Michał Kamiński
Michał Ordyniak

Charakterystyka najważniejszych problemów związanych z ochroną danych osobowych w kontekście realizacji ustawowych zadań służb specjalnych

1. Ochrona danych osobowych w służbach specjalnych w ramach polskiego systemu prawnego

W kontekście konstytucyjnych praw i wolności jednostki ochrona danych osobowych jest nierozerwalnie związana z prawem do prywatności, autonomii informacyjnej oraz wolności komunikowania się.

Tematem niniejszego artykułu nie jest jednak ochrona danych osobowych sama w sobie, tylko relacje tejże materii wobec zadań realizowanych przez służby odpowiedzialne za bezpieczeństwo państwa, przede wszystkim w kontekście zapewniania bezpieczeństwa, które może się przejawiać jako bezpieczeństwo wewnętrzne, zewnętrzne oraz publiczne. Ujęcie tej problematyki w kontekście służb, w tym służb specjalnych, skupia jak w soczewce podstawowe zagadnienie dotyczące konkurencji dwóch konstytucyjnych wartości, jakimi są prawa i wolności obywatelskie oraz bezpieczeństwo państwa. Wynika to z konieczności ograniczania w niektórych sytuacjach tychże konstytucyjnych praw jednostki z uwagi na ochronę bezpieczeństwa państwowego.

Sprawą najważniejszą jest odpowiednie ważenie obu tych wartości i wprowadzanie niezbędnych ograniczeń w taki sposób, aby żadna z nich nie utraciła swego podstawowego znaczenia. Sam Trybunał Konstytucyjny podkreślił, że (…) *graniczenie praw jednostki jest możliwe w sytuacji konfliktu dwóch wartości, z jednej strony ochrony konstytucyjnej wolności lub prawa jednostki, ochrony bezpieczeństwa lub porządku publicznego, ochrony środowiska, zdrowia i moralności publicznej albo wolności i praw innych osób z drugiej strony* (wyrok z 29 stycznia 2002 r., sygn. K 19/01). Jednocześnie Trybunał podkreślił wagę zasady proporcjonalności, która winna być punktem wyjścia przy stosowaniu tego typu ograniczeń. W orzeczeniu z 26 kwietnia 1995 r., sygn. K 11/94, stwierdził, że (…) *dla oceny, czy doszło do naruszenia zasady zakazu nadmiernej ingerencji konieczne jest zbadanie, czy wprowadzona regulacja ustawodawcza jest w stanie doprowadzić do zamierzonych przez nią skutków, czy jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana oraz czy efekty wprowadzanej regulacji pozostają w proporcji do ciężarów nakładanych przez nią na obywatela, bowiem ustawodawca konstytucyjny szczególny nacisk położył na kryterium konieczności*. To stwierdzenie zostało później potwierdzone przez Trybunał, m.in. w wyrokach z 11 kwietnia 2000 r. (sygn. K 15/98) czy z 23 listopada 2009 r. (sygn. K 61/08), w których podkreślił, że proporcjonalność jest składową trzech zasad: zasady przydatności, zasady konieczności oraz zasady proporcjonalności sensu stricto, tzn. zakazu nadmiernej ingerencji.

Celem niniejszych rozważań, nie jest wskazywanie, której z tych wartości należy nadać przymiot pierwszeństwa. Ważniejszą sprawą jest znalezienie tzw. złotego środka, sposobu na realizowanie zarówno jednej, jak i drugiej wartości przez wprowadzanie

niezbędnych ograniczeń na gruncie ustawy. Rzeczą niezbędną jest dokonanie właściwej oceny zadań i uprawnień służb na tle poszanowania i ochrony przez władze publiczne praw i wolności jednostki. Należy pamiętać, że nadanie którejkolwiek z tych konstytucyjnych wartości prymatu może spowodować, iż albo prawa i wolności obywatelskie będą nagminnie łamane, albo organy państwa nie będą mogły skutecznie stać na straży bezpieczeństwa państwa.

Samo zagadnienie bezpieczeństwa można porównać do państwa jako tarczy, której personifikacją są powołane i należycie zadaniowane służby, w tym służby specjalne. Rolą ustawodawcy, ale także Trybunału Konstytucyjnego, jest określenie ram realizowania w tym wymiarze zadań przy uwzględnieniu ochrony praw i wolności jednostki. Jednak przy opracowywaniu właściwych rozwiązań nie można zapominać o stanowisku instytucji pro-wolnościowych, których zadaniem jest wskazywanie zagrożeń wynikających z uprawnień nadanych służbom przez ustawodawcę lub przydzielonych zadań. Należy podkreślić, że wyłącznie przez współdziałanie wszystkich tych podmiotów będzie możliwe wypracowanie stosownych rozwiązań.

Sam Trybunał Konstytucyjny w wyroku z 30 lipca 2015 r. (sygn. K 23/11) wskazał, że:

> (…) ciążący na organach państwa obowiązek zagwarantowania wolności i praw oznacza nie tylko zakaz nadmiernej ingerencji, w tym polegającej na niejawnym pozyskiwaniu przez organy państwa informacji o osobach, ale ma szerszy wymiar. Wynika z niego obowiązek stworzenia przez państwo warunków, w których obywatele z zagwarantowanych im wolności i praw mogą swobodnie korzystać. Warunkiem zapewnienia wolności i praw jest zaś poczucie bezpieczeństwa w państwie i braku zagrożeń obywateli. Osiągnięcie tego stanu możliwe jest m.in. poprzez zwalczanie przestępczości mogącej zagrażać wolności człowieka, korzystanie z własności czy podejmowanie działalności gospodarczej. Z drugiej strony, korelatem konstytucyjnego obowiązku państwa, o którym mowa w art. 5 Konstytucji RP, jest także prawo obywateli do ochrony ich bezpieczeństwa przed zewnętrznymi i wewnętrznymi zagrożeniami, w tym terroryzmem i przestępczością.

W tym samym wyroku Trybunał uznał, że:

> (…) choć czynności operacyjno-rozpoznawcze popadają w konflikt z prawem do ochrony prywatności, wolnością i ochroną tajemnicy komunikowania się czy autonomią informacyjną, mogą być uznane za konieczne w demokratycznym państwie prawa z uwagi na ochronę bezpieczeństwa państwa, porządku publicznego bądź ochronę wolności i praw innych osób.

Tym samym Trybunał wskazał na zależność istniejącą pomiędzy tymi dwiema wartościami, którą skrótowo można określić jako: bezpieczne państwo to bezpieczny obywatel.

Efektem tych rozważań, zarówno w opracowywaniu wniosków krótkofalowych, jak i długofalowych, powinna być świadomość istnienia tych dwóch – w sumie przeciwstawnych – konstytucyjnych wartości obok siebie, a co za tym idzie – konieczność ich stałego ważenia w celu znalezienia najwłaściwszego rozwiązania.

Jak już zwrócono uwagę na wstępie, celem niniejszych rozważań jest ochrona danych osobowych w odniesieniu do działalności służb, w tym służb specjalnych. Dlatego też w dalszej części ta problematyka będzie rozwijana.

W pierwszej kolejności należy zwrócić uwagę, że tę sprawę można interpretować w dwojaki sposób. W ujęciu wąskim pod pojęciem ochrona danych osobowych będziemy rozumieli wyłącznie problem ochrony i przetwarzania tego typu danych zgromadzonych przez poszczególne służby specjalne, bez odnoszenia się do sposobu i trybu ich uzyskiwania. Zastosowanie w tym zakresie będą miały przepisy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. Z drugiej strony przedmiot rozważań można rozpatrywać w znaczeniu szerokim, w którego ramach będzie konieczne odniesienie się do właściwości danej służby, jej zadań, a także formy realizacji tych zadań, podczas realizacji których może pojawić się problem dostępu do danych osobowych.

Najważniejsze znaczenie dla wąskiego spojrzenia na ochronę danych osobowych przetwarzanych przez Agencję Bezpieczeństwa Wewnętrznego ma wspomniana ustawa o ochronie danych osobowych, która zawiera przepisy ogólne i podstawowe odnoszące się do omawianej kwestii. W art. 3 jest mowa o zakresie stosowania tej ustawy przez organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne. Kolejne istotne przepisy to art. 40 oraz 43. Zgodnie z pierwszym z nich administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych. Drugi przywołany artykuł zawiera wykaz zbiorów informacji, których zgłoszenie do GIODO jest wyłączone spod tego obowiązku. Przykładowo należy wskazać dane zawierające informacje niejawne (ust. 1 pkt 1), dane które zostały uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do wykonywania tych czynności (ust. 1 pkt 1a), przetwarzane przez właściwe organy na potrzeby postępowania sądowego (ust. 1 pkt 2) czy też np. dane przetwarzane przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (ust. 1 pkt 2c), które są najistotniejsze z punktu widzenia ABW.

Należy w tym miejscu zwrócić uwagę, że w 2010 r. te ogólne regulacje zostały uzupełnione o lex specialis regulujący omawiane zagadnienie w kontekście funkcjonowania jednej ze służb, tj. Centralnego Biura Antykorupcyjnego. Przepisy, o których mowa, są zawarte w art. 22b ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym, który wprowadza nową instytucję – pełnomocnika do spraw kontroli przetwarzania w CBA danych osobowych. Trzeba nadmienić, że w przepisach prawa powszechnego nie ma wyraźnie wyodrębnionych trybów postępowania z informacjami stanowiącymi dane osobowe, właściwych tylko dla tej grupy informacji i tak rozbudowanego od strony formalnej systemu ochrony, jak ma to miejsce w odniesieniu do CBA. W okresie sprawowania rządów przez sejm poprzedniej kadencji trwały prace legislacyjne mające na celu wprowadzenie tego rodzaju instytucji w Agencji Bezpieczeństwa Wewnętrznego. Jednakże w związku z tym, że zostały one wstrzymane, należy przyjąć, iż w odniesieniu do ABW wyznacznikiem są tylko przepisy ustawy o ochronie danych osobowych. Na tej podstawie prawnej zbudowano w Agencji system zabezpieczania informacji zawierających dane osobowe, który opiera się na aktach prawnych o charakterze wewnętrznym, wydanych przez szefa ABW. Te przepisy w pełni uwzględniają dyrektywy wynikające z art. 36 ustawy o ochronie danych osobowych przez to, że zapewniają zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, przywłaszczeniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Trzeba wskazać, że dane osobowe są jedynie jednym z elementów informacji przetwarzanych w ABW. W większości są to informacje niejawne, w tym dane zdobyte

