Rozdział I. Historia kształtowania się prawa do ochrony danych osobowych

1. Pojęcie prywatności

Być może dzisiaj trudno w to uwierzyć, ale do powstania prawa do prywatności przyczyniła się firma Kodak. W 1888 r. firma Eastman wprowadziła na rynek pierwszą amatorską kamerę migawkową Kodak I, reklamowaną jako najmniejszy, najlżejszy i najłatwiejszy w obsłudze aparat detektywistyczny. Wcześniej kamery były wielkie, a wykonanie jednego zdjęcia trwało dość długo. Zastąpienie płyt światłoczułych filmem rolkowym umożliwiło wykonanie wielu zdjęć bez konieczności każdorazowej wymiany materiału światłoczułego w ciemni, co przyspieszyło cały proces. Po raz pierwszy można było uchwycić zapis wyglądu i życia człowieka bez pozowania[1]. Osoby robiące aparatem zdjęcia z ukrycia naruszały prywatność innych, przez co rozwinęło się tzw. żółte dziennikarstwo (prasa brukowa, tabloidy). Prekursorami tego rodzaju dziennikarstwa byli *J. Pulitzer* i *W. Hearst* – przez sensacyjne relacje na temat morderstw czy krwawych wypadków starali się zaspokoić rosnącą, ich zdaniem, potrzebę zabawienia zwykłych ludzi. W efekcie doprowadziło to do potrzeby ochrony prywatności.

W 1890 r. *L. Brandeis* i *S. Warren* opublikowali w „Harvard Law Review" artykuł pt. „The Right to Privacy"[2], w którym postulowali uznanie nowego prawa osoby fizycznej – prawa do bycia pozostawionym samemu sobie (ang. *to be let alone*). Powodem powstania artykułu było upowszechnienie się nowej technologii – fotografii prasowej – i tym samym nowego nośnika informacji. Bostońska prasa nadmierne i w sposób krępujący relacjonowała życie prywatne *Warrena*, a przede wszystkim spotkania towarzyskie organizowane przez jego żonę[3]. Pojawienie się i rozwój prawnej ochrony prywatności to zatem efekt poczucia zagrożenia wywołanego przez zbyt szybko następujące zmiany technologiczne[4].

---

1 Zob. *R.E. Mensel*, Kodakers Lying in Wait: Amateur Photography and the Right to Privacy in New York, 1885–1915, „American Quarterly" 1991, Nr 43, s. 24–45.

2 *L. Brandeis*, *S. Warren*, The Right to Privacy, „Harvard Law Review", vol. IV, 15.12.1890 r.

3 W literaturze można spotkać się z poglądami, że gdyby Warren nie ożenił się z córką senatora Stanów Zjednoczonych, prawo do prywatności zapewne by nie powstało albo powstałoby później – zob. *A. Gajda*, What If Samuel D. Warren Hadn't Married A Senator's Daughter?: Uncovering The Press Coverage That

Prywatność można zatem definiować na wiele sposobów. Ogólnie uważa się, że jest to stan, w którego ramach jednostka (człowiek) decyduje o zakresie i zasięgu informacji udostępnianych i zakomunikowanych innym osobom. Na użytek tej publikacji przyjmuję szeroko akceptowaną definicję prywatności, którą podał *A. Westin*: prywatność to zdolność osoby do samodzielnego zadecydowania, kiedy, w jaki sposób i jak dalece informacja ich dotycząca może być komunikowana innym[5]. *Krzysztof Motyka* podzielił tak rozumianą prywatność na cztery kategorie:

1) prawo do bycia pozostawionym w spokoju,
2) prawo do kontroli informacji na swój temat,
3) kontrola dostępu do osoby,
4) autonomia jednostki[6].

Na stronie Europejskiego Inspektora Ochrony Danych można przeczytać, że w UE godność ludzką uznaje się za absolutne prawo podstawowe. Prywatność czy też prawo do życia prywatnego, do bycia niezależnym, kontrolowania informacji na własny temat i do bycia pozostawionym w spokoju odgrywa zasadniczą rolę w odniesieniu do godności. Jest to nie tylko wartość związana z osobą, lecz także wartość społeczna[7].

W ten instrument ochrony niezależności jednostki wpisuje się inna instytucja, zwana zazwyczaj autonomią informacyjną lub, co jest nam lepiej znane, prawem do ochrony danych osobowych[8].

2. Pojęcie ochrony danych osobowych

Powstanie pierwszych regulacji dotyczących prywatności i ochrony danych osobowych było konsekwencją postępującego rozwoju technologii – najpierw fotografii, a następnie postępu w digitalizacji i komputerowym przetwarzaniu informacji. Prawo do prywatności jest nieco starsze, gdyż odpowiadało na wcześniejsze zagrożenia prywatności, ochrona danych osobowych powstała później jako odpowiedź na rozwój technologii informatycznych – świadczą o tym już same nazwy przepisów prawa chroniącego dane osobowe. Przykładowo, Konwencja Nr 108 w swojej nazwie ma określenie mówiące o związku z automatycznym, tj. komputerowym przetwarzaniem.

Led To The Right To Privacy, http://educationnewyork.com/files/SSRN-id1026680privacyorigin.pdf (dostęp: 31.7.2018 r.). Inną ciekawostką może być stwierdzenie, że dążenie do prywatności ma podstawy fizjologiczne – zob. *B. Schneier*, Dane i Goliat. Ukryta bitwa o Twoje dane i kontrolę nad światem, Gliwice 2017.

4 *W. Gogłoza*, Prawo do prywatności w społeczeństwie informacyjnym, s. 1, https://wgogloza.files.wordpress.com/2007/12/prywatnosc2.pdf (dostęp: 31.7.2018 r.).

5 *A.F. Westin*, Privacy and Freedom, New York 1967, s. 166.

6 Za: *J. Rzucidło*, Prawo do prywatności i ochrona danych osobowych, (w:) *M. Jabłoński* (red.), Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym, Prace Naukowe Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2014, s. 153 (http://www.bibliotekacyfrowa.pl/Content/52906/Realizacja_i_ochrona_konstytucyjnych_praw.pdf).

