Agnieszka Grzelak

PROJEKT REFORMY OCHRONY DANYCH OSOBOWYCH – CZY RZECZYWIŚCIE POWSTANIE JEDNOLITY I SPÓJNY SYSTEM?[1]

Wprowadzenie

Od ponad 2 lat trwają prace nad projektami aktów prawnych przedstawionymi przez Komisję Europejską w styczniu 2012 r., które mają doprowadzić do reformy systemu ochrony danych osobowych w Unii Europejskiej. W komunikacie Komisji do Parlamentu Europejskiego i Rady, wprowadzającym projekty, Komisja proponuje „solidne i spójne ramy prawne dotyczące wszystkich obszarów polityki UE, wzmacniające prawa osób fizycznych, wymiar jednolitego rynku dotyczący ochrony danych oraz ograniczające obciążenia administracyjne dla przedsiębiorstw"[2]. Już w tym miejscu zapowiada też, że konieczne będzie przedstawienie na późniejszym etapie zmian w niektórych aktach prawnych w celu dostosowania instrumentów szczególnych i sektorowych. Czy zatem zaproponowany przez Komisję Europejską system, polegający na przyjęciu dwóch aktów prawnych (reżim ogólny i szczególny – dotyczący wymiaru sprawiedliwości w sprawach karnych i współpracy policyjnej)[3], będzie spełniał zaproponowane założenia i czy przede wszystkim będzie spójny i jednolity?

[1] Opracowanie przygotowane w ramach badań statutowych: *Ochrona danych osobowych w Unii Europejskiej – reforma nowego modelu ochrony prywatności i danych osobowych* nr badania 02/S/0012/13. Stan prawny na dzień 1 sierpnia 2014 r.

[2] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku, KOM(2012) 9 wersja ostateczna, s. 4.

[3] Zob. Projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych KOM(2012) 11 wersja ostateczna (dalej: Projekt rozporządzenia albo Projekt rozporządzenia ogólnego) oraz Projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, KOM(2012) 10 wersja ostateczna (dalej: Projekt dyrektywy).

Już na wstępnym etapie analiz można było wyrażać wątpliwości[4], które zostaną rozwinięte w niniejszym opracowaniu, poświęconym spójności (a właściwie brakowi spójności) projektowanych regulacji i tworzonego systemu.

Opracowanie podzielone jest na trzy części. Pierwsza – najogólniejsza – dotyczy traktatowej podstawy prawnej do uregulowania zasad ochrony danych osobowych w kontekście przedłożenia przez Komisję dwóch odrębnych projektów (rozporządzenia i dyrektywy). Część druga poświęcona jest obecnemu systemowi prawnemu i ma stać się tłem do odpowiedzi na pytanie, na ile nowe regulacje zmienią istniejący system ochrony danych osobowych w Unii Europejskiej, na który składa się wiele aktów prawnych poświęconych ochronie danych osobowych. Wreszcie trzecia – najważniejsza – dotyczy Projektu rozporządzenia i Projektu dyrektywy przedłożonych przez Komisję Europejską. Nie będą w niej omawiane wszystkie możliwe zagadnienia, ale zostaną przedstawione te, które budzą obawy odnośnie do braku spójności przyjmowanych aktów i tworzonego systemu ochrony danych osobowych. Systematyka tej części oparta jest o strukturę projektowanych aktów.

1. Traktatowa podstawa prawna do uregulowania zasad ochrony danych osobowych w UE

Analizując wątek spójności systemu ochrony danych osobowych w Unii Europejskiej, warto rozpocząć od przypomnienia, że Traktat z Lizbony (dalej: TL), wprowadzający podstawę prawną do przyjęcia nowych aktów prawnych, umożliwia ustanowienie odrębnych reguł dla współpracy w obszarze policyjnej i sądowej w sprawach karnych w UE. Wielokrotnie podkreślano już, że TL dokonuje szeregu reform ustrojowych UE, w tym wzmacnia ochronę praw podstawowych, w szczególności poprzez nadanie Karcie Praw Podstawowych UE (dalej: KPP) charakteru prawnie wiążącego, ale także poprzez stworzenie podstawy prawnej do przystąpienia UE do Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności (dalej: EKPCz) oraz potwierdzenie znaczenia ochrony praw podstawowych jako części prawa UE (zasad ogólnych Unii Europejskiej) w art. 6 ust. 3 Traktatu o Unii Europejskiej (dalej: TUE). Trzeba jednak zauważyć, że jedną z dalszych reform, mniej analizowaną w doktrynie prawa europejskiego, jest podkreślenie wagi niektórych praw podstawowych, zwłaszcza prawa do ochrony danych osobowych, któremu przyznano nową, szczególną

[4] Por. A. Grzelak, *Projekt ochrony danych osobowych w sprawach karnych w UE – kolejny krok na drodze do społeczeństwa nadzorowanego?*, „Europejski Przegląd Sądowy" 2012, nr 11, s. 20–28.

podstawę prawną nie tylko w KPP (art. 8), ale przede wszystkim w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (dalej: TfUE). Artykuł 16 TfUE w sposób wyjątkowy podkreśla znaczenie prawa podstawowego, jakim jest prawo do ochrony danych osobowych[5]. Przepis ten ma jednak ogólne zastosowanie, czyli dotyczy przetwarzania danych osobowych zarówno w sektorze prywatnym, jak i w publicznym, w tym w dziedzinie współpracy policyjnej i sądowej w sprawach karnych. Dotyczy również przetwarzania danych osobowych przez instytucje UE.

Już w tym miejscu pojawia się zatem pierwszy wyłom w jednolitym systemie ochrony danych osobowych, do którego dąży Komisja Europejska. Prawo do ochrony danych osobowych nie będzie chronione w identyczny sposób we wszystkich obszarach, bo nadal ochrona danych osobowych w ramach Wspólnej Polityki Zagranicznej i Bezpieczeństwa (dalej: WPZiB) będzie odbywała się w oparciu o inną podstawę traktatową i na innych zasadach. Na podstawie przepisów regulujących współpracę w ramach WPZiB, zamieszczonych w TUE (art. 39 TUE), Rada jest upoważniona do przyjęcia decyzji określającej zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania rozdziału regulującego WPZiB oraz zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów. Przepis TUE wyraźnie wskazuje, że jest to odstępstwo od art. 16 ust. 2 TfUE. Zatem oprócz instrumentu prawnego (decyzja Rady *versus* rozporządzenie/dyrektywa Parlamentu Europejskiego i Rady), odmienne będą również konsekwencje przyjęcia takiego aktu, chociażby w zakresie wdrożenia go przez państwa członkowskie i skutków nieprawidłowego wdrożenia do prawa krajowego.

Z kolei jeżeli chodzi o współpracę policyjną i sądową w sprawach karnych, to należy pamiętać, że chociaż art. 16 TfUE ma brzmienie ogólne, odnoszące się całościowo do wszystkich rodzajów polityki UE, to jednak sytuacja nie jest całkowicie spójna i klarowna. Do Aktu końcowego Konferencji międzyrządowej, która przyjęła TL, dołączono bowiem Deklarację nr 21, w której Konferencja przyznaje, że konieczne może okazać się wprowadzenie zasad szczególnych dotyczących ochrony danych osobowych i swobodnego przepływu tych danych w dziedzinach współpracy sądowej w sprawach karnych i współpracy policyjnej, zapewnianej na podstawie art. 16 TfUE, ze względu na charakter tych dziedzin. Z kolei w Deklaracji nr 20 Konferencja oświadczyła, że w każdym przypadku przyjęcia na podstawie art. 16 TfUE

[5] Na ten temat zob. A. Grzelak, *Prawo do ochrony danych osobowych a konieczność walki z przestępczością. Uwagi na tle art. 16 Traktatu o funkcjonowaniu Unii Europejskiej*, w: *Prawo Unii Europejskiej a prawo konstytucyjne państw członkowskich*, red. S. Dudzik, N. Półtorak, Warszawa 2013, s. 407–435.

zasad dotyczących ochrony danych osobowych, które mogłyby mieć bezpośredni wpływ na bezpieczeństwo narodowe, powinno to być należycie wzięte pod uwagę. Państwa członkowskie uważają zatem, że ogólne ramy ochrony danych mogą nie mieć zastosowania w tej dziedzinie i mogą być w tym względzie potrzebne przepisy szczególne.

Osobną kwestią jest problem spójności terytorialnej, trzeba bowiem pamiętać o wyłączeniach, jakie zagwarantowano niektórym państwom członkowskim w protokołach dołączonych do TFUE i TUE przez TL[6].

2. Obecny system ochrony danych osobowych – obowiązujące akty prawne

Obowiązujący stan prawny w omawianej dziedzinie jest skomplikowany, co jest efektem struktury UE, w tym jej systemu prawnego, istniejącego przed wejściem w życie TL. Szczególnie interesujący wydaje się rozdźwięk w regulacji systemu ochrony danych między dawnymi I i III filarem UE[7], który odzwierciedla się również w przedstawionych przez Komisję i omawianych w niniejszym opracowaniu dwóch projektach: Projekcie rozporządzenia i Projekcie dyrektywy.

Przetwarzanie danych osobowych w dawnym I filarze UE zasadniczo objęło czynności dokonywane przez jednostki prywatne w ramach prowadzonej przez nie działalności. Przyjęcie regulacji dotyczącej ochrony danych w ramach rynku wewnętrznego było spowodowane tym, że integracja gospodarcza i społeczna, do której dochodziło stopniowo wraz z rozwojem rynku wewnętrznego, prowadzi do znacznego zwiększenia transgranicznego przepływu danych osobowych między wszystkimi podmiotami zaangażowanymi w taką działalność w państwach członkowskich, w tym między przedsiębiorcami. Podstawowym, ale nie jedynym aktem prawnym w tym zakresie, nadal obowiązującym, jest Dyrektywa 95/46/WE[8], na mocy której państwa członkowskie zobowiązały się chronić podstawowe prawa i wolności osób

[6] Zob. postanowienia Protokołu (nr 21) w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz Protokołu (nr 22) w sprawie stanowiska Danii, DzUrz. C 326, 26.10.2012.

[7] Do wejścia w życie TL można było mówić o strukturze filarowej UE, która zanikła (przynajmniej częściowo) w związku z dokonaną reformą ustrojową UE.

[8] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, DzUrz. WE L 281, 23.11.1995, s. 31 (dalej: Dyrektywa 95/46/WE albo Dyrektywa ogólna w sprawie ochrony danych).

fizycznych, w szczególności ich prawo do prywatności w odniesieniu do przetwarzania danych osobowych. Dyrektywę stosuje się do przetwarzania danych osobowych w całości lub w części w sposób zautomatyzowany oraz innego przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych, z wyłączeniem przypadków, o których mowa w art. 2 ust. 2 Dyrektywy ogólnej (w tym w zakresie dawnego III filaru UE). Poza tym aktem, który ma charakter ogólny, istnieje cały szereg sektorowych aktów prawnych, w tym chociażby (wymieniając tylko te podstawowe):

- Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego[9],
- Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej[10],
- Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca Dyrektywę 2002/58/WE[11],
- Dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady zmieniająca Dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, Dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz Rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów[12].

Należy również pamiętać o szczególnym akcie prawnym, jakim jest Rozporządzenie (WE) nr 45/2001 dotyczące ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy UE[13].

---

[9] Tzw. Dyrektywa o handlu elektronicznym, DzUrz. L 178, 17.07.2000, s. 1. Projekt rozporządzenia w art. 2 ust. 1 wyraźnie wyklucza jego zastosowanie do sytuacji opisanych w dyrektywie.

[10] Tzw. Dyrektywa o prywatności i łączności elektronicznej, DzUrz. L 201, 31.07.2002, s. 37.

[11] Tzw. Dyrektywa w sprawie retencji danych, DzUrz. L 105, 13.04.2006, s. 54.

[12] DzUrz. L 337 z 18.12.2009, s. 11.

