing Face of Privacy Protection in the European Union and the United States, Indiana Law Review 1999, s. 210–216.

Kup książkę

wego stojącego na straży przestrzegania postanowień w zakresie ochrony danych osobowych.

Jednocześnie z powstawaniem przedsięwzięć legislacyjnych na poziomie państwowym prowadzone były na forum międzynarodowym prace zmierzające do zinstytucjonalizowania ochrony danych osobowych na poziomie ogólnoeuropejskim. Za jeden z najstarszych instrumentów ochrony danych osobowych na płaszczyźnie międzynarodowej uważa się Konwencję 108 Rady Europy z 28.1.1981 r. dotyczącą ochrony osób w związku z automatycznym przetwarzaniem danych osobowych[21]. Mimo że prace prawodawcze nad Konwencją 108 rozpoczęto już w 1976 r., to dopiero po ratyfikacji tego aktu przez Szwecję, Francję, Hiszpanię, Norwegię i RFN weszła ona w życie 1.10.1985 r. Zasadniczą przyczyną tak późnego wprowadzenia Konwencji 108 w życie było nieuzyskanie wymaganej w akcie zgody minimalnej liczby państw członkowskich Rady Europy na związanie postanowieniami konwencji (art. 22 ust. 2 Konwencji 108). Konwencja 108 została podpisana przez Polskę 21.4.1999 r. (ratyfikacja miała miejsce 24.4.2002 r.). Konwencja 108 była pierwszym aktem prawnym o zasięgu międzynarodowym, którego rozwiązania normatywne miały wiążący charakter w odniesieniu do państw członkowskich. Warunkiem przystąpienia do Konwencji 108 było stworzenie w ustawodawstwie wewnętrznym państwa przystępującego instrumentów umożliwiających realizację podstawowych zasad ochrony danych osobowych statuowanych w postanowieniach Konwencji 108, która nie zawiera w sobie norm samowykonalnych, a nakłada na państwa ratyfikujące ten akt określone obowiązki mające dostosować poziom ochrony danych osobowych w danym ustawodawstwie krajowym do przyjętego standardu europejskiego. Z Konwencji 108 wynika zobowiązanie każdego sygnatariusza do wprowadzenia do swojego ustawodawstwa wewnętrznego podstawowych środków ochrony prawnej danych osobowych (art. 4 Konwencji 108). Dokument ten nie narzuca sygnatariuszom gotowych rozwiązań prawnych, ale pozostawia im pewien zakres swobody w kształtowaniu odpowiednich środków urzeczywistniających konwencyjne standardy w prawie wewnętrznym. Regulacja ta miała przyczynić się do wzmocnienia prawnej ochrony jednostki w związku z automatycznym przetwarzaniem danych osobowych oraz wprowadzić pewien ustandaryzowany poziom ochrony

[21] Jak podkreślają autorzy Podręcznika europejskiego prawa o ochronie danych Konwencja 108 jest jedynym prawnie wiążącym międzynarodowym aktem dotyczącym ochrony danych osobowych. Zob. Podręcznik europejskiego prawa o ochronie danych, Luksemburg 2014, s. 16. Tak też: *A. Mednis*, Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej, PiP 1997, Nr 6, s. 29.

