Opinia 5/2023 w sprawie projektu decyzji wykonawczej Komisji Europejskiej stwierdzającej odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA

Przyjęta 28 lutego 2023 r.

Streszczenie

13 grudnia 2022 r. Komisja Europejska opublikowała projekt decyzji stwierdzającej odpowiedni stopień ochrony („projekt decyzji"), który zawiera załączniki stanowiące nowe ramy transatlantyckiej wymiany danych osobowych – ramy ochrony danych UE–USA („DPF"), które mają zastąpić wcześniejszą Tarczę Prywatności UE–USA unieważnioną przez Trybunał Sprawiedliwości Unii Europejskiej („TSUE") w wyroku z dnia 16 lipca 2020 r. w sprawie Schrems II. Kluczowym elementem DPF są zasady ram ochrony danych UE–USA, w tym zasady uzupełniające (zwane dalej łącznie „zasadami DPF").

Zgodnie z art. 70 ust. 1 lit. s) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] („RODO") Komisja zwróciła się do Europejskiej Rady Ochrony Danych („EROD") o opinię w sprawie projektu decyzji.

Na podstawie analizy projektu decyzji EROD oceniła, czy stopień ochrony danych zapewniany w USA jest odpowiedni. Przeprowadziła ocenę zarówno aspektów handlowych, jak i dostępu do danych osobowych przekazywanych z UE przez organy publiczne w USA oraz ich wykorzystywania.

EROD wzięła pod uwagę mające zastosowanie unijne ramy prawne ochrony danych określone w RODO, a także prawa podstawowe – prawo do życia prywatnego i prawo do ochrony danych zapisane w art. 7 i 8 Karty praw podstawowych Unii Europejskiej oraz w art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności. Rozważyła również prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu określone w art. 47 Karty, a także orzecznictwo dotyczące tych poszczególnych praw podstawowych.

Ponadto EROD wzięła pod uwagę wymogi określone w przyjętym przez nią dokumencie w sprawie odpowiedniego stopnia ochrony[2].

Podstawowym celem EROD jest przedstawienie Komisji opinii na temat odpowiedniego stopnia ochrony danych zapewnianego osobom fizycznym, których dane osobowe są przekazywane do USA. Należy zauważyć, że EROD nie oczekuje, aby ramy ochrony danych USA powielały europejskie przepisy o ochronie danych.

EROD przypomina jednak, że w art. 45 RODO oraz w orzecznictwie TSUE wymaga się, aby prawodawstwo państwa trzeciego zapewniało osobom, których dane dotyczą, stopień ochrony zasadniczo odpowiadający stopniowi ochrony gwarantowanemu w UE, aby można je było uznać za zapewniające odpowiedni stopień ochrony.

1.1. Ogólne aspekty ochrony danych

DPF stanowią, że w niektórych przypadkach przestrzeganie zasad DPF przez podmioty objęte DPF może być ograniczone (np. w zakresie niezbędnym do wykonania orzeczenia sądowego lub do realizacji celów interesu publicznego). Aby lepiej określić wpływ tych wyłączeń na stopień ochrony osób, których

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

[2] Grupa Robocza Art. 29, dokument pt. „Odpowiedni stopień ochrony przekazywanych danych osobowych", WP254 rev.01, 28 listopada 2017 r., ostatnio zmieniony i przyjęty 6 lutego 2018 r., zatwierdzony przez EROD 25 maja 2018 r. (zwany dalej „dokumentem w sprawie odpowiedniego stopnia ochrony").

dane dotyczą, EROD zaleca, aby Komisja uwzględniła w projekcie decyzji doprecyzowanie zakresu wyłączeń, w tym mających zastosowanie zabezpieczeń na podstawie prawa USA.

EROD zauważa, że struktura załączników i ich numeracja utrudniają znalezienie informacji i odniesienie do nich. Przyczynia się to do ogólnej niejasnej prezentacji nowych ram, które zawierają w załącznikach dokumenty o różnej wartości prawnej, i może nie sprzyjać właściwemu zrozumieniu zasad DPF przez osoby, których dane dotyczą, podmioty objęte DPF i unijne organy ochrony danych. EROD podkreśla również, że w całych DPF należy spójnie stosować odpowiednią terminologię. W tym względzie też brakuje definicji niektórych istotnych terminów[3].

EROD z zadowoleniem przyjmuje aktualizacje zasad DPF[4], które będą stanowiły wiążące ramy prawne dla podmiotów objętych DPF, ale zauważa, że mimo szeregu zmian i dodatkowych wyjaśnień wprowadzonych w motywach projektu decyzji zasady DPF, których muszą przestrzegać podmioty objęte DPF, pozostają zasadniczo niezmienione w porównaniu z zasadami, które miały zastosowanie w ramach Tarczy Prywatności (której dotyczyły coroczne wspólne przeglądy Grupy Roboczej Art. 29 i EROD). Zasady DPF są również w dużej mierze takie same jak zasady zawarte w projekcie Tarczy Prywatności, na którym Grupa Robocza Art. 29 oparła swoją opinię z 2016 r.[5] W odniesieniu do tych zasad DPF, które pozostają zasadniczo niezmienione, EROD nie uważa za konieczne powtarzania wszystkich uwag zgłoszonych wcześniej przez Grupę Roboczą Art. 29. EROD postanowiła skupić się na konkretnych aspektach, które uważa obecnie za jeszcze bardziej istotne z uwagi na zmiany, jakie zaszły w otoczeniu prawnym i technologicznym.

EROD zauważa na przykład, że niektóre budzące obawy kwestie poruszone wcześniej przez Grupę Roboczą Art. 29 i EROD w odniesieniu do zasad Tarczy Prywatności pozostają aktualne. Dotyczą one w szczególności praw osób, których dane dotyczą (np. niektórych wyjątków od prawa dostępu oraz terminów i trybów wykonywania prawa do sprzeciwu), braku kluczowych definicji, braku jasności co do stosowania zasad DPF w odniesieniu do podmiotów przetwarzających oraz szerokiego wyłączenia dotyczącego publicznie dostępnych informacji[6].