[13] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, DzUrz. L 8 z 12.01.2001, s. 1 (dalej: Rozporządzenie 45/2001). Projekt rozporządzenia w art. 2 ust. 1 wyraźnie wyklucza zastosowanie go do przetwarzania danych przez instytucje, organy i jednostki organizacyjne Unii, a zatem Rozporządzenie 45/2001 będzie nadal obowiązywało bez zmian.

Istnieje także cały szereg innych aktów, które formalnie dotyczą tematyki należącej do materii I filaru UE (np. polityki migracyjnej UE) i które dotyczą ochrony danych, ale nie są objęte postanowienia obecnie obowiązującej dyrektywy ogólnej w sprawie ochrony danych, ponieważ są to dane, które nie są przetwarzane w kontekście działalności gospodarczej, przez podmioty publiczne[14]. Chodzi tu o przepisy nieodnoszące się wprost do problematyki ochrony danych osobowych, ale ustanawiające procedurę, w której ramach dane osobowe powinny być w sposób odpowiedni chronione i które są przetwarzane przez podmioty publiczne. Takim przykładem jest chociażby Dyrektywa 2005/85/WE w sprawie ustanowienia minimalnych norm dotyczących procedur nadawania i cofania statusu uchodźcy w państwach członkowskich[15], w której kwestia ochrony danych osobowych jest pochodną postępowania w innych sprawach (azylowych)[16].

W dawnym III filarze UE również stało się konieczne uregulowanie niektórych aspektów przetwarzania danych, czy to w ramach agencji UE zajmujących się walką z przestępczością, czy też na potrzeby przekazywania danych między właściwymi organami pochodzącymi z różnych państw członkowskich. Przetwarzanie danych w ramach dawnego III filaru UE, które odnosiło się do działalności organów wymiaru sprawiedliwości (sądów) i organów ścigania (policji, organów celnych i in.), wiązało się zatem z wykonywaniem obowiązków z zakresu porządku i bezpieczeństwa publicznego. Kolejność przyjmowania regulacji była jednak odwrotna niż w I filarze UE: tu najpierw przyjęto szereg aktów o charakterze szczegółowym, a dopiero później akt o charakterze ogólnym.

Wśród najistotniejszych szczegółowych można wymienić m.in.:

- w ramach Systemu Informacyjnego Schengen (SIS): Konwencję wykonawczą do Układu z Schengen oraz obecnie obowiązujące akty prawne dotyczące SIS II, w szczególności Decyzję 2007/533/WSiSW[17],
- w ramach Europolu: Decyzję 2009/371/WSiSW[18], ale także umowy zawierane przez Europol z państwami trzecimi[19],

---

[14] Nie jest też jasna relacja między projektami aktów prawnych: rozporządzenia i dyrektywy a tymi aktami. Wydaje się, że to o nich mowa jest w art. 2 ust. 1 pkt c Projektu rozporządzenia, ale sprawa nie jest oczywista, patrząc na pierwotną wersję projektu. Zob. również opinię Agencji Praw Podstawowych, Opinia 2/2012, s. 9.

[15] DzUrz. UE L 326 z 13.12.2005, s. 13.

[16] W ramach tej dyrektywy państwa członkowskie zobowiązały organy wdrażające dyrektywę do zachowania poufności określonej w prawie krajowym, w odniesieniu do wszelkich informacji, które uzyskują w trakcie swojej pracy. Por. art. 41 Dyrektywy 2005/85/WE.

[17] Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), DzUrz. L 205 z 7.08.2007, s. 63.

[18] Decyzja Rady 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol), DzUrz. UE L 121, 15.05.2009, s. 37.

[19] Decyzja Rady 2009/934/WSiSW z dnia 30 listopada 2009 r. w sprawie przyjęcia przepisów wykonawczych regulujących stosunki Europolu z partnerami, w tym wymianę danych osobowych i informacji

- w ramach Eurojustu: Decyzję 2002/187/WSiSW[20],
- w ramach systemu Prüm: decyzje 2008/615/WSiSW i 2008/616/WSiSW[21],
- inne przepisy, również częściowo odnoszące się do ochrony danych, w tym:
  - Konwencję o pomocy wzajemnej w sprawach karnych z 2000 r.[22],
  - Decyzję ramową dotyczącą wymiany danych wywiadowczych[23],
  - Decyzję ramową dotyczącą europejskiego nakazu aresztowania[24],
  - Decyzję ramową dotyczącą wymiany informacji z rejestrów karnych (ECRIS)[25],
  - umowy międzynarodowe dotyczące przekazywania danych dotyczących przelotu pasażera (dane PNR)[26].

Dopiero w 2008 r. przyjęto Decyzję ramową 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[27], bardziej ogólną w tym sensie, że dotyczyła różnych aspektów współpracy, ale nieustanawiającą standardu postępowania ze względu na ograniczony zakres przedmiotowy jej zastosowania[28].

---

niejawnych, DzUrz. L z 11.12.2009, s. 6.

[20] Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością, DzUrz. 63 z 6.03.2002, s. 1, następnie zmieniona Decyzją 2003/659/WSiSW oraz Decyzją 2009/426/WSiSW.

[21] Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, DzUrz. L 219 z 6.08.2008, s. 1–11 oraz Decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia Decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, DzUrz. L 210 z 6.08.2008, s. 12.

[22] Konwencja ustanowiona przez Radę zgodnie z art. 34 TUE o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej, DzUrz. C 197 z 12.07.2000, s. 3.

[23] Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej, DzUrz. UE L 386 z 29.12.2006, s. 89–100.

[24] Decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi, DzUrz. L 190 z 18.07.2002, s. 1.

[25] Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji, DzUrz. L 93 z 7.04.2009, s. 23.

[26] Przykładowo Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (danych PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS), DzUrz. L 204 z 4.08.2007, s. 18. Por. również Komunikat Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, KOM(2010) 492 wersja ostateczna.

[27] Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, DzUrz. L 350 z 30.12.2008, s. 60 (dalej: Decyzja ramowa w sprawie ochrony danych).

[28] Więcej na ten temat zob. A. Grzelak, *Projekt ochrony...*, op.cit., s. 21–23.

W efekcie takiego rozbicia rozwój prawodawstwa w zakresie ochrony danych był nierównomierny, jeśli chodzi o dawny I i III filar UE. Jak zostało wspomniane, przetwarzanie danych w I filarze zostało objęte spójnymi regulacjami, wynikającymi przede wszystkim z Dyrektywy ogólnej w sprawie ochrony danych. Od momentu jej przyjęcia ukształtowało się zatem całe *acquis*: prawodawstwo, instytucje[29] czy też wypracowane zostało orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Natomiast w przypadku dawnego III filaru UE rozwój prawodawstwa następował w odwrotnej kolejności – rozwijało się ono *ad hoc*, w zależności od potrzeb, w odniesieniu do poszczególnych instytucji[30].

Na całą mozaikę przepisów przyjętych w ramach Unii Europejskiej nakładają się dodatkowo standardy bardziej ogólne, wynikające z reżimu innej organizacji międzynarodowej, czyli Rady Europy. Należy tu wskazać przede wszystkim Konwencję nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[31], a także orzecznictwo Europejskiego Trybunału Praw Człowieka (dalej: ETPCz).

Podsumowując te wyliczenia i odnosząc się do tematu opracowania, należy podkreślić, że taka wielość obecnie obowiązujących aktów prawnych UE oznacza, że system ochrony danych osobowych nie może mieć charakteru jednolitego, stosowane są bowiem różne rozwiązania w zależności od konkretnego sektora i dziedziny[32]. Powstaje zatem pytanie, czy faktycznie Projekt rozporządzenia i Projekt dyrektywy, mające zastąpić wyłącznie te z wyżej wymienionych aktów, które mają charakter ogólny, a zatem Dyrektywę 95/46/WE oraz Decyzję ramową 2008/977/WSiSW, wprowadzą spójne rozwiązania. W dalszej części rozważań przedstawione zostaną uwagi wskazujące na różnice w konkretnych rozwiązaniach zaproponowanych w obu aktach i podjęta zostanie próba odpowiedzi na pytanie, czy wprowadzenie takich różnic jest uzasadnione.

---

[29] Grupa robocza ds. ochrony danych ustanowiona na mocy art. 29 Dyrektywy 95/46/WE (dalej: Grupa robocza Art. 29) czy też Europejski Inspektor Ochrony Danych (EIOD).

[30] Na ten temat zob. również H. Maroń, *Ochrona danych osobowych w III filarze Unii Europejskiej*, w: *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów*, red. G. Goździewicz, M. Szabłowski, Toruń 2008, a także A. Gajda, *Ochrona danych osobowych w III filarze Unii Europejskiej*, „Studia i Prace Kolegium Ekonomiczno-Spolecznego" 2008, z.n. 15, s. 423.

[31] Konwencja nr 108 Rady Europy sporządzona w Strasburgu dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (DzU 2003, nr 3, poz. 25), uzupełniona Protokołem dodatkowym (DzU 2005, nr 11, poz. 1) (dalej: Konwencja nr 108). Obecnie trwają prace nad jej nowelizacją. Por. dokument z 15 listopada 2011 r. T-PD-BUR(2011) 27_en, dostępny na stronie: http://www.giodo.gov.pl

[32] Szerzej na ten temat zob. chociażby M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010.

3. Problem spójności propozycji zawartych w Projekcie rozporządzenia i w Projekcie dyrektywy

W tej części opracowania przedstawione zostały wybrane zagadnienia ukazujące brak spójności w propozycji przedstawionej przez Komisję Europejską w Projekcie rozporządzenia i w Projekcie dyrektywy. Rozważania prowadzone będą w oparciu o pierwotną wersję projektu, ponieważ do końca października 2013 r. nie przedstawiono wersji projektów, która byłaby uzgodniona ostatecznie przez Radę i Parlament Europejski. Przedstawione niżej wnioski oraz przykłady nie mogą mieć charakteru ostatecznego i wyczerpującego, po pierwsze, ze względu na objętość opracowania, po drugie – z uwagi na stan prac w UE nad projektami.

3.1. Cel projektowanych aktów

Oba projekty, zarówno rozporządzenia, jak i dyrektywy, w pierwszych przepisach wskazują swój cel, który wyjaśniony jest również w ich preambułach. Cele te są nieco inaczej sformułowane. Zgodnie z art. 1 Projektu rozporządzenia jego celem ma być ustanowienie przepisów dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz przepisów dotyczących swobodnego przepływu danych osobowych. Natomiast zgodnie z art. 1 Projektu dyrektywy państwa członkowskie z jednej strony mają chronić prawa podstawowe i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych, ale jednocześnie mają zapewnić, by wymiana danych osobowych przez właściwe organy w Unii nie była ani ograniczana, ani zakazywana z przyczyn związanych z ochroną osób fizycznych.

W tym miejscu wyraźnie pojawia się pewien dysonans: podczas gdy Projekt rozporządzenia na pierwszym miejscu stawia ochronę praw jednostki, to jednak dyrektywa za podstawowy cel stawia sobie zagwarantowanie stosownych uprawnień właściwym organom, nawet kosztem poświęcenia praw jednostki. Można zatem stwierdzić, że poziom ochrony jednostki w zakresie będącym przedmiotem dyrektywy będzie niższy niż poziom ochrony jednostki w zakresie objętym przepisami rozporządzenia.

Czy takie zróżnicowanie jest uzasadnione? Próbę wyjaśnienia można znaleźć w pkt. 7 preambuły do Projektu dyrektywy, w którym stwierdza się, że zapewnienie spójnego, wysokiego poziomu ochrony danych osobowych osób fizycznych oraz ułatwienie wymiany danych osobowych między właściwymi organami państw członkowskich ma zasadnicze znaczenie dla zagwarantowania skutecznej współpracy wymiarów

sprawiedliwości w sprawach karnych i współpracy policyjnej. Podstawowym celem tego aktu jest zatem skuteczna współpraca organów wymiaru sprawiedliwości – to jej ma służyć zapewnienie jednolitego poziomu ochrony jednostki w zakresie jej danych osobowych tak, by został osiągnięty cel w postaci zapobiegania przestępstwom, prowadzenia skutecznych postępowań w ich sprawie czy też ich wykrywania i ścigania. W tym przypadku standard ochrony danych osobowych będzie niższy niż w systemie ogólnym z racji konieczności zagwarantowania bezpieczeństwa i porządku publicznego. Wyważenia jedynie wymaga to, na ile ten standard może być obniżony – tzn. jak daleko posunięta ingerencja organów wymiaru sprawiedliwości i organów ścigania uzasadnia ograniczenie prawa do ochrony danych osobowych.

