Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz

Fragment

Przejdź do produktu na **ksiegarnia.beck.pl**

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

z dnia 27 kwietnia 2016 r. (Dz.Urz. UE L 2016, Nr 119, s. 1)

(zm.: Dz.Urz. UE L 2018, Nr 127, s. 2; Dz.Urz. UE L 2021, Nr 74, s. 35)

Wprowadzenie

Spis treści

	Nb
I. Geneza ram prawnych ochrony danych osobowych	1–3
II. Konwencja Nr 108	4
III. Ochrona danych osobowych w prawie Unii Europejskiej	5–11
1. Prawo pierwotne Unii Europejskiej	5–8
2. Dyrektywa 95/46/WE	9–11
IV. Unijna reforma ochrony danych osobowych	12–21
1. Założenia reformy ochrony danych osobowych	12–16
2. Wybór rozporządzenia jako instrumentu reformy ochrony danych osobowych	17–18
3. Procedura przyjęcia RODO	19–21
V. Ustawa o ochronie danych osobowych i przepisy sektorowe	22–26

I. Geneza ram prawnych ochrony danych osobowych

1. Geneza ram prawnych dotyczących ochrony danych osobowych sięga przełomu **1**
lat 70. i 80. XX w. Słusznie podkreśla się w literaturze przedmiotu, że bezpośrednią przyczyną objęcia ochroną prawną danych osobowych była obawa przed pojawieniem się nowych rozwiązań technologicznych umożliwiających ich gromadzenie oraz coraz bardziej zaawansowane przetwarzanie informacji, w tym o charakterze osobowym (*A. Krasuski*, *D. Skolimowska*, Dane osobowe w przedsiębiorstwie, Warszawa 2016, s. 19). Dowodem na to jest fakt, że okres zainteresowania problematyką ochrony danych osobowych pokrywał się z początkiem tzw. rewolucji informatycznej. Zagrożenia płynące z wykorzystywania informatycznych metod i środków przetwarzania danych były też często dostrzegane w możliwości nieograniczonego i pełnego wglądu władzy administracyjnej w informacje dotyczące konkretnych jednostek (*P. Fajgielski*, Ochrona danych osobowych w telekomunikacji – aspekty prawne, Lublin 2003, s. 27). Gwałtowny rozwój systemów i sieci informatycznych spowodował również, że przetwarzanie danych stało się znacznie tańsze, a tym samym powszechniejsze. Bez wątpienia trafne jest więc twierdzenie *M. Wyrzykowskiego*, że „rozwój prawa człowieka do ochrony danych został zapoczątkowany u samego progu ery informatycznej" [*M. Wyrzykowski*, w: Ochrona danych osobowych. Materiały z konferencji naukowej nt. ochrony danych osobowych, która odbyła się w Warszawie w dniach 27–28 lutego 1998 r. (red. *M. Wyrzykowski*), Warszawa 1999, s. 35]. Jak wskazuje *A. Mednis*, niewystarczające okazały się również klasyczne cywilnoprawne instrumenty ochrony dóbr osobistych, które nie wywierały skutku prewencyjnego, a miały zastosowanie dopiero w chwili samego zagrożenia (*A. Mednis*, Ochrona danych osobowych w Konwencji Rady Europy i Dyrektywie Unii Europejskiej, cz. I, Biuletyn Administratorów Bezpieczeństwa Informacji: Ochrona Danych Osobowych 2000, Nr 1, s. 9). Powyższe znalazło swoje odzwierciedlenie w ustawodawstwach krajowych, które już w latach 70. zaczęły regulować wprost kwestię ochrony danych osobowych. Pierwszą ustawą dotyczącą ochrony danych była ustawa uchwalona w 1970 r. w Hesji (Das Hessische Datenschutzgesetz z 7.10.1970 r., Dziennik Ustaw i Rozporządzeń I, s. 201).

2. Prekursorem, jeśli chodzi z kolei o przyjęcie aktu ogólnopaństwowego **2**
regulującego problematykę ochrony danych osobowych, była Szwecja, która już w 1973 r. uchwaliła ustawę o informacji [Datalagen z 13.5.1973 r. (1973:289); zob. *W. Kilian*, Ochrona danych w przedsiębiorstwach, w: Ochrona danych osobowych.

Materiały z konferencji naukowej nt. ochrony danych osobowych, która odbyła się w Warszawie w dniach 27–28.2.1998 r. (red. *M. Wyrzykowski*), Warszawa 1999, s. 99]. Jako kolejne kraje odpowiednie ustawy przyjęły: Francja, Austria, Dania, Norwegia i Luksemburg, czyli te państwa, w których najszybciej wdrożono nowe technologie w administracji państwowej. Proces uzupełniania porządków prawnych o instrumenty gwarantujące ochronę informacji był więc charakterystyczny w pierwszej kolejności dla krajów wysoko rozwiniętych (*P. Fajgielski*, Ochrona, s. 31). Wskazane inicjatywy ustawodawcze miały różne podłoża, ich wspólny element stanowiło jednak bez wątpienia dostrzeżenie, że obywatele zaczynają tracić możliwość wpływu na procesy zbierania i przechowywania informacji ich dotyczących [*A. Lewiński*, Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. 10-lecie polskiej ustawy o ochronie danych osobowych, w: Prawna ochrona danych osobowych w Polsce na tle europejskich standardów (red. *G. Goździewicz*, *M. Szabłowska*), Toruń 2008, s. 9]. Należy jednak wskazać, że jednocześnie z pojawianiem się ustaw krajowych chroniących dane osobowe coraz więcej aktów wymuszało pozyskiwanie danych o obywatelach, tak więc występowało – i wciąż występuje – samonapędzające się zjawisko polegające na tym, że ustawodawca z jednej strony zezwala na gromadzenie coraz szerszego zakresu danych, a z drugiej zaostrza zasady ich ochrony. Jest to jednak, jak się wydaje, normalny proces rozwoju gospodarczego państwa, w którym ze stałym wzrostem liczby usług świadczonych na rzecz obywateli nierozerwalnie wiąże się konieczność ich identyfikacji. Już zresztą EKPC dopuszcza w art. 8 ust. 2 ingerencję organów państwowych w uprawnienia wynikające z prawa do prywatności, gdy jest to konieczne w demokratycznym państwie prawnym ze względu na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