EROD pragnie także przypomnieć, że stopień ochrony osób fizycznych, których dane są przekazywane, nie może być naruszony przez dalsze przekazywanie danych przez pierwotnego odbiorcę przekazanych danych[7]. EROD ponownie zwraca się do Komisji o doprecyzowanie, że zabezpieczenia nałożone przez pierwotnego odbiorcę na podmiot odbierający dane w państwie trzecim muszą być skuteczne w świetle przepisów państwa trzeciego przed dalszym przekazaniem w kontekście DPF.

Szczególną uwagę należy zwrócić na szybkie zmiany w dziedzinie zautomatyzowanego podejmowania decyzji i profilowania – w coraz większym stopniu za pomocą technologii sztucznej inteligencji. EROD z zadowoleniem przyjmuje odniesienia Komisji do szczególnych zabezpieczeń przewidzianych w odpowiednich przepisach prawa USA w różnych dziedzinach[8]. Wydaje się jednak, że stopień ochrony osób fizycznych różni się w zależności od tego, które przepisy sektorowe – o ile takie istnieją – mają

[3] Chodzi o terminy „przedstawiciel" i „podmiot przetwarzający". Ponadto pojęcie „danych dotyczących zasobów ludzkich" nadal wymaga omówienia z władzami USA.
[4] Na przykład doprecyzowanie, że dane kodowane za pomocą klucza stanowią dane osobowe.
[5] Grupa Robocza Art. 29, Opinia 01/2016 w sprawie projektu decyzji stwierdzającej odpowiedni stopień ochrony w ramach Tarczy Prywatności UE–USA, przyjęta w dniu 13 kwietnia 2016 r. (zwana dalej „opinią Grupy Roboczej Art. 29 nr 01/2016").
[6] Tarcza Prywatności UE–USA – trzeci roczny wspólny przegląd, sprawozdanie EROD przyjęte w dniu 12 listopada 2019 r., pkt 11.
[7] Rozdział 3 część A pkt 9 dokumentu w sprawie odpowiedniego stopnia ochrony na podstawie RODO.
[8] Motyw 35 projektu decyzji.

zastosowanie do danej sytuacji. EROD utrzymuje, że niezbędne są przepisy szczegółowe dotyczące zautomatyzowanego podejmowania decyzji, które zapewnią odpowiednie zabezpieczenia, w tym prawo osoby fizycznej do poznania logiki, zakwestionowania decyzji i uzyskania interwencji ludzkiej, w przypadku gdy dana decyzja ma na tę osobę istotny wpływ.

EROD przypomina o znaczeniu skutecznego nadzoru i egzekwowania DPF i uważa, że niezwykle ważne są kontrole zgodności w odniesieniu do bardziej zasadniczych wymogów. Kwestie te będą ściśle monitorowane przez EROD, w tym w kontekście okresowych przeglądów. EROD przyjmuje do wiadomości odnowione zobowiązania zawarte w pismach Federalnej Komisji Handlu a („FTC")[9] i Departamentu Transportu („DoT")[10] w odniesieniu do egzekwowania przepisów, np. dotyczące priorytetowego traktowania postępowania w sprawie domniemanych naruszeń DPF.

EROD zauważa, że osobom z UE, których dane dotyczą, zapewniono siedem środków dochodzenia roszczeń, w przypadku gdy ich dane osobowe są przetwarzane z naruszeniem DPF. Te mechanizmy dochodzenia roszczeń są takie same jak te zawarte w unieważnionej Tarczy Prywatności, co do których Grupa Robocza Art. 29 przedstawiła swoje uwagi[11]. EROD będzie ściśle monitorować skuteczność tych mechanizmów dochodzenia roszczeń, w tym w kontekście okresowych przeglądów.

1.2. Dostęp do danych osobowych przekazywanych z Unii Europejskiej i ich wykorzystywanie przez organy publiczne w USA

W projekcie decyzji Komisja Europejska stwierdza, że „wszelkie ingerencje w interesie publicznym, w szczególności do celów ścigania przestępstw i do celów związanych z bezpieczeństwem narodowym, ze strony amerykańskich organów publicznych w prawa podstawowe osób fizycznych, których dane osobowe są przekazywane z Unii do Stanów Zjednoczonych na podstawie ram ochrony danych UE–USA, będą ograniczone do tego, co jest bezwzględnie niezbędne do osiągnięcia określonego prawnie uzasadnionego celu, oraz że istnieje skuteczna ochrona prawna przed taką ingerencją"[12].

Komisja Europejska doszła do takiego wniosku po przeprowadzeniu szeroko zakrojonej oceny rozporządzenia wykonawczego 14086 zwiększającego zabezpieczenia w kontekście działań USA w obszarze rozpoznania radioelektronicznego („rozporządzenie wykonawcze 14086"). Rozporządzenie wykonawcze 14086 zostało opublikowane przez Prezydenta Stanów Zjednoczonych w dniu 7 października 2022 r. w następstwie negocjacji przeprowadzonych przez Komisję Europejską z rządem Stanów Zjednoczonych w związku z unieważnieniem przez TSUE wcześniejszej decyzji stwierdzającej odpowiedni stopień ochrony zwanej Tarczą Prywatności.

EROD z zadowoleniem przyjęłaby uzależnienie nie tylko wejścia w życie, ale również przyjęcia decyzji od m.in. przyjęcia przez wszystkie amerykańskie agencje wywiadowcze zaktualizowanych strategii politycznych i procedur wdrażania rozporządzenia wykonawczego 14086. EROD zaleca Komisji przeprowadzenie oceny tych zaktualizowanych strategii politycznych i procedur oraz przekazanie tej oceny EROD.

Jeżeli chodzi o dostęp organów rządowych do danych osobowych przekazywanych do USA, EROD skoncentrowała swoją analizę na ocenie nowego rozporządzenia wykonawczego 14086, ponieważ ma ono skutecznie zaradzić niedociągnięciom stwierdzonym przez TSUE w wyroku w sprawie Schrems II, w którym Trybunał uznał poprzednią decyzję stwierdzającą odpowiedni stopień ochrony za nieważną.

[9] Załącznik IV do projektu decyzji.
[10] Załącznik V do projektu decyzji.
[11] Zob. w szczególności sekcja 2.2.6 lit. a) opinii Grupy Roboczej Art. 29 nr 01/2016.
[12] Motyw 195 projektu decyzji.