Takie zróżnicowanie już na poziomie zdefiniowania celu regulacji uzasadnia wybór dokonany przez Komisję w kwestii, czy przyjąć jeden akt, który całościowo regulowałby wszystkie zagadnienia z zakresu ochrony danych, czy też dwa odrębne akty i tym samym kontynuować istniejące już rozróżnienie między podejściem ogólnym a podejściem szczególnym dla spraw związanych z bezpieczeństwem publicznym i zwalczaniem przestępczości. Ze względu na konieczność dokonania zróżnicowania Komisja zdecydowała się na wybór drugiej opcji. Stworzenie całościowego i spójnego systemu ochrony danych nie wyklucza bowiem przyjęcia odrębnych przepisów w omawianym sektorze. Nie można zatem negatywnie ocenić faktu, że przedstawiono dwa odrębne projekty – Projekt dyrektywy dotyczy bowiem dziedziny, w której ochrona danych musi niewątpliwie być uregulowana w sposób szczególny, chociażby ze względu na konieczność przechowywania danych w długim okresie, potrzebę ciągłego porównywania danych z napływającymi informacjami czy oczywistą konieczność ograniczenia dostępu określonej kategorii osób, np. podejrzanych, do danych zbieranych przez właściwe organy na ich temat. Te szczególne cechy skutkują koniecznością przyjęcia szczególnych uregulowań.

3.2. Wybór instrumentu prawnego

Nie kwestionując konieczności przyjęcia dwóch odrębnych regulacji dotyczących ochrony danych osobowych w systemie tzw. ogólnym i w ramach współpracy policyjnej i sądowej w sprawach karnych, dużym znakiem zapytania pozostaje jednak dokonany przez Komisję Europejską wybór konkretnego instrumentu prawnego. Nie jest zupełnie jasne, dlaczego w przypadku systemu ogólnego ochrony danych osobowych będziemy mieć do czynienia z rozporządzeniem, a więc aktem obowiązującym bezpośrednio (art. 288 ak. 2 TfUE), natomiast w odniesieniu do aktów z zakresu współpracy policyjnej i sądowej w sprawach karnych z dyrektywą, która będzie musiała być implementowana do porządku krajowego państw członkowskich (art. 288 ak. 3

TfUE) i wiąże zasadniczo co do celu, pozostawiając poszczególnym państwom duży zakres uznania w zakresie sposobu osiągnięcia wskazanego celu.

Komisja w uzasadnieniu do Projektu dyrektywy wskazuje, że dyrektywa pozostawia państwom niezbędną elastyczność przy wdrażaniu zasad, przepisów i wyjątków od nich na szczeblu krajowym[33]. Jednocześnie dostrzega, że materia jest bardzo skomplikowana i ocena prawidłowości implementacji będzie wymagała, by państwa członkowskie wyjaśniły związek między elementami aktu prawa UE a przyjętymi dla jego wykonania instrumentami krajowymi. Z kolei w przypadku rozporządzenia Komisja podaje, że jest to najbardziej odpowiedni instrument prawny, ponieważ doprowadzi do zmniejszenia rozdrobnienia prawnego i zapewni większą pewność prawa poprzez wprowadzenie ujednoliconego zestawu przepisów podstawowych[34].

Takie rozróżnienie ma niewątpliwy związek z tym, o czym była mowa w punkcie poprzednim, a mianowicie podkreśleniem odmiennego celu regulacji – podczas gdy celem rozporządzenia ma być ochrona praw jednostki, to jednak celem dyrektywy ma być zapewnienie efektywnego funkcjonowania wymiaru sprawiedliwości (przy zagwarantowaniu praw jednostki, ale o nieco niższym standardzie). Z tego względu zezwala się na większą elastyczność w przepisach krajowych w przypadku współpracy w sprawach karnych i patrząc na ten problem przez pryzmat efektywności bezpieczeństwa publicznego, można takie działanie zrozumieć. Powstaje jednak pytanie o to, czy prawa jednostki będą zatem należycie chronione w tym przypadku i czy inny cel, jakim jest spójność systemu ochrony danych, zostanie osiągnięty. W zaistniałej sytuacji nie będzie mowy o jednolitych ramach prawnych dla całego systemu ochrony danych osobowych w UE, ale czy zastosowanie dyrektywy, w której pozostawia się państwom członkowskim wiele miejsca na decyzję co do sposobu prowadzenia poszczególnych działań, budzi zasadnicze wątpliwości. Należy wskazać, że może to spowodować nierówności w systemie ochrony danych między państwami, zwłaszcza w sytuacji, gdy przepisy dyrektywy będą tak nieprecyzyjne, jak w przedłożonym projekcie[35].

Osobną kwestią, która musi zostać rozstrzygnięta przed przyjęciem aktów, jest ustalenie, czy wejście w życie dyrektywy w zaproponowanym kształcie nie spowoduje obniżenia standardów w niektórych państwach członkowskich, które już wcześniej

---

[33] COM(2012) 10, s. 7.

[34] COM(2012) 11, s. 6.

[35] Wybór dyrektywy może jednak powodować również pewne trudności praktyczne w transpozycji, bowiem jak przykładowo przenieść do prawa krajowego treść art. 49 Projektu dyrektywy, określającego zadania Europejskiej Rady Ochrony Danych, czyli organu ustanowionego rozporządzeniem ogólnym. Zadania tego organu nie powinny chyba być określane w aktach prawnych poszczególnych państw, lecz powinny wynikać z aktu obowiązującego bezpośrednio (rozporządzenia lub może decyzji). Szerzej na ten temat zob. A. Grzelak, *Projekt ochrony...*, op.cit., s. 24.

uregulowały przetwarzanie danych w ramach wymiaru sprawiedliwości i współpracy policyjnej w sposób lepiej chroniący prawa jednostki[36]. Przyjęcie dyrektywy nie może skutkować tym, że państwa obniżą standard obowiązujący, powołując się na postanowienia dyrektywy.

3.3. Chronione prawa podstawowe

W uzasadnieniu do Projektu rozporządzenia poza prawem podstawowym, jakim jest prawo do ochrony danych osobowych, Komisja wskazuje i wymienia inne prawa podstawowe, na które projekt może mieć wpływ (z odniesieniem do stosownych przepisów KPP). Są to m.in.: wolność wypowiedzi; wolność działalności gospodarczej; prawo własności; zakaz dyskryminacji innych osób ze względu na takie czynniki, jak: rasa, pochodzenie etniczne, cechy genetyczne, religia lub przekonania, poglądy polityczne lub wszelkie inne poglądy, niepełnosprawność lub orientacja seksualna; prawa dziecka; prawo do wysokiego poziomu ochrony zdrowia ludzkiego; prawo dostępu do dokumentów czy też prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu[37]. W Projekcie dyrektywy lista ta jest o wiele krótsza: w uzasadnieniu wymienia się zakaz dyskryminacji ze względu na takie czynniki, jak: płeć, pochodzenie etniczne, cechy genetyczne, religię lub światopogląd, przekonania polityczne lub inne przekonania, niepełnosprawność lub orientację seksualną; prawa dziecka; prawo do skutecznego sądowego środka ochrony prawnej oraz prawo do rzetelnego procesu[38].

W żadnym z projektów nie przedstawiono uzasadnienia dla takiego zróżnicowania. Trzeba podkreślić, że – jak zauważa Agencja Praw Podstawowych[39] – z Projektu dyrektywy jasno wynika, że dotyka ona również innych praw, np. obowiązku zapewnienia wysokiego poziomu ochrony zdrowia (art. 35 KPP), zwłaszcza że Projekt dyrektywy odwołuje się do danych dotyczących zdrowia w kontekście ograniczenia przetwarzania tzw. danych wrażliwych. Przetwarzanie danych w oparciu o przepisy dyrektywy dotyczy również wolności wypowiedzi. Można zatem postawić pytanie, czy – skoro nie zostały wymienione w uzasadnieniu do Projektu dyrektywy, a w Projekcie rozporządzenia są – to oznacza, że te konkretne prawa podstawowe nie będą chronione w oparciu o przepisy dyrektywy albo poziom ich ochrony będzie ograniczony. Agencja Praw Podstawowych, oceniając oba projekty, zasugerowała ich

[36] Por. Opinię Grupy roboczej Art. 29 nr 2/2012 z 23.03.2012, WP 191, s. 27.
[37] COM(2012) 11, s. 7.
[38] COM(2012) 10, s. 8.
[39] Zob. opinię przedstawioną przez Agencję Praw Podstawowych, Opinia 2/2012, 1.10.2012, s. 8.

wzajemne dostosowanie[40] i poddała pod rozwagę wprowadzenie ogólnej klauzuli, w której stwierdza się konieczność ochrony wszelkich innych praw podstawowych.

Wydaje się, że brak odniesienia do kilku chronionych przez KPP praw w Projekcie dyrektywy, a wymienienie ich w Projekcie rozporządzenia nie niesie za sobą istotnych skutków i nie będzie powodowało braku spójności przyjętych rozwiązań. Ochrona praw podstawowych wynikających z KPP jest obecnie obowiązkiem i instytucji UE, i państw członkowskich w zakresie, w jakim stosują one prawo UE, a zatem wszelkie przyjmowane akty prawne powinny być z nimi zgodne[41] bez względu na to, czy prawa te są wymienione w uzasadnieniu, preambule, czy przepisach, czy też nie są wyraźnie wymienione.

3.4. Materialny zakres zastosowania

Zakres zastosowania obu aktów prawnych wyznaczają pierwsze ich przepisy. Zgodnie z art. 2 ust. 1 Projektu rozporządzenia „rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób w całości lub w części zautomatyzowany oraz innych rodzajów przetwarzania danych osobowych, stanowiących część zbioru danych lub mających stanowić część zbioru danych". Z kolei w art. 2 ust. 2 Projektu rozporządzenia znajduje się wyłączenie – wykaz dziedzin, do których rozporządzenie nie będzie miało zastosowania, czyli: a) „w ramach działalności wykraczającej poza zakres prawa Unii, w szczególności dotyczącej bezpieczeństwa narodowego, b) przetwarzania danych przez instytucje, organy i jednostki Unii[42], c) przez państwa członkowskie w wykonywaniu działań wchodzących w zakres rozdziału 2 TfUE[43], d) przez osobę fizyczną w celach innych niż zarobkowe w ramach działań o charakterze czysto osobistym lub domowym i wreszcie e) przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania albo wykonywania kar kryminalnych"[44]. W art. 2 ust. 3 wyłączono również zastosowanie rozporządzenia do sytuacji uregulowanych Dyrektywą 2000/31/WE, a zatem objętych przepisami dyrektywy o handlu elektronicznym.

W Projekcie dyrektywy, w art. 2 stwierdza się, że dyrektywa ma zastosowanie do przetwarzania danych osobowych przez właściwe organy do celów, o których mowa w art. 1 ust. 1, a zatem zapobiegania przestępstwom, prowadzenia dochodzeń w ich

[40] Ibidem, s. 9.

[41] Por. art. 51 Karty Praw Podstawowych.

[42] Tu zastosowanie znajdzie niezmieniane Rozporządzenie 45/2001.

[43] Nie jest jasne, o jaki rozdział 2 chodzi – którego tytułu TfUE ma to dotyczyć. Wydaje się, że chodzi o tytuł V TfUE, rozdział 2, czyli o polityki dotyczące kontroli granicznej, azylu i imigracji, chociaż sprawa nie jest oczywista.