Kup książkę

prawnej danych osobowych we wszystkich państwach członkowskich Rady Europy. Jak wynika z odwołania zawartego w preambule Konwencji 108 celem tego aktu było przede wszystkim pogodzenie podstawowej dla jednostki wartości, jaką jest poszanowanie jej prywatności ze swobodnym obiegiem informacji między narodami. Konwencja 108 po raz pierwszy wyznaczyła na gruncie międzynarodowym podstawowe wzorce prawnej ochrony danych osobowych poprzez zdefiniowanie danych osobowych (art. 2 Konwencji 108), określenie zasad i celów zbierania i przetwarzania danych osobowych (art. 5 Konwencji 108), zakresu szczególnej kategorii danych osobowych (art. 6 Konwencji 108), zapewnienie właściwych środków bezpieczeństwa ochrony danych osobowych (art. 7 Konwencji 108) i gwarancji dodatkowej dla podmiotu danych (art. 8 Konwencji 108), wprowadzenie odpowiednich sankcji i systemów odszkodowawczych (art. 10 Konwencji 108). Regulacje zawarte w Konwencji 108 tworzą pewnego rodzaju *consensus* w zakresie ochrony danych osobowych pomiędzy interesem społecznym, a interesem jednostki. Ponadto z przepisów Konwencji 108 wynika, że normy prawne w niej zawarte stanowią jedynie minimum konwencyjne, które na gruncie krajowym może zostać rozszerzone o dalej idące środki prawnej ochrony danych osobowych[22]. W akcie tym przyjęta została zasada swobodnego transferu danych osobowych między państwami członkowskimi oraz określono warunki wzajemnej pomocy i współpracy krajów członkowskich. Stworzona w ramach Rady Europy regulacja ujednolica zasady ochrony danych osobowych jednostki wprowadzając pewien wspólny poziom ochrony prawnej, a przy tym nie stwarza barier dla rozwoju nowych technologii. Zaznaczyć jednak należy, że regulacja ta kreuje jedynie minimalne wzorce ochrony, które na podstawie przepisów wewnętrznych prawa krajowego mogą zostać rozszerzone na inne niż te wynikające z postanowień konwencji[23].

Poza Konwencją 108 Rada Europy w celu zapewnienia skuteczniejszej ochrony danych osobowych wypracowała szereg aktów prawnych zarówno odnoszących się do poszczególnych dziedzin życia społecznego, doprecyzowujących normy prawne zawarte w konwencji, jak i stanowiących rozwinięcie jej przepisów w postaci rezolucji i rekomendacji Komitetu Ministrów Rady

[22] *A. Mednis*, Prawna ochrona danych osobowych, Warszawa 1995, s. 22.

[23] *K. Czarnecki*, Ochrona danych osobowych w systemie Rady Europy na przykładzie Konwencji Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, [w:] Prawna ochrona danych..., s. 190.

Kup książkę

Europy lub Zgromadzenia Parlamentarnego Rady Europy[24]. Ponadto w Strasburgu 8.11.2001 r. został sporządzony protokół dodatkowy do Konwencji 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, dotyczący organów nadzoru i transgranicznych przepływów danych wprowadzający kolejne warunki zarówno materialne, jak i formalne do przetwarzania danych osobowych[25].

Konieczność pogodzenia konfliktu pomiędzy jednostką, a społeczeństwem dla dobra rozwoju stosunków społecznych i ekonomicznych została dostrzeżona przez Organizację Współpracy Gospodarczej i Rozwoju (OECD), która 23.9.1980 r. wydała wytyczne w sprawie ochrony prywatności i przekazywania danych osobowych pomiędzy krajami[26]. W akcie tym podkreślono znaczenie wpływu międzynarodowego obrotu danych osobowych na światowy rozwój gospodarczy i ujemny wpływ ograniczeń w tym zakresie. Wytyczne OECD wyznaczyły na gruncie międzynarodowym wzorce w zakresie przetwarzania danych osobowych przez określenie m.in. zasad: ograniczenia zbierania danych osobowych, uzyskiwania danych osobowych zgodnie z prawem i za zgodą ich beneficjenta, dokładnego określenia celu przetwarzania danych, ograniczonego przetwarzania danych ze względu na ich prawidłowość oraz cel, wprowadzenia odpowiednich przedsięwzięć zabezpieczających, powszechnej polityki jawności co do rozwoju i praktyk dotyczących roszczeń osób, których dane dotyczą, eksploatowania danych jedynie w granicach wyszczególnionych celów, przyznania każdemu uprawnienia dostępu do dotyczących go danych[27]. Treść tej regulacji zasadniczo zawiera rozwiązania zbieżne z tymi, które zostały przyjęte w Konwencji 108. Zaznaczyć jednak należy, że o ile przepisy Konwencji 108 zwracają uwagę na kwestie związane z ochroną prywatności, o tyle w preambule wytycznych OECD podkreślono również wpływ i wagę międzynarodowego przepływu danych osobowych na światowy rozwój gospodarczy oraz negatywny wpływ ograniczeń w powyższym zakresie[28]. Z uwagi na niewiążący charakter wytycznych oraz brak obowiązku ich implementacji

[24] Dla przykładu wymienić można rekomendację 10(84) w sprawie rejestrów karnych i rehabilitacji osób skazanych oraz rekomendację 15(87) o korzystaniu z danych osobowych w działalności Policji.