EROD uznaje, że amerykańskie ramy prawne dotyczące działań w obszarze rozpoznania radioelektronicznego zostały zmienione przez przyjęcie rozporządzenia wykonawczego 14086, a wprowadzenie w tym rozporządzeniu dodatkowych zabezpieczeń uważa za znaczną poprawę. Rozporządzeniem wykonawczym 14086 wprowadzono do amerykańskich ram prawnych dotyczących rozpoznania radioelektronicznego pojęcie konieczności i proporcjonalności, a w przypadku, gdy UE zostanie wskazana jako kwalifikująca się regionalna organizacja integracji gospodarczej, przewidziano nowy mechanizm dochodzenia roszczeń dla osób fizycznych z UE. EROD uważa, że nowy mechanizm dochodzenia roszczeń został znacznie ulepszony w porównaniu z poprzednim mechanizmem ochrony prawnej przez Rzecznika ds. Tarczy Prywatności. W przeciwieństwie do poprzednich ram prawnych, w których nie utworzono praw dla osób fizycznych z UE, jak wyraźnie zauważył TSUE, nowe rozporządzenie wykonawcze 14086 tworzy takie uprawnienia i zapewnia więcej zabezpieczeń niezależności Sądu Odwoławczego ds. Ochrony Danych oraz skuteczniejsze uprawnienia do usuwania naruszeń.

Po porównaniu dodatkowych zabezpieczeń zawartych w rozporządzeniu wykonawczym 14086 z tym, co EROD nazwała niezbędnymi gwarancjami europejskimi, stanowiącymi normę opracowaną na podstawie orzecznictwa TSUE i Europejskiego Trybunału Praw Człowieka (ETPC), EROD wskazała w swojej ocenie szereg elementów, które w dalszym ciągu wymagają dodatkowego doprecyzowania, którym należy poświęcić więcej uwagi lub które budzą obawy. Wynika to z faktu, że EROD oparła swoją opinię na wyroku w sprawie Schrems II, jednak zakres oceny EROD musi obejmować kwestie, które wykraczają poza konkretne ustalenia zawarte w wyroku w sprawie Schrems II.

EROD dostrzega potrzebę dalszego doprecyzowania kwestii dotyczących w szczególności „tymczasowego hurtowego gromadzenia" oraz dalszego zatrzymywania i rozpowszechniania (hurtowo) zgromadzonych danych w amerykańskich ramach prawnych.

Ponieważ analiza zasadniczej odpowiedniości nie polega na stwierdzeniu identyczności, a zabezpieczenia zawarte w nowych ramach prawnych dotyczących rozpoznania radioelektronicznego zostały wzmocnione, główną kwestią, która zwraca uwagę EROD i budzi obawy, jest ocena wszystkich zabezpieczeń, w ujęciu całościowym, obejmująca zabezpieczenia dla całego cyklu przetwarzania, od gromadzenia danych po ich rozpowszechnianie, z uwzględnieniem elementów nadzoru i środków dochodzenia roszczeń.

W tym względzie EROD podkreśla następujące ustalenia:

Choć EROD uznaje, że rozporządzenie wykonawcze 14086 wprowadza pojęcia konieczności i proporcjonalności do ram prawnych dotyczących rozpoznania radioelektronicznego, podkreśla potrzebę ścisłego monitorowania skutków tych zmian w praktyce, w tym przeprowadzenia przeglądu wewnętrznych strategii politycznych i procedur wdrażających zabezpieczenia przewidziane w rozporządzeniu wykonawczym na poziomie agencji.

EROD z zadowoleniem przyjmuje również fakt, że rozporządzenie wykonawcze 14086 zawiera wykaz konkretnych celów, w których gromadzenie danych może i nie może mieć miejsca, a jednocześnie odnotowuje możliwość aktualizacji tych celów i ich uzupełnienia o dodatkowe – niekoniecznie publiczne – cele w świetle nowych nadrzędnych względów bezpieczeństwa narodowego.

EROD stwierdziła w szczególności, że niedociągnięciem w obecnych ramach jest fakt, iż amerykańskie ramy prawne, które dopuszczają gromadzenie danych masowych na podstawie rozporządzenia wykonawczego 12333, nie zawierają wymogu uzyskania uprzedniego zezwolenia niezależnego organu, co jest wymagane w najnowszym orzecznictwie ETPC, ani nie przewidują systematycznej niezależnej kontroli *ex post* przeprowadzanej przez sąd lub równoważny niezależny organ. W odniesieniu do

uprzedniego niezależnego zezwolenia na nadzór na podstawie art. 702 ustawy o kontroli wywiadu EROD wyraża ubolewanie, że Sąd ds. Kontroli Wywiadu („FISC") nie dokonuje przeglądu wniosku dotyczącego programu pod kątem zgodności z rozporządzeniem wykonawczym 14086 przy certyfikacji programu i udzielaniu zezwolenia na ukierunkowanie działań na osoby niebędące obywatelami ani rezydentami USA, mimo że organy wywiadowcze realizujące program są tym rozporządzeniem związane. Zdaniem EROD dodatkowe zabezpieczenia zawarte w tym rozporządzeniu powinny jednak zostać uwzględnione, w tym przez FISC. EROD przypomina, że szczególnie przydatne do oceny sposobu wdrożenia zabezpieczeń zawartych w rozporządzeniu wykonawczym 14086 oraz sposobu stosowania tych zabezpieczeń w przypadku gromadzenia danych na podstawie art. 702 ustawy o kontroli wywiadu i rozporządzenia wykonawczego 12333 byłyby sprawozdania Rady Nadzoru nad Ochroną Prywatności i Wolnościami Obywatelskimi („PCLOB").