w wyniku czynności operacyjno-rozpoznawczych i podczas przeprowadzania czynności śledczych, związane z realizacją zadań, o których mowa w art. 5 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. W ich ramach mogą być zbierane m.in. dane osobowe. Ochrona tego rodzaju informacji jest jednym z obowiązków ABW wyrażonym w art. 35 ust. 1 tej ustawy, zgodnie z którym ABW w związku z wykonywaniem swoich zadań zapewnia ochronę środków, form i metod służących ich realizacji, a także zgromadzonych informacji oraz własnych obiektów i danych identyfikujących funkcjonariuszy Agencji. Należy również mieć na względzie przepisy ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych. Zgodnie z art. 11 tej ustawy szef ABW pełni funkcję krajowej władzy bezpieczeństwa. Z tego powodu systemy ochrony danych i informacji w Agencji muszą spełniać najwyższe standardy bezpieczeństwa, a zatem zbiory, w których zawarte są m.in. dane osobowe, są chronione na najwyższym poziomie. Dane osobowe uzyskane w ten sposób są jedynie elementem innych informacji przetwarzanych w ABW, które w większości są informacjami niejawnymi. Do ochrony tego rodzaju informacji zostały zastosowane środki o najwyższym możliwym poziomie bezpieczeństwa. Z powyższego wynika, że system ochrony informacji niejawnych w ABW obejmuje również ochronę danych osobowych. Należy również stwierdzić, że ten system spełnia wymogi wynikające z ustawy o ochronie danych osobowych oraz z ustawy o ochronie informacji niejawnych. Ponadto charakter danych przetwarzanych w ABW uzasadnia podstawę do odstąpienia od obowiązku zgłaszania prowadzonych zbiorów informacji GIODO i jednocześnie ją stanowi. Na marginesie trzeba dodać, że w ABW nie został powołany administrator bezpieczeństwa informacji, o którym mowa w art. 36a ustawy o ochronie danych osobowych, gdyż ten przepis ma charakter fakultatywny, a w przypadku ABW te zadania szef Agencji realizuje za pośrednictwem struktury wewnętrznej ABW, a obowiązki dla poszczególnych jednostek organizacyjnych określa w aktach prawa wewnętrznego. Zadania w tym zakresie są zatem skorelowane z wymogami dotyczącymi bezpieczeństwa innych informacji, w tym zwłaszcza informacji niejawnych.

Wspomniane akty prawne dotyczą informacji niejawnych i z tego względu nie mogą być przedstawione szczegółowe rozwiązania. W ramach wspomnianego systemu zapewniono:

- mechanizm ewidencjonowania baz danych z jednoczesnym określeniem zakresu gromadzonych w nich informacji i sposobu ich pozyskiwania, wynikający m.in. z zarządzenia nr Pf-15 szefa ABW z 28 marca 2013 r. w sprawie ewidencji operacyjnej i innych zbiorów informacji w Agencji Bezpieczeństwa Wewnętrznego. Ta regulacja koreluje z normą wynikającą z art. 40 ustawy o ochronie danych osobowych;
- system ochrony danych osobowych, który jest skorelowany z pozostałymi systemami bezpieczeństwa działającymi w ABW. Przykładowo można wskazać zarządzenie nr Z-46 szefa ABW z 9 grudnia 2014 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych i jawnych w Agencji Bezpieczeństwa Wewnętrznego;
- system kontroli wewnętrznej, który odnosi się do wszelkich spraw związanych z bezpieczeństwem i przetwarzaniem informacji zawartych zarówno w bazach danych ABW, jak i w bazach danych innych uprawnionych podmiotów, do których dostęp mają funkcjonariusze Agencji. Te zadania są realizowane jako jeden z obowiązków jednostki organizacyjnej uprawnionej do prowadzenia kontroli oraz audytu wewnętrznego.

Mając na uwadze powyższe, a także zakres i sposób pozyskiwania informacji przez poszczególne służby specjalne, należy stwierdzić, że kwestie związane z ochroną danych osobowych muszą, oprócz respektowania wcześniej wskazanych konstytucyjnych praw i wolności obywatelskich, uznawać dyrektywy dotyczące bezpieczeństwa państwa oraz konieczność zapewniania bezpieczeństwa jego obywatelom, wynikające również z Konstytucji RP. Trzeba też wywnioskować, że nie można zbudować jednolitego, wspólnego systemu ochrony danych osobowych dla wszystkich służb i organów państwowych. Dostrzegł to również sam ustawodawca, robiąc wyjątek od obowiązku zgłaszania pewnych zbiorów informacji GIODO. W pełni uzasadnione jest twierdzenie, że zasady ochrony danych osobowych poszczególnych służb powinny być ściśle powiązane z zadaniami i zakresem informacji, które są gromadzone przez te służby. Jak się wydaje, taką właśnie okoliczność miał na uwadze również sam ustawodawca podczas uchwalania ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i ustawy o Centralnym Biurze Antykorupcyjnym. Ustawa o ochronie danych osobowych została uchwalona w 1997 r., pozostałe zaś, wymienione wyżej, w 2002 i 2010 r. (art. 22b ustawy o Centralnym Biurze Antykorupcyjnym). W przypadku, gdyby celem ustawodawcy było ustanowienie takiego systemu ochrony danych osobowych, który byłby wspólny dla wszystkich podmiotów państwowych, nie zawierałby on żadnych wyłączeń w przepisach, zwłaszcza takich, jakie dotyczą art. 43 ustawy o ochronie danych osobowych. Ten przepis bez wątpienia odnosi się do służb odpowiedzialnych za jedną z najważniejszych funkcji państwa, jakim jest zapewnianie bezpieczeństwa, w tym bezpieczeństwa obywateli. Ponadto przy uchwalaniu art. 22b ustawy o Centralnym Biurze Antykorupcyjnym również nie doszło do nowelizacji ustaw pozostałych służb pod kątem uwzględnienia w nich wspomnianego wcześniej pełnomocnika ochrony informacji niejawnych.

Na zakończenie problematyki dotyczącej ochrony danych osobowych należałoby zasygnalizować inne, szerokie spojrzenie na ten temat. Jak wspomniano na wstępie, państwo, realizując obowiązki gwaranta bezpieczeństwa własnego i własnych obywateli, pełni funkcję swoistej tarczy przed zagrożeniami. Uprawnienia odnoszące się do przeciwdziałania zagrożeniom muszą być wyrażone w formie przepisów prawnych odpowiedniego poziomu. Konieczne przy tym jest, aby te przepisy były skorelowane z zadaniami nałożonymi na daną służbę, a także aby nie ingerowały w kompetencje innych podmiotów. Tylko w taki sposób zbudowany system prawny pozwoli na sprawną i skuteczną realizację zadań ustawowych oraz będzie odpowiadał zasadzie legalizmu wynikającej z art. 7 Konstytucji RP.

W tym miejscu trzeba wspomnieć o roli ABW w procesie legislacyjnym. Jak wiadomo inicjatywa ustawodawcza przysługuje posłom, senatowi, Prezydentowi RP, Radzie Ministrów oraz grupie obywateli. W tym zakresie ABW może pełnić jedynie funkcję konsultacyjną. W przypadku, gdy rządowy projekt aktu prawnego dotyczy zadań, uprawnień bądź też w inny sposób odnosi się do działalności ABW, jest on zgodnie z § 35 ust. 3 uchwały nr 190 Rady Ministrów z 29 października 2013 r. – Regulamin pracy Rady Ministrów, przekazywany szefowi ABW do konsultacji. W przypadku zaś, gdy dany projekt ustawy jest na etapie prac parlamentarnych, ABW ma uprawnienie jedynie do wyrażenia opinii na temat projektowanych rozwiązań w trakcie prac nad stanowiskiem rządu opracowywanym wobec pozarządowego projektu ustawy. Ponadto należy zauważyć, że sprawy związane z bezpieczeństwem państwa należą do właściwości Rady Ministrów. Dlatego też podjęcie decyzji o nałożeniu zadań na daną służbę należy do tego właśnie podmiotu, na który ABW praktycznie nie ma żadnego wpływu. Nie może być

bowiem mowy o „samozadaniowaniu się" służb, tylko o wykonywaniu poleceń organów, którym są podległe. Opinie ABW mogą dotyczyć zwłaszcza przepisów określających uprawnienia danej służby, ich skuteczności bądź nieprzydatności w odniesieniu do zadań, które mają być wykonywane.

2. System ochrony danych osobowych w Unii Europejskiej z perspektywy służb specjalnych

2.1. Obecny stan prawny

Omawiając kwestie związane z ochroną danych osobowych, należy zaznaczyć, że kształt polskiego ustawodawstwa w tym zakresie jest w znacznej mierze determinowany przepisami prawa Unii Europejskiej.

Jako najistotniejsze akty prawa regulujące materię związaną z ochroną danych należy wymienić:

- *Dyrektywę 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* (Dz.Urz. UE L z 1995 r. nr 281, s. 31)
- oraz *Decyzję ramową Rady 2008/977/WSiSW z dnia 27 listopada 2008 roku w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych* (Dz.Urz. UE L z 2008 r. Nr 350, s. 60).

2.1.1. Dyrektywa 95/46/WE

Celem dyrektywy 95/46/WE było zapewnienie harmonizacji przepisów o ochronie danych osobowych na terenie Wspólnoty Europejskiej wobec zaobserwowania tego, że różnica w stopniu ochrony praw i wolności jednostek w odniesieniu do prawa do prywatności może uniemożliwiać przesyłanie tych danych pomiędzy państwami członkowskimi, utrudniając realizację wielu przedsięwzięć ekonomicznych i zakłócając tym samym funkcjonowanie Wspólnego Rynku[1]. W motywach preambuły znajdują się również odniesienia do aktów prawa międzynarodowego regulujących ochronę prawa do prywatności – artykułu 8 Europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności[2] oraz Konwencji Rady Europy z 28 stycznia 1981 r. w sprawie ochrony jednostek w zakresie automatycznego przetwarzania danych osobowych[3], jako wyznacznika ram standardów ochrony tego typu danych obowiązujących na terenie Europy, które twórcy wzięli pod uwagę, jednak bez wskazania, że realizacja praw jednostki zapisanych w tych przepisach jest celem wydania dyrektywy. O uchwaleniu omawianej dyrektywy zadecydowały zatem głównie przesłanki ekonomiczne, zgodnie z podstawowym celem Wspólnoty Europejskiej, jakim było ustanowienie i zapewnienie funkcjonowania wspólnego rynku. Motyw 13 preambuły omawianej dyrektywy stanowi, że działania określone w tytułach V i VI (wspólna polityka zagraniczna i bezpieczeństwa oraz współpraca w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych) Traktatu o Unii Europejskiej (dalej: TUE) dotyczące bezpieczeństwa

[1] Motyw 7 preambuły.
[2] Motyw 10 preambuły.
[3] Motyw 11 preambuły.

publicznego, obronności i bezpieczeństwa państwa w dziedzinie prawa karnego nie wchodzą w zakres stosowania prawa wspólnotowego. Również przetwarzanie danych osobowych konieczne do zapewnienia ochrony dobrego stanu gospodarczego państwa nie wchodzi w zakres stosowania niniejszej dyrektywy, o ile takie przetwarzanie dotyczy spraw odnoszących się do bezpieczeństwa państwa. Podobny zapis został zawarty w art. 3 omawianej dyrektywy, określającym zakres jej obowiązywania. Zgodnie z ust. 2 wskazanego artykułu:

> 2. Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych:
> – w ramach działalności wykraczającej poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI Traktatu o Unii Europejskiej, a w żadnym razie do działalności na rzecz bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa (łącznie z dobrą kondycją gospodarczą państwa, gdy działalność ta dotyczy spraw związanych z bezpieczeństwem państwa) oraz działalności w obszarach prawa karnego,
> – przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze.