[25] T.j. Dz.U. z 2006 r. Nr 3, poz. 15.

[26] Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, October 1, 1980, C (80) 58 final.

[27] Szerzej na temat genezy wytycznych OECD zob. *R. Jay*, *A. Hamilton*, Data protection. Law and practice, London 2003, s. 6–7.

[28] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych..., s. 83.

Kup książkę

do prawa wewnętrznego określone w nich zasady stanowią jedynie zalecenia Rady OECD w zakresie ochrony prywatności i przepływu danych osobowych pomiędzy państwami.

Pierwotnie Unia Europejska nie zajmowała się kwestią stworzenia własnej regulacji w zakresie ochrony danych osobowych, postulowała jednak, aby do 1982 r. państwa członkowskie Unii Europejskiej ratyfikowały Konwencję 108[29]. Doniosłość problematyki związanej z ochroną danych osobowych, jak również występujące w wewnętrznych regulacjach państw członkowskich rozbieżności wymusiły na organach Unii Europejskiej podjęcie w 1990 r. prac nad stworzeniem jednolitej regulacji obejmującej problematykę danych osobowych. Konsekwencją tych prac było wydanie dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[30]. Implementację tego aktu przez państwa członkowskie wyznaczono na 23.10.1998 r. Twórcy dyrektywy 95/46/WE jako podstawowy cel tej regulacji uznali przyznanie w krajach wspólnoty jednolitej ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych oraz zagwarantowanie możliwości swobodnego przepływu danych osobowych między krajami Unii Europejskiej[31]. Przepisy dyrektywy 95/46/WE recypowały cele, dla których fundament stworzyły normy Konwencji 108, a do których należą prawne określenie minimalnego standardu ochrony danych osobowych oraz uregulowanie zasad przetwarzania danych osobowych między państwami Unii Europejskiej[32]. Akt ten przyjął szeroką definicję danych osobowych i przetwarzania danych osobowych (art. 2 dyrektywy 95/46/WE). W dyrektywie określono ponadto standardy przetwarzania danych osobowych przez wyznaczenie w niej zasad przetwarzania i gromadzenia danych osobowych, jakości danych, zagwarantowania wpływu i kontroli przetwarzania danych osobie, której dane dotyczą, bezpieczeństwa danych. Dyrektywa 95/46/WE za naczelną zasadę przetwarzania danych osobowych przyjęła rzetelność i legalność przetwarzania danych osobowych[33]. Ponadto re-

[29] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych..., s. 64.

[30] Dz.Urz. WE L Nr 281 z 23.11.1995 r., s. 31 ze zm.; Dz.Urz. UE polskie wyd. specj. Rozdz. 13, t. 15, 3. 355.

[31] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych..., s. 64.

[32] *K. Gałaj-Emiliańczyk*, Ochrona danych osobowych – praktyczny komentarz, wzorcowa dokumentacja (z suplementem elektronicznym), Gdańsk 2015, s. 15.

[33] *M. Jagielski*, Prawo do ochrony danych osobowych. Standardy europejskie, Warszawa 2010, s. 78.

Kup książkę

gulacja ta uznaje za podstawę przetwarzania danych zgodę ich beneficjenta, natomiast dopuszcza przetwarzanie danych osobowych pomimo braku zgody osoby, której informacje dotyczą jedynie w ściśle określonych sytuacjach (art. 7 dyrektywy 95/46/WE). Przepisy tego aktu zawierają również postanowienia dotyczące warunków dopuszczających zbieranie danych o szczególnym charakterze (tzw. danych wrażliwych). Dyrektywa zawiera również wyraźne postanowienia odnośnie do praw służących beneficjentom danych osobowych, w tym przyznaje tym osobom prawo dochodzenia swoich roszczeń na drodze sądowej i przewiduje powołanie organów nadzorczych i Grupy Roboczej ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych. Dyrektywa 95/46/WE nie ma zastosowania do działalności państwa w ramach prawa karnego (art. 3 ust. 2 dyrektywy 95/46/WE). Niektórzy autorzy analizują jednak, czy po wejściu w życie Traktatu z Lizbony i po likwidacji struktury filarowej UE nie należałoby uznać, że dyrektywa 95/46/WE obejmuje także materię współpracy policyjnej i sądowej w sprawach karnych[34]. Z uwagi na jednoznaczną treść art. 3 ust. 2 dyrektywy 95/46/WE należy zdecydowanie odrzucić taką możliwość.