3 3. Ochrona danych osobowych stanowi jeden z podstawowych aspektów prawa do prywatności (zob. *M. Krzysztofek*, Ochrona danych osobowych w Unii Europejskiej, Warszawa 2014, s. 36 i n.), będąc jej wyspecjalizowaną postacią. Akceptując takie stanowisko i odwołując się do źródeł prawa międzynarodowego, podwalin prawnej ochrony danych osobowych należy szukać już w art. 12 Powszechnej Deklaracji Praw Człowieka z 10.12.1948 r., którym zagwarantowano, że nikt nie może być poddany arbitralnemu ingerowaniu w jego życie prywatne, rodzinne, domowe lub korespondencję ani też stać się obiektem ataków godzących w jego honor i dobre imię. Powyższe wynika również z art. 17 MPPOiP, w którym wprost stwierdzono, że nikt nie może być „narażony na samowolną lub bezprawną ingerencję w jego życie prywatne (...)". Nie sposób również nie wskazać, że w systemie prawnym Organizacji Narodów Zjednoczonych kwestii ochrony danych osobowych dotyczy rezolucja 34/169 przyjęta przez Zgromadzenie Ogólne ONZ 17.12.1979 r. – Kodeks postępowania funkcjonariuszy porządku prawnego. W powołanym dokumencie sformułowano dyrektywy dla funkcjonariuszy odpowiadających za dostęp do danych osobowych. Odwołując się z kolei do aktów prawnych wydanych przez Radę Europy, szczególne znaczenie należy w systemie prawnym Rady Europy przypisać rezolucji Komitetu Ministrów Nr 73/22 z 26.9.1973 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym oraz rezolucji Komitetu Ministrów Nr 74/29 z 20.9.1974 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze publicznym. Nie bez znaczenia pozostają również wytyczne europejskiej Organizacji Współpracy Go-

spodarczej i Rozwoju w sprawie ochrony prywatności i przepływu danych osobowych pomiędzy krajami (Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data z 23.9.1980 r., Internationaler und europäischer Datenschutz. Materialien zum Datenschutz, Berlin 1996, s. 21–24). Ujęcie ochrony danych osobowych w powołanych powyżej aktach prawnych wewnątrzpaństwowych oraz międzynarodowych bez wątpienia nadawało jej od samego początku status jednego z najważniejszych praw człowieka i podstawowych wolności (*M. Krzysztofek*, Ochrona, s. 36).

II. Konwencja Nr 108

1. Unia Europejska w początkowym okresie swojego działania nie dostrzegała potrzeby przyjęcia ogólnych ram prawnych ochrony danych osobowych, poprzestając na Konwencji Nr 108 Rady Europy z 28.1.1981 r. o ochronie osób ze względu na automatyczne przetwarzanie danych o charakterze osobowym (Dz.U. z 2003 r. Nr 3, poz. 25), przyjętej jednak nie przez UE, lecz właśnie przez Radę Europy (*J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych. Komentarz, Warszawa 2011, s. 83). Konwencję w skali międzynarodowej uważa się za pierwszy akt prawny z dziedziny ochrony danych osobowych. Konwencja przyjęta przez Radę Europy nie stanowi źródła prawa unijnego. Mimo to jej zupełne pominięcie w tym miejscu w ocenie autorów nie jest możliwe, a to z uwagi na częste powoływanie się na jej treść wprost w przepisach unijnych. Tylko tytułem przykładu należy wskazać, że zgodnie z treścią motywu 11 preambuły do dyrektywy 95/46/WE „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 28 stycznia 1981 r. w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych". Postanowienia konwencji oddziałują jednak jedynie w sferze publicznoprawnej, nie wywołują natomiast żadnych skutków prawnych bezpośrednio po stronie obywateli państw, które ją ratyfikowały (*J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych. Komentarz, Kraków 2004, s. 71; por. także *A. Mednis*, Ochrona danych, s. 31). **4**

III. Ochrona danych osobowych w prawie Unii Europejskiej

1. Prawo pierwotne Unii Europejskiej

1. Ogólnym podziałem źródeł prawa wydawanych przez organy i instytucje unijne jest podział na prawo pierwotne, a więc tzw. traktatowe, oraz prawo wtórne. Mówiąc najogólniej, normy prawa pierwotnego zawarte są w traktatach unijnych, a prawo wtórne to wydane na ich podstawie dyrektywy, rozporządzenia oraz decyzje. Nie ulega wątpliwości, że po Traktacie lizbońskim [Traktat zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13.12.2007 r. (Dz.Urz. UE C 306, s. 1)] źródłami prawa pierwotnego UE przyznającymi jej kompetencje do objęcia swoją regulacją ochrony danych osobowych są postanowienia TUE, TFUE oraz KPP. Na wstępie należy jednak wskazać, że przed wejściem w życie TL, z uwagi na filarową konstrukcję UE, prawodawstwo dotyczące ochrony danych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości było podzielone pomiędzy I filar (ochrona danych do celów prywatnych i handlowych – z wykorzystaniem metody wspólnotowej) a III filar **5**

(ochrona danych do celów egzekwowania prawa – na poziomie międzyrządowym). Przetwarzanie danych osobowych w ramach I filaru UE zostało objęte spójnymi regulacjami, wynikającymi przede wszystkim z dyrektywy 95/46/WE. Szczególnej regulacji poddana została jednak ochrona danych osobowych przetwarzanych przez organy i instytucje unijne. W prawie pierwotnym zasadniczą rolę przypisać należało bowiem w tym zakresie art. 286 TWE. Zgodnie z treścią powołanego przepisu „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". Powołany przepis, mimo że nie miał charakteru normy bezpośrednio skutecznej, uzupełniał system stworzony w głównej mierze przez dyrektywę 95/46/WE w taki sposób, że rozszerzał zakres podmiotowy obowiązku ochrony danych osobowych również na instytucje i organy UE (ówczesnej Wspólnoty) [*K. Karasiewicz*, Komentarz do art. 286, w: Traktat ustanawiający Wspólnotę Europejską. Komentarz (red. *A. Wróbel*), t. 3, Warszawa 2010, s. 841]. Powołane postanowienie traktatowe nie nałożyło jednak na państwa członkowskie zobowiązania do ochrony danych osobowych swoich obywateli, ale wskazało jedynie na potrzebę przeniesienia istniejących standardów w tym względzie również na poziom instytucji wspólnotowych (*A. Gajda*, Ochrona danych osobowych i kierunki zmian w tej dziedzinie w prawie Unii Europejskiej, Kwartalnik Kolegium Ekonomiczno-Społecznego „Studia i Prace" 2014, Nr 4, s. 70). W prawie pierwotnym nie było natomiast żadnej podstawy prawnej, która umożliwiłaby przyjęcie ogólnych regulacji ochrony danych w ramach III filaru. Uwzględniając powyższe, przyjmowane były *ad hoc* regulacje szczegółowe dotyczące ochrony danych osobowych zawarte w różnych aktach prawnych tworzonych w ramach współpracy policyjnej i sądowej w sprawach karnych. W tym zakresie regulacje ochrony danych osobowych były (oraz są obecnie) rozproszone i znajdują się w aktach prawnych regulujących poszczególne systemy informacyjne oraz wymianę określonych kategorii informacji [decyzja ramowa Rady 2006/960/WSiSW z 18.12.2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej (Dz.Urz. UE L 386, s. 89)] – przybierając głównie formę decyzji oraz decyzji ramowych niewywierających bezpośredniego skutku. Najogólniejszym aktem w tym zakresie jest wydana 27.11.2008 r. decyzja ramowa Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.Urz. UE L 350, s. 60). Rozwiązanie przyjęte do wejścia w życie TL skutkowało więc fragmentaryzacją zasad ochrony danych osobowych. Traktat lizboński wprowadził w tym zakresie znaczącą zmianę, znosząc strukturę filarową w UE oraz wprowadzając ogólną podstawę prawną do przyjęcia jednolitych ram prawnych ochrony danych osobowych w art. 16 TFUE i obejmując nimi dawne filary UE: I oraz III.