Jeżeli chodzi o mechanizm dochodzenia roszczeń, EROD dostrzega znaczne usprawnienia w zakresie uprawnień Sądu Odwoławczego ds. Ochrony Danych („DPRC") i jego większej niezależności w porównaniu z Rzecznikiem ds. Tarczy Prywatności. EROD uznaje również dodatkowe zabezpieczenia przewidziane w nowym mechanizmie dochodzenia roszczeń, takie jak funkcja specjalnych rzeczników, która obejmuje opowiadanie się w interesie skarżącego, a także przegląd mechanizmu dochodzenia roszczeń przez PCLOB. Biorąc pod uwagę charakter względów bezpieczeństwa narodowego i zabezpieczenia przewidziane w rozporządzeniu wykonawczym 14086, EROD jest jednak zaniepokojona ogólnym stosowaniem standardowej odpowiedzi DPRC, w której sąd ten powiadamia skarżącego, że albo nie stwierdzono żadnych naruszeń objętych zakresem, albo wydano decyzję wymagającą odpowiednich środków zaradczych, a także brakiem możliwości odwołania się od takich decyzji. Zważywszy na duże znaczenie mechanizmu dochodzenia roszczeń, EROD wzywa Komisję do ścisłego monitorowania funkcjonowania tego mechanizmu w praktyce.

EROD oczekuje, że Komisja podejmie działania następcze w związku ze swoim zobowiązaniem do zawieszenia, uchylenia lub zmiany decyzji stwierdzającej odpowiedni stopień ochrony ze względu na pilny charakter sprawy, w szczególności jeżeli organ wykonawczy USA podjąłby decyzję o ograniczeniu zabezpieczeń zawartych w rozporządzeniu wykonawczym[13].

Ogólnie rzecz biorąc, EROD z zadowoleniem odnotowuje znaczną poprawę, jaką oferuje rozporządzenie wykonawcze w porównaniu z poprzednimi ramami prawnymi, w szczególności w odniesieniu do wprowadzenia zasad konieczności i proporcjonalności oraz indywidualnego mechanizmu dochodzenia roszczeń dla osób z UE, których dane dotyczą. Biorąc pod uwagę wyrażone obawy i wymagane doprecyzowania, EROD zwraca uwagę, że należy rozwiązać kwestie budzące obawy, oraz proponuje, aby Komisja przedstawiła wymagane doprecyzowania w celu wzmocnienia podstaw projektu decyzji i zapewnienia ścisłego monitorowania rzeczywistego wdrażania tych nowych ram prawnych, a w szczególności przewidzianych w nich zabezpieczeń, w przyszłych wspólnych przeglądach.

[13] Motyw 212 projektu decyzji.

Spis treści

Europejska Rada Ochrony Danych

Europejska Rada Ochrony Danych (EROD) przyjęła następujące oświadczenie:

Uwzględniając art. 70 ust. 1 lit. s) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO")[1],

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[2],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NASTĘPUJĄCĄ OPINIĘ:

1 WPROWADZENIE

1.1 Ramy ochrony danych Stanów Zjednoczonych

1. Stany Zjednoczone („USA") i Unia Europejska („UE") stosują różne podejścia do prywatności i ochrony danych. Podczas gdy w UE prywatność i ochrona danych są prawami podstawowymi zagwarantowanymi w art. 7 i 8 Karty praw podstawowych Unii Europejskiej, w USA ochrona danych jest kwestią zasadniczo podnoszoną z punktu widzenia ochrony konsumentów. W rezultacie podejścia regulacyjne w USA i UE różnią się od siebie[3].

2. W przeciwieństwie do unijnego kompleksowego podejścia przyjętego w RODO, w USA na szczeblu federalnym nie istnieje kompleksowa ogólna ustawa o ochronie danych. Ochrona prywatności w Stanach Zjednoczonych jest raczej realizowana w ramach podejścia sektorowego i stanowego. Przykładowo niektóre konkretne sektory objęte są konkretnymi aktami prawnymi, takimi jak:

   - ustawa o możliwości przenoszenia ubezpieczenia zdrowotnego i odpowiedzialności w zakresie ubezpieczenia zdrowotnego (HIPAA)[4]

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz.U. L 119 z 4.5.2016, s. 1.

[2] Odniesienia do „państw członkowskich" zawarte w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG".

[3] Zob. również sekcja I załącznika I do projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 stwierdzającej odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA, opublikowanego w dniu 13 grudnia 2022 r. (zwanego dalej „projektem decyzji").

[4] Ustawa o możliwości przenoszenia ubezpieczenia zdrowotnego i odpowiedzialności w zakresie ubezpieczenia zdrowotnego (HIPAA) z 1996 r. jest aktem amerykańskiego prawa federalnego. Tworzy ona normy krajowe służące ochronie szczególnie chronionych informacji dotyczących zdrowia pacjentów. Celem HIPAA jest

- ustawa o ochronie prywatności dzieci w internecie (COPPA)[5]
- ustawa Gramma-Leacha-Blileya (GLBA)[6].

3. W obszarze dostępu organów rządowych do danych osobowych przekazywanych z UE do USA zastosowanie ma szereg różnych podstaw, ograniczeń i zabezpieczeń prawnych. Pisma sądowe na potrzeby dostępu do informacji do celów egzekwowania prawa wynikają bezpośrednio z konstytucji Stanów Zjednoczonych (czwartej poprawki), z prawa stanowionego i procesowego albo z wytycznych i strategii politycznych Departamentu Sprawiedliwości na szczeblu federalnym lub na szczeblu stanowym. Dostęp do informacji do celów związanych z bezpieczeństwem narodowym jest regulowany szeregiem instrumentów prawnych, a w szczególności ustawą o kontroli wywiadu (FISA), rozporządzeniem wykonawczym 12333, niedawno przyjętym rozporządzeniem wykonawczym 14086 oraz zarządzeniem prokuratora generalnego[7] ustanawiającym Sąd Odwoławczy ds. Ochrony Danych („DPRC").

4. 13 grudnia 2022 r. Komisja opublikowała projekt decyzji wykonawczej na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 stwierdzającej odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA („projekt decyzji"), zawierający sześć załączników, w których przedstawiono ramy ochrony danych UE–USA („DPF"). Z powodów wyjaśnionych powyżej projekt decyzji nie opiera się na szczegółowych i kompleksowych federalnych ramach prawnych, lecz właśnie na DPF.