Po wprowadzeniu dyrektywy 95/46/WE nastąpił dalszy wzrost znaczenia prawa do ochrony danych osobowych. Na szczycie w Kolonii mającym miejsce 2–4.6.1999 r. Rada Europejska postanowiła umieścić w Karcie Praw Podstawowych Unii Europejskiej regulacje dotyczące danych osobowych uznając, że prawo ochrony danych osobowych powinno stanowić jedną z fundamentalnych zasad Unii Europejskiej. Pierwszy projekt Karty Praw Podstawowych Unii Europejskiej został ogłoszony na posiedzeniu Rady Europejskiej 19–20.6.2000 r. podczas szczytu w Santa Maria da Feira. Końcowy projekt dokumentu uchwalono 2.10.2000 r. na posiedzeniu Konwentu w Brukseli, zaś na szczycie w Nicei 7.12.2000 r. nastąpiła proklamacja Karty przez organy unijne. W art. 8 KPP zostało przyznane jednostce prawo do ochrony jej danych osobowych. W artykule tym zawarte zostały również ogólne wytyczne dotyczące zasad przetwarzania danych osobowych, w ramach których wymaga się, aby przetwarzanie to prowadzone było w sposób rzetelny, w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Akt ten określił, że przetwarzanie danych osobowych może odbywać się jedynie zgodnie z zasadami współżycia społecznego, w okre-

[34] Szerzej na ten temat zob. *A. Grzelak*, Projekt ochrony danych osobowych w sprawach karnych w UE – kolejny krok na drodze do społeczeństwa nadzorowanego?, EPS 2012, Nr 11, s. 20–21.

Kup książkę

ślonym celu i za zgodą osoby, której dane dotyczą, bądź też na ustawowej podstawie prawnej. Karta Praw Podstawowych Unii Europejskiej zagwarantowała jednostce prawo otrzymania informacji o zgromadzonych na jej temat danych oraz prawo ich skorygowania. Ponadto w KPP uznano, że przestrzeganie powyższych praw podlega kontroli niezależnego organu. Na skutek wejścia w życie Traktatu z Lizbony KPP uzyskała prawnie wiążący charakter, a w konsekwencji prawu do ochrony danych osobowych jednostki przyznano status samodzielnego prawa podstawowego[35].

Na gruncie unijnym wydane zostały również odrębne regulacje prawne dotyczące tematyki przetwarzania danych osobowych przez instytucje i organy wspólnotowe[36]. Powyższe przedsięwzięcie miało na celu uwzględnienie specyfiki związanej z przetwarzaniem danych osobowych pomiędzy unijnymi instytucjami i organami, a także stanowić uszczegółowienie i konkretyzację w powyższym zakresie norm zawartych w dyrektywie 95/46/WE.

W odniesieniu do aktów prawa Unii szczególną uwagę zwrócić należy na wyrok Trybunału Sprawiedliwości z 8.4.2014 r. w sprawie C-293/12 i C-594/12 *Digital Rights Ireland Ltd*[37], w którym Trybunał Sprawiedliwości uznał, że dyrektywa 2006/24/WE o retencji danych telekomunikacyjnych jest nieważna, ponieważ ze względu na zbyt szeroki zakres i brak odpowiednich gwarancji chroniących przed nadużyciami w sposób nieproporcjonalny ingerowała w gwarantowane w KPP prawo do prywatności i ochrony danych osobowych. Trybunał Sprawiedliwości w powyższym wyroku zaakcentował, że akty, takie jak dyrektywy prawa Unii, powinny być interpretowane z uwzględnieniem praw podstawowych.