7 Zob. https://edps.europa.eu/data-protection/data-protection_en (dostęp: 31.7.2018 r.).

8 Prawo to określa się także prawem do autonomii informacyjnej. Pojęciami „autonomia informacyjna jednostki" oraz „prawo do ochrony danych osobowych" posługuje się w swym orzecznictwie Trybunał Konstytucyjny (zob. wyr. TK z 17.6.2008 r., K 8/04, Legalis).

W RODO za dane osobowe uważa się wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Należy zauważyć, że prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych, choć ściśle ze sobą związane, są odrębne. Prawo do prywatności – określane w prawie europejskim jako prawo do poszanowania życia prywatnego – polega na ogólnym zakazie wkraczania w sferę prywatną. Natomiast ochrona danych osobowych jest prawem aktywnym, związanym z ochroną wszelkich informacji o określonej osobie, takich jak imiona, nazwisko, data urodzin, zdjęcia, nagrania wideo, dane kontaktowe itd. Przykładowo zebranie określonych informacji o danej osobie bez jej wiedzy nie stanowi naruszenia prawa do prywatności, gdyż prawo do poszanowania życia prywatnego nie zostało naruszone. Tak się stanie dopiero wtedy, gdy dane te zostaną wykorzystane. Natomiast przepisy o ochronie danych zabraniają przetwarzania danych bez podstawy prawnej i nie ma znaczenia, czy dane planuje się kiedykolwiek użyć, czy nie. Widać tutaj wyraźną różnicę, że prawo do ochrony danych osobowych jest bardziej proaktywne, chroni osoby mu podlegające już na znacznie wcześniejszym etapie niż prawo do prywatności.

Odwołując się do stworzonego przez *K. Motykę* podziału prawa do prywatności, wskazanego w poprzednim punkcie, należy stwierdzić, że prawo do ochrony danych osobowych wspiera prawo do prywatności przede wszystkim w kwestii kontrolowania obiegu informacji na swój temat. Pozostałe aspekty są wspierane pośrednio i raczej w niewielkim stopniu.

3. Dane osobowe jako tajemnica

Kontrolowanie obiegu informacji na swój temat ma związek z pojęciem tajemnicy. Jeśli coś postanawiamy zachować w tajemnicy, to tego nie ujawniamy wszystkim, a jedynie ograniczonej liczbie osób. **Informacja w ograniczonym obiegu staje się zatem tajemnicą.** Dzięki przepisom takim jak m.in. RODO, a dawniej OchrDanychU97, które ograniczają obieg danych osobowych i krąg osób mogących mieć do nich dostęp, **dane osobowe uznaje się za tajemnicę prawnie chronioną**.

4. Regulacje dotyczące ochrony danych i prywatności

Regulacje prawne dotyczące prywatności i ochrony danych osobowych zaczęły pojawiać się względnie od niedawna. Już wspomniano, najpierw z powodu rozwoju prasy (głównie brukowej) i techniki fotograficznej powstała konieczność unormowania prawa do prywatności, a następnie ze względu na rozwój informatyki – ochrony danych osobowych przetwarzanych w sposób zautomatyzowany. Już kilkadziesiąt lat temu zaczęły powstawać duże zbiory informacji o osobach, nazywane „bankami danych". Możliwość przeszukiwania tych danych, ich kojarzenia i analizowania rodziła duże ryzyko dla prywatności. Uznano, że jeśli nie wprowadzi się żadnych ograniczeń, zarządzający takim bankiem danych mógłby zgromadzić dowolną ilość informacji o określonej osobie, a w konsekwencji – wiedzieć o niej w zasadzie prawie wszystko. Zaistniała więc potrzeba wprowadzenia regulacji nakładających pewne ograniczenia zbierania i przetwarzania danych, w tym

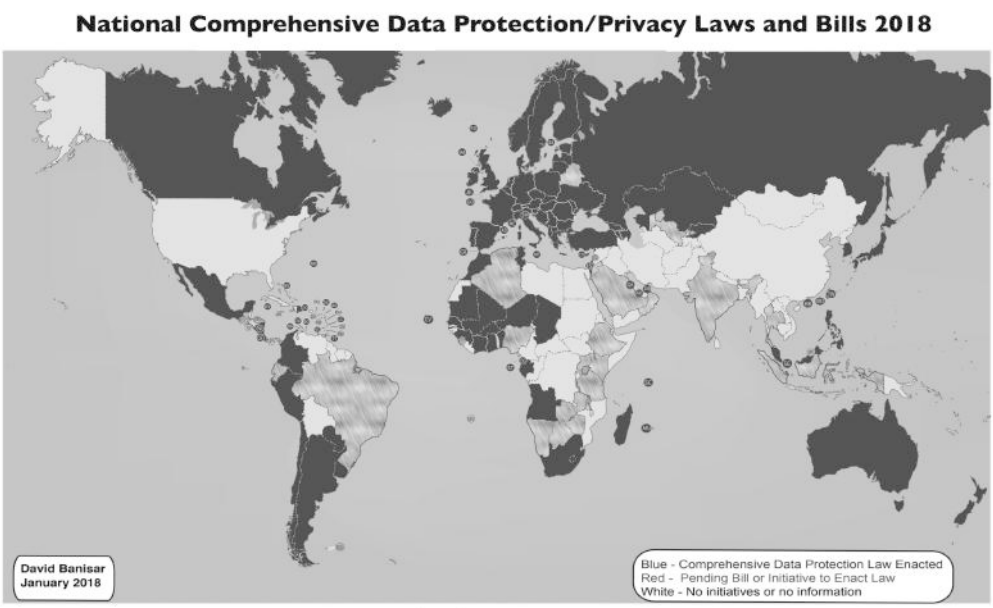
formułujących zasady odpowiedniej ich ochrony, zapewniające równocześnie określone prawa osobom, których dane przetwarza się w sposób zautomatyzowany.

Przepisy chroniące prywatność i dane osobowe powstawały w następującej kolejności:
1) powszechna deklaracja praw człowieka – 1948 r.,
2) europejska konwencja praw człowieka – 1950 r.,
3) ustawa o ochronie danych osobowych w Hesji – 1970 r.,
4) rezolucja 22 i 29 – 1973 i 1974 r.,
5) wytyczne OECD – 1980 r.,
6) konwencja Nr 108 – 1981 r.,
7) dyrektywa 95/46/WE – 1995 r.,
8) Karta praw podstawowych Unii Europejskiej (2000/C364/01) – 2000 r.,
9) ogólne rozporządzenie o ochronie danych – 2016 r.