5. DPF funkcjonują w następujący sposób: *„Departament Handlu Stanów Zjednoczonych („DoC") wydaje zasady ram ochrony danych UE–USA, w tym zasady uzupełniające (zwane łącznie „zasadami") oraz załącznik I do zasad („załącznik I"), zgodnie ze swoim uprawnieniem na mocy prawa stanowionego do*

odpowiednia ochrona informacji dotyczących zdrowia osób fizycznych, a jednocześnie umożliwienie przepływu takich informacji w celu świadczenia i propagowania wysokiej jakości usług opieki zdrowotnej. HIPAA reguluje kwestie wykorzystywania i ujawniania informacji dotyczących zdrowia przez podmioty podlegające zasadzie dotyczącej prywatności. Obejmuje ona również normy dotyczące praw osób fizycznych do zrozumienia i kontrolowania sposobu wykorzystywania ich informacji dotyczących zdrowia. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html; https://www.justice.gov/opcl/privacy-act-1974.

[5] Głównym celem COPPA jest zapewnienie rodzicom kontroli nad tym, jakie dane osobowe dotyczące ich dzieci w wieku poniżej 13 lat są gromadzone przez operatorów stron internetowych i usług online skierowanych do dzieci (w tym aplikacji mobilnych i urządzeń IoT takich jak inteligentne zabawki) lub strony internetowe skierowane do ogółu społeczeństwa. COPPA wymaga, aby operatorzy ci przedstawiali ostrzeżenie dla rodziców i uzyskiwali możliwą do zweryfikowania zgodę rodziców. Jeżeli strony internetowe lub usługi są obsługiwane w USA i podlegają COPPA, dotyczy to również danych pochodzących od małoletnich cudzoziemców. Jednocześnie przepisy te mają też zastosowanie do zagranicznych stron internetowych i usług, jeżeli są one skierowane do dzieci w USA. Zob.: https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions oraz załącznik IV do projektu decyzji, s. 3.

[6] Jednym z celów ustawy Gramma-Leacha-Blileya jest ochrona prywatności konsumenta w sektorze finansowym. Ustawa ta zawiera wymóg, zgodnie z którym instytucje finansowe muszą wyjaśniać klientom swoje praktyki udostępniania informacji, a także tworzy zabezpieczenia służące ochronie informacji o kliencie (np. w przypadku przedsiębiorstw podlegających FTC zgodnie z zasadą dotyczącą zabezpieczeń FTC). https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[7] Zarządzenie prokuratora generalnego nr 5517-2022, które zmienia regulamin Departamentu Sprawiedliwości Stanów Zjednoczonych zgodnie z upoważnieniem i zarządzeniem zawartym w rozporządzeniu wykonawczym 14086.

ułatwiania, wspierania i rozwijania handlu międzynarodowego (tytuł 15 § 1512 Kodeksu Stanów Zjednoczonych (U.S.C.))"[8].

6. Opracowanie „zasad" („zasady DPF") zostało przeprowadzone w porozumieniu z Komisją Europejską („Komisja"), przedstawicielami przemysłu i innymi zainteresowanymi stronami, z myślą o osiągnięciu celu, jakim jest ułatwienie handlu między UE a USA[9], przy jednoczesnym zapewnieniu osobom, których dane dotyczą, stopnia ochrony zasadniczo odpowiadającego stopniowi gwarantowanemu w UE.

7. Zasady DPF opisano jako „kluczowy element" DPF. Z jednej strony stanowią one „gotowy mechanizm" na potrzeby przekazywania danych z UE do USA. Z drugiej strony dane osobowe przekazywane z UE do USA są zabezpieczone i chronione zgodnie z wymogami prawa UE.

8. Ramy ochrony danych mają zastosowanie tylko do podmiotów amerykańskich, które poddały się certyfikacji własnej zgodnie z wymogami określonymi w tych ramach („podmioty objęte DPF"). Na chwilę obecną jest to możliwe tylko wówczas, gdy podlegają one właściwości Federalnej Komisji Handlu („FTC") lub Departamentu Transportu („DoT"). W przyszłości w nowym załączniku mogą zostać dodane inne organy ustawowe, posiadające kompetencje w zakresie nadzoru nad wdrażaniem zasad DPF.

9. W zasadach DPF wyjaśniono, że za egzekwowanie wykonania warunków ram odpowiadają (i) FTC na podstawie sekcji 5 ustawy o Federalnej Komisji Handlu („ustawa o FTC") zakazującej nieuczciwych lub wprowadzających w błąd praktyk w handlu lub mających wpływ na handel[10] (ii) DoT na podstawie tytułu 49 § 41712 U.S.C. zakazującego przewoźnikowi lub pośrednikowi sprzedaży biletów stosowania nieuczciwych lub wprowadzających w błąd praktyk w transporcie lotniczym w celu sprzedaży lub przewozu lotniczego lub (iii) inne organy na podstawie innych przepisów ustawowych lub wykonawczych, zgodnie z którymi takie praktyki są zakazane.

10. W zasadach DPF wskazano, że nie mają one wpływu na stosowanie RODO ani nie ograniczają istniejących obowiązków w zakresie ochrony prywatności, które w innych przypadkach mają zastosowanie zgodnie z prawem USA.

1.2 Zakres oceny przeprowadzonej przez EROD

11. Projekt decyzji odzwierciedla przeprowadzoną przez Komisję ocenę DPF, która jest wynikiem rozmów z rządem USA. Zgodnie z art. 70 ust. 1 lit. s) RODO od EROD oczekuje się przedstawienia opinii na temat ustaleń Komisji w odniesieniu do odpowiedniego stopnia ochrony w państwie trzecim oraz w razie potrzeby podjęcia starań w celu przedstawienia propozycji zaradzenia ewentualnym problemom.

12. EROD z zadowoleniem przyjmuje aktualizacje zasad DPF[11], które będą stanowić wiążące ramy prawne dla podmiotów objętych DPF. EROD zauważa jednak, że zasady DPF pozostają zasadniczo takie same jak zasady określone w Tarczy Prywatności[12] (której dotyczyły coroczne wspólne przeglądy Grupy Roboczej Art. 29 i EROD). Zasady DPF są również w dużej mierze takie same jak zasady zawarte

[8] Sekcja I załącznika I do projektu decyzji.
[9] *Tamże*.
[10] Tytuł 15 § 45 lit. a) U.S.C.
[11] Na przykład doprecyzowanie, że dane kodowane za pomocą klucza stanowią dane osobowe.
[12] Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA, Dz.U. L 207 z 1.8.2016, s. 1.

w projekcie Tarczy Prywatności, który był podstawą opinii Grupy Roboczej Art. 29 z 2016 r.[13] („opinia Grupy Roboczej Art. 29 nr 01/2016"). W odniesieniu do tych zasad DPF, które pozostają zasadniczo niezmienione, EROD nie uważa za konieczne powtarzania wszystkich uwag zgłoszonych wcześniej przez Grupę Roboczą Art. 29. EROD postanowiła skupić się na konkretnych aspektach, które uważa obecnie za jeszcze bardziej istotne z uwagi na zmiany, jakie zaszły w otoczeniu prawnym i technologicznym.