[44] Tu zastosowanie ma znaleźć dyrektywa, której projekt przedstawiony jest równolegle.

sprawie, wykrywania ich lub ścigania i wykonywania „kar kryminalnych”[45]. W artykule 2 ust. 3 Projektu dyrektywy proponuje się wyłączenia, a mianowicie dyrektywa nie będzie miała zastosowania do przetwarzania danych osobowych „a) w ramach działalności wykraczającej poza zakres prawa Unii, b) przez instytucje, organy i jednostki organizacyjne Unii”[46].

Takie określenie zakresu stosowania obu aktów prawnych rodzi jednak szereg wątpliwości w odniesieniu do ich spójności.

Po pierwsze, projektodawca zakłada, że przyjmowane rozporządzenie, dyrektywa, obowiązujące Rozporządzenie 45/2001 oraz obowiązujące akty szczególne dotyczące wymiany danych w ramach takich organów, jak Europol czy Eurojust, będą się wzajemnie uzupełniać[47]. Podstawowym problemem, który powinien jednak zostać rozwiązany, a projekty na razie tej kwestii nie podnoszą, jest zatem relacja między obowiązującymi aktami prawnymi. Projekt rozporządzenia i dyrektywy nie przewiduje bowiem ani uchylenia, ani nawet ustanowienia ich hierarchii. Wręcz przeciwnie, pozostawiają bez uszczerbku wcześniej przyjęte akty prawne[48], a zatem zamiast ujednolicać system – w systemie prawnym UE obowiązywać będzie nadal wiele aktów prawnych regulujących kwestie ochrony danych osobowych. To zdecydowanie stoi w sprzeczności z postulatem stworzenia jednolitych ram prawnych. Co prawda Projekt dyrektywy zakłada konieczność dokonania przeglądu obowiązujących aktów prawnych[49], ale dopiero 3 lata po wejściu w życie dyrektywy – jest to zdecydowanie za długi okres, zwłaszcza że obowiązujące przepisy nie zawierają identycznych rozwiązań, również w porównaniu z projektem. Komisja także w sposób dość zaskakujący próbuje uregulować kwestię ewentualnej niezgodności zawartych przez państwa członkowskie umów międzynarodowych, zakładając ich zmianę w ciągu 5 lat od wejścia w życie dyrektywy[50]. Nie bierze jednak w ogóle pod uwagę drugiej strony takiej umowy i jej ewentualnej woli do wprowadzenia zmian.

---

[45] Ang. *criminal sanctions*, czyli raczej w jęz. polskim chodzi o sankcje karne.

[46] Tu należy również zwrócić uwagę na art. 59 Projektu dyrektywy, zgodnie z którym mają pozostać w mocy przepisy szczególne dotyczące ochrony danych osobowych w zakresie ich przetwarzania przez właściwe organy w tym samym celu, o którym mowa w art. 1 ust. 1, a które zostały przyjęte przed datą przyjęcia dyrektywy, regulujące przetwarzanie danych osobowych między państwami członkowskimi lub dostęp wyznaczonych organów państw członkowskich do systemów informacyjnych ustanowionych na mocy traktatów w zakresie zastosowania dyrektywy. Chodzi tu m.in. o system SIS. Również wymiana danych w ramach Eurojustu i Europolu wyłączona będzie na moc art. 2 ust. 2 pkt b Projektu dyrektywy, jako wymiana danych przez organy i jednostki organizacyjne Unii.

[47] Naturalnie nie obejmą również przetwarzania danych w ramach Wspólnej Polityki Zagranicznej i Bezpieczeństwa, objętej inną podstawą traktatową UE.

[48] Por. art. 59 Projektu dyrektywy oraz art. 88 i 89 Projektu rozporządzenia.

[49] Art. 61 ust. 2 Projektu dyrektywy.

[50] Por. art. 60 Projektu dyrektywy.

Po drugie, oba akty prawne w swoim założeniu nie mają dotyczyć przetwarzania danych w ramach działalności wykraczającej poza zakres prawa Unii. Jeśli w przypadku rozporządzenia można stwierdzić, że obejmie ono *de facto* całą sferę działalności gospodarczej, to jednak w przypadku dyrektywy sprawa nie jest oczywista. Projekt dyrektywy w swoim założeniu ma całościowo uregulować przetwarzanie danych osobowych w ramach współpracy policyjnej i współpracy sądowej w sprawach karnych, a zatem również przetwarzanie danych na poziomie krajowym (co do tej pory nie było przedmiotem Decyzji ramowej 2008/977/WSiSW)[51]. Założenie to jednak nie jest w pełni słuszne. Wyłączenie zastosowania Projektu dyrektywy w odniesieniu do działalności wykraczającej poza zakres prawa Unii, w połączeniu z brzmieniem art. 16 TfUE, który stanowi, że Parlament Europejski i Rada określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także w związku z treścią art. 82–89 TfUE, wcale nie dają podstaw do twierdzenia o całościowej regulacji. Przyjęte zasady ochrony danych osobowych będą bowiem dotyczyć tylko tych kwestii, w których właściwe jest prawo Unii Europejskiej, a to nie reguluje całości zagadnień działalności organów wymiaru sprawiedliwości czy organów ścigania, a jedynie niektóre zagadnienia[52]. Postęp w stosunku do obowiązującego stanu prawnego byłby zatem w takim sensie, że Projekt dyrektywy nie ogranicza się wyłącznie do transgranicznego przekazywania danych, ale również do krajowego przetwarzania danych, o ile ma ono związek z kwestiami uregulowanymi w prawie UE.

Po trzecie, problemem pozostaje ustalenie, do jakich konkretnie organów i podmiotów planowana dyrektywa i rozporządzenie miałyby mieć zastosowanie. Zgodnie z art. 1 Projektu dyrektywy chodzi o „przetwarzanie danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania i wykonywania kar kryminalnych"[53]. W artykule 2 ust. 2 lit. e Projektu rozporządzenia to sformułowanie się powtarza. Trzeba

---

[51] Por. A. Grzelak, *Projekt ochrony...*, op.cit., s. 22. Zob. również Opinię EIOD z 7 marca 2012 r., http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf; data pobrania 15 marca 2012 r.) czy też przywoływaną Opinię Grupy roboczej Art. 29, WP 191, s. 28.

[52] Art. 82 TfUE dotyczy współpracy w oparciu o zasadę wzajemnego uznawania orzeczeń, a także zbliżania przepisów państw członkowskich w dziedzinach wymienionych w tym przepisie. Art. 83 TfUE odnosi się do harmonizacji prawa karnego materialnego w dziedzinach wymienionych w przepisie. Z kolei zakres współpracy policyjnej określa w szczególności art. 87 TfUE.

[53] Na marginesie należy zauważyć, że jeżeli dyrektywa zostałaby uchwalona w obecnym kształcie, to w polskim systemie prawnym kontroli krajowego organu nadzorczego (Generalny Inspektor Ochrony Danych Osobowych lub jakiś nowy organ) powinny być poddane organy, które dotychczas z takiej kontroli były wyłączone, jak Agencja Bezpieczeństwa Wewnętrznego czy Centralne Biuro Antykorupcyjne.

jednak pamiętać, że państwa członkowskie różnie podchodzą do charakteru prawnego swoich organów, w szczególności w obszarze ceł czy imigracji, i niekiedy nie zaliczają ich do organów prowadzących postępowanie karne, lecz do organów administracji, prowadzących postępowanie administracyjne. Takie ogólne sformułowanie użyte w projektach może w efekcie prowadzić do sytuacji, w której te same dane w jednym państwie będą podlegały reżimowi ogólnemu wynikającemu z rozporządzenia, a w innym z dyrektywy[54]. Konieczne jest zatem doprecyzowanie od strony podmiotowej, do których konkretnie organów dyrektywa będzie miała zastosowanie. Warto przy okazji dodać, że Projekt rozporządzenia, posługujący się pojęciem „właściwego organu do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania albo wykonywania kar kryminalnych" w art. 2 ust. 2 lit. e nie definiuje go i nie odsyła również do definicji z Projektu dyrektywy, która w art. 3 pkt 14 stanowi, że chodzi o organ publiczny. Można zadać pytanie, czy na pewno chodzi o ten sam organ, a zatem czy jest to błąd projektu, czy też jest to zamierzone działanie, które prowadziłoby do wniosku o braku tożsamości tego pojęcia w obu aktach. Na tym etapie należy jedynie wypunktować ten problem i podnieść po raz kolejny brak spójności między obydwoma aktami.

W tym kontekście pojawia się również inny problem, a mianowicie jakiemu reżimowi podlega przetwarzanie danych przez podmioty prywatne na potrzeby związane z walką z przestępczością – czy będzie to wchodzić w zakres rozporządzenia, czy też w zakres dyrektywy. Problem ten znany jest i dyskutowany już w obecnym stanie prawnym. Obowiązująca Decyzja ramowa 2008/977/WSiSW nie dotyczy przetwarzania danych przez podmioty, które nie są organem policyjnym lub sądowym, a które przetwarzają dane dla celów związanych z bezpieczeństwem publicznym. Z kolei Dyrektywa ogólna 95/46/WE również zawiera stosowne wyłączenia. W takiej sytuacji organy prywatne przetwarzające dane osobowe, nawet na potrzeby związane ze zwalczaniem przestępczości, które to dane później będą wykorzystane przez organy policji czy organy wymiaru sprawiedliwości, powinny podlegać systemowi ogólnemu ochrony danych[55]. Teza ta nie znalazła jednak swojego odzwierciedlenia w orzecznictwie ETS, który zajmował się umową zawieraną przez UE z USA w sprawie przekazywania przez przewoźników lotniczych odpowiednim organom amerykańskim danych pasażerów (tzw. danych PNR). W połączonych sprawach C-317/04 i 318/04[56]

[54] Słusznie zwraca na to uwagę Grupa robocza Art. 29 w swojej opinii do obu projektów, WP 191, s. 26.

[55] Za tą tezą powinno przemawiać również dotychczasowe orzecznictwo ETS, chociażby w sprawach połączonych C-465/00, C-138/01 i C-139/01 Österreichischer Rundfunk, Zb. Orz. 2003, s. I-4989.

[56] Wyrok Trybunału z 30 maja 2006 r. w sprawie Parlament Europejski przeciwko Radzie Unii Europejskiej (C-317/04) i Komisji Wspólnot Europejskich (C-318/04), Zb. Orz. 2006, s. I-4721.

(tzw. sprawa PNR) ETS wyraźnie wskazał, że przekazywanie takich danych, chociaż dokonywane przez podmioty prywatne, to jednak jest prowadzone w ramach określonych przez władze publiczne i dotyczy bezpieczeństwa publicznego, a zatem wyłączone jest z systemu ogólnego ochrony danych osobowych[57]. Z kolei w sprawie dotyczącej retencji danych telekomunikacyjnych[58], mimo że dane, o których mowa, mają być przechowywane przez podmioty prywatne do celów służących zabezpieczeniu porządku publicznego i bezpieczeństwa publicznego, Trybunał Sprawiedliwości uznał, że obowiązki wynikające z dyrektywy o retencji danych podlegają systemowi ogólnemu. Uzasadnieniem dla tego stanowiska był fakt, że w tym przypadku dane dotyczą działalności dostawców usług telekomunikacyjnych, a nie organów publicznych. Niejasny stan prawny wyraźnie zatem udowadnia, że konieczne jest przyjęcie i uregulowanie zasad dotyczących przetwarzania danych przez podmioty prywatne na cele związane z ochroną porządku publicznego[59]. Obydwa projekty nie rozwiązują kwestii rozdziału czy w ogóle uregulowania przetwarzania danych na potrzeby komercyjne od przetwarzania danych na potrzeby bezpieczeństwa, bez względu na podmiot przetwarzający, zwłaszcza ze względu na istniejące wątpliwości co do pojęcia „właściwy organ". Wydaje się, że skoro w Projekcie dyrektywy pod pojęciem „właściwego organu" rozumie się każdy organ publiczny, a Projekt rozporządzenia nie odsyła do właściwej definicji, to oznaczałoby – w oparciu o przedstawione pierwotne projekty – że do przetwarzania danych przez organy prywatne znajdzie zastosowanie rozporządzenie ogólne.