Zagadnienie przetwarzania danych osobowych znalazło również odzwierciedlenie w specjalistycznych porozumieniach między krajami europejskimi. Wymienić w tym miejscu należy Układ z Schengen z 14.6.1985 r. poświęcony stopniowemu znoszeniu kontroli granicznej pomiędzy państwami Wspólnoty Europejskiej. Dnia 19.6.1990 r. została zawarta konwencja wykonawcza do Układu z Schengen[38], na podstawie której utworzono System Informacyjny

35 Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, Dz.Urz. UE C Nr 306 z 17.12.2007 r.

36 Zob. rozporządzenie 2001/45/WE Parlamentu Europejskiego i Rady z 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. WE L Nr 8 z 12.1.2001 r., s. 1).

37 Zob. wyr. Trybunału Sprawiedliwości z 8.4.2014 r. w sprawie C-293/12 i C-594/12 *Digital Rights Ireland Ltd.*, ECLI:EU:C:2014:238.

38 Dz.Urz. UE L Nr 239 z 22.09.2000 r., s. 19.

Kup książkę

Schengen, umożliwiający wymianę informacji między krajami odnośnie do osób przekraczających granice. Dokument ten unormował w sposób rozbudowany zagadnienia dotyczące zasad gromadzenia i rozpowszechniania danych osobowych między sygnatariuszami tego aktu.

Zmiany, które do konstrukcji UE i praw podstawowych przez nią chronionych wniósł Traktat z Lizbony, 30-lecie obowiązywania Konwencji 108 i 15-lecie obowiązywania dyrektywy 95/46/WE[39] stały się impulsem do podjęcia działań dążących do zmiany podstaw prawnych ochrony danych osobowych w Europie[40]. Celem prac było dokonanie reformy systemu ochrony danych osobowych w Unii Europejskiej, zwłaszcza przez doprowadzenie do spójności systemu i jednolitości stosowania przepisów w państwach członkowskich[41]. Efektem powziętych prac było przedstawienie przez Komisję Europejską 25.1.2012 r. projektu pakietu legislacyjnego, zawierającego nowe ramy ochrony danych osobowych w UE[42]. Pakiet ten objął dwa akty prawne, tj. dyrektywę 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 oraz rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Rozporządzenie 2016/679 zostało przyjęte przez Parlament Europejski i Radę 27.4.2016 r., weszło w życie 24.5.2016 r., natomiast zgodnie z art. 99 zaczęło obowiązywać bezpośrednio w krajowych porządkach prawnych od 25.5.2018 r. Założeniem regulacji jest zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi, ale również wprowadzenie zasad, zgodnie z którymi przetwarzanie danych osobowych będzie ujedno-

[39] *J. Barcz*, Unia Europejska na rozstajach. Traktat z Lizbony. Dynamika i główne kierunki reformy ustrojowej, Warszawa 2010, s. 114–120.

[40] *W. Wiewiórowski*, Nowe ramy ochrony danych osobowych w Unii Europejskiej jako wyzwanie dla polskiego sądownictwa, KRS 2013, Nr 1, s. 14. Jako powód prac wskazuje się przede wszystkim to, że konstrukcje prawne ochrony danych osobowych nie przystawały do realiów współczesnego świata, gdyż nie uwzględniały one specyfiki przetwarzania danych w środowisku cyfrowym, Internetu, czy też innych aspektów rozwoju technologii informacyjnej. Tak: *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych..., s. 78.

[41] *M. Kusak*, Ochrona danych osobowych w sprawach karnych – rekomendacja na tle transpozycji dyrektywy 2016/680/UE, EPS 2017, Nr 10, s. 10–11.

[42] Zob. http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52012AR0625, [dostęp: 5.11.2018 r.].