13. Ponadto, zgodnie z orzecznictwem TSUE[14], bardzo istotna część analizy obejmuje system prawny regulujący dostęp organów rządowych do danych osobowych przekazywanych do USA.

14. W ocenie EROD uwzględniła obowiązujące europejskie ramy ochrony danych osobowych, w tym art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej („Karta"), chroniące odpowiednio prawo do życia prywatnego i rodzinnego, prawo do ochrony danych osobowych oraz prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu, a także art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności („EKPC") zapewniający ochronę prawa do życia prywatnego i rodzinnego. Oprócz powyższego EROD wzięła pod uwagę wymogi RODO, odpowiednie orzecznictwo oraz dokument w sprawie odpowiedniego stopnia ochrony przyjęty przez EROD („dokument w sprawie odpowiedniego stopnia ochrony na podstawie RODO")[15].

15. Celem tego działania jest dostarczenie Komisji opinii dotyczącej oceny odpowiedniego stopnia ochrony danych osobowych zapewnianego przez DPF. Pojęcie odpowiedniego stopienia ochrony, które istniało już na podstawie dyrektywy 95/46/WE, zostało doprecyzowane przez TSUE. W związku z tym należy przypomnieć normę ustanowioną przez TSUE w wyrokach w sprawie Schrems I[16] (unieważnienie „bezpiecznej przystani") oraz Schrems II[17] (unieważnienie Tarczy Prywatności).

16. W wyroku w sprawie Schrems I TSUE orzekł, że – choć „poziom ochrony" w państwie trzecim musi być „merytorycznie równoważny" temu gwarantowanemu w UE – „środki, z jakich to państwo trzecie korzysta w tym względzie dla zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w Unii"[18]. W związku z tym celem nie jest dokładne powielanie prawodawstwa europejskiego, lecz ustalenie zasadniczych i podstawowych wymogów analizowanego prawodawstwa. Odpowiedni stopień ochrony danych można osiągnąć poprzez połączenie praw osób, których dane dotyczą, i obowiązków podmiotów, które przetwarzają dane osobowe lub sprawują kontrolę nad takim przetwarzaniem i nadzorem ze strony niezależnych organów. Przepisy o ochronie danych są jednak skuteczne tylko wtedy, gdy są możliwe do wyegzekwowania i przestrzegane w praktyce. Konieczne jest zatem rozważenie nie tylko treści przepisów mających zastosowanie do danych osobowych

[13] Grupa Robocza Art. 29, Opinia 01/2016 w sprawie projektu decyzji stwierdzającej odpowiedni stopień ochrony w ramach Tarczy Prywatności UE–USA, przyjęta w dniu 13 kwietnia 2016 r. (zwana dalej „opinią Grupy Roboczej Art. 29 nr 01/2016").

[14] W szczególności: wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., Maximilian Schrems/Data Protection Commissioner, sprawa C-362/14, ECLI:EU:C:2015:650 oraz wyrok Trybunału Sprawiedliwości z dnia 16 lipca 2020 r., Data Protection Commissioner/Facebook Ireland Limited i Maximillian Schrems, sprawa C-311/18, ECLI:EU:C:2020:559.

[15] Grupa Robocza Art. 29, dokument pt. „Odpowiedni stopień ochrony przekazywanych danych osobowych", WP254 rev.01, 28 listopada 2017 r., ostatnio zmieniony i przyjęty 6 lutego 2018 r., zatwierdzony przez EROD 25 maja 2018 r. (zwany dalej „dokumentem w sprawie odpowiedniego stopnia ochrony na podstawie RODO").

[16] Wyrok TSUE z dnia 6 października 2015 r. w sprawie Schrems I, Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650 (zwany dalej „wyrokiem TSUE w sprawie Schrems I").

[17] Wyrok Trybunału Sprawiedliwości z dnia 16 lipca 2020 r., Data Protection Commissioner/Facebook Ireland Limited i Maximillian Schrems, sprawa C-311/18, ECLI:EU:C:2020:559 (zwany dalej „wyrokiem TSUE w sprawie Schrems II").

[18] Wyrok TSUE w sprawie Schrems I, pkt 73–74.

przekazywanych do państwa trzeciego lub organizacji międzynarodowej, ale także systemu stworzonego w celu zapewnienia skuteczności tych przepisów. Skuteczne mechanizmy egzekwowania prawa mają nadrzędne znaczenie dla skuteczności przepisów o ochronie danych[19].

17. W orzeczeniu w sprawie Schrems II TSUE stwierdził, że przepisy, na podstawie których amerykańskie organy wywiadowcze mają dostęp do danych osobowych przekazywanych do USA (art. 702 ustawy o kontroli wywiadu/rozporządzenie wykonawcze 12333), nieproporcjonalnie ograniczają prawa zapisane w art. 7 i 8 Karty praw podstawowych Unii Europejskiej („Karta"), a tym samym nie stanowią uregulowania tych ograniczeń w sposób odpowiadający wymogom merytorycznie równoważnym tym ustanowionym w prawie Unii w art. 52 ust. 1 zdanie drugie Karty[20].

18. Ponadto TSUE stwierdził, że poprzednie ramy prawne nie zapewniały zabezpieczeń merytorycznie równoważnych tym wymaganymi w art. 47 Karty, ponieważ mechanizmem ochrony prawnej przez Rzecznika ds. Tarczy Prywatności nie mógł zrekompensować faktu, że ani dyrektywa polityczna prezydenta nr 28 (PPD-28), ani rozporządzenie wykonawcze 12333 nie zapewniają osobom niebędącym obywatelami ani rezydentami USA skutecznego środka prawnego[21]. Zdaniem TSUE Rzecznik nie był wystarczająco niezależny w stosunku do władzy wykonawczej i nie był uprawniony do podejmowania decyzji wiążących dla amerykańskich służb wywiadowczych[22].