W żadnym z dwóch projektów nie uregulowano również dodatkowych warunków i zasad, na jakich takie przetwarzanie może mieć miejsce[60]. Ani Projekt rozporządzenia, ani Projekt dyrektywy nie rozstrzygają w ogóle wątpliwości, czy dopuszczalne jest rutynowe pobieranie i przetwarzanie danych osobowych, w celach prewencyjnych przez podmioty prywatne, np. w ramach systemu PNR, a także w ogóle nie reguluje również kwestii dostępu policji do danych w sektorze prywatnym. *De lege ferenda*, kryterium regulacji (przetwarzania) powinny stanowić dane i cel ich wykorzystania, a nie organ przetwarzający.

---

[57] Trybunał w pkt. 58 wyroku przypomniał, że dane te są gromadzone przez podmioty prywatne do celów działalności gospodarczej, to te podmioty przekazują dane do państwa trzeciego, ale jednak to przekazanie następuje w ramach ustanowionych przez władze publiczne i mających na celu ochronę bezpieczeństwa publicznego.

[58] Wyrok Trybunału z 10 lutego 2009 r. w sprawie Irlandia przeciwko Parlamentowi Europejskiemu i Radzie Unii Europejskiej (C-301/06), Zb. Orz. 2009, s. I-593.

[59] Sugeruje to również Els de Busser. Zob. E. de Busser, *The Data Protection Gap. From Private Databases to Criminal Files*, „Eucrim" 2013, No. 2, s. 17–22.

[60] Art. 7 lit. b Projektu dyrektywy, który mógłby dotyczyć sytuacji, w której organ publiczny jest zobowiązany przekazać podmiotowi prywatnemu określone dane, stanowi wyłącznie ogólną podstawę prawną takich działań i nie określa żadnych szczegółowych warunków.

Wreszcie po czwarte, oba projekty posługują się wyłączeniem dotyczącym bezpieczeństwa narodowego[61]. Jest to kolejny przykład dowodzący tezy o braku spójności systemu, który ma zostać stworzony. Prawdopodobnie projektodawca w ten sposób zamierza oddać treść art. 72 i 73 TfUE, pozostawiających pewne kwestie z zakresu bezpieczeństwa wewnętrznego i narodowego w kompetencji państw członkowskich. Podstawowym problemem praktycznym może być jednak określenie zakresu tego wyłączenia i samo zdefiniowanie pojęcia „bezpieczeństwo narodowe", które przecież każde z państw może postrzegać odmiennie[62], a co w efekcie może prowadzić do omijania zasad ochrony danych przez właściwe organy. Chociaż dokumenty międzynarodowe takie wyłączenie również przewidują[63], to jednak powszechnie wskazuje się, że generalność takich postanowień stwarza szerokie pole interpretacyjne i w efekcie pozostawia dużą swobodę w zakresie implementacji i stosowania przepisów[64]. Konieczne jest zatem sprecyzowanie w toku dalszych prac, jakich konkretnie sytuacji dotyczy to ograniczenie[65]. Jest to bardzo poważny sygnał wskazujący na niepełność regulacji i możliwość wprowadzenia pewnych wyłomów w jednolitym systemie współpracy, co już oznacza, że podstawowe założenie reformy może nie zostać spełnione.

3.5. Zasady przetwarzania danych osobowych

Zasady przetwarzania danych osobowych w obu projektach znalazły się w rozdziale II. Nie są one jednak identycznie uregulowane[66] i należy zwrócić uwagę na kilka różnic, które – jak się wydaje – w większości przypadków nie mają szczególnego uzasadnienia, natomiast potwierdzają tezę o braku spójności projektowanego systemu ochrony danych osobowych.

---

[61] Por. art. 2 lit. a Projektu rozporządzenia oraz art. 2 ust. 3 lit. a Projektu dyrektywy.

[62] Por. A. Grzelak, *Komentarz do art. 72 i komentarz do art. 73*, w: *Komentarz do Traktatu o funkcjonowaniu Unii Europejskiej*, t. I, red. A. Wróbel, D. Miąsik, N. Półtorak, Warszawa 2012, s. 1091–194, 1097–1098.

[63] Przykładowo Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z 23.09.1980 r. w sprawie wytycznych regulujących ochronę prywatności i przepływ danych osobowych przez granice posługuje się w tym kontekście określeniami „suwerenność narodowa" i „bezpieczeństwo narodowe" (pkt 1). Z kolei Rezolucja 45(95) Zgromadzenia Ogólnego ONZ z 14 grudnia 1990 r. zawierająca wytyczne w sprawie regulacji skomputeryzowanych zbiorów danych osobowych również posługuje się ogólną kategorią „bezpieczeństwo narodowe" (pkt 6).

[64] Por. M. Jagielski, op.cit., s. 62.

[65] W ww. wytycznych OECD z 1980 r. wskazano, że wyjątki powinny być „możliwie nieliczne", zaś w wytycznych ONZ są one dopuszczalne, jeżeli są „konieczne".

[66] Pewne wątpliwości pojawiają się również w odniesieniu do polskiego tłumaczenia projektu – przykładowo w KOM(2012) 10 używa się pojęcia dane „dokładne" w art. 4, natomiast w KOM(2012) 11 – dane „ścisłe". W wersji angielskiej w obu przypadkach jest to to samo pojęcie *accurate*. Należy zatem dopilnować spójności w tłumaczeniu obu projektów, które w polskiej wersji językowej będą obowiązującym prawem.

Przykładowo w art. 4 Projektu dyrektywy nie wprowadza się postanowienia na wzór tego, które jest w Projekcie rozporządzenia, by dane były przetwarzane w sposób przejrzysty w odniesieniu do podmiotu danych, co można uzasadnić szczególnym charakterem danych zbieranych przez organy wymiaru sprawiedliwości i co może znaleźć swoje uzasadnienie z przyczyn związanych z efektywnością działania stosownych organów. Jednakże w dyrektywie nie znalazły się również istotne elementy dotyczące przechowywania danych przez okres dłuższy niż jest to niezbędne dla celów, dla których są one przetwarzane[67], co już trudno jest wyjaśnić.

Wśród innych różnic warto wspomnieć o uregulowaniach dotyczących zasady celowości, w szczególności w dyrektywie nie wyjaśnia się, co może oznaczać „przetwarzanie niezgodne z celami" (w domyśle – zgodnymi z prawem)[68]. W preambule do Projektu rozporządzenia można znaleźć motywy wyjaśniające, na czym polegać może przetwarzanie danych osobowych do innych celów[69], ale w Projekcie dyrektywy nie ma odpowiednika, a zatem pojawia się pytanie, czy dalsze przetwarzanie danych w celu zwalczania przestępczości, ale w innym niż cel pierwotny, będzie dopuszczalne, czy może jednak nie. Generalnie należy postulować jasne określenie i wprowadzenie rozróżnienia między legalnością przetwarzania danych w celach określonych, wyraźnych i uzasadnionych oraz derogacjami od tej zasady, zgodnie z którymi dane mogą być wykorzystane w przyszłości do celów innych niż pierwotny, zwłaszcza że takie rozróżnienie wprowadza orzecznictwo ETPCz.

Ponadto ograniczenie czasu przechowywania danych nie będzie mieć – w przypadku obu projektów – zastosowania do danych, które poddane zostały anonimizacji. Różnica polega jednak na tym, że Projekt rozporządzenia wprowadza ograniczenie dopuszczalności zbierania takich danych (dotyczy to wyłącznie ich przetwarzania do celów dokumentacji, statystyki lub badań naukowych na warunkach określonych w przepisie), natomiast dyrektywa żadnych ograniczeń nie przewiduje. Ograniczenie, zawarte w art. 4 Projektu dyrektywy, odnoszące się do przechowywania przez czas nie dłuższy niż jest to konieczne do celów, dla których dane są przetwarzane, dotyczy wyłącznie danych umożliwiających identyfikację podmiotów.

Projekt dyrektywy nie zawiera również przepisu zezwalającego na przetwarzanie danych do celów naukowych czy historycznych, chociaż stosowna regulacja jest w Projekcie rozporządzenia[70].

---

[67] Zgodnie z art. 4 lit. c Projektu dyrektywy państwa członkowskie stanowią przepisy nakazujące, by dane osobowe były prawidłowe, właściwe oraz by nie wykraczały poza zakres niezbędny do celów, dla których są przetwarzane. Por. art. 5 lit. e Projektu rozporządzenia z art. 4 lit. e Projektu dyrektywy.

[68] Por. art. 4 lit. b Projektu dyrektywy.

[69] Motyw 40 preambuły do Projektu rozporządzenia.

[70] Por. art. 9 ust. 2 lit. i Projektu rozporządzenia.

W Projekcie dyrektywy rozluźniono również obowiązek dowiedzenia zgodności operacji przetwarzania z jej przepisami w porównaniu z odpowiednim obowiązkiem nałożonym w Projekcie rozporządzenia. W art. 4 lit. f Projektu dyrektywy stwierdza się wyłącznie, że administrator ma zapewnić zgodność takiej operacji z przepisami przyjętymi na mocy dyrektywy, podczas gdy w art. 5 lit. f Projektu rozporządzenia wskazuje się na obowiązek polegający na zapewnieniu, ale i wykazaniu zgodności każdej operacji z przepisami rozporządzenia. Nie jest jasna przyczyna takiego rozróżnienia.

Z kolei Projekt dyrektywy proponuje rozróżnienie, które nie ma swojego odpowiednika w Projekcie rozporządzenia i które jest uzasadnione szczególnym charakterem projektu[71], dotyczące rozróżnienia danych osobowych poszczególnych kategorii podmiotów danych, takich jak: a) osoby, w stosunku do których istnieją poważne podstawy, by przypuszczać, że popełniły lub zamierzają popełnić przestępstwo, b) osoby skazane za przestępstwo, c) osoby, które padły ofiarą przestępstwa lub w przypadku których określone fakty wskazują, że mogły paść ofiarą przestępstwa, d) osoby trzecie w stosunku do przestępstwa, takie jak osoby, które mogą być wezwane do złożenia zeznań w ramach dochodzenia dotyczącego przestępstwa lub dalszych etapów postępowania karnego lub osoby mogące dostarczyć informacji o przestępstwach albo osoby mające kontakt jedną z osób wymienionych w lit. a lub b, albo wspólnicy tych osób, oraz e) osoby, które nie należą do żadnej z wyżej wymienionych kategorii[72]. Treść tego przepisu nie jest jednak jasna, co umniejsza pozytywną ocenę jego wprowadzenia. W szczególności ogranicza się rozróżnienie poprzez dodanie słów „w możliwym zakresie" oraz wprowadza szeroki zakres kategorii „osób różnych" (art. 5 ust. 1 lit. e Projektu dyrektywy), których dane mogą być przetwarzane. Ponadto art. 6 Projektu dyrektywy, w którym nakłada się na państwa członkowskie obowiązek, by kategorie danych osobowych poddawanych przetwarzaniu były rozróżniane według stopnia ich dokładności i wiarygodności, jest bardzo istotny, bowiem w przypadku przetwarzania danych przez odpowiednie służby często dochodzi do oparcia wniosków o przypuszczenia, a nie o fakty. Jednak użycie sformułowania „na ile to możliwe" zdecydowanie osłabia skuteczność tego przepisu.

---

[71] Wprowadzenie takiego rozróżnienia nakazuje Rekomendacja R(87)15 Komitetu Ministrów Rady Europy, co – jak dotychczas – nie było zrealizowane w obowiązujących przepisach. Por. A. Grzelak, *Projekt ochrony...*, op.cit., s. 27.