Dodatkowo należy wskazać, że w Polsce ochrona prywatności i danych osobowych jest regulowana przez OchrDanychU (dawniej: OchrDanychU97, implementującą dyrektywę 95/46/WE) i odpowiednie przepisy Konstytucji RP oraz KC.

Na ilustracji przedstawiono stan implementacji przepisów o ochronie danych osobowych bądź prywatności na całym świecie.

Rysunek 1. Status implementacji przepisów chroniących prywatność i dane osobowe. Kolorem niebieskim oznaczono kraje, w których przyjęto kompleksowe przepisy chroniące dane osobowe, czerwonym te, w których takie przepisy są w trakcie przyjmowania lub tworzenia, a białym te, w których nie odnotowano żadnych inicjatyw.



Źródło: D. Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2018, January, 2018, https://ssrn.com/abstract=1951416 (dostęp: 31.7.2018 r.).

4.1. Powszechna deklaracja praw człowieka

Poszukując podstaw prawa do prywatności w prawie międzynarodowym, warto sięgnąć do Powszechnej deklaracji praw człowieka[9] z 10.12.1948 r., uchwalonej przez Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych. W art. 12 tego aktu postanowiono, że nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Ponadto każdemu człowiekowi zagwarantowano prawo do ochrony prawnej przeciwko takiej ingerencji lub takiemu uwłaczaniu.

4.2. Konwencja o ochronie praw człowieka i podstawowych wolności

Rządy państw europejskich chciały podjąć kroki w celu zbiorowego zagwarantowania niektórych praw zamieszczonych w Powszechnej deklaracji praw człowieka. W tym celu w 1950 r. przyjęły EKPCz, na której podstawie powołano Europejski Trybunał Praw Człowieka z siedzibą w Strasburgu.

Przepis art. 8 EKPCz reguluje prawo do prywatności, czyli poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji każdej osoby. Zakazano w nim ingerencji w prawo do prywatności, z wyjątkiem „przypadków przewidzianych przez ustawę" i „koniecznych w demokratycznym społeczeństwie" z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób, czyli wyraźnie wymienionych określonych rodzajów ważnych interesów publicznych. Warto zwrócić uwagę, że konstrukcje z EKPCz można znaleźć w polskiej Konstytucji RP, przykładowo w art. 51 Konstytucji RP.

4.3. Ustawa o ochronie danych osobowych w Hesji

Ustawa o ochronie danych osobowych (niem. *Datenschutzgesetz*) w niemieckim landzie Hesja (niem. *Hessen*) była pierwszym takim aktem prawa nie tylko w Niemczech, ale i na całym świecie. Uchwalona 7.10.1970 r., opublikowana w Dzienniku Urzędowym landu Hesja Nr 41 (Gesetz- und Verordnungsblatt fur das Land Hessen, Teil 1, Nr. 41)[10]. Ustawa była dość skromna, bo składało się na nią zaledwie 17 niezbyt rozbudowanych paragrafów. Stanowiła odpowiedź na rozwijające się technologie przetwarzania danych komputerowo. Ustawa wprowadzała organ nadzorczy (niem. *Datenschutzbeauftragter*), pierwszą osobą pełniącą tę rolę był *Willi Birkelbach*, wybrany przez władze w dniu 8.6.1971 r.

9 Zob. http://www.unesco.pl/fileadmin/user_upload/pdf/Powszechna_Deklaracja_Praw_Czlowieka.pdf (dostęp: 31.7.2018 r.).

10 Zob. http://starweb.hessen.de/cache/GVBL/1970/00041.pdf (dostęp 26.9.2018 r.).

4.4. Rezolucja 22 i 29

W Europie sygnał do ochrony danych osobowych stanowiła rezolucja (73) 22 z 26.9.1973 r. o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym, wydana przez Komitet Ministrów Rady Europy. Dotyczyła ona ochrony prywatności osób, których dane były przetwarzane w bankach danych w sektorze prywatnym. Rok później – w 1974 r. – wydano rezolucję (74) 29 dla banków danych w sektorze publicznym. Już wtedy, ponad 40 lat temu, dane dzieliło się na zwykłe i ujawniające szczegóły życia prywatnego (*intimate private life of individuals*). Obie rezolucje podkreślały, że dane osobowe powinny być adekwatne do celu, w jakim są zbierane i przechowywane, przy czym w sektorze prywatnym dodano jeszcze, że dane mogą być przechowywane jedynie przez określony czas.

4.5. Wytyczne OECD

Organizacja Współpracy Gospodarczej i Rozwoju (*Organization for Economic Cooperation and Development* – OECD) 23.9.1980 r. wydała „Wytyczne regulujące ochronę prywatności i przepływ danych osobowych przez granice". Miały one charakter zaleceń i na żaden z krajów nie nakładały obowiązku implementacji postanowień, jednak były kolejnym sygnałem potwierdzającym, że ochrona danych osobowych jest ważna.

Rekomendacje odnoszące się do ochrony prywatności i przekazywania danych osobowych pomiędzy krajami nie są dokumentem o wiążącym charakterze. To jedynie zalecenia rady OECD odnośnie do regulacji krajowych dotyczących ochrony prywatności i przepływu danych osobowych przez granice. W wytycznych podkreślono wagę międzynarodowego transferu danych i jego wpływ na światowy rozwój gospodarczy oraz niekorzystne działanie ograniczeń w tym zakresie. Wprawdzie wytyczne dopuszczają wprowadzenie takich ograniczeń w przepisach krajowych, jednak zalecają ich eliminowanie.