19. Rozporządzeniem wykonawczym 14086, które zasadniczo zastępuje PPD-28, wprowadzono w prawie amerykańskim dwa nowe wymogi, które są zgodne z wyrokiem TSUE w sprawie Schrems II: z jednej strony wprowadzono wymóg, aby działania w obszarze rozpoznania radioelektronicznego były prowadzone wyłącznie w zakresie niezbędnym do gromadzenia danych w ramach zatwierdzonego priorytetu wywiadowczego oraz wyłącznie takim w zakresie i w taki sposób, który będzie proporcjonalny do zatwierdzonego priorytetu wywiadowczego; a z drugiej strony wprowadzono mechanizm dochodzenia roszczeń.

20. W niniejszej opinii EROD ocenia w szczególności, w jakim stopniu DPF, a także niedawno przyjęte rozporządzenie wykonawcze 14086 skutecznie odnoszą się do ustaleń w wyroku TSUE.

1.3 Uwagi i zastrzeżenia ogólne

1.3.1 Ocena prawa krajowego

21. EROD rozumie, że ocena zawarta w projekcie decyzji dotyczy zasad DPF. Z zadowoleniem przyjęłaby jednak pewne informacje na temat kontekstu prawnego USA, w którym działają podmioty objęte DPF. Umożliwiłoby to lepsze zrozumienie interakcji DPF z prawem amerykańskim. Na przykład w sekcji I pkt 1 załącznika I[23] ustalono, że zasady DPF „nie ograniczają obowiązków związanych z ochroną prywatności, które w innym wypadku mają zastosowanie w prawie amerykańskim", choć nie opisano tych obowiązków.

1.3.2 Zobowiązania międzynarodowe zaciągnięte przez USA

22. Zgodnie z art. 45 ust. 2 lit. c) RODO i dokumentem w sprawie odpowiedniego stopnia ochrony na podstawie RODO przy ocenie odpowiedniego stopienia ochrony danych w państwie trzecim Komisja musi brać pod uwagę m.in. międzynarodowe zobowiązania państwa trzeciego lub inne obowiązki

[19] Dokument w sprawie odpowiedniego stopnia ochrony na podstawie RODO, s. 2.
[20] Wyrok TSUE w sprawie Schrems II, pkt 184–185.
[21] Wyrok TSUE w sprawie Schrems II, pkt 192.
[22] Wyrok TSUE w sprawie Schrems II, pkt 195.
[23] Sekcja I zdanie ostatnie załącznika I do projektu decyzji.

wynikające z jego udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych, a także realizację takich obowiązków.

23. USA są stroną kilku umów międzynarodowych gwarantujących prawo do prywatności, takich jak Międzynarodowy pakt praw obywatelskich i politycznych (art. 17), Konwencja o prawach osób niepełnosprawnych (art. 22) oraz Konwencja o prawach dziecka (art. 16). Ponadto USA, jako członek OECD, przestrzegają ram ochrony prywatności OECD, w szczególności wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami. 14 grudnia 2022 r. ministrowie i przedstawiciele wysokiego szczebla państw członkowskich OECD i Unii Europejskiej przyjęli deklarację OECD w sprawie dostępu organów rządowych do danych osobowych będących w posiadaniu podmiotów sektora prywatnego. USA są również stroną budapeszteńskiej Konwencji o cyberprzestępczości.

24. Ponadto USA są członkiem systemu transgranicznych zasad ochrony prywatności (CBPR) Współpracy Gospodarczej Azji i Pacyfiku (APEC), będącego wspieranym przez rząd systemem certyfikacji ochrony danych, do którego przedsiębiorstwa mogą przystąpić w celu wykazania zgodności z uznanymi na szczeblu międzynarodowym zasadami ochrony prywatności. Te zasady ochrony prywatności zostały zatwierdzone przez przywódców APEC.

25. EROD przyjmuje także do wiadomości udział USA jako państwa obserwatora w pracach Komitetu Konsultacyjnego ds. Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych.

26. Ponadto EROD z zadowoleniem przyjmuje stałe zaangażowanie organów USA w prace nowo ustanowionego w 2021 r. formatu „okrągłego stołu organów ochrony danych i prywatności grupy G-7”, w ramach którego zwoływane są posiedzenia niezależnych organów nadzorczych ochrony danych i prywatności w państwach G-7. W tym kontekście USA poparły na przykład najnowszy komunikat okrągłego stołu organów ochrony danych grupy G-7[24] przyjęty 8 września 2022 r. w Bonn w Niemczech, w którym skoncentrowano się na koncepcji swobodnego przepływu danych opartego na zaufaniu.

1.3.3 Postępy w obszarze prawodawstwa USA dotyczącego ochrony danych

27. EROD zwraca szczególną uwagę na zmiany w prawodawstwie dotyczącym ochrony danych na szczeblu stanowym w USA. EROD z zadowoleniem przyjmuje przyjęcie przepisów o ochronie danych, które już weszły w życie lub wejdą w życie do 2023 r. w pięciu stanach (Kalifornia, Kolorado, Connecticut, Virginia i Utah)[25]..

28. EROD zauważa również, że w wielu innych stanach USA podjęto już odpowiednie inicjatywy dotyczące kolejnych ustaw stanowych.

---

[24] Okrągły stół organów ochrony danych i prywatności grupy G-7, Promowanie swobodnego przepływu danych opartego na zaufaniu oraz dzielenie się wiedzą na temat perspektyw międzynarodowych przestrzeni danych, 8 września 2022 r., https://www.bfdi.bund.de/SharedDocs/Downloads/EN/G7/Communique-2022.pdf?__blob=publicationFile&v=1

[25] Kalifornia: ustawa o ochronie prywatności konsumenta (2018; ze skutkiem od 1 stycznia 2020 r.); ustawa o prawie do prywatności (2020; w pełni obowiązująca od 1 stycznia 2023 r.); Kolorado: ustawa o ochronie prywatności (2021; ze skutkiem od 1 lipca 2023 r.); Connecticut: ustawa o ochronie danych (2022; ze skutkiem od 1 lipca 2023 r.); Virginia: ustawa o ochronie danych konsumenta (2021; ze skutkiem od 1 stycznia 2023 r.); Utah: ustawa o ochronie prywatności konsumenta (2022; ze skutkiem od 31 grudnia 2023 r.).