Warto jednak zauważyć, że wskazane wyłączenie odsyła do traktatu o Unii Europejskiej w wersji sprzed wejścia w życie traktatu lizbońskiego[4]. Obecny Tytuł VI TUE nie reguluje już zagadnienia współpracy w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych, która to dziedzina, stanowiąca dawny trzeci filar Unii Europejskiej, stała się jedną z rodzajów polityki Unii Europejskiej (Przestrzeń wolności, bezpieczeństwa i sprawiedliwości), objętych zakresem jej kompetencji (w tym wypadku są to kompetencje dzielone między Unię Europejską i państwa członkowskie, stosownie do art. 4 ust. 2 lit. j traktatu o funkcjonowaniu Unii Europejskiej), co może budzić wątpliwości odnośnie do aktualności tego wyłączenia. Jak pisze Agnieszka Grzelak w pracy *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*:

> Wskazanie, iż wyłączona z zakresu zastosowania dyrektywy jest działalność wykraczająca „poza zakres prawa Wspólnoty, jak np. dane, o których stanowi tytuł V i VI TUE", straciło w chwili obecnej znaczenie o tyle, że obecnie Unia Europejska zastąpiła Wspólnoty Europejskie, a TUE nie reguluje już kwestii związanych ze współpracą policyjną i sądową w sprawach karnych. Można by było zadać pytanie, czy zatem dyrektywa 95/46 w obecnym stanie prawnym nie reguluje już kwestii związanych z omawianym obszarem, jednak przepis art. 3 ust. 2 tiret pierwsze dyrektywy zawiera dodatkowe wskazanie, stwierdzając, że dyrektywa nie ma zastosowania „w żadnym razie" do działalności na rzecz bezpieczeństwa publicznego czy też działalności państwa w obszarach prawa karnego. Nie ma zatem wątpliwości, że wejście w życie TL nie zmieniło zakresu zastosowania dyrektywy 95/46 (…)[5].

Przepisy omawianej dyrektywy nie odnoszą się zatem w dalszym ciągu do przetwarzania danych osobowych zarówno przez organa ścigania, jak i służby specjalne.

---

[4] Traktat z Lizbony zmieniający traktat o Unii Europejskiej i traktat ustanawiający Wspólnotę Europejską (Dz. Urz. UE C z 2007 r. nr 306, s. 1, ze zm.) wszedł w życie 1 grudnia 2009 r.

[5] A. Grzelak, *Ochrona danych osobowych we współpracy państw członkowskich UE w zwalczaniu przestępczości. W stronę standardu europejskiego*, Warszawa 2015, s. 196–197.

Transpozycja dyrektywy 95/46/WE do polskiego porządku prawnego nastąpiła w przepisach ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych.

2.1.2. Decyzja ramowa Rady 2008/977/WSiSW

Decyzja ramowa Rady 2008/977/WSiSW została wydana jako instrument III filaru Unii Europejskiej. Powodem jej wydania było ustanowienie wspólnych norm przetwarzania i ochrony danych osobowych w celu zapobiegania i zwalczania przestępczości z zamiarem poprawy współpracy policyjnej i sądowej w sprawach karnych pod kątem jej skuteczności i legalności oraz zgodności z prawami podstawowymi, w szczególności z prawem do prywatności i do ochrony danych osobowych[6].

Celem powyższej decyzji, zgodnie z jej art. 1 ust. 1, jest zapewnienie wysokiego poziomu ochrony praw podstawowych i wolności osób fizycznych, a zwłaszcza ich prawa do prywatności, podczas przetwarzania danych osobowych w ramach współpracy policyjnej i sądowej w sprawach karnych.

Decyzja ramowa ma stosunkowo wąski zakres regulacji, ograniczony do przetwarzania danych osobowych przekazywanych lub udostępnianych między państwami członkowskimi Unii Europejskiej w ramach współpracy policyjnej i sądowej w sprawach karnych. Ponadto jej art. 1 ust. 4 stanowi, że *Niniejsza decyzja ramowa nie narusza podstawowych interesów bezpieczeństwa narodowego i określonych działań wywiadowczych w zakresie bezpieczeństwa narodowego*. Nie będzie więc nadużyciem stwierdzenie, że obowiązujące w chwili obecnej przepisy prawa Unii Europejskiej tylko w niewielkim stopniu regulują ochronę danych osobowych przetwarzanych przez organy ścigania, przetwarzanie danych przez organy wywiadowcze (służby specjalne) zaś jest w zasadzie wyłączone z ich regulacji.

Decyzja ramowa nakazuje poddanie przetwarzania danych osobowych przez właściwe organy zasadom legalności, proporcjonalności i celowości (art. 3), nakazuje także korygowanie danych nieścisłych, usuwanie lub anonimizowanie danych, których dalsze przetwarzanie nie jest już potrzebne (art. 4), wprowadza ograniczenia w zakresie przetwarzania kategorii danych szczególnie wrażliwych (art. 6) oraz wprowadza zasadę, zgodnie z którą transfer danych osobowych jest dokonywany wyłącznie do tych krajów trzecich, które zapewniają odpowiedni poziom ochrony (art. 13). Decyzja ramowa nakazuje, aby państwa członkowskie zapewniły podstawowe prawa podmiotu danych: prawo do informacji o gromadzeniu lub przetwarzaniu danych osobowych oraz ich udostępnieniu (art. 16–17), prawo do uzyskania korekty danych, ich usunięcia lub zablokowania do nich dostępu (art. 18), prawo do odszkodowania, w przypadku poniesienia szkody na skutek niezgodnej z prawem operacji przetwarzania danych (art. 19) oraz możliwość skorzystania ze środków odwoławczych (art. 20). Jednocześnie państwa członkowskie uzyskały uprawnienie w zakresie ograniczania wykonywania przez podmiot danych prawa do informacji, jeśli takie ograniczenie stanowiłoby skuteczny i proporcjonalny środek pozwalający na uniknięcie przeszkód w prowadzonych postępowaniach, pozwalałoby uniknąć niekorzystnego wpływu na zapobieganie przestępstwom, ich ściganie, wykrywanie lub karanie oraz wykonywanie sankcji karnych, jeśli służyłoby ochronie bezpieczeństwa publicznego, bezpieczeństwa narodowego oraz ochronie osoby, której dotyczą dane, a także praw i wolności innych osób

[6] Tak stanowi motyw 3 preambuły decyzji ramowej Rady 2008/977/WSiSW.

(art. 17 ust. 2). Zgodnie z art. 17 ust. 3 każda odmowa lub ograniczenie dostępu powinno zostać przedstawione na piśmie osobie, której dane dotyczą, wraz z pouczeniem o możliwości wniesienia odwołania.

Decyzja ramowa została zaimplementowana do prawa polskiego w przepisach ustawy z 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (Dz.U. z 2011 r. nr 230 poz. 1371, ze zm.). Ta ustawa wdrożyła jeszcze trzy inne instrumenty z zakresu trzeciego filaru Unii Europejskiej, a mianowicie:

- decyzję Rady 2008/615/WSiSW z 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości zorganizowanej (Dz. Urz. UE L z 2008 r. nr 210, s. 1),
- decyzję Rady 2007/845/WSiSW z 6 grudnia 2007 r. dotyczącą współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem (Dz. Urz. UE L z 2007 r. nr 332, s. 103),
- decyzję ramową Rady 2006/960/WSiSW z 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami państw członkowskich Unii Europejskiej (Dz. Urz.UE L z 2006 r. nr 386, s. 89 oraz z 2007 r. nr 75 poz. 36).

Zgodnie z art. 1 ust. 1 ustawy implementującej: *Ustawa określa zasady i warunki wymiany informacji z organami ścigania państw członkowskich Unii Europejskiej w celu wykrywania i ścigania sprawców przestępstw lub przestępstw skarbowych oraz zapobiegania przestępczości i jej zwalczania oraz przetwarzania informacji, a także podmioty uprawnione w tych sprawach*. Ochrona danych osobowych nie została zatem nawet wymieniona wśród głównych celów ustawy. Natomiast wśród podmiotów uprawnionych do wymiany informacji (na jej podstawie) z organami ścigania państw członkowskich Unii Europejskiej w celu wykrywania i ścigania przestępstw lub przestępstw skarbowych, zapobiegania przestępczości i jej zwalczania oraz przetwarzania informacji przepis art. 1 ust. 2 ustawy wymienia: Agencję Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Policję, Krajową Administrację Skarbową[7], Straż Graniczną i Żandarmerię Wojskową. Objęcie zakresem niniejszej ustawy Agencji Bezpieczeństwa Wewnętrznego jest związane z przyznaniem jej roli punktu kontaktowego do wymiany informacji, w tym danych osobowych, służących zapobieganiu przestępstwom terrorystycznym, co uczyniono w jej art. 32, dodającym ustęp 3 do artykułu 5 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Obowiązek ustanowienia przez każde państwo członkowskie Unii Europejskiej takiego punktu kontaktowego został przewidziany w art. 16 ust. 3 Decyzji Rady 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości zorganizowanej, której wdrożeniu do polskiego porządku prawnego służy również omawiana ustawa.