Wytyczne OECD opracowano równolegle z konwencją Nr 108. W obu aktach znajdują się podobne koncepcje legalności, chociaż pojęcie to jest wyrażane w inny sposób. Wytyczne zaktualizowano w 2013 r., lecz w przypadku zasady legalności nie wprowadzono zmian merytorycznych. W części drugiej pkt 7 wytycznych OECD wyrażono zasadę ograniczenia zbierania, zgodnie z którą powinno się ustanowić zasady zbierania danych osobowych, wszelkie takie dane powinny być zbierane za pomocą uczciwych i rzetelnych środków oraz za wiedzą lub zgodą podmiotu danych, tam gdzie jest to właściwe[11]. Podstawa prawna, jaką stanowi zgoda, jest wyraźnie wskazana jako możliwość, którą należy wykorzystywać w stosownych przypadkach.

4.6. Konwencja Nr 108

Celem konwencji Nr 108 Rady Europy z 28.1.1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych było wprowadzenie w krajach euro-

[11] Przegląd, Wytyczne OECD w zakresie ochrony prywatności i przepływu danych osobowych przez granice, http://www.oecd.org/sti/ieconomy/15590241.pdf (dostęp: 31.7.2018 r.), s. 4.

pejskich ujednoliconej, działającej na podobnej zasadzie, ochrony danych osobowych, a przez to umożliwienie idei swobodnego przepływu danych osobowych w obrębie państw członkowskich. Polska podpisała konwencję 21.4.1999 r., a ratyfikowała[12] ją 24.5.2002 r.

Ważne

Konwencja Nr 108 uznawana jest za podstawowy i zarazem jeden z najstarszych instrumentów międzynarodowej ochrony danych osobowych. Znamienny jest przy tym jej cel, wskazany w art. 1 konwencji Nr 108: zapewnienie każdej osobie fizycznej, bez względem na narodowość lub miejsce zamieszkania, poszanowania jej praw i podstawowych wolności na terytorium każdej ze stron konwencji, a w szczególności jej prawa do prywatności w związku z automatycznym przetwarzaniem dotyczących jej danych osobowych.

W preambule podkreślono, że sygnatariusze konwencji Nr 108 uzgodnili jej postanowienia w przekonaniu, że pożądane jest rozszerzenie zakresu ochrony praw i podstawowych wolności każdej osoby, a w szczególności prawa do poszanowania prywatności, biorąc pod uwagę stale rosnący przepływ przez granice danych osobowych, podlegających automatycznemu przetwarzaniu, uznając konieczność pogodzenia podstawowych wartości, takich jak poszanowanie prywatności i swobody przepływu informacji między ludźmi.

Warto zauważyć, że konwencja Nr 108 jest wciąż żywym aktem prawa i nie zrezygnowano z niej, a co więcej – postanowiono ją unowocześnić. Jak podkreśla Komisja Europejska, konwencja Nr 108 powstała długo przed erą Internetu i komunikacji elektronicznej. Rozwój technologii i globalizacja tworzą nowe wyzwania w sferze ochrony danych osobowych. Celem protokołu zmieniającego jest modernizacja konwencji Nr 108, aby nadążyć za tymi zmianami[13].

Pośród państw, które ratyfikowały konwencję Nr 108, jest m.in. Tunezja, Urugwaj, Meksyk i Senegal. Jak widać, możliwość jej ratyfikowania nie jest ograniczona terytorialnie[14]. Co roku **28 stycznia – w rocznicę jej uchwalenia – obchodzi się Dzień Ochrony Danych Osobowych**.

4.7. Dyrektywa 95/46/WE

Dyrektywa 95/46/WE stanowiła przełom w zakresie ochrony danych osobowych w Europie. Podczas jej tworzenia opierano się na konwencji Nr 108 oraz wytycznych OECD, uwzględniano także wczesne doświadczenia z ochroną danych osobowych w niektórych państwach członkowskich. Można uznać ją zatem za następczynię konwencji Nr 108, z tą jednak różnicą, że dyrektywa 95/46/WE zobowiązuje państwa członkowskie UE do im-

12 Ratyfikacja jest w zasadzie tym samym co zatwierdzenie, ale ma bardziej uroczystą formę – zob. m.in. art. 89 i 133 Konstytucji RP.

13 Komisja Europejska, *Proposal for a Council Decision authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*, Bruksela, 5.6.2018 r., http://data.consilium.europa.eu/doc/document/ST-9765-2018-INIT/en/pdf (dostęp: 31.7.2018 r.), s. 1.

14 Na stronie https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=LupaBodI (dostęp: 31.7.2018 r.) można sprawdzić, które państwa ratyfikowały konwencję Nr 108.

plementacji pożądanego stanu rzeczy, tzn. muszą one osiągnąć cele w niej wyznaczone, a sposób i metody ich osiągnięcia pozostawiono do decyzji każdego z tych państw.

Jednym z najważniejszych celów dyrektywy 95/46/WE, podobnie jak konwencji Nr 108, było umożliwienie swobodnego przepływu danych osobowych w ramach Europejskiego Obszaru Gospodarczego poprzez zastosowanie jednolitego poziomu bezpieczeństwa danych w każdym z państw UE. W dyrektywie 95/46/WE wprowadzono konkretny zbiór dodatkowych wymagań, które jako takie nie były jeszcze obecne ani w konwencji Nr 108, ani w wytycznych OECD. Przetwarzanie danych osobowych musi być oparte na jednej z sześciu podstaw prawnych określonych w art. 7 dyrektywy 95/46/WE. Mianowicie państwa członkowskie zapewniają, że dane osobowe mogą być przetwarzane tylko wówczas, gdy:

1) osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę lub
2) przetwarzanie danych jest konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy, lub
3) przetwarzanie danych jest konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega, lub
4) przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą, lub
5) przetwarzanie danych jest konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane, lub
6) przetwarzanie danych jest konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę na podstawie art. 1 ust. 1 dyrektywy 95/46/WE.