6 2. Zgodnie z kolei z treścią powołanego art. 16 ust. 1 TFUE każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Ustęp 2 tego przepisu wskazuje natomiast, że 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. Należy się zgodzić z *J. Sobczakiem*, że źródła wskazanego powyżej przepisu upatrywać należy w powołanym już art. 286 TWE, w którym poszerzono zakres podmiotowy obowiązku

ochrony danych osobowych na instytucje i organy Unii, w zakresie, w jakim stosują prawo UE [*J. Sobczak*, Komentarz do art. 16, w: Traktat o funkcjonowaniu Unii Europejskiej. Komentarz (red. *D. Miąsik*, *N. Półtorak*, *A. Wróbel*), t. 1, Warszawa 2012, s. 329]. Powołany przepis znajduje więc zastosowanie do przetwarzania danych osobowych zarówno przez państwa członkowskie, jak i organy oraz instytucje unijne. Zamieszczenie art. 16 TFUE w Tytule II TFUE „Postanowienia ogólne" nie pozostawia wątpliwości, że ma on stanowić samodzielną podstawę prawną ochrony danych osobowych jako jednego z fundamentalnych praw w UE, wywierającą horyzontalny skutek w tym zakresie. Ogólny charakter tego przepisu oznacza więc, że znajduje zastosowanie zarówno do organów i instytucji UE, jak i państw członkowskich, a w tym drugim przypadku również do podmiotów z sektora prywatnego (*A. Grzelak*, Projekt reformy ochrony danych osobowych – czy rzeczywiście powstanie jednolity i spójny system?, Kwartalnik Kolegium Ekonomiczno-Społecznego „Studia i Prace" 2014, Nr 4, s. 95). W związku z powyższym z chwilą wejścia w życie Traktatu lizbońskiego UE, znosząc strukturę filarową, wprowadziła jedną wspólną podstawę ochrony danych osobowych. Powołany przepis stanowi więc źródło do objęcia „zrewidowanymi unijnymi ramami ochrony danych osobowych zarówno transgranicznego, jak i krajowego przetwarzania danych osobowych" (*A. Gajda*, Ochrona danych osobowych, s. 89). Celem UE było więc objęcie jednym przepisem całości prawa unijnego, z tym zastrzeżeniem, że wyłączona została możliwość jego zastosowania do dawnego II filaru, tj. polityki zagranicznej i bezpieczeństwa (art. 39 TUE). Dodatkowo, zgodnie z dołączoną do TL deklaracją Nr 20, w przypadku wydania na podstawie art. 16 TFUE aktów prawa wtórnego mających wpływ na bezpieczeństwo narodowe okoliczność ta powinna być „należycie wzięta pod uwagę". Z kolei zgodnie z deklaracją Nr 21 konieczne może się okazać wprowadzenie zasad szczególnych dotyczących ochrony danych osobowych i swobodnego przepływu tych danych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, zapewnianej na podstawie art. 16 TFUE, ze względu na szczególny charakter tych dziedzin. W kwestiach związanych z bezpieczeństwem wewnętrznym państwa członkowskie zarezerwowały sobie zatem furtkę do przyjęcia własnych środków dotyczących wolności, bezpieczeństwa i sprawiedliwości, a związanych z ochroną danych osobowych (*F. Boehm*, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, Berlin 2014, s. 112).

7 3. Odnosząc się do współpracy policyjnej w sprawach karnych (a więc dawnego III filaru), nie sposób również nie wskazać, że wejście w życie TL nie spowodowało automatycznego wyłączenia z porządku prawnego dyrektywy 95/46/WE, która nie znajduje z kolei zastosowania do współpracy policyjnej i sądowej w sprawach karnych (art. 3 ust. 2). Jak zostało to już jednak zauważone, z uwzględnieniem wskazanych wyjątków art. 16 TFUE stanowi bezpośrednią podstawę ochrony danych osobowych na obszarze UE, w tym do przyjęcia przez organy unijne jednolitych ram ochrony danych osobowych, również zastępujących dyrektywę 95/46/WE. Powyższe nie oznacza jednak ograniczenia swobodnego przepływu danych, który we wskazanej dyrektywie ma na celu stymulowanie rynku wewnętrznego państw członkowskich. Jak wskazuje się w literaturze przedmiotu, jest wręcz odwrotnie – art. 16 ust. 2 TFUE stanowi podstawę prawną do przyjęcia jednolitych zasad ochrony danych osobowych, w tym w zakresie „przepływu danych" nie tylko w kontekście rynku wewnętrznego, ale „w całym spektrum działania Unii Europejskiej" (*G.G. Fuster*, The Emergence of Personal Data Protection as a Fundamental Right of the EU,