Ochrony danych osobowych dotyczy rozdział 4 omawianej ustawy. Przepisy tego rozdziału nakazują podmiotom uprawnionym dokonanie weryfikacji prawidłowości, aktualności i kompletności danych osobowych przekazywanych organom ścigania państw członkowskich Unii Europejskiej (art. 19), przechowywanie danych osobowych wyłącznie przez okres niezbędny do realizacji celu, w jakim zostały przekazane (art. 20), respektowanie ograniczeń dotyczących czasu przechowywania danych nałożonych przez organy ścigania państw członkowskich Unii Europejskiej (art. 21) i sposobu ich przetwarzania (art. 22)

[7] W pierwotnej wersji ustawy na liście właściwych organów w miejscu KAS znajdowały się: Służba Celna oraz organy kontroli skarbowej.

oraz dokumentowania przekazania lub udostępnienia albo otrzymania danych osobowych (art. 23). Określono warunki dopuszczalności przetwarzania danych osobowych otrzymanych od organu ścigania państwa członkowskiego Unii Europejskiej bez zgody tego organu (art. 24 ust. 1) i przetwarzania tych danych przez inne podmioty (art. 24 ust. 2). Wymiana informacji została poddana kontroli Generalnego Inspektora Ochrony Danych Osobowych (art. 25).

2.2. Reforma europejskiego systemu ochrony danych osobowych

Pod koniec pierwszej dekady XXI w. w prawie pierwotnym Unii Europejskiej zaszły zmiany, które otworzyły drogę wielkiej reformie europejskiego systemu ochrony danych osobowych. Mowa tu o przyjęciu traktatu z Lizbony oraz Karty Praw Podstawowych Unii Europejskiej.

Karta praw podstawowych Unii Europejskiej z 12 grudnia 2007 r. (Dz. Urz. UE C z 2007 r. nr 303 s. 1 oraz z 2010 r. nr 81 s. 9)[8] zawiera artykuł 8 przyznający każdemu mieszkańcowi Unii Europejskiej prawo do ochrony dotyczących go danych osobowych. Ustęp 3 wskazanego artykułu stanowi, iż *Dane te muszą przetwarzane być 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*. Sformułowane zostają zatem zasady rzetelności, celowości i legalności przetwarzania danych osobowych oraz prawa podmiotu danych: dostępu do dotyczących go danych i prawo do sprostowania. Ustęp 3 art. 8 stanowi, iż przestrzeganie tych zasad podlega kontroli niezależnego organu.

Jednocześnie w traktacie o funkcjonowaniu Unii Europejskiej, w brzmieniu określonym traktatem z Lizbony znalazł się artykuł 16, również regulujący kwestię ochrony danych osobowych. W ustępie 1 powtarza on zasadę wynikającą już z Karty Praw Podstawowych, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Natomiast ustęp 2 zawiera upoważnienie dla Parlamentu Europejskiego i Rady do określenia zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie zasad ochrony danych osobowych ma podlegać kontroli niezależnych organów. Uregulowanie tych kwestii przez Parlament Europejski i Radę ma nastąpić w ramach zwykłej procedury prawodawczej.

W wyniku wejścia w życie traktatu z Lizbony wraz z Kartą Praw Podstawowych Unia Europejska zyskała samoistną podstawę do uregulowania swoimi przepisami ochrony danych osobowych na swoim obszarze. Jest to zmiana rewolucyjna. Dotychczas obowiązująca dyrektywa 95/46/WE została wydana w celu ochrony wspólnego rynku, w wyniku konstatacji, że zróżnicowanie przepisów o ochronie danych osobowych na terenie Unii Europejskiej zaburza jego funkcjonowanie. Obecnie organy Unii Europejskiej są upoważnione do prawnego uregulowania tej kwestii i nie muszą zasadniczo ograniczać się w swoim podejściu perspektywą rynkową.

Jednocześnie traktat z Lizbony zniósł trzeci filar Unii Europejskiej, włączając w rzeczywistości współpracę policyjną i sądową w sprawach karnych do pierwszego filaru jako element przestrzeni wolności, bezpieczeństwa i sprawiedliwości.

Jednocześnie do aktu końcowego konferencji międzyrządowej, która przyjęła traktat z Lizbony podpisany w 13 grudnia 2007 r. dołączono *Deklarację 21* o treści:

[8] Karta Praw Podstawowych weszła w życie 1 grudnia 2009 r.

> Konferencja przyznaje, że konieczne może okazać się wprowadzenie zasad szczególnych dotyczących ochrony danych osobowych i swobodnego przepływu tych danych w dziedzinach współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej, zapewnianej na podstawie artykułu 16 Traktatu o funkcjonowaniu Unii Europejskiej, ze względu na szczególny charakter tych dziedzin[9].

W 2009 r. Komisja Europejska przeprowadziła przegląd istniejących ram prawnych w zakresie ochrony danych osobowych, rozpoczynając od konferencji na wysokim szczeblu w maju tego roku, po której nastąpiły konsultacje publiczne trwające do końce tego roku. Prowadzono również wiele analiz[10]. W opublikowanym 4 listopada 2010 r. Komunikacie Komisji Europejskiej do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów zatytułowanym *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej* stwierdzono, że z perspektywy piętnastu lat obowiązywania dyrektywy 95/46/WE należy zauważyć, iż szybki rozwój technologiczny i globalizacja doprowadziły do głębokich przemian w otaczającym nas świecie i przyniosły nowe wyzwania w zakresie ochrony danych osobowych. Wymieniono tu głównie rozwój usług świadczonych drogą elektroniczną, sieci społecznościowe w internecie oraz problem przetwarzania danych „w chmurze". Jak zauważyła Komisja Europejska:

> Równocześnie metody gromadzenia danych osobowych stały się coraz bardziej wyrafinowane i trudniej wykrywalne. Przykładowo użycie zaawansowanych narzędzi umożliwia podmiotom gospodarczym lepsze dobranie strategii przyjmowanej wobec poszczególnych jednostek dzięki monitorowaniu ich zachowania. (…) Także organy publiczne wykorzystują coraz większą ilość danych osobowych do różnych celów, takich jak ustalanie miejsca pobytu osób fizycznych w przypadku epidemii choroby zakaźnej, zapobieganie terroryzmowi i przestępczości oraz zwalczanie tych zjawisk, zarządzanie systemami zabezpieczenia społecznego do celów podatkowych, posługując się aplikacjami używanymi do administracji elektronicznej itd.[11]

Działania analityczne Komisji doprowadziły do wniosku, że podstawowe zasady zawarte w dyrektywie są nadal aktualne, jednak zidentyfikowano następujące sprawy problematyczne:

- reakcję na oddziaływanie nowych technologii (potrzeba sprecyzowania zasad ochrony danych osobowych w odniesieniu do nowych technologii),
- poprawę sytuacji w zakresie ochrony danych osobowych związanych z rynkiem wewnętrznym (brak dostatecznej harmonizacji przepisów),
- reakcję na globalizację oraz poprawę międzynarodowego przekazywania danych,
- zapewnienie lepszych rozwiązań instytucjonalnych w celu skutecznego egzekwowania przepisów o ochronie danych (wzmocnienie roli organów ochrony danych).

---

[9] http://oide.sejm.gov.pl/oide/index.php?option=com_content&view=article&id=14807&Itemid=948#21 [dostęp: 17 IX 2017].

[10] Komunikat Komisji do Parlamentu Europejskiego, Rady, Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów pt. *Całościowe podejście do kwestii ochrony danych osobowych w Unii Europejskiej*, s. 2, http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52010DC0609&from=EN [dostęp: 17 X 2017].

[11] Tamże, s. 1–2.

Komisja Europejska stwierdziła, że:

> Powyższe wyzwania wymagają od UE wypracowania kompleksowego i spójnego podejścia gwarantującego pełne poszanowanie podstawowego prawa osób fizycznych do ochrony ich danych osobowych poza nią: Traktat Lizboński zapewnił UE dodatkowe środki umożliwiające UE osiągnięcie tego celu: Kartę praw podstawowych UE, w art. 8 której uznano niezależne prawo do ochrony danych osobowych (…) wprowadzono również nową podstawę prawną umożliwiającą ustanowienie całościowych i spójnych unijnych przepisów o ochronie osób fizycznych w odniesieniu do przetwarzania ich danych osobowych oraz swobodnego przepływu takich danych[12].

Jako zasadnicze cele reformy europejskiego systemu ochrony danych osobowych Komisja Europejska wymieniła:
- wzmocnienie praw osób fizycznych,
- poprawę wymiaru związanego z rynkiem wewnętrznym,
- rewizję przepisów o ochronie danych w zakresie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych,
- globalny wymiar ochrony danych,
- zapewnienie lepszych rozwiązań instytucjonalnych w celu skuteczniejszego egzekwowania przepisów o ochronie danych.

Na wzmocnienie praw osób fizycznych miały się składać:
- zagwarantowanie odpowiedniej ochrony osobom fizycznym we wszystkich okolicznościach,
- zwiększenie przejrzystości wobec osób, których dane dotyczą,
- poprawę kontroli podmiotu danych nad własnymi danymi,
- pogłębianie świadomości społeczeństwa,
- zapewnienie osobie fizycznej realizacji prawa do świadomej i dobrowolnej zgody na przetwarzanie dotyczących jej danych osobowych,
- zapewnienie ochrony danych szczególnie chronionych,
- zapewnienie większej skuteczności sankcji i środków zaradczych.

Jako elementy poprawy wymiaru związanego z rynkiem wewnętrznym Komisja wymieniła:
- zwiększenie pewności prawnej oraz zapewnienie równych szans administratorom danych,
- zmniejszenie obciążeń administracyjnych,
- wyjaśnienie przepisów dotyczących prawa właściwego oraz odpowiedzialności państw członkowskich,
- wzmocnienie odpowiedzialności administratorów danych,
- zachęcanie do inicjatyw w dziedzinie samoregulacji oraz analizę unijnych systemów certyfikacji.

W zakresie globalnego wymiaru ochrony danych Komisja dostrzegła potrzebę:
- wyjaśnienia i uproszczenia przepisów dotyczących międzynarodowych transferów danych,
- propagowania uniwersalnych zasad.

[12] Tamże, s. 4–5.

W zakresie rewizji przepisów o ochronie danych osobowych w sferze współpracy policyjnej i sądowej w sprawach karnych Komisja Europejska powołała się na swoje stanowiska dotyczące programu sztokholmskiego (COM(2009)262 z 10 czerwca 2009 r.) oraz sztokholmskiego planu działania (COM(2010)171 z 20 kwietnia 2010 r.), w których podkreślono potrzebę zapewnienia (…) *systemu pełnej ochrony" oraz „wzmocnienia stanowiska UE dotyczącego ochrony danych osobowych w kontekście wszystkich obszarów polityki UE, w tym w dziedzinie egzekwowania prawa i zapobiegania przestępstwom*[13].