Z łatwością można zauważyć, że podstawy prawne przetwarzania są zgodne z tymi, które wynikają z RODO. Warto podkreślić, że w motywie 2 dyrektywy 95/46/WE podkreśla się, że systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi, muszą więc szanować podstawowe prawa i wolności osób fizycznych, a szczególnie prawo do prywatności. Znalazło to swoje odzwierciedlenie w motywie 4 RODO: przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Właściwie gdyby dzisiaj porównać wymagania dyrektywy oraz RODO, to nie znajdzie się zasadniczych różnic. Wydaje się, że pewne różnice powstały raczej na etapie implementacji dyrektywy 95/46/WE w porządkach prawnych poszczególnych państw członkowskich. Zdaje się, że dano temu wyraz w motywie 9 RODO: „Cele i zasady dyrektywy 95/46/WE pozostają aktualne, jednak wdrażając ochronę danych w Unii, nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami w Internecie. Różnice w stopniu ochrony praw i wolności osób fizycznych w państwach członkowskich – w szczególności prawa do ochrony danych osobowych – w związku z przetwarzaniem danych osobowych mogą utrudniać swobodny przepływ danych osobowych w Unii. Mogą zatem stanowić przeszkodę w prowadzeniu działalności gospodarczej na szczeblu Unii, zakłócać konkurencję oraz utrudniać organom wykonywanie obowiązków nałożo-

nych na nie prawem Unii. Różnice w stopniu ochrony wynikają z różnic we wdrażaniu i stosowaniu dyrektywy 95/46/WE".

Wytyczne dyrektywy 95/46/WE w Polsce zostały zaimplementowane 29.8.1997 r. – przez uchwalenie OchrDanychU97 – w ramach starań o członkostwo w UE.

4.8. Konstytucja RP

W Polsce podstaw do ochrony danych osobowych należy doszukiwać się w Konstytucji RP. Na jej treść wpływ miały bez wątpienia akty europejskie, w tym także dyrektywa 95/46/WE. Konstytucja RP stanowi swojego rodzaju wzorzec oceny wszystkich innych krajowych aktów prawnych, ponieważ jest najwyższym prawem Rzeczypospolitej Polskiej. Rozdział II Konstytucji RP określa wolności, prawa i obowiązki obywateli względem państwa, które stanowią podstawę do regulacji chroniących dane osób. Stosownie do art. 47 Konstytucji RP każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Dane osobowe są elementem życia prywatnego i mogą stanowić o dobrym imieniu osoby, a decydowanie o tym, czy chce się je ujawniać, jest jednym z przejawów prawa do prywatności. Prawo to wyrażone jest w art. 51 Konstytucji RP, zgodnie z którym:

1) nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby,
2) władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym,
3) każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa,
4) każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą,
5) zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Ważne

W pewnym sensie osoba jest właścicielem danych jej dotyczących i powinna mieć możliwość decydowania o nich. To prawo może być ograniczone jedynie ustawowo, co Konstytucja RP wyraźnie akcentuje: „nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby", podkreślając, że: „zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa".

Z powyższego wynika, że **przepisy o randze niższej niż ustawa – np. polskie rozporządzenia – nie mogą regulować kwestii legalności przetwarzania danych osobowych**. Takie stanowisko przyjmuje także GIODO, który wskazuje, że powinność udostępnienia danych, w tym danych szczególnie chronionych w rozumieniu art. 27 ust. 1 OchrDanychU97, w żadnym razie nie może wynikać z aktu prawnego o randze rozporządzenia[15].

[15] Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2012 r., https://giodo.gov.pl/data/filemanager_pl/sprawozdaniaroczne/2012.pdf (dostęp: 31.7.2018 r.), s. 149.

4.9. Ustawa o ochronie danych osobowych z 1997 r.

Ustawa o ochronie danych osobowych z 29.8.1997 r. była w Polsce pierwszym aktem prawnym zajmującym się kompleksowo ochroną danych osobowych. Przyjęto go w ramach dążenia do otrzymania członkostwa w UE, co wymagało zaimplementowania m.in. postanowień dyrektywy 95/46/WE. Prace nad OchrDanychU97 nie były oparte w całości na polskich doświadczeniach związanych z kwestiami dotyczącymi prywatności, co nie oznacza, że prywatność nie była wcześniej chroniona. Dotychczasowe regulacje (cywilne i karne) gwarantowały bowiem ochronę w przypadku naruszenia lub zagrożenia dobra osobistego (a więc jakby po fakcie), natomiast OchrDanychU97 zapewniła ochronę prewencyjną.

Zanim OchrDanychU97 została uchwalona do Sejmu trafiły jej dwa projekty:
1) poselski z 23.8.1996 r. (druk Nr 1890, Sejm II kadencji),
2) rządowy z 3.10.1996 r. (druk Nr 1928, Sejm II kadencji).

Projekt rządowy był, jak czytamy w uzasadnieniu, wzorowany głównie na konwencji Nr 108 oraz na obowiązujących w tym zakresie przepisach w państwach zrzeszonych w UE, a zwłaszcza na projekcie dyrektywy Rady Wspólnot Europejskich EC 1/95 z 20.2.1995 r. Podkreślono, że celem projektu jest określenie praw i obowiązków obu stron w taki sposób, aby zagwarantować maksymalną ochronę praw i wolności każdej osoby fizycznej (jednostki) oraz poszanowanie jej życia prywatnego. Uwagę zwraca próba określenia ilości danych w zbiorze powodujących konieczność jego rejestracji – zaproponowano, aby nie rejestrować zbiorów z mniejszą ilością danych niż dane 100 osób.

Projekt poselski w porównaniu do rządowego był nieco skromniejszy, różnił się także definicjami, np. zamiast Generalnego Inspektora Ochrony Danych Osobowych zaproponowano Rzecznika Ochrony Danych. W projekcie pojawił się wyraz „prywatność", a dane wrażliwe zdefiniowano jako „dane intymne".

Ostatecznie przyjęto projekt rządowy, uwzględniono w nim jednak niektóre zapisy projektu poselskiego. Dzisiaj niektóre określenia i wymagania mogą bawić (takie jak zgoda, z której znaczenia zdaje sobie sprawę osoba, dane intymne, kasowanie i blokowanie danych, obowiązek wyrażania zgody pisemnie, informowanie o sprostowaniu lub skasowaniu danych, w przypadku marketingu bezpośredniego – podawanie adresatowi numer zbioru w rejestrze zbiorów danych osobowych), pamiętajmy jednak, że był to pierwszy tego rodzaju akt prawny w Polsce.