Berlin 2014, s. 234). W literaturze przedmiotu wskazuje się, że art. 16 ust. 1 TFUE ma charakter normy bezpośrednio skutecznej, przyznającej ochronę danym osobowym dotyczącym jednostek nawet w razie braku jakiegokolwiek aktu prawa wtórnego w tym zakresie (*F. Boehm*, Information, s. 120). Jak wskazują *H. Hijmans* oraz *A. Scirocco*, bezpośrednią skuteczność art. 16 TFUE wyinterpretować można również z orzecznictwa TSUE, który przyznał taki status art. 21 TFUE (prawo do swobodnego przemieszczania się i przebywania na terytorium państw członkowskich), odpowiadającemu stopniem precyzyjności art. 16 TFUE (*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, Nr 5, s. 1517–1518). Na podstawie art. 39 TUE państwa członkowskie przyznały Radzie kompetencję do przyjęcia decyzji określającej zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres wspólnej polityki zagranicznej i bezpieczeństwa oraz zasady dotyczące swobodnego przepływu takich danych. Powołany przepis ma więc charakter czysto proceduralny i wprowadza szczególną formę przyjęcia ogólnych zasad ochrony danych osobowych wyłącznie w zakresie wspólnej polityki zagranicznej i bezpieczeństwa, z pominięciem Parlamentu Europejskiego. Podstawą do uregulowania zasad przetwarzania danych osobowych w pozostałych obszarach jest jedynie będący przedmiotem uprzedniej analizy art. 16 TFUE. Mimo – jak jest to dalej wskazane – horyzontalnego charakteru art. 16 TFUE art. 39 TUE wprowadza odstępstwo od niego, polegające na rezygnacji z ogólnego modelu przyjmowania zasad dotyczących ochrony danych osobowych w drodze wspólnego procesu decydowania przez Parlament i Radę. Uwzględniając powyższe, należy się zgodzić z poglądem wyrażonym przez *H. Blanka* oraz *M. Stelio*, że art. 39 TUE, choć umieszczony w TUE, jest w rzeczywistości przepisem typu mieszanego, ponieważ reguluje relacje instytucjonalne i proceduralne dotyczące podejmowania decyzji w Unii [*H. Blank*, *M. Stelio*, The Treaty on European Union (TEU). A Commentary, Berlin 2013, s. 1163]. Powołany przepis stanowi swoiste *novum* i próżno szukać jego odpowiednika w jakichkolwiek dotychczasowych źródłach prawa pierwotnego UE. Zgodzić się należy z poglądem *Z. Brodeckiego*, że „artykuł 39 TUE zobowiązuje Radę do konsultacji z Parlamentem przed uchwaleniem decyzji ramowej mającej na celu zbliżenie przepisów ustawodawczych i wykonawczych państw członkowskich, decyzji uchwalanych w każdym innym celu oraz ustanowienie konwencji, których przyjęcie zaleca się państwom członkowskim, zgodnie z ich właściwymi regułami konstytucyjnymi" [*Z. Brodecki*, Komentarz do art. 39 Traktatu o Unii Europejskiej, w: Traktat o Unii Europejskiej. Traktat ustanawiający Wspólnotę Europejską (red. *Z. Brodecki*), Warszawa 2006, s. 99]. Na szczególną uwagę zasługuje uzasadnienie podjęcia przez ustawodawcę unijnego decyzji o objęciu wspólnej polityki zagranicznej i bezpieczeństwa szczególną procedurą. Jest to istotne również ze względu na to, że wyłączona została tutaj możliwość podjęcia stosownej wykładni przez TSUE, który zgodnie z treścią art. 275 TFUE (oraz art. 24 ust. 1 TUE) nie jest właściwy w zakresie postanowień dotyczących wspólnej polityki zagranicznej i bezpieczeństwa ani w zakresie aktów przyjętych na ich podstawie. Podejmowane więc w tej sferze decyzje Rady oraz podstawy prawne ich wydania nie podlegają wykładni Trybunału. Zgodnie z kolei z orzecznictwem TSUE każdy wyjątek od zasady – którym bez wątpienia w stosunku do art. 16 TFUE jest art. 39 TUE – powinien być intepretowany maksymalnie ściśle. Jak się wydaje, głównym

celem założenia polegającego na przyjęciu prawnych rozwiązań dotyczących ochrony danych osobowych na etapie międzyrządowym jest chęć użycia jednego instrumentu harmonizującego ochronę danych osobowych przy jednoczesnym pozostawieniu jak najwięcej decyzyjności po stronie samych państw członkowskich, które z drugiej strony mogą w razie swojej dezaprobaty zawetować podjęte rozwiązanie. Mimo że do chwili przygotowania niniejszego komentarza Rada nie wydała decyzji, o której mowa w art. 39 TUE, należy się zgodzić z *H. Blankiem* oraz *M. Stelio*, że dotychczasowe doświadczenia [w tym z wydania decyzji Rady 2008/977/WSiSW z 27.11.2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz.Urz. UE L 350, s. 60)] pokazują tendencję do przyznawania w takich decyzjach dużej swobody decyzyjnej państwom członkowskim – wyrazić należy jedynie nadzieję, że decyzja będzie regulowała co najmniej szczegółowo zasady przetwarzania danych (*H. Blank*, *M. Stelio*, The Treaty, s. 1165–1166).

4. W prawie UE ochrona danych osobowych sformułowana została również w art. 8 **8**
KPP, przyjętej w grudniu 2000 r. w Nicei. Do wejścia w życie Traktatu lizbońskiego KPP mogła być zakwalifikowana jedynie jako niewiążąca deklaracja moralności europejskiej. Z chwilą rozpoczęcia obowiązywania TL Karcie została nadana moc prawna równa TFUE oraz TUE i z tą chwilą stała się jednym z prawnych filarów UE. Karta, oprócz ogólnych postanowień dotyczących ochrony prywatności (art. 7 KPP), zawiera regulacje mówiące wprost o ochronie danych osobowych. Zgodnie bowiem z treścią art. 8 ust. 1 KPP każdy ma prawo do ochrony danych osobowych, które go dotyczą. Zamieszczenie obu wskazanych przepisów, tj. art. 7 i 8 KPP, obok siebie podkreśla jedynie utrwalony już w orzecznictwie unijnym oraz literaturze przedmiotu fakt nierozerwalnego związku pomiędzy ochroną prywatności a ochroną danych osobowych (zob. *A. Gajda*, Ochrona danych osobowych, s. 77; wyr. TSUE z 9.11.2010 r., C-92/09 i C-93/09, EU:C:2010:662, pkt 52). Powyższe podkreśla również ustawodawca unijny w motywie 10 preambuły do dyrektywy 95/46/WE, wskazując że „celem przepisów prawa dotyczących ochrony danych osobowych jest ochrona podstawowych praw i wolności, szczególnie prawa do prywatności". Zgodnie z treścią art. 8 KPP dane muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Powołany przepis wskazuje więc warunki, których spełnienie legalizuje przetwarzanie danych osobowych, konstytuując zasadę legalności takiego przetwarzania. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Z kolei na podstawie ust. 3 powołanego przepisu przestrzeganie tych zasad podlega kontroli niezależnego organu. Rozwinięciem i uzupełnieniem art. 8 KPP jest z kolei wspomniany już powyżej art. 16 ust. 1 TFUE [*J. Sobczak*, Komentarz do art. 8, w: Karta Praw Podstawowych Unii Europejskiej. Komentarz (red. *A. Wróbel*), Warszawa 2013, s. 295]. Odnosząc się do mocy prawnej powołanej normy, w pierwszej kolejności przywołać należy słynny wyr. TSUE z 13.5.2014 r. (C-131/12, EU:C:2014:317). W tym orzeczeniu Trybunał wskazał, że wykładnia przepisów regulujących przetwarzanie danych osobowych mogąca naruszyć podstawowe wolności, „a w szczególności prawo do prywatności, musi być bezwzględnie dokonywana z punktu widzenia praw podstawowych, które zgodnie z utrwalonym orzecznictwem stanowią część składową ogólnych zasad prawnych, których przestrzeganie zapewnia Trybunał i które zostały zawarte w karcie". Zgodzić się należy z wyrażonymi w literaturze przedmiotu poglądami, że w powołanym wyroku Trybunał przyznał