[72] To sformułowanie jest niejasne i rodzi wątpliwości, czy dopuszczalne jest tak szerokie przetwarzanie danych osobowych na potrzeby dyrektywy. Wydaje się, że dopuszczenie przetwarzania danych osobowych osób należących do tej kategorii powinno być ograniczone czasowo i dopuszczalne wyłącznie na określonych warunkach. Projekt dyrektywy tego postulatu nie uwzględnia. Zob. również propozycję zmiany tego przepisu zaproponowaną przez Grupę roboczą Art. 29. Por. Opinia 01/2013 stanowiąca dalszy wkład w dyskusję nad Projektem dyrektywy o ochronie danych osobowych przetwarzanych przez organy policyjne i sądowe w sprawach karnych, WP 201, 00379/13/PL, s. 3–5.

Szeroki zakres wyłączeń zawartych zarówno w art. 8 Projektu dyrektywy, jak i w Projekcie rozporządzenia (art. 9) również nasuwa szereg pytań. Obydwa projekty w szczególności zabraniają przetwarzania danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, wierzenia religijne lub przekonania filozoficzne, przynależność do związków zawodowych oraz przetwarzania danych genetycznych lub danych dotyczących zdrowia i życia seksualnego. To ograniczenie nie ma jednak zastosowania, gdy przetwarzanie danych jest niezbędne „w celu ochrony żywotnych interesów podmiotu danych lub innej osoby" lub przetwarzanie dotyczy danych, które „zostały wyraźnie podane do publicznej wiadomości" przez ich podmiot. Te wyłącznie są bardzo szerokie, a ich interpretacja i praktyka stosowania może być całkowicie rozbieżna w poszczególnych państwach członkowskich. Konieczne jest zatem ich doprecyzowanie[73].

Wreszcie, Projekt dyrektywy – w odróżnieniu od Projektu rozporządzenia – nie wprowadza przepisów uwzględniających szczególną sytuację dzieci[74]. Problem ten podkreślony jest również w wielu opiniach[75], w których zaznacza się, że powinny zostać ustanowione progi wieku, poniżej których dane nie powinny być przetwarzane na potrzeby związane z urzeczywistnianiem celu dyrektywy, a państwa członkowskie powinny przewidzieć krótsze okresy przechowywania danych dotyczących dzieci w aktach policyjnych i sądowych.

Projekt dyrektywy w tym rozdziale porusza również kwestię profilowania, podczas gdy w Projekcie rozporządzenia stosowny przepis znajduje się kolejnym rozdziale dotyczącym praw podmiotów danych. Pomijając tę różnicę systemową, należy zwrócić również uwagę na rozbieżności w treści przepisów – w szczególności w Projekcie dyrektywy nie objęto zakazem profilowania elementów związanych z zachowaniem. Projekt rozporządzenia obejmuje zakazem nie tylko ocenę niektórych aspektów osobistych tej osoby fizycznej (tak również projekt dyrektywy), ale również analizę bądź przewidzenie zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności czy też zachowania tej osoby fizycznej[76].

W kontekście braku spójności projektowanych rozwiązań warto zaznaczyć, że Projekt rozporządzenia w odniesieniu do zasad przetwarzania danych wprowadza szereg wyjątków dla organów publicznych, co jest uzasadniane koniecznością ochrony

[73] Por. Uwagi Fundacji Panoptykon do Projektu dyrektywy, 6.04.2012 r., opublikowane na stronie Fundacji: http://www. panoptykon.org

[74] Zob. art. 8 Projektu rozporządzenia.

[75] Zob. np. przywoływane już opinie: Agencji Praw Podstawowych, pkt 47, s. 18, Opinię EIOD, § 79 czy Opinię Grupy roboczej Art. 29, s. 16.

[76] Kolejne uwagi dotyczące samej definicji profilowania znalazły się w przywołanych wyżej Uwagach Fundacji Panoptykon, s. 3.

interesu publicznego. Przykładowo w art. 6 ust. 4 wprowadza się szerokie możliwości zmiany pierwotnego celu postępowania na inny niezgodny z nim cel (np. cel niezbędny do wykonania zadania realizowanego w interesie publicznym), zaś w art. 9 ust. 2 lit. g Projektu rozporządzenia umożliwia się przetwarzanie danych szczególnie chronionych na potrzeby zadań realizowanych „w interesie publicznym"[77]. Takie ogólne wyjątki mogą być ocenione jako odstępstwo od próby kompleksowego uregulowania ochrony danych, zwłaszcza że są one niedookreślone i obszerne. Poziom ochrony danych w sektorze publicznym w poszczególnych państwach członkowskich jest zróżnicowany, a projektowane rozwiązania nie powinny spowodować obniżenia standardu ochrony danych.

3.6. Prawa podmiotów danych

Pojęcie „podmiotu danych" zostało zdefiniowane w Projekcie rozporządzenia i Projekcie dyrektywy w identyczny sposób[78]. Definicja odzwierciedla poglądy przyjęte jeszcze w 2007 r. opinii Grupy roboczej Art. 29, która uznała, że osoba fizyczna może być uznawana za możliwą do identyfikacji w grupie osób, jeżeli można ją odróżnić od innych członków grupy, a tym samym traktować inaczej[79].

Prawa podmiotu danych w obu aktach uregulowane zostały w rozdziale III, ale już w odmienny sposób. Zarówno Projekt rozporządzenia, jak i Projekt dyrektywy przewidują szereg praw, z których można korzystać na żądanie, w tym prawo do informacji, prawo dostępu do danych oraz prawo do skorygowania lub usunięcia nieprawidłowych lub przetworzonych niezgodnie z prawem danych. Szczególnie w odniesieniu do Projektu dyrektywy jest to krok naprzód, bowiem uzyskanie informacji o tym, jakie dane są przetwarzane i z jakiej przyczyny, są kluczowym aspektem prawa do ochrony danych. Jednak Projekt rozporządzenia zakłada szereg dalej idących uprawnień podmiotu danych, natomiast Projekt dyrektywy zawiera ograniczenia i nie przyznaje jednostce tak szerokich praw. Takie zróżnicowanie jest jednak zrozumiałe, ze względu na charakter przetwarzanych danych – organy wymiaru sprawiedliwości i organy ścigania nie mogą zawsze wyjawiać sposobów przetwarzania danych oraz w ogóle ujawniać, jakie dane posiadają, ponieważ mogłoby to niewątpliwie mieć wpływ na prowadzone postępowania. Zrozumiałe jest, że w przypadku systemu wymiaru sprawiedliwości i organów ścigania ograniczenie praw jednostki

[77] Wśród innych wyjątków związanych z koniecznością ochrony „interesu publicznego" w Projekcie rozporządzenia należy wskazać art. 21 czy art. 33 ust. 5.

[78] Por. art. 3 pkt 1 Projektu dyrektywy oraz art. pkt 1 Projektu rozporządzenia.

[79] Por. Opinię Grupy roboczej Art. 29, WP 136.

w odniesieniu do ochrony danych osobowych musi iść dalej niż w innych dziedzinach współpracy państw członkowskich. Te ograniczenia powinny być jednak niezbędne i proporcjonalne, a przede wszystkim uzasadnione.

Uznając zasadność ograniczenia praw przysługujących podmiotowi danych, wydaje się, że niektóre wyłączenia w Projekcie dyrektywy idą jednak za daleko. Przykładowo, w art. 11 ust. 4 Projektu dyrektywy dotyczącym informacji o podmiocie danych określono przypadki, w których państwa członkowskie będą mogły opóźnić, ograniczyć lub uchylić udzielenie informacji podmiotowi danych, o ile takie częściowe lub całkowite ograniczenie będzie stanowiło konieczny i proporcjonalny środek w społeczeństwie demokratycznym i dla celów wymienionych w tym przepisie. Pomijając fakt, że cele te są opisane w sposób mało precyzyjny, zezwalający na bardzo szerokie uznanie państw (np. pkt c – „aby chronić bezpieczeństwo publiczne" albo pkt d – „aby chronić bezpieczeństwo narodowe"), to w art. 11 znalazł się jeszcze ust. 5, na mocy którego państwa członkowskie będą mogły ustalić kategorie przetwarzania danych, które będą mogły zostać objęte w całości lub w części tymi wyjątkami. To daje państwom członkowskim maksymalnie szeroki zakres uznania i może doprowadzić do sytuacji, w której w ogóle nie zostanie zrealizowane żadne prawo wynikające z przepisów dyrektywy, zwłaszcza gdy implementując przepisy dyrektywy, państwa uznają możliwość wyłączania określonych praw niejako „odgórnie", powielając jej przepis wprost. Ograniczenie praw jednostki powinno być wynikiem jednostkowej i konkretnej decyzji, podjętej w indywidualnym przypadku, po dokonaniu indywidualnej oceny i nie może prowadzić do wyłączania całych kategorii niejasnych sytuacji z praw przyznanych na mocy przepisów ogólnych.

Nie sposób nie wskazać kolejnych wątpliwości. Przykładowo w przeciwieństwie do Projektu rozporządzenia[80], który określa, że administrator ma obowiązek poinformowania podmiotu danych niezwłocznie i najpóźniej w ciągu miesiąca od dnia otrzymania wniosku o tym, czy zostaną podjęte działania dotyczące usunięcia lub poprawienia danych (z możliwością przedłużenia tego okresu o miesiąc), w Projekcie dyrektywy nie określa się limitu czasowego dla administratora do poinformowania osoby o sposobie reakcji na wniosek – mowa jest jedynie o „niezwłoczności". Standard ochrony jednostki ma zatem zostać obniżony w przypadku danych przetwarzanych na potrzeby określone w Pojekcie dyrektywy, chociaż nie ma ku temu żadnego uzasadnienia. Dalej, w art. 10 ust. 1 Projekt dyrektywy stanowi o obowiązku administratora do podjęcia „wszystkich rozsądnych kroków, aby dysponować przejrzystymi i łatwo dostępnymi politykami w zakresie przetwarzania danych osobowych

[80] Zob. art. 12 ust. 2 Projektu rozporządzenia oraz art. 10 ust. 4 Projektu dyrektywy.

i wykonywania praw przez podmioty danych"[81], a zatem nie określa precyzyjnie żadnych obowiązków administratora i wprowadza wyjątkowo niejasne pojęcie „rozsądnych" kroków, co w kontekście wyjątków od prawa do informacji (ograniczenia prawa do dostępu) określonych w art. 13 Projektu dyrektywy wydaje się już zbyt daleko idącym odstępstwem.

Z kolei w art. 10 ust. 5 Projektu dyrektywy określa się zasadę zwolnienia z opłat odpowiedzi na wniosek złożony przez podmiot danych, jednak wprowadza się wyjątek, a mianowicie „jeżeli wnioski są dokuczliwe[82], w szczególności ze względu na ich składanie w sposób uporczywy albo ze względu na zakres wniosku", wprowadzenie opłat będzie dopuszczalne. Jednocześnie nie wyjaśnia się w ogóle użytych terminów, a zatem ponownie pozostawia się bardzo szeroki zakres uznania państwom członkowskim. W przypadku Projektu rozporządzenia wprowadza się podobny przepis, chociaż z nieco innym terminem (wnioski wyraźnie przesadne)[83], jednak przewiduje się wydanie przez Komisję aktu delegowanego, w którym kryteria te zostaną doprecyzowane. Projekt dyrektywy pozostawia zatem wolną rękę państwom członkowskim, z których każde będzie mogło wdrożyć te postanowienia odmiennie.

Nie można być też pewnym, że ograniczenia wprowadzone w Projekcie dyrektywy w art. 15 (prawo do poprawienia) i w art. 16 (prawo do usunięcia) w porównaniu ze stosownymi przepisami Projektu rozporządzenia mają swoje uzasadnienie, zwłaszcza że takich przyczyn nie przedstawiono we wniosku Komisji. W szczególności, w określonych przypadkach administrator – zamiast usuwać dane – będzie uprawniony na mocy rozporządzenia do ograniczenia ich przetwarzania[84], natomiast Projekt dyrektywy stanowi o prawie administratora do oznaczenia danych[85]. Projekt dyrektywy nie przewiduje również w ogóle prawa do bycia zapomnianym[86]. Wreszcie Projekt dyrektywy nie określa prawa do sprzeciwienia się przetwarzaniu danych, chociaż można sobie wyobrazić wiele sytuacji, w których podmioty danych, takie jak chociażby ofiary przestępstwa czy świadkowie, powinny mieć możliwość oznaczenia danych tak, by ich przetwarzanie po zakończonym postępowaniu było ograniczone.