Podczas analizy decyzji ramowej Komisja zidentyfikowała następujące wady tego aktu:

- decyzja, o której mowa, dotyczy wyłącznie transgranicznej wymiany danych osobowych w granicach UE, nie mając zastosowania do wewnętrznych operacji przetwarzania danych w państwach członkowskich; w praktyce trudno odróżnić obie sytuacje, co może utrudniać faktyczne wprowadzenie w życie i stosowanie tego dokumentu,
- decyzja zawiera zbyt szerokie wyłączenie zasady celowości,
- w decyzji brakuje przepisów nakazujących rozróżnienie miedzy różnymi kategoriami danych,
- decyzja nie zastąpiła różnych sektorowych aktów legislacyjnych dotyczących współpracy policyjnej i wymiaru sprawiedliwości w sprawach karnych, przyjętych na szczeblu UE.

Komisja doszła do wniosku dotyczącego potrzeby rozważenia rewizji przepisów o ochronie danych w zakresie współpracy policyjnej i wymiarów sprawiedliwości w sprawach karnych. Zapowiedziała też ewentualne rozszerzenie stosowania ogólnych przepisów o ochronie danych na obszar współpracy policyjnej i sądowej w sprawach karnych, w tym na przetwarzanie danych na szczeblu krajowym, przy zapewnieniu harmonizacji ograniczeń praw podmiotów danych w tych sferach. Nie wykluczyła jednak przyjęcia szczególnych przepisów o ochronie danych w sektorze policyjnym i sądowym[14].

Komisja zapowiedziała przedstawienie w 2011 r. projektów przepisów zmierzających do rewizji prawnych ram ochrony danych osobowych w duchu podejścia kompleksowego, w kontekście wszystkich rodzajów polityki UE (w tym egzekwowania prawa i zapobiegania przestępczości), przy uwzględnieniu specyfiki tego obszaru[15].

W dniu 24 lutego 2011 r. Rada Unii Europejskiej przyjęła konkluzję, w której poparła zamiar Komisji dotyczący zreformowania ram ochrony danych[16]. To samo uczynił Parlament Europejski w rezolucji z 6 lipca 2011 r.[17]

W dniu 25 stycznia 2012 r. Unijna Komisarz ds. Sprawiedliwości i Praw Podstawowych Viviane Reding przedstawiła projekt kompleksowej reformy przepisów o ochronie danych osobowych. W uzasadnieniu wskazała, że obecnie obowiązujące przepisy w tym zakresie powstały w połowie lat 90. ubiegłego wieku i całkowicie nie przystają do realiów zinformatyzowanego społeczeństwa XXI wieku. Ochrona danych osobowych stanowi

[13] Tamże, s. 14.

[14] Tamże, s. 5–20

[15] Tamże, s. 20.

[16] *Uzasadnienie Wniosku Komisji Europejskiej – rozporządzenie 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), Bruksela dnia 25.1.2012 r. COM(2012) 11 final*, s. 4.

[17] Tamże; *Rezolucja PE z dnia 6 lipca 2011 r. w sprawie całościowego podejścia do kwestii ochrony danych osobowych w Unii Europejskiej (2011/2025(INI))*, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PL [dostęp: 21 IX 2017].

prawo podstawowe wszystkich Europejczyków, ale obywatele nie zawsze mają poczucie pełnej kontroli nad informacjami, które ich dotyczą. W przekonaniu V. Reding zmiany powinny budować zaufanie do usług internetowych oraz wpływać bezpośrednio na większy dostęp do danych osobowych tych osób, których one dotyczą. Komisja Europejska zaprezentowała projekt pakietu reform mających w sposób kompleksowy regulować problematykę związaną z ochroną danych osobowych w ramach Unii Europejskiej[18].

Pierwszym z projektów należących do przedstawionego pakietu był projekt *Ogólnego rozporządzenia o danych*[19]. Miał on derogować obowiązującą dyrektywę 95/46/WE oraz stworzyć nowe zasady regulujące system ochrony danych osobowych z wyłączeniem obszarów, w których będą obowiązywać regulacje szczególne, takich jak: przetwarzanie danych przez organy UE czy przetwarzanie danych w sferze policyjnej i sądowej w sprawach karnych. Projekt ogólnego rozporządzenia o danych został oparty na założeniu, że w całej Unii Europejskiej będzie obowiązywał jeden kompleksowy akt prawny, którego przepisy będą odnosiły bezpośredni skutek oraz będą bezpośrednio stosowane na płaszczyznach krajowych systemów prawnych.

Nieco inne podejście przyjęto w odniesieniu do sfery policyjnej i sądowej w sprawach karnych. W tym zakresie zdecydowano się na uchwalenie w miejsce obecnie obowiązującej decyzji ramowej Rady dyrektywy o ochronie danych osobowych[20]. Zakresem regulacji dyrektywy miało zostać objęte przetwarzanie danych przez organy policyjne i sądowe państw członkowskich na potrzeby ścigania przestępstw i zapobiegania im. Zniknęła znana z decyzji ramowej przesłanka wymiany danych między państwami członkowskimi.

Po trwającym ponad cztery lata procesie legislacyjnym obie części pakietu reformującego europejski system ochrony danych osobowych zostały ostatecznie przyjęte przez Parlament Europejski i Radę 27 kwietnia 2016 r., w brzmieniu nie odbiegającym zasadniczo od pierwotnych założeń.

W dniu 4 maja 2016 r. zostały opublikowane w Dzienniku Urzędowym Unii Europejskiej teksty następujących aktów prawnych:

1) *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (Dz. Urz. UE L nr 119, s. 1), zwane dalej: „rozporządzeniem odo";
2) *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW* (Dz. Urz. UE L z 2016 r. nr 119, s. 89), zwana dalej: „dyrektywą odo".

[18] http://europa.eu/rapid/press-release_IP-12-46_pl.htm [dostęp: 22 IX 2017]

[19] Wniosek Komisji Europejskiej – rozporządzenie 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), Bruksela 25 I 2012 r. COM(2012) 11 final.

[20] Wniosek Komisji Europejskiej – dyrektywa Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, Bruksela 25 I 2012 r. COM(2012) 10 final.

W rzeczywistości reforma europejskiego systemu ochrony danych osobowych zostanie wdrożona w maju 2018 r. Rozporządzenie odo wejdzie w życie 25 maja 2018 r., termin implementacji dyrektywy odo upływa zaś 6 maja tego samego roku.

Uwagę zwraca zasadnicze wzmocnienie czynnika regulacyjnego na poziomie europejskim: w zakresie ochrony danych osobowych w „sferze cywilnej" akt harmonizujący ustawodawstwa krajowe, jakim jest dyrektywa, zastąpiono bezpośrednio skutecznym rozporządzeniem, w „sferze policyjnej" zaś szczątkową, bardzo ograniczoną regulację w postaci decyzji ramowej (regulującej wyłącznie ochronę danych osobowych wymienianych w ramach współpracy międzynarodowej) zastąpiono harmonizacją krajowych porządków prawnych w postaci dyrektywy.

2.2.1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679

Po wprowadzeniu w życie projektu ogólnego rozporządzenia o danych w całej Unii Europejskiej będzie obowiązywał jeden kompleksowy akt prawny, którego przepisy będą odnosiły bezpośredni skutek oraz będą bezpośrednio stosowane na płaszczyznach krajowych systemów prawnych. Zgodnie z art. 2 ust. 2 rozporządzenia odo jego przepisy nie mają zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii,
b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakresu tytułu V rozdział 2 TUE (*Postanowienia szczególne dotyczące wspólnej polityki zagranicznej i bezpieczeństwa*),
c) przez osobę fizyczną w ramach czynności o charakterze czysto osobistym lub domowym,
d) przez właściwe organy w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Regulacje rozporządzenia nie dotyczą zatem działalności organów wymiaru sprawiedliwości (lit. d) ani służb specjalnych (lit. a).

2.2.2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680

Inaczej sytuacja będzie wyglądała w sferze współpracy policyjnej i sądowej w sprawach karnych. W tym zakresie zdecydowano się na zastosowanie mechanizmu harmonizacji ustawodawstw krajowych państw członkowskich przez uchwalenie dyrektywy w miejsce obecnie obowiązującej decyzji ramowej Rady.

Przepis art. 1 ust. 1 dyrektywy odo stanowi, że *Niniejsza dyrektywa ustanawia przepisy o ochronie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postepowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*. Art. 2 ust. 2 dyrektywy stanowi, że ma ona zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów określonych w art. 1 ust. 1. Aby więc właściwie określić zakres podmiotowy dyrektywy odo należy zdekodować pojęcie właściwy organ. Definicja tego pojęcia jest zawarta w art. 3 pkt 7. Zgodnie z treścią wskazanej definicji właściwy organ oznacza: (…) *organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępo-*

wań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, a także (…) *inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*.

Zakresem regulacji dyrektywy ma być zatem objęte przetwarzanie danych przez organy policyjne i sądowe państw członkowskich na potrzeby ścigania przestępstw, jak również zapobiegania im. Zniknęła przesłanka wymiany danych między państwami członkowskimi znana z decyzji ramowej.

Dyrektywa odo wymaga, aby dane osobowe zbierane przez organy egzekwowania prawa były: przetwarzane zgodnie z prawem (zasada legalności) i rzetelnie (zasada rzetelności), w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami (zasada celowości), adekwatne, stosowne i nienadmierne w stosunku do celów, w jakich są przetwarzane (zasada adekwatności), prawidłowe i w razie potrzeby uaktualniane, przechowywane w formie umożliwiającej identyfikację osób przez okres nie dłuższy niż jest to niezbędne do ich przetwarzania, odpowiednio zabezpieczane, w tym przed niedozwolonym lub niezgodnym z prawem przetwarzaniem.

Kraje UE zostały zobowiązane do przyjęcia terminów usuwania danych osobowych lub regularnego przeglądu konieczności ich przechowywania (art. 5).

Ważną nowością w stosunku do dotychczasowych regulacji jest wymóg, aby organy egzekwowania prawa wyraźnie rozróżniły dane osobowe poszczególnych kategorii osób, w tym:

- osób, w stosunku do których istnieją poważne podstawy, aby przypuszczać, że popełniły lub zamierzają popełnić czyn zabroniony,
- osób skazanych za czyn zabroniony,
- pokrzywdzonych czynem zabronionym lub w których przypadku można zasadnie uznać, że mogą stać się ofiarą czynu zabronionego,
- osób innych w stosunku do czynu zabronionego, w tym potencjalnych świadków.