prawu do prywatności oraz prawu do ochrony danych osobowych skutek bezpośredni w stosunkach horyzontalnych, jednak uzasadnił to tym, że powołane prawa podstawowe stanowią ogólne zasady prawa UE (*M. Kręcisz*, Glosa do wyroku TS z 13.5.2014 r., C-131/12, Lex 2014). Trybunał nie odwołał się jednak w tym zakresie do samej mocy prawnej Karty, która z chwilą wejścia w życie TL stała się źródłem prawa pierwotnego UE. W literaturze przedmiotu podnosi się również, że Trybunał, wypowiadając się w przedmiocie charakteru prawnego art. 8 KPP, nie uwzględnił art. 11 KPP, konstytuującego prawo do wypowiedzi, które może w pewnych przypadkach stać w sprzeczności z samą ochroną danych osobowych. Uwzględniając powyższe, jak wskazuje *M. Czerniawski*, „przyznanie przez Trybunał niemal bezwzględnego prymatu prawu do ochrony danych osobowych bez przeprowadzenia analizy w zakresie art. 11 karty, należy ocenić krytycznie" (*M. Czerniawski*, Glosa do wyroku TS z 13.5.2014 r., C-131/12, Lex 2015). Wynikające z KPP prawo do ochrony danych osobowych nie ma również charakteru absolutnego i może podlegać pewnym ograniczeniom. Po pierwsze, zgodnie ze stanowiskiem wyrażonym przez TSUE „prawo do ochrony danych osobowych nie stanowi prerogatywy o charakterze absolutnym i powinno być oceniane w świetle jego funkcji społecznej" (wyr. TSUE z 5.5.2011 r., C-543/09, EU:C:2011:279, pkt 51). Jak wskazał Trybunał w innym z wydanych przez siebie wyroków, „wykonanie tych praw może być więc przedmiotem ograniczeń w zakresie, w jakim ograniczenia te są rzeczywiście podyktowane względami interesu ogólnego i nie stanowią dysproporcjonalnej i niedopuszczalnej ingerencji naruszającej istotę chronionych praw, przy uwzględnieniu celu realizowanego przez te ograniczenia" (wyr. TSUE z 12.6.2003 r., C-112/00, EU:C:2003:333). Po drugie, art. 52 ust. 1 KPP dopuszcza wprowadzenie ograniczeń w wykonywaniu praw, takich jak prawa ustanowione w art. 7 i 8 Karty, 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. Przykładem takiego ograniczenia przewidzianego przez krajowego ustawodawcę jest art. 34 pkt 2 OchrDanychU, zgodnie z którym administrator może odmówić podmiotowi danych dostępu do jego danych, gdy przemawia za tym „zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego". Preambuła do dyrektywy 95/46/WE w motywie 10 wskazuje z kolei przykładowo, że państwa członkowskie muszą być również uprawnione – w sytuacjach, gdy jest to uzasadnione ważnym interesem publicznym – do uchylania zakazu przetwarzania sensytywnych kategorii danych w takich dziedzinach, jak zdrowie publiczne i ochrona socjalna. O ile prawo do ochrony danych osobowych ma charakter prawa podstawowego UE, o tyle nie jest absolutne, na wzór np. zakazu przeprowadzania tortur. Warto również wskazać, że Karta uzyskała moc obowiązującą dopiero z chwilą wejścia w życie TL, a przestrzeganie zawartych w niej zasad ochrony danych osobowych wymuszone zostało przepisami dyrektywy 95/46/WE, w szczególności jej art. 6, 7, 12, 14 i 28. Trybunał wielokrotnie powoływał się na wskazane przepisy, uznając je za czyniące zadość wymogom stawianym w art. 8 KPP. Na przykład w wyr. z 17.7.2014 r. (C-141/12 i C-371/12, EU:C:2014:2081) Trybunał stwierdził, że art. 12 dyrektywy 95/46/WE, pozostający w całości zgodny z art. 8 Karty, należy interpretować w taki sposób, że osoba korzystająca ze swojego prawa dostępu do danych osobowych powinna uzyskać „dostęp do wszystkich danych osobowych jej dotyczących, które są przedmiotem przetwarzania przez krajowe władze administracyjne" (w stanie faktycznym, którego

dotyczył wspomniany wyrok, chodziło o dostęp do dokumentów pobytowych). Warto podkreślić, że KPP ma zastosowanie zarówno do organów i instytucji unijnych, jak i organów państw członkowskich, stąd ochrona danych osobowych podniesiona została do rangi prawa podstawowego całej Unii, niezależnie od dawnej struktury filarowej (zob. *A. Gajda*, Ochrona danych osobowych, s. 77).

2. Dyrektywa 95/46/WE

1. Prace nad pierwszym kompleksowym ujęciem ochrony danych osobowych **9**
w akcie prawnym UE trwały więc dopiero od 1990 r., a ich efektem było przyjęcie przez Wspólnotę 24.10.1995 r. dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych. Podstawą prawną przyjęcia tej dyrektywy był art. 100a TWE (po zmianach wprowadzonych Jednolitym aktem europejskim – umową międzynarodową z 1986 r. zawartą w ramach Wspólnot Europejskich wprowadzającą pierwszą znaczącą modyfikację TWE – art. 95 TWE). Zgodnie z treścią art. 95 TWE Rada uprawniona była do przyjęcia środków dotyczących zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego. Jak wskazuje *K. Kowalik-Bańczyk*, „dobrym przykładem szerokiego traktowania zagadnień podlegających harmonizacji na podstawie art. 95 może być dyrektywa 95/46 o ochronie danych osobowych" [*K. Kowalik-Bańczyk*, Komentarz do art. 95 Traktatu ustanawiającego Wspólnotę Europejską, w: Traktat ustanawiający Wspólnotę Europejską Komentarz (red. *A. Wróbel*), t. 2, Warszawa 2010, s. 660]. Obecnie podstawą prawną harmonizacji ogólnych zasad ochrony danych osobowych dokonanej na podstawie dyrektywy jest z kolei art. 16 TFUE. Warto w tym miejscu jeszcze wskazać, że wszystkie państwa członkowskie Wspólnoty zobowiązane były do implementacji postanowień dyrektywy nie później niż w terminie do 23.10.1998 r. Przedmiotem niniejszej części Wprowadzenia jest więc charakterystyka wskazanej dyrektywy, a w dalszej części – innych najważniejszych aktów unijnego prawa wtórnego mających wpływ na ochronę danych osobowych.

2. Dyrektywa definicje podstawowych terminów odnoszących się do dziedziny **10**
danych osobowych oraz ustala zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych. Określa także zasady i warunki zgodności przetwarzania danych osobowych z prawem oraz prawa osób, których dane dotyczą. Mimo stałego postępu nowych technologii zagadnienia te pozostały aktualne do dnia dzisiejszego i w wersji mocno zmodyfikowanej oraz poszerzonej zostały w znacznej mierze przeniesione do RODO, zawierającego ogólne regulacje w zakresie ochrony danych. Mimo że wstępne rozważania dotyczące RODO przedstawiono w dalszej części niniejszego Wprowadzenia, już w tym miejscu warto wskazać, że motywy uzasadniające konieczność przyjęcia dyrektywy łudząco przypominają wprowadzone przez Komisję do projektu RODO. RODO stanowi więc bez wątpienia kontynuację działania podjętego już w 1995 r. przez organy unijne, jednak wtedy na dużo mniejszą skalę, a zmierzającego jedynie do zbliżenia ustawodawstw celem upodobnienia gwarantowanej przez nie ochrony danych. Przykładowo, zgodnie z motywem 4 preambuły do dyrektywy 95/46/WE „coraz częściej we Wspólnocie korzysta się z przetwarzania danych osobowych w różnych sferach życia gospodarczego i społecznego; postęp w dziedzinie technologii informatycznych sprawia, że przetwarzanie i wymiana takich danych stają się coraz łatwiejsze". Zgodnie z kolei z motywem 5 preambuły do