---

[81] W angielskiej wersji projektu: *Member States shall provide that the controller takes all reasonable steps to have transparent and easily accessible policies with regard to the processing of personal data and for the exercise of the data subjects' rights*.

[82] Ang. *vexatious*. W Projekcie rozporządzenia posłużono się innym pojęciem, a mianowicie wnioski „wyraźnie przesadne" – ang. *manifestly excessive*.

[83] Por. art. 12 ust. 5 Projektu rozporządzenia.

[84] Por. art. 17 ust. 4 Projektu rozporządzenia.

[85] Art. 16 ust. 3 Projektu dyrektywy.

[86] Sposób uregulowania prawa do bycia zapomnianym w Projekcie rozporządzenia też nasuwa wiele wątpliwości. Por. Opinię Grupy roboczej Art. 29, WP 191, s. 14.

3.7. Administrator danych

W rozdziale IV obu projektów zamieszczono przepisy dotyczące obowiązków administratora danych i podmiotu przetwarzającego. Oba akty – ze względu na swoją specyfikę – odmiennie definiują pojęcie administratora danych. Zgodnie z Projektem rozporządzenia „administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który samodzielnie lub wspólnie z innymi organami ustala cele, warunki i sposoby przetwarzania danych osobowych”[87], podczas gdy Projekt dyrektywy stanowi, że administratorem jest „właściwy organ publiczny, który samodzielnie lub wspólnie z innymi organami ustala cele, warunki i sposoby przetwarzania danych osobowych”[88]. Dalej jednak, w pierwszym przepisie określającym obowiązki administratora danych pojawia się różnica, która nie znajduje swojego uzasadnienia, a mianowicie zgodnie z Projektem rozporządzenia administrator nie tylko przyjmuje polityki i realizuje odpowiednie środki w celu zapewnienia, by przetwarzanie danych osobowych odbywało się zgodnie z rozporządzeniem, ale również w celu wykazania tej zgodności. W Projekcie dyrektywy zobowiązano jedynie państwa członkowskie, by przyjęły przepisy przewidujące, że administrator przyjmuje polityki i realizuje odpowiednie środki w celu zapewnienia, że przetwarzanie danych osobowych będzie odbywało się zgodnie z przepisami przyjętymi na mocy dyrektywy. Nie będzie już musiał wykazywać tej zgodności, co nie znajduje uzasadnienia i może spowodować brak jednolitości w zakresie obowiązków administratora i w efekcie jest kolejnym wyłomem w spójnym w swoim założeniu systemie ochrony danych[89].

Obydwa akty zawierają postanowienia dotyczące uwzględnienia ochrony danych już w fazie projektowania (*protection by design*) oraz jako opcji domyślnej (*by default*). O ile w przypadku Projektu rozporządzenia kryteria i wymogi dotyczące właściwych środków i mechanizmów, inne niż określone w projekcie, ustalać będzie Komisja Europejska, o tyle w przypadku dyrektywy pozostawiono to uznaniu państw członkowskich, co będzie oznaczać, że środki te będą się różnić w zależności od państwa oraz będą odmienne od tych ustanowionych na mocy rozporządzenia[90].

Projekt rozporządzenia w art. 33 ust. 1 stanowi, że jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swojego

[87] Por. art. 4 pkt 5 Projektu rozporządzenia.
[88] Por. art. 4 pkt 5 Projektu dyrektywy.
[89] Por. art. 22 ust. 1 Projektu rozporządzenia oraz art. 18 ust. 1 Projektu dyrektywy.
[90] Por. art. 19 Projektu dyrektywy oraz art. 23 Projektu rozporządzenia. Grupa robocza Art. 29 podkreśla w swojej opinii, że nie widzi przyczyn rozbieżności tych przepisów w obu projektach. Por. Opinia Grupy roboczej Art. 29, WP 191, s. 31.

charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie danych osobowych. W artykule 33 ust. 2 wymienia się operacje przetwarzania, które stwarzają szczególne ryzyko, takie jak np. przetwarzanie danych oparte na profilowaniu, albo przetwarzanie tzw. danych wrażliwych. W Projekcie dyrektywy nie znalazły się jednak przepisy dotyczące oceny skutków w zakresie ochrony danych, co zostało szczególnie podkreślone w opinii Grupy roboczej Art. 29, która wręcz wzywa do uzupełnienia tego braku[91]. Taka ocena jest szczególnie istotna właśnie w obszarze przetwarzania danych osobowych przez organy ścigania ze względu na zwiększone ryzyko dla osób fizycznych wynikające z tych działań.

Również obowiązki dotyczące dokumentacji w Projekcie dyrektywy zostały sformułowane mniej szczegółowo niż w Projekcie rozporządzenia[92]. W odniesieniu do bezpieczeństwa danych nie jest jasne, dlaczego w Projekcie dyrektywy – inaczej niż w Projekcie rozporządzenia – nie zobowiązano administratora lub podmiotu przetwarzającego do ochrony danych przez przypadkowym zniszczeniem lub przypadkową utratą danych[93].

3.8. Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

W rozdziale V obu projektów znalazły się przepisy dotyczące zasad przekazywania danych osobowych do państw trzecich lub do organizacji międzynarodowych. Wprowadzenie stosownych rozwiązań w Projekcie dyrektywy ma swoje uzasadnienie po pierwsze dlatego, że było to dotychczas przedmiotem Decyzji ramowej 2008/977/WSiSW i po drugie, efektywna wymiana danych między państwami jest szczególnie konieczna w sektorze walki z przestępczością, stąd też istotne jest szczegółowe uregulowanie zasad wymiany danych w dziedzinie współpracy organów wymiaru sprawiedliwości. Rozwój współpracy międzynarodowej wpływa na zakres wymiany danych, w tym na ilość wymienianych danych.

W przypadku Projektu rozporządzenia należy zwrócić uwagę, że zmienia się obecnie obowiązująca zasada: zakaz przekazywania danych do państw trzecich, które nie są uznane za wykazujące odpowiedni poziom ochrony, jest zastąpiony ogólną zasadą określoną w art. 40, zgodnie z którą przekazywanie danych osobowych może nastąpić tylko wtedy, gdy administrator lub podmiot danych spełnią warunki wymienione

[91] Zob. ibidem.
[92] Por. art. 23 Projektu dyrektywy i art. 28 Projektu rozporządzenia.
[93] Por. art. 27 Projektu dyrektywy oraz art. 30 ust. 2 Projektu rozporządzenia.

w rozdziale V Projektu rozporządzenia, czyli – zasadniczo – gdy Komisja stwierdzi, że państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni poziom ochrony[94]. Należy zaznaczyć, że nie jest zupełnie oczywiste, czy w przypadku, w którym Komisja przyjmie decyzję negatywną, transfer danych będzie zupełnie zakazany, czy też dopuszcza się go po spełnieniu określonych warunków[95]. W kolejnych przepisach Projektu rozporządzenia określa się dopuszczalne wyjątki, w tym wynikający z ochrony interesu publicznego, na mocy którego w braku decyzji stwierdzającej odpowiedni poziom ochrony przekazanie może nastąpić wyłącznie pod warunkiem, że jest niezbędne ze względu na istotny interes publiczny (art. 44 ust. 1 pkt d).

Projekt dyrektywy kwestie przekazywania danych do państw trzecich i do organizacji międzynarodowych reguluje odmiennie niż Projekt rozporządzenia. Przede wszystkim wskazuje wyraźnie na cel przekazania: w art. 33 Projektu dyrektywy wyrażono podstawową zasadę, zgodnie z którą przekazywanie do państw trzecich może mieć miejsce jedynie wtedy, gdy jest to „konieczne do zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania albo do wykonywania kar kryminalnych, oraz administrator i podmiot przetwarzający spełnią warunki ustanowione w niniejszym rozdziale". Jednocześnie w dalszych przepisach[96] wprowadza się bardzo szerokie odstępstwa od tej zasady, które mogą doprowadzić do systemowych nadużyć i omijania podstawowych zasad ochrony danych przy ich przekazywaniu do państw trzecich lub do organizacji międzynarodowych. W szczególności, zgodnie z art. 35 ust. a lit. b Projektu dyrektywy, dopuszczalne będzie przekazanie danych, jeżeli administrator lub podmiot przetwarzający ocenili wszystkie okoliczności towarzyszące przekazaniu danych osobowych i stwierdzają, że istnieją odpowiednie gwarancje w zakresie ochrony danych. Wszelkie odstępstwa tymczasem powinny być interpretowane zawężająco, tak by transfery dokonywane na ich podstawie nie stały się normą.

Różnice w podejściu do zasad przekazywania danych w obu projektach mogą być uzasadnione celem, dla jakiego dane są przekazywane, więc z założenia pewien stopień braku spójności jest akceptowalny. Nie jest jednak jasne, dlaczego zasady Projektu dyrektywy różnią się od zasad przyjętych w innych aktach dawnego III filaru UE[97], w tym w art. 33 pomija się wymóg, by administrator w państwie trzecim lub organizacji międzynarodowej był organem właściwym w rozumieniu dyrektywy[98].

---

[94] Projekt rozporządzenia określa również mechanizmy dotyczące przypadków, gdy taka decyzja Komisji nie została podjęta.

[95] Por. art. 41 ust. 6 Projektu rozporządzenia oraz motyw 82 preambuły.

[96] Por. art. 35 ust. 1 pkt b oraz art. 36 Projektu dyrektywy.

[97] Por. art. 17 ust. 1 Decyzji ramowej 2009/934/WSiSW czy art. 13 ust. 1 lit b Decyzji ramowej 2008/977/WSiSW.

[98] Wymóg ten pojawia się wyłącznie w motywie 45 preambuły do Projektu dyrektywy.

Projekt dyrektywy, podobnie jak Projekt rozporządzenia, przyznaje Komisji prawo do podejmowania decyzji stwierdzającej, że państwo trzecie lub organizacja międzynarodowa zapewniają odpowiedni poziom ochrony i w takim przypadku przekazywanie danych nie wymaga żadnego dalszego zezwolenia[99]. Określa również zasady postępowania w przypadku braku stosownej decyzji Komisji. W odróżnieniu jednak od Projektu rozporządzenia, Projekt dyrektywy nie przewiduje zasad postępowania administratora w sytuacji, gdy prawnie wiążący instrument nie określa odpowiednich gwarancji w zakresie ochrony danych. Odmiennie, w art. 35 ust. 1 lit. b stwierdza, że to wyłącznie administrator lub podmiot przetwarzający mają ocenić wszystkie okoliczności towarzyszące przekazaniu danych i stwierdzić, czy istnieją odpowiednie gwarancje w tym zakresie. Należy postulować, by przepisy dyrektywy zostały ujednolicone w tym zakresie z zasadami postępowania administratora lub podmiotu przetwarzającego określonymi w Projekcie rozporządzenia.

3.9. Organy nadzorcze

Kolejne rozdziały obu projektów dotyczą uprawnień i obowiązków niezależnych organów nadzorczych, zasad współpracy oraz środków ochrony prawnej, odpowiedzialności i sankcji. Trzeba zaznaczyć, że w przypadku Projektu dyrektywy ich wprowadzenie to duży krok naprzód w ochronie danych, ponieważ obecnie obowiązujące przepisy dawnego III filaru UE nie określają w ogóle obowiązków i uprawnień niezależnych organów nadzorczych. W szczególności należy podkreślić, że Projekt dyrektywy zawiera przepisy dotyczące nie tylko posiadania niezależnego organu nadzorczego, ale również specjalny rozdział dotyczący współpracy między organami ochrony danych.