Wraz z przyjęciem OchrDanychU97 wszyscy obywatele otrzymali potwierdzenie szerokiego katalogu praw:
1) dane o osobie należą do osoby i może ona decydować o ich losie, w szczególności o tym, czy zechce je ujawnić,
2) dane o osobie można przetwarzać wyłącznie na podstawie obowiązującego prawa,
3) osoba, której dane dotyczą, ma prawo sprawować kontrolę nad tym, kto i jakie dane jej dotyczące przetwarza,
4) zebrane dane nie są dostępne dla wszystkich,
5) dane można przetwarzać wyłącznie w ograniczonym czasie i celu.

Prawo osoby do kontroli nad tym, kto przetwarza dane jej dotyczące oraz jaki jest ich zakres, wyrażało się przez:
1) obowiązek informowania jej o tym, kto te dane przetwarza,
2) prawo do informacji o tym, jakie jej dane są przetwarzane,
3) możliwość sprostowania danych, ich aktualizacji bądź usunięcia, gdy są niepełne lub nieprawdziwe,
4) możliwość sprzeciwienia się przetwarzaniu danych.

Przyznane prawa były wspierane przez model rejestracji systemów przetwarzania danych osobowych. Każdy, kto przetwarzał dane osobowe w sposób usystematyzowany (uporządkowany), był zobowiązany zgłosić ten fakt do określonego organu administracji publicznej (tj. musiał zarejestrować zbiór danych osobowych). Była to tzw. wstępna kontrola przetwarzania[16], gdyż organ państwowy oceniał, czy przetwarzanie nie będzie niosło za sobą zagrożeń dla prywatności osób i nie będzie naruszało przepisów OchrDanychU97. Organ administracji publicznej prowadził rejestr takich systemów i umożliwiał wgląd do niego każdemu zainteresowanemu, co mogło ułatwić rozeznanie, kto przetwarza dane osobowe w sposób zorganizowany[17].

Podstawowym założeniem OchrDanychU97 było to, że przetwarzanie jakichkolwiek danych osobowych jest możliwe tylko wtedy, gdy zostanie spełniona co najmniej jedna przesłanka legalności przetwarzania danych, np.:
1) osoba wyrazi na to zgodę,
2) przetwarzanie jest konieczne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z prawa (np. wypłata emerytury, renty, zachowanie zgodności z innymi ustawami, np. RachunkU),
3) przetwarzanie jest konieczne do działań związanych z zawarciem lub realizacją umowy (np. dokonanie zakupu towaru lub usługi, do której niezbędne jest podanie swoich danych),
4) przetwarzanie jest niezbędne dla usprawiedliwionych prawem celów i jednocześnie nie narusza praw i wolności osoby, której dane dotyczą (dochodzenie roszczeń, marketing bezpośredni własnych towarów i usług, windykacja),
5) przetwarzanie jest niezbędne do wykonania zadań określonych prawem i realizowanych dla dobra publicznego.

Ustawa o ochronie danych osobowych wyróżniała szczególną kategorię danych o osobie, mających istotne znaczenie dla jej prywatności, ujawniających informacje np. o zdrowiu, kodzie genetycznym, preferencjach seksualnych czy skazaniach. Dane te, określane potocznie jako dane wrażliwe, były szczególnie chronione, a ich przetwarzanie było dopuszczalne tylko wtedy, gdy były spełnione specjalne warunki, np.:
1) osoba wyraziła na to zgodę (zawsze na piśmie),
2) przepis OchrDanychU97 na to pozwalał,

16 Motyw 54 preambuły oraz art. 20 dyrektywy 95/46/WE również odnoszą się do wstępnej kontroli przetwarzania.
17 Warto zauważyć, że RODO przerzuciło obowiązek oceny ryzyka na administratorów danych, a nowym odpowiednikiem dokumentacji dotyczącej zbiorów danych osobowych stała się ocena skutków dla ochrony danych oraz rejestry czynności przetwarzania.

3) przetwarzanie danych było niezbędne do ochrony żywotnych interesów osoby (ratowanie życia),
4) osoba, której dane dotyczą, sama je upubliczniła.

Ustawodawca uznawał, że szczególna ochrona należy się danym osobowym przetwarzanym w systemach informatycznych. Dlatego podmiot, który komputerowo przetwarzał dane osobowe, był zobowiązany aktem wykonawczym do OchrDanychU97 do tego, aby:
1) przygotować odpowiednią dokumentację (oprócz polityki bezpieczeństwa także instrukcję zarządzania systemem),
2) zapewnić, że system informatyczny ma określone funkcje (np. odnotowywał automatycznie, kto i kiedy wprowadził do niego dane osobowe),
3) odpowiednio zabezpieczyć system informatyczny (np. przez stosowanie szyfrowania, programów antywirusowych, odpowiednich haseł).

4.10. Kodeks cywilny

Regulacja art. 23 KC zawiera przykładowy zestaw rodzajów dóbr osobistych, które podlegają ochronie: zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska[18]. W KC jest zawarta jedynie ogólna zasada, że dobra osobiste pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach, przykładowo dotyczących ochrony danych osobowych. Środki ochrony tych dóbr zostały wymienione art. 24 KC. Warto w tym miejscu odwołać się do wyroku Sądu Apelacyjnego w Gdańsku.

Orzecznictwo

Dobro osobiste podlega ochronie prawnej, gdy jest zagrożone cudzym bezprawnym działaniem (art. 24 § 1 KC). Nie można wszakże przyjąć, iż posłużenie się danymi osobowymi osoby fizycznej w ofercie handlowej do niej skierowanej było bezprawnym działaniem oferenta. Podstawowe dane osobowe człowieka (nazwisko i imię) są jego dobrem osobistym, ale jednocześnie są dobrem powszechnym w tym znaczeniu, iż istnieje publiczna zgoda na posługiwanie się nimi w życiu społecznym (towarzyskim, urzędowym, handlowym itd.) (wyr. SA w Gdańsku z 15.3.1996 r., I ACr 33/96, Legalis).

Dopóki więc dane osobowe człowieka są używane zgodnie z regułami społecznymi, nie można mówić ani o bezprawności działań innych osób, ani o zagrożeniu dóbr osobistych tymi działaniami. Pozwala to wyciągnąć wniosek, że potrzebne są przepisy prawa chroniące dobra osobiste. W przeciwnym wypadku nie występuje cudze bezprawne działanie, a skoro takiego działania nie ma, to nie można mówić o naruszeniu.