RODO „szybki rozwój technologiczny i globalizacja przyniosły nowe wyzwania w zakresie ochrony danych osobowych. Niezwykle wzrosła skala wymiany i zbierania danych", co wymusiło stworzenie nowych ram prawnych ochrony danych. Głównym uzasadnieniem przyjęcia ram prawnych zawartych w dyrektywie, podobnie jak tych zawartych w RODO, był więc stały rozwój nowych technologii. Mimo to należy się zgodzić z *S. Szmakiem*, że dyrektywa jest technologicznie neutralna – jej postanowienia mają bowiem zastosowanie bez względu na wykorzystywane do przetwarzania danych środki technologiczne [*S. Szmak*, Europejskie standardy w zakresie ochrony danych osobowych – zarys problemu, w: Prawna ochrona danych osobowych w Polsce na tle europejskich standardów (red. *G. Goździewicz*, *M. Szabłowska*), Toruń 2008, s. 169]. Na uwagę zasługuje również fakt, że ustawodawstwo wewnętrzne państw członkowskich dotyczące ochrony danych, powstałe w dużej części po wdrożeniu Konwencji Nr 108, okazało się bardzo zróżnicowane (*D. Fleszer*, Zakres przetwarzania danych osobowych w działalności gospodarczej, Warszawa 2008, s. 17). Zatem w celu wyeliminowania przeszkód dla swobodnego przepływu danych bez równoczesnego zmniejszania ich ochrony (*S. Szmak*, Europejskie standardy, s. 169) oraz dla upodobnienia porządków prawnych państw członkowskich w tym zakresie wdrożono dyrektywę 95/46/WE. Ustawodawca unijny, przeprowadzając w 1995 r. reformę ochrony danych osobowych, wybrał jednak najłagodniejszy z możliwych instrumentów, przyjmując dyrektywę zakładającą tzw. harmonizację minimalną. Dyrektywa 95/46/WE dopuszcza więc w dużym stopniu swobodę państw członkowskich w jej implementacji.

11 3. Dokonując krótkiej charakterystyki dyrektywy 95/46/WE, w pierwszej kolejności należy wskazać, że bez wątpienia celem jej wydania było pogodzenie interesów podmiotów informacji oraz interesów administratorów wykorzystujących dane osobowe w swojej działalności (*P. Fajgielski*, Ochrona, s. 34). Znajduje ona zastosowanie do wszelkich operacji lub zestawu operacji dokonywanych na danych osobowych, określanych jako przetwarzanie danych. Dyrektywa dotyczy danych przetwarzanych automatycznie oraz będących częścią lub mających być częścią nieautomatycznych zbiorów danych, w których informacje dostępne są na podstawie określonych kryteriów. Odwołując się z kolei do terminologii wprowadzonej przez art. 2 dyrektywy, dane osobowe powinny być rozumiane jako informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Dyrektywa konstytuuje obowiązek notyfikacyjny względem podmiotów danych polegający na konieczności poinformowania ich o fakcie przetwarzania danych. Każdej z osób, której dane osobowe dotyczą, przyznane zostało również prawo dostępu do ich treści i sprzeciwu wobec ich przetwarzania (o ile to możliwe, a przetwarzanie danych nie jest wymuszone np. przepisami prawa). Ustawodawca unijny zdecydował się również na objęcie pewnych kategorii danych szczególną ochroną z uwagi na ich wyjątkowy związek ze sferą intymności człowieka. Do kategorii tych należą dane dotyczące pochodzenia etnicznego lub rasowego, poglądów politycznych, przekonań religijnych, członkostwa w związkach zawodowych oraz informacje o szeroko rozumianym stanie zdrowia i życiu seksualnym. Dyrektywa zobowiązuje również administratorów danych do przedsięwzięcia odpowiednich technicznych oraz organizacyjnych środków ochrony przetwarzanych przez nich danych osobowych. Konstruuje ona również zasady przetwarzania danych, w tym najważniejszą zasadę legalności oraz celowości przetwarzania danych. W świetle pierwszej z nich dane osobowe powinny być przetwarzane zgodnie z prawem, a drugiej – zgodnie z celami, dla jakich zostały zebrane. Na szczególną uwagę zasługuje jednak fakt, że mimo rozbudowanych postanowień dotyczących zasad przetwarzania

danych osobowych dyrektywa nie wyeliminowała rozdrobnienia ustawodawstw państw członkowskich w tym zakresie. Po pierwsze bowiem przepisy krajowe w niektórych przypadkach mogą dopuszczać wyjątki od postanowień dyrektywy. Mogą one dotyczyć m.in. przesłanek legalizujących przetwarzanie szczególnych kategorii danych osobowych (art. 8 ust. 4 dyrektywy 95/46/WE), prawa dostępu do danych (art. 12 ust. 2 dyrektywy 95/46/WE) czy obowiązku notyfikowania faktu przetwarzania danych właściwemu organowi państwowemu (art. 18 ust. 3 dyrektywy 95/46/WE). Wyjątki mogą objąć m.in. sytuacje, gdy uzasadnione jest to bezpieczeństwem narodowym, obronnością, czynnościami dochodzeniowo-śledczymi, związanymi z egzekwowaniem prawa karnego lub ochroną osób, których dane dotyczą. Po drugie, dyrektywa jest instrumentem wiążącym państwa członkowskie wyłącznie co do wskazanego w niej celu, pozostawiając im swobodę w wyborze środków realizujących takie cele. Ma to szczególne znaczenie w przypadku dyrektyw zakładających tzw. harmonizację minimalną, jaka właśnie występuje w dyrektywie 95/46/WE. Na uwagę zasługuje również to, że w ocenie części przedstawicieli doktryny z uwagi na dużą swobodę w jej implementacji dyrektywa nie wyznacza nawet minimalnego standardu ochrony (*P. Barta*, *P. Litwiński*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2013, s. 5–6). Powyższe zdeterminowało fakt, że państwa członkowskie w swoich ustawodawstwach bardzo różnie zdefiniowały nawet podstawowe instytucje ochrony danych osobowych. Tytułem przykładu, w świetle art. 8 ust. 1 dyrektywy 95/46/WE do kategorii danych objętych szczególną ochroną należą dane ujawniające pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, jak również dotyczące zdrowia i życia seksualnego. Polska OchrDanychU w art. 27 poszerzyła jednak wskazany katalog, uznając, że danymi takimi są również dane o kodzie genetycznym oraz „dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym". Podobne rozwiązanie przyjęła brytyjska ustawa o ochronie danych osobowych, która za dane wrażliwe uznała informacje związane z karalnością danej osoby. Litwa zdecydowała się z kolei na niemal literalne przeniesienie do ustawy krajowej art. 8 ust. 1 dyrektywy 95/46/WE (zob. art. 2 litewskiej ustawy o ochronie danych osobowych z 21.1.2003 r., Nr IX-1296, Wilno). Powyższe znajduje swoje źródło w – jak zostało to już wskazane – minimalnej harmonizacji przewidzianej w dyrektywie. Zgodnie bowiem z motywem 4 preambuły do dyrektywy 95/46/WE „Państwa Członkowskie będą miały pozostawiony margines swobody działania, z którego mogą również, w kontekście wykonania dyrektywy korzystać partnerzy handlowi i społeczni". Z kolei zgodnie z motywem 44 „Państwa Członkowskie mogą również, na mocy przepisów prawa wspólnotowego, odstąpić od przepisów niniejszej dyrektywy odnośnie do prawa dostępu, obowiązku informowania obywateli oraz jakości danych w celu zapewnienia realizacji niektórych celów". Uwzględniając wskazaną powyżej treść dyrektywy 95/46/WE, nie można się więc zgodzić z wyr. TSUE z 24.11.2011 r. (C-468/10 i C-469/10, EU:C:2011:777, pkt 29), w którym wskazał on, że „harmonizacja ustawodawstw krajowych, których dotyczy dyrektywa 95/46 (...) nie ogranicza się do minimalnego jej zakresu, lecz prowadzi do harmonizacji, która jest co do zasady pełna". Ustawodawca unijny w zbyt wielu postanowieniach dyrektywy wskazuje bowiem wprost na swobodę państw członkowskich w jej implementacji, czego wyrazem są zresztą znaczne odrębności pomiędzy normami prawa krajowego państw członkowskich w tym zakresie.