Do najważniejszych postanowień dyrektywy odo zaliczają się przepisy dotyczące praw osoby, której dane dotyczą. Artykuły 12–14 przewidują prawo wolnego od opłat dostępu podmiotu danych do informacji, które go dotyczą (to prawo obejmuje m.in. uzyskiwanie informacji na temat: tożsamości i danych administratora, celów przetwarzania danych, odbiorców danych, planowanego okresu przechowywania danych, informacji o prawie złożenia skargi do organu nadzorczego oraz prawie do dostępu do danych osobowych oraz ich poprawienia lub usunięcia albo ograniczenia ich przetwarzania).

Zgodnie z art. 13 ust. 2 dyrektywy odo państwa członkowskie mogą przyjąć akty prawne pozwalające opóźnić, ograniczyć lub pominąć informowanie osoby, której dane dotyczą, aby:

- uniemożliwić utrudnianie czynności postepowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur,
- uniemożliwić zakłócanie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych oraz wykonywania kar,
- chronić bezpieczeństwo publiczne,
- chronić bezpieczeństwo narodowe,
- chronić prawa i wolności innych osób.

Omawiany przepis zawiera zastrzeżenie, że środki ograniczające w stosunku do realizacji prawa do informacji podmiotu danych stosowane przez państwo członkowskie mogą być stosowane w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, oraz z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej. Powyższe zastrzeżenie wymusza wąskie traktowanie tego wyłączenia.

Odrębnie od prawa do informacji dyrektywy odo traktuje prawo dostępu przysługujące osobie, której dane dotyczą. Polega ono na zapewnieniu takiej osobie uzyskania odpowiedzi na pytanie, czy przetwarzane są informacje, które jej dotyczą, a jeżeli tak – to prawa dostępu do nich oraz do informacji o:

- celu i podstawie prawnej przetwarzania,
- kategoriach odnośnych danych osobowych,
- odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały ujawnione,
- planowanym okresie przechowywania danych osobowych lub kryteriach służących określeniu tego okresu,
- prawie do żądania od administratora danych sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych osobowych jej dotyczących,
- prawie wniesienia skargi do organu nadzorczego oraz jego danych kontaktowych, a także wskazania, jakie dane osobowe są przetwarzane, oraz wszelkich dostępnych informacji o ich pochodzeniu.

Dopuszczalne ograniczenia w zakresie stosowania prawa dostępu formułuje art. 15 dyrektywy odo. Ten przepis zezwala na przyjęcie przez państwo członkowskie aktów prawnych pozwalających ograniczyć – w całości lub w części – prawo dostępu osoby, której dane dotyczą, w takim stopniu i przez taki okres, w jakim częściowe lub całkowite ograniczenie jest działaniem niezbędnym w społeczeństwie demokratycznym do osiągnięcia celów, których wykaz jest identyczny z wykazem tych celów, dla których można ograniczyć informowanie podmiotu, zgodnie z art. 13 ust. 2. Podobnie jak w odniesieniu do ograniczeń dotyczących informowania podmiotu danych, w art. 15 ust. 2 dopuszczono, aby państwa członkowskie przyjęły akty prawne ustalające kategorie przetwarzania danych w całości albo w części spełniające kryteria odmowy dostępu, zgodnie z kryteriami zawartymi w ust. 1. Zarówno jednak w przypadku, gdy odmowa realizacji prawa dostępu do danych następuje w wyniku indywidualnej oceny administratora, jak i zakwalifikowania danych do kategorii wchodzącej w całości w zakres wyłączenia, administrator danych jest obowiązany, stosownie do ust. 3, do pisemnego poinformowania osoby, której dane dotyczą, o każdej odmowie lub ograniczeniu prawa dostępu i o przyczynach tej odmowy albo ograniczenia. Te informacje można pominąć, jeśli ich ujawnienie godziłoby w którykolwiek z celów wymienionych w ustępie 1, natomiast nie można pominąć poinformowania osoby, której dane dotyczą, o możliwości wniesienia skargi do organu nadzorczego lub środka prawnego do sądu.

Administratorzy danych mają ponadto być zobowiązani do dokumentowania rzeczywistych lub prawnych powodów, na jakich jest oparta decyzja, w celu udostępnienia tych informacji organom nadzorczym (ust. 4).

Ostatnim z praw podmiotu danych wprowadzanych przepisami dyrektywy odo jest prawo do sprostowania lub usunięcia danych osobowych oraz ograniczenia ich przetwarzania. Zgodnie z ust. 1 wskazanego przepisu, osoba, której dane dotyczą, ma prawo uzyskiwania od administratora danych ich sprostowania, jeśli są one nieprawidłowe. Ustęp 2 przewiduje nałożenie na administratora danych obowiązku usunięcia bez zbędnej

zwłoki danych osobowych, jeśli ich przetwarzanie narusza zasady przetwarzania danych osobowych ustanowione dyrektywą, jest niezgodne z prawem, lub jeżeli dane osobowe muszą zostać usunięte w celu wypełnienie obowiązku prawnego ciążącego na administratorze. Zamiast usunięcia, administrator ogranicza przetwarzanie, jeśli nie można stwierdzić, czy dane są prawidłowe, lub gdy są one potrzebne do celów dowodowych (ust. 3). Zgodnie z art. 16 ust. 5 państwa członkowskie są obowiązane zapewnić, aby administrator pisemnie informował osobę, której dane dotyczą, o każdej odmowie sprostowania lub usunięcia dotyczących jej danych osobowych oraz jej przyczynach. Ten obowiązek może zostać ograniczony w ustawodawstwie krajowym na warunkach analogicznych do warunków ograniczenia prawa dostępu i obowiązków informacyjnych administratora danych.

Zgodnie z art. 17 dyrektywy odo państwa członkowskie są zobowiązane zapewnić możliwość, aby podmiot danych mógł realizować swoje uprawnienia również za pośrednictwem organu nadzorczego.

Rozdział IV dyrektywy odo reguluje obowiązki administratora danych i podmiotu przetwarzającego dane.

Na administratorze, zgodnie z dyrektywą, spoczywają obowiązki: stosowania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych odbywało się na podstawie tego właśnie dokumentu (art. 19–20); prowadzenia wykazów czynności przetwarzania danych (art. 24); ewidencjonowania czynności przetwarzania danych (art. 25); dokonywania oceny skutków planowanych operacji przetwarzania danych (art. 27); współpracy z organem nadzorczym (art. 26) i prowadzenia z nim uprzednich konsultacji, w wypadku tworzenia nowego zbioru danych (art. 28).

W zakresie bezpieczeństwa danych osobowych (art. 25–31) organy krajowe są zobowiązane podjąć środki techniczne i organizacyjne w celu zapewnienia poziomu bezpieczeństwa tych danych odpowiadającego zagrożeniu. Jeśli przetwarzanie danych jest zautomatyzowane, należy zastosować odpowiednie środki, w tym:

- uniemożliwienie osobom nieuprawnionym dostępu do sprzętu używanego do przetwarzania,
- zapobieganie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych,
- zapobieganie nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu przeglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych[21].

W przypadku naruszenia ochrony danych osobowych dyrektywa nakłada na administratora obowiązek zawiadomienia o tym organu nadzorczego oraz osoby, której dane dotyczą dane. Obowiązek zawiadomienia organu nadzorczego ma charakter bezwzględny – powinno ono nastąpić w terminie 72 godzin od stwierdzenia naruszenia. W przypadku przekroczenia tego terminu niezbędne jest dołączenie uzasadnienia (art. 30).

Natomiast zawiadomienie osoby, której dotyczą dane (art. 31), powinno nastąpić jedynie wtedy, gdy naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Ponadto zawiadomienie osoby fizycznej nie jest wymagane, jeżeli został spełniony jeden z trzech warunków:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,

[21] http://eur-lex.europa.eu/legal-content/PL/LSU/?uri=CELEX:32016L0680 [dostęp: 19 IX 2017].

– administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
– wymagałoby ono zbyt dużego wysiłku – w takim momencie zawiadomienie może zostać zastąpione przez publiczny komunikat.

Ostatecznie więc może się okazać, że omówiona norma wprowadzająca obowiązek informowania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych okaże się regulacją martwą.

Istotnym obowiązkiem nałożonym przez dyrektywy odo na administratora danych jest obowiązek wyznaczenia inspektora ochrony danych, monitorującego przestrzeganie przepisów dyrektywy i współpracującego z organem nadzorczym[22]. Z obowiązku powołania inspektora ochrony danych mogą zostać zwolnione jedynie organy sądowe[23].

Rozdział V dyrektywy odo reguluje przekazywanie danych do państw trzecich lub organizacji międzynarodowych.

Ogólne zasady przekazywania danych osobowych odbiorcom mającym siedzibę w państwach trzecich określa artykuł 35 dyrektywy odo. Zgodnie z treścią ust. 1 tego dokumentu państwa członkowskie mają obowiązek zapewnić, aby przekazanie przez właściwe organy danych osobowych, które są lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, mogło nastąpić pod warunkiem zgodności z przepisami krajowymi przyjętymi na podstawie innych przepisów dyrektywy jedynie, jeśli:

a) przekazanie jest niezbędne do celów, o których mowa w art. 1 ust. 1[24];
b) dane osobowe są przekazywane administratorowi w państwie trzecim albo organizacji międzynarodowej, który jest organem właściwym do realizacji celów, o których mowa w art. 1 ust. 1;
c) w przypadku przesyłania lub udostępniana danych od innego państwa członkowskiego to inne państwo członkowskie wyraziło uprzednią zgodę na przekazanie zgodnie ze swoim prawem krajowym;
d) Komisja wydała decyzję dotyczącą zgodności na podstawie art. 36 lub w razie braku takiej decyzji zostały zapewnione lub istnieją odpowiednie zabezpieczenia zgodnie z art. 37 albo w razie braku decyzji odnośnie do zgodności wydanej na podstawie art. 36 lub zabezpieczeń zgodnie z art. 37 zastosowanie mają wyjątki w szczególnych sytuacjach zgodnie z art. 38; oraz
e) w przypadku dalszego przekazania do innego państwa trzeciego lub organizacji międzynarodowej właściwy organ, który dokonał pierwotnego przekazania, lub inny właściwy organ tego samego państwa członkowskiego zezwala na dalsze przekazanie po należytym uwzględnieniu wszystkich istotnych czynników, w tym powagi czynu zabronionego, celu, w którym dane osobowe zostały pierwotnie przekazane, oraz stopnia ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, do których dane osobowe są dalej przekazywane.