4.11. Karta praw podstawowych Unii Europejskiej

Karta praw podstawowych Unii Europejskiej została przyjęta 7.12.2000 r. jako uroczysta wspólna proklamacja Parlamentu Europejskiego, Rady i Komisji (12.12.2007 r. insty-

[18] Interesująca jest obserwacja, że dobrem osobistym nie jest adres zamieszkania osoby fizycznej.

tucje te ponownie ją podpisały). Moc wiążąca została jej nadana przez traktat lizboński z 13.12.2007 r., który wszedł w życie 1.12.2009 r.

Karta praw podstawowych Unii Europejskiej zawiera postanowienia dotyczące:

1) **godności**, w tym: poszanowanie godności ludzkiej, prawo do życia oraz do integralności fizycznej i psychicznej, zakaz tortur i poniżającego traktowania lub karania, zakaz niewolnictwa i pracy przymusowej;
2) **wolności**, w tym m.in. prawo do wolności i bezpieczeństwa osobistego, do poszanowania prywatności i życia rodzinnego, prawo zawarcia małżeństwa i założenia rodziny, wolność myśli, sumienia i religii, wolność zgromadzania się i stowarzyszania się, prawo do nauki, wolność wyboru zawodu i prawo podejmowana pracy w każdym państwie członkowskim;
3) **równości**, w tym m.in. równość wobec prawa, zakaz wszelkiej dyskryminacji, prawa dziecka, prawa osób starszych, prawa osób niepełnosprawnych;
4) **solidarności**, w tym m.in. prawo pracowników do informacji i konsultacji, do rokowań i działań zbiorowych, dostępu do pośrednictwa pracy, prawo do ochrony przed nieuzasadnionym zwolnieniem z pracy, prawo do godziwych warunków pracy, zakaz pracy dzieci i ochrona młodocianych w pracy, prawna, ekonomiczna i społeczna ochrona rodziny, prawo do zabezpieczenia społecznego i pomocy społecznej, do ochrony zdrowia;
5) **praw obywatelskich**, w tym m.in. prawo głosowania i kandydowania w wyborach do Parlamentu Europejskiego i w wyborach lokalnych, prawo do dobrej administracji, swoboda przemieszczania się i pobytu;
6) **wymiaru sprawiedliwości**, w tym m.in. prawo dostępu do bezstronnego sądu i do skutecznego środka odwoławczego.

Artykuł 8 KPP odnosi się do ochrony danych osobowych. Zgodnie z nim każdy ma prawo do ochrony danych osobowych, które go dotyczą. 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. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

Warto zwrócić uwagę na art. 45 ust. 1 KPP, odnoszący się do swobody przemieszczania się i pobytu. Stosownie do niego każdy obywatel UE ma prawo do swobodnego przemieszczania się i przebywania na terytorium państw członkowskich. Regulacja ta jest wspierana przez RODO.

4.12. Ogólne rozporządzenie o ochronie danych

Reforma przepisów o ochronie danych osobowych nastąpiła po ponad 20 latach od uchwalenia dyrektywy 95/46/WE. Wszystko zaczęło się 4.11.2010 r., kiedy Komisja Europejska – po przeprowadzeniu szeroko zakrojonych konsultacji społecznych – opublikowała komunikat zatytułowany „Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej". Zauważyła w nim, że dyrektywa 95/46/WE stanowiła kamień milowy w historii ochrony danych osobowych w UE. Zapisano w niej dwa z najstarszych i równie istotnych dążeń w procesie integracji europejskiej: z jednej strony, jest to

ochrona praw podstawowych i podstawowych wolności jednostek, w szczególności podstawowego prawa do ochrony danych, z drugiej zaś – realizacja rynku wewnętrznego, w tym przypadku – swobodnego przepływu danych osobowych[19]. Jak podkreśliła Komisja Europejska, piętnaście lat później ten podwójny cel nadal obowiązuje, podobnie jak aktualne są zasady zapisane w dyrektywie 95/46/WE. Jednak szybki rozwój technologiczny i globalizacja doprowadziły go głębokich przemian w otaczającym nas świecie, przynosząc nowe wyzwania w zakresie ochrony danych osobowych.

Wiceprzewodnicząca *Viviane Reding*, komisarz ds. sprawiedliwości, praw podstawowych i obywatelstwa, podkreślała, że ochrona danych osobowych jest jednym z praw podstawowych, aby zagwarantować to prawo potrzebne są więc jasne i konsekwentne przepisy w zakresie ochrony danych: „Musimy również aktualizować nasze przepisy pod kątem wyzwań wynikających z nowych technologii i globalizacji. Komisja opracuje w przyszłym roku nowe akty prawne, by wzmocnić prawa jednostek, a jednocześnie zapewnić swobodny przepływ danych w ramach jednolitego rynku UE poprzez znoszenie barier biurokratycznych”[20].

W ten sposób zapowiedziano kompleksową nowelizację unijnego prawa w zakresie ochrony danych osobowych. Nieco później, 6.7.2011 r., Parlament Europejski przyjął rezolucję, w której poparł stanowisko Komisji Europejskiej[21], a 24.2.2011 r. swoje poparcie dla zmian wyraziła Rada UE. Wśród unijnych instytucji panowała zgodność co do tego, że przepisy o ochronie danych osobowych potrzebują odświeżenia i ujednolicenia.

Następnie były zbierane uwagi do propozycji, w tym także przeprowadzono konsultacje społeczne. Proces ten trwał 2 lata, a w jego rezultacie 25.1.2012 r. Komisja Europejska przedstawiła projekt kompleksowej reformy unijnych przepisów o ochronie danych oraz opis najważniejszych elementów reformy ochrony danych[22]. Miały się na nią składać dwa nowe akty prawne:

1) rozporządzenie o ochronie danych, zastępujące dyrektywę 95/46/WE,
2) dyrektywa określająca przepisy o ochronie danych osobowych przetwarzanych do celów zwalczania przestępczości, zastępująca decyzję ramową 2008/977/WSiSW[23].