IV. Unijna reforma ochrony danych osobowych

1. Założenia reformy ochrony danych osobowych

12 1. Rozwój nowych technologii wiąże się ze stale narastającą liczbą problemów prawnych, których główną przyczyną jest nienadążanie krajowego oraz unijnego ustawodawstwa za nowymi wyzwaniami, związanymi z powszechną cyfryzacją rzeczywistości. Coraz to nowsze rozwiązania technologiczne nie tylko podważają w praktyce dotychczasowe znaczenie fundamentalnych pojęć w dziedzinie ochrony danych osobowych, lecz także wymusiły konieczność stworzenia podstawowych ram prawnych ich funkcjonowania. Odpowiedzią na powyższe był projekt Komisji Europejskiej pakietu ustawodawczego z 25.1.2012 r. mającego za zadanie aktualizację i modernizację zasad ochrony danych wynikających z dyrektywy 95/46/WE. Doszło bowiem do rozwarstwienia między zakresem regulacji ochrony danych osobowych a możliwym do osiągnięcia na ich podstawie stopniem ich ochrony, ze względu, jak zostało to wskazane, na zdecydowanie inne warunki przetwarzania informacji w stosunku do okresu, w którym weszła w życie dyrektywa 95/46/WE.

13 2. Pakiet, oprócz komunikatu dotyczącego głównych celów działań Komisji, zawierał dwa wnioski ustawodawcze – dotyczące RODO oraz dyrektywy w sprawie ochrony danych osobowych przetwarzanych dla celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz pokrewnych działań wymiaru sprawiedliwości (projekt dyrektywy Parlamentu Europejskiego i Rady z 25.1.2012 r. w sprawie ochrony danych osobowych przetwarzanych dla celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz pokrewnych działań wymiaru sprawiedliwości, COM (2012) 010, https://eur\=lex.europa.eu/legal\=content/PL/TXT/PDF/?uri=CELEX:52012PC0010\&from=ES (dostęp: 29.3.2021 r.); zob. *A. Grzelak*, Projekt ochrony danych osobowych w sprawach karnych w UE – kolejny krok na drodze do społeczeństwa nadzorowanego?, EPS 2012, Nr 11, s. 20–28).

14 3. Odnosząc się do prac nad projektem RODO, należy wskazać, że głosowanie nad sprawozdaniem dotyczącym tego projektu, które zostało przygotowane w Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE), odbyło się 21.10.2013 r. Projekt Komisji LIBE został przyjęty przez Parlament Europejski 12.3.2014 r. zdecydowaną większością głosów (za projektem opowiedziało się 621 parlamentarzystów). W dniu 11.6.2015 r. Rada UE przyjęła tzw. ogólne podejście w sprawie projektu rozporządzenia ogólnego, otwierając tym samym drogę do rozpoczęcia się trilogu, czyli negocjacji pomiędzy Parlamentem oraz Radą UE przy udziale Komisji Europejskiej. Ostateczny tekst RODO został zatwierdzony przez Komisję LIBE Parlamentu oraz Komitet Stałych Przedstawicieli Komisji (COREPER) w grudniu 2015 r. Organy unijne, z uwagi na skomplikowany proces transpozycji RODO do krajowych porządków prawnych państw członkowskich, podjęły jednak polityczną decyzję o odroczeniu dalszych procesów legislacyjnych. Ogólne rozporządzenie o ochronie danych zostało przyjęte przez Parlament Europejski dopiero 14.4.2016 r.

15 4. Komisja w uzasadnieniu swojego wniosku ustawodawczego dotyczącego RODO wskazała (wniosek Komisji z 27.1.2012 r. w sprawie rozporządzenia w sprawie ochrony osób fizycznych, s. 4), że przyjęcie nowych ram prawnych ochrony danych osobowych

zostało wymuszone przez stały rozwój technologiczny, który umożliwia zarówno przedsiębiorstwom prywatnym, jak i organom publicznym wykorzystywanie danych osobowych do wykonywania powierzonych im zadań na niespotykaną dotąd skalę. Ponadto podkreśliła, że istnieje potrzeba dostosowania obecnych ram, by móc lepiej reagować na wyzwania stawiane przez szybki rozwój nowych technologii (zwłaszcza Internetu) i postępującą globalizację. Komisja zaznaczyła jednak, że przyjęte przez nią rozwiązania prawne muszą zostać skonstruowane przy jednoczesnym zachowaniu technologicznej neutralności ram prawnych. Jak się wydaje, należy to interpretować w ten sposób, że unijne rozwiązania prawne muszą pozostawać jednakowo skuteczne wobec wszystkich nowych rozwiązań technologicznych. Komisja wskazała również, że zaproponowane przez nią nowe ramy prawne ochrony danych osobowych mają także przyczynić się do realizacji celu polegającego na uproszczeniu i zmniejszeniu obciążenia administracyjnego.