Przepisy te w obu projektach nie są jednak spójne i nie podano żadnego uzasadnienia dla proponowanych rozbieżności. Można rozpocząć od wątpliwości zasadniczej i zwrócić uwagę na art. 39 ust. 2 Projektu dyrektywy, zgodnie z którym istnieje możliwość podjęcia decyzji przez państwo członkowskie, by organ ochrony danych odpowiedzialny za nadzorowanie rozporządzenia i dyrektywy był tym samym organem, co skutkowałoby spójnością w stosowaniu przepisów. Nie jest jasne, dlaczego w ogóle zakłada się możliwość powołania dwóch odrębnych organów ochrony danych.

Nie ma również uzasadnienia dla zróżnicowania uprawnień organów nadzorczych działających na podstawie przyszłego rozporządzenia i dyrektywy. W szczególności uzasadnione wydaje się zróżnicowanie wyłącznie w odniesieniu do nadzorowania organów sądowych, lecz w przypadku policji potrzebny jest wręcz pogłębiony nadzór

[99] Por. art. 34 Projektu dyrektywy.

nad działaniami. W odniesieniu do organów sądowych w art. 44 ust. 2 Projektu dyrektywy oraz w art. 51 ust. 3 Projektu rozporządzenia przewidziano uprawnienie do wyłączenia kompetencji organu nadzorczego w odniesieniu do nadzorowania operacji przetwarzania dokonywanych przez sądy w toku wykonywania przez nie funkcji sądowych[100], chociaż sądy co do zasady nie są zwolnione z ochrony danych osobowych. Termin „funkcje sądowe" nie jest jednak wystarczająco precyzyjny – obejmuje zapewne przetwarzanie danych w toku konkretnego indywidualnego postępowania sądowego, ale nie jest określone precyzyjnie, czy obejmuje również prowadzenie rozmaitych rejestrów czy publikacji orzeczeń. Wydaje się, że w takich przypadkach działanie sądów również powinno zostać objęte kompetencjami organu nadzorczego.

O ile takie wyłączenie, przewidziane zarówno w Projekcie rozporządzenia, jak i Projekcie dyrektywy, może być uzasadnione, to jednak pojawiają się kolejne problemy. W szczególności kompetencje organu ochrony danych w Projekcie dyrektywy nie są opisane w sposób wystarczająco szczegółowy. Nie są również zbieżne z kompetencjami tego organu określonymi w Projekcie rozporządzenia[101]. Przykładowo Projekt dyrektywy nie zawiera żadnych przepisów dotyczących uprawnienia organu nadzorczego w odniesieniu do dostępu do pomieszczeń, tak jak zostało to określone w Projekcie rozporządzenia[102]. Trzeba tymczasem podkreślić, że organy ochrony danych powinny mieć na terenie UE podobne uprawnienia, tak by ochrona praw obywateli była stosownie gwarantowania w sposób jednolity i spójny.

Projekt dyrektywy z nieznanych przyczyn odmiennie podchodzi również do kwestii udostępniania sprawozdania z działalności organów nadzorczych, przewidując jedynie obowiązek udostępnienia go Komisji i Europejskiej Radzie Ochrony Danych. Projekt rozporządzenia zakłada ponadto udostępnienie sprawozdania parlamentowi narodowemu.

Projekt rozporządzenia określa zasady wzajemnej pomocy organów nadzorczych, polegającej na przekazywaniu odpowiednich informacji oraz zasady realizacji określonych wniosków, takich jak wnioski o udzielanie zezwoleń i konsultacji czy wnioski o inspekcje. Przewiduje również wspólne operacje organów nadzorczych (art. 56). Odpowiednie przepisy Projektu dyrektywy są mniej precyzyjne, co może być uzasadnione obszarem działania i brakiem możliwości dokonywania działań przez jeden organ nadzorczy w obszarze należącym do kompetencji krajowych drugiego organu nadzorczego. Nie wszystkie jednak propozycje zawarte w Projekcie rozporządzenia

[100] Ang. *judicial capacity*.

[101] Por. art. 53 Projektu rozporządzenia oraz art. 46 Projektu dyrektywy.

[102] Również Grupa robocza Art. 29 wskazuje na brak uzasadnienia dla takiego zróżnicowania, WP 191, s. 34.

nie mogłyby mieć zastosowania, jak chociażby te zawarte w art. 55 ust. 2–7, które określają szybką i efektywną współpracę organów.

Pozytywnie należy ocenić kwestie instytucjonalne, takie jak stworzenie Europejskiej Rady Ochrony Danych, chociaż trzeba zaznaczyć, że z racji wyboru instrumentu, jakim jest dyrektywa, nie jest jasne, jak przepisy Projektu dyrektywy dotyczące kompetencji Europejskiej Rady Ochrony Danych miałyby być wdrożone do prawa krajowego. Jest to jednak problem systemowy, wymagający odrębnej analizy.

Wnioski

Podsumowując powyższe rozważania i podane przykłady uregulowania tych samych kwestii w obu projektach, można dojść do wstępnej konkluzji, że przygotowywany projekt reformy na pewno nie doprowadzi do osiągnięcia spójności i jednolitości systemu ochrony danych osobowych w UE. Ostateczność tej tezy uzależniona będzie oczywiście od finału prac nad obydwoma projektami w instytucjach UE, tym niemniej – na obecnym etapie – wniosek ten jest uzasadniony przez kilka argumentów.

Traktat o funkcjonowaniu Unii Europejskiej i Traktat o Unii Europejskiej określają podstawę prawną do przyjęcia aktów regulujących zasady ochrony danych osobowych w Unii Europejskiej. Już te przepisy (art. 16 TfUE i art. 39 TUE oraz dołączone do Aktu końcowego deklaracje) sugerują, że przyjęte akty prawne będą zawierały odmienne rozwiązania, uwzględniające specyfikę danej dziedziny. Będą miały także różne konsekwencje prawne, jak chociażby w zakresie skutków niewykonania zobowiązania polegającego na wdrożeniu aktu do prawa krajowego przez państwo członkowskie.

Wielość obecnie obowiązujących aktów prawnych UE oznacza, że system ochrony danych osobowych nie może mieć charakteru jednolitego i na pewno nie jest spójny. Stosowane są bowiem rozmaite przepisy w zależności od tego, z jaką dziedziną mamy do czynienia. Propozycja przyjęcia dwóch aktów, które zastąpią wyłącznie Dyrektywę 95/46/WE oraz Decyzję ramową 2008/977/WSiSW, a zatem wyłącznie dwa akty ogólne, nie przyczyni się do poprawy spójności od strony systemowej.

Ze szczegółowej analizy przedstawionych przez Komisję projektów rozporządzenia i dyrektywy wyłania się pewien dysonans, jeśli chodzi o cel obu regulacji – chociaż obydwa akty mają chronić prawa jednostki, to jednak w przypadku dyrektywy podstawowym celem jest zagwarantowanie stosownych uprawnień właściwym organom, nawet kosztem poświęcenia praw jednostki. W przypadku dyrektywy standard

ochrony danych osobowych będzie zatem niższy niż w systemie ogólnym z racji konieczności zagwarantowania bezpieczeństwa i porządku publicznego. Wyważenia jedynie wymaga to, na ile ten standard może być obniżony – tzn. jak daleko posunięta ingerencja organów wymiaru sprawiedliwości i organów ścigania może uzasadniać ograniczenie prawa do ochrony danych osobowych. O ile przyjęcie dwóch aktów jest zrozumiałe, o tyle przyjęcie dwóch aktów o różnych skutkach (rozporządzenie *versus* dyrektywa) może już nasuwać wątpliwości w kontekście zobowiązań nałożonych na państwa. W przypadku dyrektywy niewątpliwie zaistnieje szereg różnic w sposobie jej wdrożenia w poszczególnych państwach, a zatem na pewno nie będzie mowy o jednolitych i spójnych ramach prawnych dla całego systemu ochrony danych osobowych w UE.

Projekty rozporządzenia i dyrektywy nie przewidują ani uchylenia, ani nawet ustanowienia hierarchii innych aktów prawnych, regulujących przetwarzanie danych osobowych. Wręcz przeciwnie – pozostawiają bez uszczerbku wcześniej przyjęte akty prawne, a zatem zamiast ujednolicać system – w systemie prawnym UE obowiązywać będzie nadal wiele aktów prawnych regulujących kwestie ochrony danych osobowych. To zdecydowanie stoi w sprzeczności z postulatem stworzenia jednolitych ram prawnych.

Postulat jednolitych i spójnych ram prawnych nie jest również spełniony w odniesieniu do zakresu materialnego obu projektów – co wynika z przedstawionych w opracowaniu przykładów. Wskazano szereg problemów, które zostały uregulowane w Projekcie dyrektywy i Projekcie rozporządzenia w sposób odmienny, bez żadnego uzasadnienia. Jest też wiele przypadków, w których uzasadnienie dla wprowadzonych różnic istnieje. Pozostawiono także szereg przepisów, których precyzja budzi wątpliwości i które pozostawiają ogromny margines uznania państwom członkowskim, tym samym nie przyczyniając się do realizacji postulatu spójności projektowanego systemu. Są to bardzo poważne sygnały wskazujące na niepełność regulacji i możliwość wprowadzenia pewnych wyłomów w jednolitym systemie współpracy, co już oznacza, że podstawowe założenie reformy może nie zostać spełnione.

Draft of the personal data protection reform: will the EU create a uniform and consistent system?

In January 2014 two years passed since the European Commission presented a package of reforms of the system of personal data protection in the EU. Commission proposed to create, in its opinion, a uniform and consistent system across

the EU. The idea of the paper is to answer the question whether the Commission's proposal to adopt two separate acts (one as a general system, and the second for cooperation in criminal matters and police), should meet the proposed assumptions. In order to analyze that, first the treaty background is presented, then current legal status in the field of personal data in the EU, and finally a comparative analysis of the solutions of the two drafts. The analysis leads to the conclusion that there are serious concerns about the lack of consistency.

Keywords: personal data protection, justice system, police cooperation, judicial cooperation in criminal matters, data protection reform

Le projet de réforme de la protection des données personnelles: l'UE va créer un système uniforme et cohérente?

En janvier 2014 deux années ont écoulées depuis quand la Commission européenne avait présenté un ensemble de réformes du système de protection des données personnelles dans l'UE. La Commission a proposé de créer un système uniforme et cohérente dans toute l'UE. L'idée de cet article est d'analyser si la proposition de la Commission d'adopter deux actes distincts répondra aux objectifs proposés. Dans l'article, tout d'abord l'arrière-plan du Traité est présenté, puis le statut juridique actuel dans le domaine des données personnelles dans l'UE est discuté, enfin une analyse comparative des deux propositions législatives est incluse. L'analyse mène à la conclusion qu'il y a de graves préoccupations concernant le manque de cohérence.

Mots-clés: la protection des données personnelles, le système de justice, la coopération policière, la coopération judiciaire en matière pénale, la réforme de la protection des données personnelles

Проект реформы системы защиты персональных данных: создаст ли ЕС однородную и целостную систему?

В январе 2014 г. прошло два года, как Европейская комиссия представила пакет реформ системы защиты персональных данных в ЕС. Комиссия предложила создать, по ее мнению, однородную и целостную систему на всей территории ЕС. Суть статьи – дать ответ на предстоящий вопрос: позволит

ли замысел Комиссии принять два отдельных акта (один как общую систему, а второй по судебному сотрудничеству по уголовным делам и по полицейскому сотрудничеству) достичь поставленных целей? В исследовании представлены правовые основы защиты персональных данных, затем – правовая система в сфере персональных данных в ЕС и, наконец, сравнительный анализ двух проектов. Анализ приводит к выводу, что есть серьезные опасения по поводу целостности системы.

Ключевые слова: защита персональных данных, система правосудия, полицейские сотрудничество, судебное сотрудничество по уголовным делам, реформа законодательства в сфере защиты персональных данных