Zdaniem Komisji Europejskiej 27 państw członkowskich wdrożyło przepisy z 1995 r. na różne sposoby, co doprowadziło do rozbieżności w ich egzekwowaniu, a pojedynczy

---

19 W dokumencie wydanym 28.7.2015 r. – „Opinia 3/2015. Wielka szansa dla Europy. Zalecenia EIOD dotyczące możliwości reformy ochrony danych w UE” – można przeczytać, że: „celem przepisów unijnych zawsze było ułatwianie przepływu danych zarówno w obrębie UE, jak i w kontaktach z jej partnerami handlowymi, lecz nadrzędną kwestią pozostaje dbałość o prawa i wolności osób fizycznych”. Europejski Inspektor Ochrony Danych, Opinia 3/2015. Wielka szansa dla Europy. Zalecenia EIOD dotyczące możliwości reformy ochrony danych w UE, 28.7.2015 r., https://edps.europa.eu/sites/edp/files/publication/15-10-09_gdpr_with_addendum_pl.pdf (dostęp: 31.7.2018 r.), s. 1.

20 Zob. http://europa.eu/rapid/press-release_IP-10-1462_pl.htm?locale=pl (dostęp: 31.7.2018 r.).

21 Zob. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PL (dostęp: 31.7.2018 r.).

22 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, Bruksela, 25.1.2012 r., http://orka.sejm.gov.pl/sue7.nsf/pliki-zal/com_2012_9_pl_acte_f.pdf/$file/com_2012_9_pl_acte_f.pdf (dostęp: 31.7.2018 r.).

23 Zob. http://www.giodo.gov.pl/234/id_art/2501/j/pl/ (dostęp: 31.7.2018 r.).

akt prawny, jakim ma być rozporządzenie europejskie, zaradziłby temu rozdrobnieniu i kosztownym obciążeniom administracyjnym[24].

Zgodnie z art. 5 ust. 3 Traktatu o Unii Europejskiej z 7.2.1992 r. (Dz.U. z 2004 r. Nr 90, poz. 864 ze zm.) UE podejmuje działania tylko wówczas, gdy cele zamierzonego działania nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, i jeśli ze względu na rozmiary lub skutki proponowanego działania możliwe jest lepsze ich osiągnięcie na poziomie UE. Argumentów przemawiających za podjęciem takich działań było wiele, niektóre z nich to:

1) prawo do ochrony danych osobowych wymaga tego samego poziomu ochrony danych w całej UE; w przeciwnym wypadku istnieje ryzyko różnych poziomów ochrony w państwach członkowskich oraz ograniczeń w przepływie danych osobowych między państwami członkowskimi mającymi różne standardy;
2) konieczność współpracy między państwami członkowskimi i ich organami, którą należy zorganizować na szczeblu UE, by zagwarantować jednolite stosowanie prawa UE;
3) państwa członkowskie nie mogą same ograniczyć problemów w obecnej sytuacji, zwłaszcza w obliczu rozdrobnienia w krajowych przepisach;
4) proponowane działania legislacyjne UE będą bardziej skuteczne niż podobne działania na szczeblu państw członkowskich ze względu na charakter i skalę problemów, które nie ograniczają się do szczebla jednego państwa czy kilku państw członkowskich.

W marcu 2014 r. Parlament Europejski już w pierwszym czytaniu zajął pozytywne stanowisko w sprawie projektów rozporządzenia i dyrektywy[25], a rok później w czerwcu Rada zgodziła się z wnioskami Parlamentu i zatwierdziła ogólne, całościowe podejście do ochrony danych osobowych w UE[26]. Trójstronne negocjacje pomiędzy Radą Unii Europejskiej, Parlamentem Europejskim i Komisją Europejską, mające na celu ustalenie ostatecznej wersji pakietu dokumentów, zakończyły się 15.12.2015 r.

Na posiedzeniach 12.2.2016 r. Rada wypracowała porozumienie polityczne w sprawie projektu rozporządzenia (dokument 5455/15), a 8.4.2016 r. przyjęła stanowisko w pierwszym czytaniu, w pełni zgodne z kompromisowym tekstem uzgodnionym podczas nieformalnych negocjacji z Parlamentem. Oba zaproponowane akty zostały przyjęte przez Parlament Europejski 14.4.2016 r. Rozporządzenie w Dz.Urz. UE zostało opublikowane 4.5.2016 r., ale jego przepisy są stosowane od 25.5.2018 r. – co dało wszystkim przetwarzającym ponad 2 lata na przygotowania (zob. motyw 171 RODO).

---

24 Zob. http://europa.eu/rapid/press-release_IP-12-46_pl.htm (dostęp: 31.7.2018 r.).

25 Parlament Europejski głosował nad propozycją rozporządzenia 12.3.2014 r. – wniosek przyjęto 621 głosami za, 10 – przeciw, 22 osoby wstrzymały się od głosu. Zob. http://europa.eu/rapid/press-release_MEMO-14-186_en.htm (dostęp: 31.7.2018 r.). Dokładniej ze zmianami można zapoznać się w dokumencie: Rezolucja ustawodawcza Parlamentu Europejskiego z 12.3.2014 r. w sprawie wniosku dotyczącego 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) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD) – https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52014AP0212.

26 Zob. http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/pl/pdf (dostęp: 31.7.2018 r.).

4.13. Ustawa o ochronie danych osobowych z 2018 r.

Przyjęcie OchrDanychU uchyliło jej poprzednią wersję i akty wykonawcze, których była ona podstawą prawną. Służy ona stosowaniu RODO. Zatem w przypadku Polski **RODO trzeba analizować razem z OchrDanychU**. Ustawa reguluje m.in. następujące kwestie:

1) wyznaczanie inspektora ochrony danych,
2) postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych,
3) kontrola przestrzegania przepisów,
4) odpowiedzialność (cywilna, karna i administracyjne kary pieniężne) za naruszenie przepisów.

Podstawa prawna:

- art. 1 ust. 1, art. 7, 20, motyw 2 dyrektywy 95/46/WE,
- art. 8 EKPCz,
- art. 23, 24 KC,
- art. 47, 51, 133 Konstytucji RP,
- art. 1 konwencji Nr 108,
- art. 8, 45 ust. 1 KPP,
- art. 27 ust. 1 OchrDanychU,
- motyw 9 i 171 RODO,
- art. 5 ust. 3 Traktatu o Unii Europejskiej.