5. Z wydawanych przez Komisję wniosków ustawodawczych można wyinterpretować trzy główne trendy stanowiące wyzwanie dla ochrony danych osobowych oraz determinujące kształt prawny sporządzanych przez Komisję projektów legislacyjnych. Pierwszym trendem jest wspomniany już rozwój zaawansowanych technologii, drugim – zwiększona globalizacja przepływu danych, a trzecim – coraz szerszy dostęp do danych osobowych przez organy ścigania (*V. Reding*, The upcoming data protection reform for the European Union, International Data Privacy Law 2011, s. 1, http://idpl.oxfordjournals.org/?content/?early/?2010/11/17/idpl.ipq007.full, dostęp: 28.8.2017 r.). Nowa dyrektywa w sprawie ochrony danych osobowych przetwarzanych dla celów zapobiegania przestępstwom, będąca realizacją uprawnienia przyznanego UE na podstawie art. 16 ust. 2, stanowi odpowiedź na trzeci z nich. Traktat lizboński w powołanym przepisie wprowadził szczególną podstawę prawną przyjmowania norm dotyczących ochrony danych osobowych, która znajduje zastosowanie także do współpracy wymiarów sprawiedliwości w sprawach karnych oraz do współpracy policyjnej w sprawach karnych, co obejmuje przetwarzanie danych zarówno na szczeblu transgranicznym, jak i krajowym. **16**

2. Wybór rozporządzenia jako instrumentu reformy ochrony danych osobowych

1. W dyskusji prowadzonej wśród przedstawicieli państw członkowskich na forum Rady na szczególną uwagę zasługuje kwestia wyboru rozporządzenia jako instrumentu prawnego, którym Unia zdecydowała się przeprowadzić reformę sektora ochrony danych osobowych. W literaturze podkreśla się nawet, że zastąpienie dyrektywy rozporządzeniem unijnym jest rozwiązaniem rewolucyjnym, mającym duży wpływ na elastyczność przewidzianych w nim rozwiązań (*Ch. Kuner*, The European Commissionñs Proposed Data Protection Regulation: A Copernican Revolution in Data Protection Law, Privacy and Security Law Report, BNA Bloomberg, 6.2.2012, s. 1–15). Należy się zgodzić z poglądem wyrażonym przez *W.R. Wiewiórowskiego*, że wiąże się to „nie tylko z bezpośrednim obowiązywaniem rozporządzenia w systemie prawnym państw członkowskich Unii Europejskiej, ale również z bezpośrednim stosowaniem tego aktu przez wszystkie organy publiczne oraz bezpośrednim skutkiem norm wynikających z takiego aktu, szczególnie tzw. skutkiem horyzontalnym" [*W.R. Wiewiórowski*, Nowe ramy ochrony danych osobowych w Unii Europejskiej, w: Aktualne problemy ochrony danych osobowych 2012 (red. *G. Sibiga*), MoP 2012, Nr 7 – dodatek, s. 3]. Pozostaje w tym miejscu zadać sobie pytanie, czy mimo istnienia traktatowych podstaw prawnych do określenia zasad dotyczących ochrony **17**

osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez państwa członkowskie Unia była uprawniona do wyboru rozporządzenia jako instrumentu zmian. W doktrynie podnosi się, że harmonizacja zupełna, a tym bardziej unifikacja prawa, może naruszyć przewidziany w traktatach wymóg proporcjonalności działań ustawodawcy unijnego, a odbierając lokalnym społecznościom możliwość decydowania, co leży w ich interesie, szkodzi demokracji [*H.W. Micklitz*, The targeted full harmonization approach: looping behind the curtain, w: Modernising and Harmonising Consumer Contract Law (red. *G. Howells*, *R. Schulze*), Munich 2009, s. 34 i n.]. Zgodnie z treścią art. 5 protokołu w sprawie stosowania zasad proporcjonalności i pomocniczości, załączonego do TUE i TFUE po Traktacie lizbońskim, podstawy stwierdzenia, że cel może zostać lepiej osiągnięty na poziomie Unii, muszą być uzasadnione wskaźnikami jakościowymi, a tam, gdzie to możliwe, ilościowymi. Jeśli istnieje więc wybór pomiędzy środkami, które nadają się do osiągnięcia danego celu, należy wybrać środki najmniej restrykcyjne [*D. Miąsik*, w: Stosowanie prawa Unii Europejskiej przez sądy (red. *A. Wróbel*), Warszawa 2010, s. 201]. Powołany już w niniejszym Wprowadzeniu art. 16 TFUE nie przesądza natomiast o instrumencie, za którego pośrednictwem Unia powinna uregulować zasady ochrony danych osobowych. Przepisy Traktatu, nakładając na organy unijne konieczność wydania rozporządzenia w danej dziedzinie, literalnie wskazują ten instrument jako regulujący dane kwestie bądź posługują się zwrotami „jednolity" lub „ujednolicony" (przykładem może być art. 116 TFUE, w świetle którego „Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, ustanawiają środki dotyczące tworzenia europejskich praw własności intelektualnej w celu zapewnienia jednolitej ochrony praw własności intelektualnej w Unii"). Aktem wykonawczym w tym zakresie jest przykładowo rozporządzenie Rady (UE) Nr 1260/2012 z 17.12.2012 r. wprowadzające wzmocnioną współpracę w dziedzinie tworzenia jednolitego systemu ochrony patentowej w odniesieniu do mających zastosowanie ustaleń dotyczących tłumaczeń (Dz.Urz. UE L 361, s. 89), których to odwołań nie ma w powołanym art. 16 TFUE. Brak jest nawet odniesienia do wspólnych zasad ochrony danych osobowych. Tradycyjnie przyjmuje się, że w świetle art. 296 TFUE w razie możliwości wyboru pomiędzy dyrektywą a rozporządzeniem w pierwszej kolejności należy przyjąć dyrektywę jako akt, który ze swojej istoty łagodniej ingeruje w prawo krajowe [*K. Kowalik-Bańczyk*, w: Traktat o funkcjonowaniu Unii Europejskiej. Komentarz (red. *D. Kornobis-Romanowska*, *J. Łacny*, *A. Wróbel*), t. 3, Warszawa 2012, s. 761; *A. Kunkiel-Kryńska*, Metody harmonizacji prawa konsumenckiego w Unii Europejskiej i ich wpływ na procesy implementacyjne w państwach członkowskich, Warszawa 2013, s. 225]. Bez znaczenia pozostaje też argument, że sektor ochrony danych osobowych został już przez UE uregulowany dyrektywą (dyrektywa 95/46/WE), która jednak przy aktualnym poziomie rozdrobnienia ustawodawstw okazała się nieskuteczna. Dyrektywa „nie zapobiegła [bowiem] rozdrobnieniu sposobów realizacji ochrony danych osobowych w całej Unii, ugruntowaniu niepewności prawnej oraz upowszechnieniu istniejącego w społeczeństwie poglądu, zgodnie z którym z działalnością prowadzoną w Internecie wiążą się istotne ryzyka" [wniosek Komisji z 27.1.2012 r. w sprawie rozporządzenia w sprawie ochrony osób fizycznych, s. 2; zob. Specjalna ankieta Eurobarometru (EB) Nr 359 „Ochrona danych i tożsamość elektroniczna w UE (2011)", http://ec.europa.eu/?publicopinion/?archives/ebs/ebs359en.pdf, dostęp: 29.8.2017 r.]. Nie można zapomnieć, że powołana dyrektywa zakłada tzw. harmonizację minimalną. Przyjmując za *B. Kurczem*,

Przejdź do księgarni →

C.H.BECK ksiegarnia.beck.pl