Przekazanie danych osobowych bez uprzedniej zgody państwa członkowskiego, które te dane udostępniło, jest dopuszczalne wyłącznie wtedy, gdy jest ono niezbędne do zapobieżenia bezpośredniemu, poważnemu zagrożeniu bezpieczeństwa publicznego

[22] Zadania inspektora ochrony danych – art. 34 dyrektywy.

[23] Tak stanowi art. 32 ust. 1 dyrektywy.

[24] Zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych i wykonywanie kar, w tym ochrona przed zagrożeniami bezpieczeństwa publicznego i zapobieganie takim zagrożeniom.

w państwie członkowskim lub w państwie trzecim bądź też bezpieczeństwa ważnych interesów państwa członkowskiego, a uprzedniej zgody nie da się uzyskać w odpowiednim terminie.

Istotną regulację zawiera art. 36 – *Przekazywanie na podstawie decyzji stwierdzającej odpowiedni stopień ochrony*. Ten przepis przyznaje Komisji uprawnienie do oceny, czy dane państwo trzecie, terytorium lub przynajmniej jeden sektor w państwie trzecim lub organizacja międzynarodowa zapewniają adekwatny stopień ochrony. W celu ustalenia, czy stopień ochrony jest odpowiedni, Komisja bada praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie prawodawstwo, a także praktyki w zakresie ochrony danych osobowych w państwie trzecim lub organizacji międzynarodowej, istnienie i skuteczne funkcjonowanie co najmniej jednego niezależnego organu nadzorczego w zakresie ochrony danych osobowych w państwie trzecim lub organu nadzorującego organizację międzynarodową, a także międzynarodowe zobowiązania państwa trzeciego lub organizacji międzynarodowej albo inne obowiązki wynikające z prawnie wiążących konwencji lub aktów prawnych oraz z udziału w systemach wielostronnych lub regionalnych, zwłaszcza w sferze ochrony danych osobowych. Po dokonaniu oceny Komisja może w drodze aktu wykonawczego zdecydować, czy państwo trzecie, terytorium, przynajmniej jeden określony sektor w państwie trzecim albo organizacja międzynarodowa zapewniają adekwatny poziom ochrony. Akt wykonawczy Komisji określa terytorialny i sektorowy zakres jego stosowania, a także mechanizm okresowego przeglądu, odbywającego się przynajmniej raz na cztery lata. Komisja publikuje w Dzienniku Urzędowym Unii Europejskiej i na swojej stronie internetowej wykaz państw trzecich, terytoriów i określonych sektorów w państwie trzecim oraz organizacji międzynarodowych, co do których przyjęła decyzję stwierdzającą określony poziom ochrony lub jego brak[25].

W przypadku, gdy Komisja stwierdzi, że dane państwo trzecie, terytorium lub przynajmniej jeden sektor w tym państwie trzecim albo organizacja międzynarodowa zapewniają adekwatny poziom ochrony, przekazanie danych osobowych nie wymaga specjalnego zezwolenia[26].

Jeśli zaś Komisja nie podjęła stosownej decyzji, państwa członkowskie, zgodnie z art. 37 dyrektywy, mogą przekazywać dane osobowe do państwa trzeciego z zastrzeżeniem odpowiednich zabezpieczeń, tzn. gdy w prawnie wiążącym akcie wprowadzono odpowiednie zabezpieczenia ochrony danych osobowych (należy uznać, że takim aktem będzie umowa międzynarodowa łącząca państwo członkowskie z państwem trzecim albo organizacją międzynarodową), albo też jeśli administrator ocenił wszystkie okoliczności związane z przekazaniem danych osobowych i stwierdził, że istnieją odpowiednie zabezpieczenia ochrony danych osobowych. W tym drugim przypadku przekazanie danych osobowych musi zostać udokumentowane, a dokumentacja (obejmująca datę i godzinę przekazania, informacje o właściwym organie odbierającym, uzasadnienie przekazania oraz przekazane dane osobowe) – udostępniona na żądanie organowi nadzorczemu.

Artykuł 38 dyrektywy odo przewiduje ponadto *Wyjątki w szczególnych sytuacjach*, gdy brakuje zarówno decyzji stwierdzającej odpowiedni poziom ochrony danych, jak też odpowiednich zabezpieczeń, o których mowa w art. 37. W takich przypadkach przekazanie danych do państwa trzeciego lub organizacji międzynarodowej jest dopuszczalne, jeśli jest niezbędne:

[25] Art. 36 ust. 8.
[26] Tamże, ust. 1.

a) w celu ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby;
b) w celu zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą, jeżeli prawo państwa członkowskiego przekazującego dane osobowe tak stanowi;
c) dla zapobieżenia bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego;
d) w indywidualnym przypadku do celów, o których mowa w art. 1 ust. 1[27]; lub
e) w indywidualnym przypadku, dla ustalenia, dochodzenia lub obrony roszczeń w związku z celami określonymi w art. 1 ust. 1.

Również i w tym przypadku występuje obowiązek odpowiedniego udokumentowania przekazania danych osobowych i przekazania dokumentacji organowi nadzorczemu.

Kolejny wyjątek od zasad przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej zawiera art. 39, w którym zostały określone warunki przekazania danych osobowych bezpośrednio odbiorcy w państwie trzecim, który nie jest administratorem danych osobowych stanowiącym organ właściwy do realizacji celu dyrektywy. Takie przekazanie danych osobowych jest dopuszczalne jeżeli;

Artykuł 57 dyrektywy odo nałożył na państwa członkowskie obowiązek przyjęcia przepisów określających skuteczne, proporcjonalne i odstraszające sankcje za naruszenie jej przepisów.

Zgodnie z art. 63 dyrektywy odo termin jej transpozycji upływa 6 maja 2018 r. Do tego dnia państwa członkowskie są zobowiązane przyjąć i opublikować przepisy ustawowe, wykonawcze i administracyjne, niezbędne do wykonania dyrektywy. Teksty tych przepisów muszą zostać niezwłocznie przekazane Komisji Europejskiej. Wyjątek od tego terminu dotyczy zautomatyzowanych zbiorów danych utworzonych przed 6 maja 2016 r. Zgodnie z ustępem 2 takie systemy mogą zostać dostosowane do art. 25 dyrektywy, przewidującego ewidencjonowanie czynności przetwarzania danych w terminie do 6 maja 2023 r., jeśli ich dostosowanie w terminie wcześniejszym wymagałoby „niewspółmiernie dużego wysiłku". Z kolei ustęp 3 pozwala na dalsze wydłużenie terminu dostosowania do 6 maja 2026 r., (…) *jeżeli inaczej nastąpiłyby poważne problemy w funkcjonowaniu tego systemu*.

3. Wpływ reformy unijnego systemu ochrony danych osobowych na prawa i obowiązki służb specjalnych – wnioski *de lege ferenda* dla krajowego ustawodawcy

W chwili obecnej polski ustawodawca stoi przed wyzwaniem, jakim jest dostosowanie polskiego prawa do rozporządzenia i dyrektywy odo. Termin tego dostosowania upływa w maju 2018 r., wraz z wejściem w życie rozporządzenia odo z dniem 25 maja 2018 r. oraz upływem terminu transpozycji dyrektywy odo 6 maja 2018 r. W zakresie ogólnym przepisy ustawy o ochronie danych osobowych zostaną w większości zastąpione bezpośrednio skutecznymi przepisami rozporządzenia. Natomiast w sferze zwalczania przestępczości istnieje konieczność zbudowania w zasadzie od podstaw regulacji systemu ochrony danych osobowych. Stworzenie odpowiednich przepisów prawnych nie będzie łatwe z uwagi na specyfikę obszaru zwalczania przestępczości, która w odniesieniu do poważnych przestępstw polega nierzadko na prowadzeniu działań niejawnych. Może to spowodować krzyżowanie się zakresu regulacji ustawy implementującej dyrektywę odo z zakresem ustawy o ochronie informacji niejawnych.

[27] Zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych i wykonywanie kar, w tym ochrona przed zagrożeniami bezpieczeństwa publicznego i zapobieganie takim zagrożeniom.

Do najpoważniejszych kontrowersji wymagających rozstrzygnięcia przy tworzeniu ustawy implementacyjnej będzie należało określenie jej zakresu podmiotowego.

Jak już wspomniano wyżej, omawiając poszczególne przepisy dyrektywy odo, jej zakres, stosownie do art. 1 ust. 1, obejmuje przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Niniejszy przepis wyodrębnia dwa zakresy dyrektywy, które muszą zaistnieć łącznie, aby jej przepisy znalazły zastosowanie do danej sytuacji, tj. zakres podmiotowy i przedmiotowy. Zakres przedmiotowy dyrektywy to przetwarzanie danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniem bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Zakres podmiotowy zaś jest związany z pojęciem właściwy organ, zdefiniowanym w art. 3 pkt 7 dyrektywy odo. Zgodnie z treścią definicji zawartej w tym przepisie właściwy organ oznacza (…) *organ publiczny właściwy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*, a także: *inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom*.

Nie ulega wątpliwości, że ustawa implementująca dyrektywę odo powinna objąć swoim zakresem Policję i inne służby właściwe do ścigania przestępstw, zapobiegania im i ochrony bezpieczeństwa publicznego, takie jak: Straż Graniczna, Żandarmeria Wojskowa czy Krajowa Administracja Skarbowa. Powinna objąć również organy wymiaru sprawiedliwości, a zwłaszcza Prokuraturę (w stosunku do sądów sama dyrektywa formułuje wyjątki).

Największa kontrowersja dotyczy kwestii, czy i w jakim zakresie implementacja dyrektywy powinna objąć służby specjalne. Ten problem raczej nie dotyczy służb wywiadowczych odpowiedzialnych za bezpieczeństwo zewnętrzne państwa, tj. Agencji Wywiadu i Służby Wywiadu Wojskowego, w których ustawowych kompetencjach nie znajduje się zwalczanie przestępczości (ustawodawca, w odniesieniu do służb wywiadowczych, posługuje się konstrukcją rozpoznawania i przeciwdziałania „zagrożeniom", a nie „przestępstwom"[28]). Natomiast Służba Kontrwywiadu Wojskowego ma w zakresie swoich kompetencji rozpoznawanie, zapobieganie i wykrywanie przestępstw[29], Agencja Bezpieczeństwa Wewnętrznego i Centralne Biuro Antykorupcyjne zaś – również ściganie ich sprawców.[30]

[28] Art. 6 ust. 1 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2016 r. poz. 1897, ze zm.) i art. 6 ust. 1 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego (Dz.U. z 2016 r. poz. 1318, ze zm.).