Kup książkę

licone na terenie całej Unii Europejskiej. Akt ten wprowadza szereg istotnych zmian mających na celu unowocześnienie oraz uaktualnienie ochrony danych osobowych[43]. Do zasadniczych zmian zaliczyć należy m.in. bezpośrednią odpowiedzialność przetwarzającego dane, zgłoszenie przez administratora danych naruszeń, prawo do bycia zapomnianym, uprawnienie do żądania przeniesienia danych, wzmocnienie prawa dostępu i wglądu jednostki w jej dane, ograniczenia w zakresie profilowania, ocenę wpływu ochrony danych.

Z kolei dyrektywa 2016/680 weszła w życie pierwszego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej, tj. 5.5.2016 r. (zob. art. 64 dyrektywy). Implementacja przepisów dyrektyw 2016/680 przez państwa członkowskie miała nastąpić do 6.5.2018 r. Przed wejściem w życie dyrektywy, prawo wspólnotowe regulowało zagadnienie przetwarzania danych osobowych przez organy policyjne i sądowe w sprawach karnych przepisami decyzji ramowej Rady 2008/977/WSiSW. Akt ten ograniczał się wyłącznie do transgranicznego przetwarzania danych, zaś przetwarzanie danych osobowych niebędące przedmiotem transgranicznej wymiany informacji, nie było w żaden sposób objęte kompleksowymi regulacjami Unii Europejskiej. Wynikało to z ograniczeń związanych z brakiem traktatowej podstawy prawnej dla przyjęcia takiego aktu prawnego. Wejście w życie Traktatu z Lizbony wprowadziło w tym zakresie istotne zmiany. Uchwalenie nowego art. 16 TFUE pozwoliło przyjąć akt prawny, który regulowałby zasady przetwarzania danych w sposób kompleksowy, jednolity i spójny[44]. Dyrektywa 2016/680 swym zakresem normowania objęła zarówno reguły transgranicznego, jak i krajowego przetwarzania danych przez właściwe organy państw członkowskich w celu ścigania przestępstw, przy jednoczesnym zachowaniu specyfiki współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych. Dyrektywa 2016/680 ma zapewnić odpowiednią ochronę danych osobowych uczestników postępowania, świadków, ofiar i sprawców, jak również usprawnić komunikację między organami ścigania. W przeciwieństwie do rozporządzenia

[43] Szerzej na ten temat zob. *E. Bielak-Jomaa*, *D. Lubasz* (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018; *P. Litwiński* (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2017; *M. Sakowska-Baryła* (red.), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Warszawa 2018; *P. Fajgielski* (red.), Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018.

[44] Zob. *A. Grzelak*, Prawo do ochrony danych osobowych a konieczność walki z przestępczością. Uwagi na tle art. 16 traktatu o funkcjonowaniu Unii Europejskiej, [w:] Prawo Unii Europejskiej a prawo konstytucyjne państw członkowskich, Warszawa 2013, s. 407–434.

Kup książkę

2016/679, dyrektywa 2016/680 wymaga transpozycji do prawa krajowego, czyli przyjęcia przez ustawodawcę krajowego przepisów, które zrealizują cel wskazany w dyrektywie. Termin na przyjęcie właściwych przepisów ustawowych, wykonawczych i administracyjnych, niezbędnych do wykonania dyrektywy 2016/680, został wyznaczony w art. 63 dyrektywy na 6.5.2018 r.

Choć obydwa akty dotykają materii istotnej dla zagwarantowania podstawowych praw jednostki, to szczególny charakter przyznać należy dyrektywie. Wiąże się to po pierwsze z tym, że materia, jaką obejmuje przedmiotowy akt, bezpośrednio dotyka problematyki przetwarzania danych osobowych przez organy ścigania i wymiaru sprawiedliwości w ramach postępowania karnego, a po drugie, akcentuje kwestię ważenia interesów pomiędzy ochroną danych jednostki a zapewnieniem jej bezpieczeństwa[45]. Wprowadzone zmiany oznaczają, że wszelkie czynności podejmowane i wykonywane przez organy ścigania i wymiaru sprawiedliwości, a związane z przetwarzaniem danych osobowych dla celów zapobiegania przestępstwom, prowadzenia dochodzeń, wykrywania i ich ścigania, są poddane regulacjom nowej dyrektywy[46]. Natomiast przetwarzanie danych pracowników wymiaru sprawiedliwości i ścigania obejmuje rozporządzenie 2016/679[47].