[29] Art. 5 ust. 1 pkt 1 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego.

[30] Art. 5 ust. 1 pkt 2 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i art. 2 ust. 1 pkt 1 ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2016 r. poz. 1310, ze zm.).

Z drugiej jednak strony, zgodnie artykułem 2 lit. a dyrektywy odo, nie ma ona zastosowania do działalności nieobjętej zakresem prawa Unii. W tym miejscu należy przypomnieć, że stosownie do art. 4 ust. 2 traktatu o Unii Europejskiej (…) *bezpieczeństwo narodowe pozostaje w sferze wyłącznej odpowiedzialności każdego państwa członkowskiego*. Istotną wskazówkę co do kierunku interpretacji tego wyłączenia stanowi motyw 14 preambuły dyrektywy odo, zgodnie z którym: (…) *dyrektywa nie powinna mieć zastosowania do przetwarzania danych osobowych w toku działalności wykraczającej poza zakres prawa Unii, dlatego czynności w zakresie bezpieczeństwa narodowego, czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym* (…) *nie należy uznawać za czynności wchodzące w zakres niniejszej dyrektywy*. Warto zauważyć, że zgodnie z treścią tego zapisu z zakresu regulacji dyrektywy ODO zostają wyłączone zarówno (…) *czynności w zakresie bezpieczeństwa narodowego*, jak i *czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym* wyodrębnione przez ustawodawcę unijnego do odrębnej kategorii. Według niniejszego zapisu istnieje zatem możliwość wyłączenia z zakresu implementacji przedmiotowej dyrektywy do prawa krajowego sfery bezpieczeństwa narodowego na podstawie kryterium podmiotowego (*czynności agencji lub jednostek zajmujących się bezpieczeństwem narodowym*) oraz funkcjonalnego (*czynności w zakresie bezpieczeństwa narodowego*). W przypadku zastosowania wyłączenia podmiotowego wystarcza, jeśli dana agencja lub jednostka „zajmuje się" bezpieczeństwem narodowym, nie jest zaś niezbędne prowadzenie przez dany podmiot działalności wyłącznie w sferze bezpieczeństwa narodowego. Należy uznać, że gdyby racjonalny ustawodawca unijny chciał ograniczyć możliwość wyłączenia z zakresu implementacji dyrektywy jedynie czynności wykonywane w zakresie bezpieczeństwa narodowego, mógłby ograniczyć omawiane wyłączenie do kryterium funkcjonalnego albo też w wyłączeniu podmiotowym dodać słowo „wyłącznie" przed wyrażeniem „bezpieczeństwem narodowym", a przecież żadnej z tych rzeczy nie uczynił.

Przed ustawodawcą krajowym stoi zatem poważne zadanie odpowiedniego sformułowania wyłączenia z zakresu stosowania ustawy implementującej dyrektywę odo organów zajmujących się ochroną bezpieczeństwa narodowego. Wymaga to również stosownego określenia w punkcie wyjścia zakresu pojęcia bezpieczeństwo narodowe, które nie ma przecież legalnej definicji. Należy uznać, że w pojęciu bezpieczeństwo narodowe mieści się występujące w polskim prawie pojęcie bezpieczeństwo państwa. Wobec tego w zakresie bezpieczeństwa narodowego z pewnością mieszczą się zadania służb specjalnych ukierunkowane na ochronę suwerenności państwa i jego podstawowych funkcji, takie jak: ochrona porządku konstytucyjnego, prowadzenie działalności kontrwywiadowczej, ochrona informacji niejawnych czy ściganie przestępstw przeciwko bezpieczeństwu państwa.

Jako przykład obrazujący trudności związane z rozgraniczeniem sfery bezpieczeństwa narodowego, pozostającej w zakresie wyłącznej odpowiedzialności państw członkowskich, od sfery wspólnej przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w której kompetencje ma Unia Europejska, należy wskazać problem przeciwdziałania terroryzmowi oraz zwalczania tego zagrożenia. Z jednej strony działalność służb specjalnych w tym obszarze bywa traktowana jako wchodząca w zakres zapewniania bezpieczeństwa narodowego, z drugiej zaś ten obszar coraz częściej jest poddawany regulacji prawa Unii Europejskiej, zwłaszcza w odniesieniu do współpracy międzynarodowej. Granice sfer kompetencji Unii Europejskiej i jej państw członkowskich stają się w tym zakresie coraz mniej przejrzyste.

Przed polskim ustawodawcą stoi więc w chwili obecnej trudne i delikatne zadanie polegające na właściwym wyważeniu rozbieżnych nieraz interesów w toku implementacji dyrektywy odo do polskiego prawa, w sytuacji gdy do upływu terminu transpozycji prawa pozostały już jedynie miesiące. Ustawodawca powinien wziąć pod uwagę prawnie chroniony interes służb specjalnych do ochrony niejawności swoich działań, która jest ich podstawowym modus operandi odróżniającym je od innych organów powołanych do ochrony bezpieczeństwa publicznego, drugiej zaś strony – prawa jednostki wspierane przez ewolucję prawa międzynarodowego, wśród których poczesne miejsce zajmuje w ostatnich latach prawo do ochrony danych osobowych.

Ochronie niejawności działań służb specjalnych służy wiele przepisów prawnych, spośród których na przytoczenie zasługuje np. art. 7 ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r. poz. 1167, ze zm.). Określa on kategorie informacji, które powinny być chronione jako informacje niejawne, bez względu na upływ czasu, a mianowicie: dane mogące doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb i instytucji uprawnionych do wykonywania na podstawie ustawy czynności operacyjno-rozpoznawczych, jako osób wykonujących te czynności, jak również dane mogące doprowadzić do identyfikacji osób, które udzieliły pomocy w zakresie czynności operacyjno-rozpoznawczych służbom i instytucjom uprawnionym do ich wykonywania na podstawie ustawy. Należy uznać, że „dane mogące doprowadzić do identyfikacji osób" mieszczą się w pojęciu danych osobowych w rozumieniu dyrektywy odo. Co prawda ten przepis nie odnosi się tylko do służb specjalnych, ale do wszystkich organów uprawnionych do prowadzenia czynności operacyjno-rozpoznawczych, należy jednak mieć na uwadze, że dla służb specjalnych tego rodzaju czynności, inaczej niż dla służb policyjnych, stanowią podstawową formę ich działalności. Istnieją ponadto rygorystyczne przepisy o ochronie określonych informacji zawarte w ustawach pragmatycznych służb specjalnych. W tym kontekście należy wymienić: art. 39 ust. 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i analogiczne do niego: art. 43 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego oraz art. 28 ust. 2 ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym. Te przepisy wprowadzają bliski bezwzględnego zakaz ujawniania przez służby specjalne informacji o osobie, jeśli te informacje zostały pozyskane w wyniku czynności operacyjno-rozpoznawczych prowadzonych przez służby, a także o osobach udzielających im pomocy. Ujawnienie tego typu informacji jest możliwe tylko w wąsko określonym zakresie przypadków, tj. w przypadku żądania prokuratora lub sądu, zgłoszonego w celu ścigania karnego za czyn zabroniony stanowiący zbrodnię lub występek, którego skutkiem jest śmierć (w przypadku CBA również uszczerbek na zdrowiu albo szkoda w mieniu), lub postępowania sprawdzającego na podstawie przepisów o ochronie informacji niejawnych (w przypadku SKW i SWW również żądania Rzecznika Interesu Publicznego w ramach toczącego się postępowania lustracyjnego), albo w przypadku żądania prokuratora lub sądu, uzasadnionego podejrzeniem popełnienia przestępstwa ściganego z oskarżenia publicznego w związku z wykonywaniem czynności operacyjno-rozpoznawczych. Należy uznać, że „informacje o osobie", o których mowa w tych przepisach, obejmują dane osobowe. Te przepisy kłócą się z uprawnieniami podmiotu danych, takimi jak prawo do informacji o przetwarzaniu dotyczących go danych, dostępu do dotyczących go danych czy uprawnieniami niezależnego organu nadzorczego, w tym prawo dostępu do wszelkich danych osobowych przetwarzanych przez podmiot nadzorowany, formułowanymi w przepisach dyrektywy odo (art. 47 ust. 1).

Wskazane powyżej okoliczności przemawiają za pełnym, podmiotowym wyłączeniem służb specjalnych z zakresu obowiązywania przyszłej ustawy transponującej dyrektywę odo do polskiego porządku prawnego.

Krytycy takiego rozwiązania mogą podnosić, że przepisy dyrektywy odo zawierają mechanizmy pozwalające ograniczyć niektóre uprawnienia podmiotu danych. Na przykład art. 15 ust. 1 dyrektywy odo pozwala na przyjęcie rozwiązań umożliwiających ograniczenie w całości lub w części prawa dostępu osoby, której dane dotyczą, do odnoszących się do niej danych, jeśli jest to niezbędne i proporcjonalne do tego, aby np. uniemożliwić utrudnianie postępowania przygotowawczego albo chronić bezpieczeństwo narodowe. Zamiast więc całkowicie wyłączać służby specjalne z zakresu ustawy transponującej dyrektywę odo, można by stworzyć mechanizm pozwalający im na odmowę realizacji praw podmiotu dotyczących przetwarzanych przez nie danych z uwagi na ochronę bezpieczeństwa narodowego. Gdyby jednak taki mechanizm powstał, to należy sądzić, że byłby powszechnie stosowany przez służby specjalne w celu ochrony ich zainteresowań operacyjnych. Wobec tego korzyść, jaką odniósłby podmiot danych, mogłaby się okazać iluzoryczna.

Inną kwestią są uprawnienia nadzorcze niezależnego organu ochrony danych, ponieważ w tym zakresie dyrektywa nie przewiduje możliwości formułowania wyłączeń.

Wobec powyższego, w odniesieniu do planowanej implementacji dyrektywy odo nasuwa się konkluzja, że w sytuacji, gdy prawo Unii Europejskiej daje państwom członkowskim możliwość ochrony atrybutu swojej suwerenności, jakim jest bezpieczeństwo narodowe, przez stosowne wyłączenia, państwo polskie powinno w interesie swoich organów chroniących je przed najpoważniejszymi zagrożeniami skorzystać z nich w najdalej idącym zakresie.