Celem zmian jest przejście od harmonizacji prawa ochrony danych osobowych w krajach członkowskich do ujednolicenia zasad tej ochrony na terenie UE, podniesienie poziomu ochrony danych osobowych przez uzupełnienie i wprowadzenie dotychczas nieistniejących uprawnień, obowiązków i regulacji w zakresie przetwarzania danych, mających na celu zwiększenie efektywności istniejących rozwiązań prawnych i zapewnienie im skuteczność w związku z szybkim rozwojem technologicznym[48]. Proces modernizacji jest konieczny w obliczu nowych wyzwań stawianych przez cyfryzację, pojawienie się nowych kategorii danych osobowych czy wzrastającą skalę ich przetwarzania[49]. *Ratio*

[45] *A. Grzelak*, Projekt ochrony danych..., s. 20.

[46] *A. Wolska-Bagińska*, Podstawy prawne przetwarzania danych osobowych w postępowaniu karnym, Prok. i Pr. 2018, Nr 6, s. 46.

[47] *W. Wiewiórowski*, Nowe ramy ochrony..., s. 18.

[48] *A. Dmochowska*, *M. Zadrożny*, Unijna reforma ochrony danych osobowych. Analiza zmian, Warszawa 2016, s. 49.

[49] Szerzej na temat genezy projektu rozporządzenia zob. *M. Krzysztofek*, Ochrona danych osobowych Unii Europejskiej. Transfer danych osobowych z Unii Europejskiej, ze szczególnym uwzględnieniem transferu do Stanów Zjednoczonych, w obecnym i nadchodzącym stanie prawnym, Warszawa 2014, s. 64 i n.; *U. Góral*, Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobod-

Kup książkę

legis nowych ram prawnych ochrony danych w Unii Europejskiej jest więc uwspółcześnienie ochrony danych osobowych, podniesienie poziomu ochrony oraz przyznanie większej kontroli nad całością procesów przetwarzania danych jednostce, której dane dotyczą. Zasadniczy kierunek rozwiązań, w tym wyraźne określenie zasad przetwarzania danych oraz praw osób, których dane dotyczą, uznać należy za właściwy, gdyż przyczyni się on do poprawy praw jednostki w zakresie ochrony danych[50].

Aktualnie prowadzone są również prace nad modyfikacją Konwencji 108, które zmierzają do uszczegółowienia jej przepisów, przy jednoczesnym zachowaniu podstawowych regulacji[51]. Propozycje zmian dążą do zapewnienia spójności z prawodawstwem Unii Europejskiej, zachowania neutralności konwencji pod względem technologicznym, zapewnienia efektywności środków oraz prostoty sformułowań oraz podtrzymania zasady, że obejmuje ona zarówno sektor prywatny, jak i publiczny[52]. Z punktu widzenia tematyki pracy znaczące zmiany Konwencji 108 nie wpływają bezpośrednio na przetwarzanie danych osobowych na płaszczyźnie karnoprocesowej[53].

W Powszechnej Deklaracji Praw Człowieka z 10.12.1948 r., w Europejskiej Konwencji Praw Człowieka z 4.11.1950 r. oraz w Międzynarodowym Pakcie Praw Obywatelskich i Politycznych z 16.12.1966 r. nie unormowano wprost kwestii ochrony danych osobowych, ponieważ problem ten ujawnił się dopiero później i związany był z rozwojem technologii teleelektronicznych, tworzeniem elektronicznych baz danych i wykorzystywaniem informacji tam zawartych dla potrzeb obrotu gospodarczego przez prywatne podmioty. Przepisy zarówno Powszechnej Deklaracji Praw Człowieka (art. 12 PDPCz), Międzynarodowego Paktu Praw Obywatelskich i Politycznych (art. 17 MPPOiP), jak i Europejskiej Konwencji Praw Człowieka (art. 8 EKPC) poruszają zagadnienie prywatności, które jednak na gruncie tych aktów ma różne zakresy[54]. Za-

nym przepływem takich danych – zagadnienia wybrane, [w:] *G. Sibiga* (red.), Aktualne problemy prawnej ochrony danych osobowych 2013, dodatek specjalny do MoP 2013, Nr 8, s. 5–8.

50 Tak też: *A. Grzelak*, Projekt ochrony danych..., s. 28.

51 Zob. http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp [dostęp: 5.11.2018 r.].

52 *A. Grzelak*, Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego, Warszawa 2015, s. 152–153.

53 *W. Wiewiórowski*, Nowe ramy ochrony..., s. 14.

54 W piśmiennictwie podnosi się, że art. 8 EKPC dotyczy szeroko rozumianego prawa do poszanowania prywatnej sfery życia jednostki, tym która jest rozumiana bardzo szeroko i wykracza poza tradycyjne pojmowanie prywatności. Zob. szerzej: *L. Garlicki* (red.), Konwencja o Ochronie

Kup książkę

kres ochrony prawa do prywatności najszerzej został określony w MPPOiP, w którym objęto nim także cześć i dobre imię, a które nie znalazły się w przepisach EKPC. W związku z powyższym w literaturze przedmiotu spotkać można stanowisko, że przepisy EKPC w zakresie prawa do prywatności odnoszą się tylko do życia i działań jednostki, nie zaś do ochrony czci i dobrego imienia[55]. Co więcej ochrona prywatności na gruncie MPPOiP realizowana jest przez ustanowienie zakazu ingerencji w życie prywatne, w sytuacji gdy przepisy EKPC obejmują również ochroną życie prywatne w sposób pozytywny, tj. przez ustanowienie prawa jednostki do poszanowania życia prywatnego[56]. Odmienny sposób uregulowania tej materii na gruncie obydwu aktów prawnych (w MPPOiP w sposób negatywny poprzez ustanowienie zakazu ingerencji, a w EKPC także w sposób pozytywny przez ustanowienie określonego rodzaju prawa) skłania do wniosków, że przepisy EKPC ustanawiają szerszą ochronę prywatności, albowiem nie tylko realizują ochronę przewidzianą w MPPOiP, tj. wprowadzają zakaz ingerencji w określone sfery, lecz także nakładają na sygnatariuszy EKPC obowiązek podejmowania czynności mających na celu poszanowanie życia prywatnego.

Z wymienionych aktów prawnych wynika, że podstawową wartością objętą ochroną jest ogólnie pojmowana prywatność jednostki, co w konsekwencji może budzić wątpliwości odnośnie do relacji między prawem do prywatności a prawem do ochrony danych osobowych. Niejednoznaczność w zdefiniowaniu treści i granic prawa do prywatności[57] powoduje, że prawo to podlega zróżnicowanym interpretacjom w kontekście prawa do ochrony danych osobowych[58]. W nauce prawa rozbieżności poglądów koncentrują się wokół trzech stanowisk. Akcentuje się związek prawa do prywatności i ochrony danych osobowych, widząc w ochronie danych osobowych szczególną postać prywatności[59], jego konkretyzację, zwłaszcza w aspekcie proceduralnym[60], roz-

Praw Człowieka i Podstawowych Wolności. Komentarz do artykułów 1–18, t. I, Warszawa 2010, s. 481.

[55] *Z. Mielnik*, Prawo do prywatności. Zagadnienia wybrane, RPEiS 1996, Nr 2, s. 32.

[56] *A. Sakowicz*, Prawnokarne gwarancje prywatności, Kraków 2006, s. 123.

[57] Szerzej na temat prywatności zob. *A. Sakowicz*, Prywatność jako samoistne dobro prawne (per se), PiP 2006, Nr 1, s. 17–29; *A. Kopff*, Koncepcje prawa do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne, SC 1972, t. XX, s. 3–40.

[58] *M. Krzysztofek*, Ochrona danych osobowych..., s. 36.

[59] *M. Safjan*, Ochrona danych osobowych – granice autonomii informacyjne, [w:] *M. Wyrzykowski* (red.), Ochrona danych osobowych, Warszawa 1999, s. 10.

[60] *A. Zoll*, Ochrona prywatności w prawie karnym, CzPKiNP 2000, Nr 1, s. 222.

Kup książkę