29. Ponadto EROD z wyraźnym zadowoleniem przyjmuje starania związane z dwustronną inicjatywą na rzecz przyjęcia federalnej ustawy o ochronie danych – amerykańskiej ustawy o prywatności i ochronie danych (ADPPA).

1.3.4 Zakres projektu decyzji

30. W art. 1 projektu decyzji Komisja stwierdza, że Stany Zjednoczone zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych z UE do podmiotów w Stanach Zjednoczonych, które są wymienione w „wykazie DPF" prowadzonym i udostępnianym publicznie przez amerykański Departament Handlu („DoC") zgodnie z sekcją I.3 załącznika I [26].

31. DPF są dostępne dla przedsiębiorstw podlegających jurysdykcji FTC lub DoT. Należy zauważyć, że w przyszłości mogą zostać dodane inne amerykańskie organy ustawowe o podobnych uprawnieniach [27].

1.3.5 Ograniczenia obowiązku przestrzegania zasad DPF

32. Sekcja I pkt 5 załącznika I stanowi, że przestrzeganie zasad DPF przez podmioty objęte DPF może być ograniczone, między innymi: (i) w zakresie niezbędnym do wykonania orzeczenia sądowego lub do spełnienia wymogów interesu publicznego, egzekwowania prawa [28] lub bezpieczeństwa narodowego [29] (w tym w przypadku gdy ustawa lub rozporządzenie rządowe nakładają sprzeczne obowiązki) oraz (ii) ustawą, orzeczeniem sądowym lub rozporządzeniem rządu, którymi udzielono wyraźnego upoważnienia, pod warunkiem że działając na mocy jakiegokolwiek upoważnienia tego rodzaju, podmiot objęty DPF potrafi wykazać, że nieprzestrzeganie przez niego zasad DPF jest ograniczone do zakresu koniecznego do zaspokojenia nadrzędnych prawnie uzasadnionych interesów wspieranych tym upoważnieniem.

33. Bez pełnej znajomości prawa USA zarówno na szczeblu federalnym, jak i stanowym EROD trudno jest szczegółowo ocenić zakres wyłączeń wymienionych w tym punkcie. W związku z tym EROD zaleca, aby Komisja uwzględniła w projekcie decyzji doprecyzowanie zakresu wyłączeń, w tym mających zastosowanie zabezpieczeń na podstawie prawa USA, w celu lepszego określenia wpływu tych wyłączeń na stopień ochrony osób, których dane dotyczą. EROD podkreśla również, że Komisja powinna być informowana o stosowaniu i przyjmowaniu wszelkich ustaw lub rozporządzeń rządu, które mogłyby mieć wpływ na przestrzeganie zasad DPF, oraz monitorować ich stosowanie i przyjmowanie.

1.3.6 Zmiany w odniesieniu do Tarczy Prywatności

34. EROD z zadowoleniem przyjmuje starania podjęte w celu uwzględnienia wymogów wyroku w sprawie Schrems II. Bardziej zadowalające byłoby jednak, gdyby przy okazji negocjacji w sprawie DPF

[26] Sekcja „Uwagi końcowe" art. 1 projektu decyzji, s. 57. EROD rozumie, że projekt decyzji nie obejmie przekazywania danych przez podmioty zlokalizowane poza UE, ale podlegające RODO na podstawie art. 3 ust. 2 RODO, do certyfikowanych podmiotów w USA.

[27] Sekcja I pkt 2 załącznika I do projektu decyzji.

[28] Zob. sekcja 3.1 niniejszej opinii, aby zapoznać się z dalszymi uwagami na temat wykorzystania danych osobowych objętych DPF UE–USA do celów egzekwowania prawa.

[29] Zob. sekcja 3.2 niniejszej opinii, aby zapoznać się z dalszymi uwagami na temat wykorzystania danych osobowych objętych DPF UE–USA do celów związanych z bezpieczeństwem narodowym.

uwzględniono także więcej kwestii wskazanych (i) w opinii Grupy Roboczej Art. 29 nr 01/2016 oraz (ii) w poprzednich wspólnych przeglądach[30].

35. EROD zauważa także, że mimo szeregu zmian i dodatkowych wyjaśnień wprowadzonych w motywach projektu decyzji zasady DPF, których muszą przestrzegać podmioty objęte DPF, pozostają zasadniczo niezmienione w porównaniu z zasadami, które miały zastosowanie w ramach Tarczy Prywatności.

1.3.7 Brak jasności w dokumentach DPF

36. EROD zauważa, że struktura załączników i ich numeracja utrudniają znalezienie informacji i odniesienie do nich. Przyczynia się to do ogólnej niejasnej prezentacji nowych ram, które zawierają w załącznikach dokumenty o różnej wartości prawnej, i może nie sprzyjać właściwemu zrozumieniu zasad DPF przez osoby, których dane dotyczą, podmioty objęte DPF i unijne organy ochrony danych.

37. EROD podkreśla również, że w całych DPF należy spójnie stosować odpowiednią terminologię, co obecnie nie ma miejsca, na przykład w przypadku pojęcia przetwarzania. W niektórych częściach DPF zamiast użycia terminu „przetwarzanie" wymieniono niektóre rodzaje operacji przetwarzania danych. Może to skutkować niepewnością prawa i możliwymi lukami w ochronie[31].

38. EROD z zadowoleniem przyjmuje fakt, że w DPF zawarto definicje niektórych stosowanych w nich terminów[32]. Nie przedstawiono jednak definicji niektórych innych istotnych terminów, takich jak choćby „przedstawiciel" lub „podmiot przetwarzający", które zdaniem EROD wymagają jasnej i szczegółowej definicji w sekcji I pkt 8 załącznika I do DPF, co do której USA i UE będą zgodne, tak aby uniknąć nieporozumień na późniejszym etapie wśród podmiotów objętych DPF i opierających się na DPF, organów nadzorczych i opinii publicznej.

39. Jeżeli chodzi o kwestię rozbieżnych interpretacji w UE i USA pojęcia danych dotyczących zasobów ludzkich, EROD zgadza się ze sprawozdaniem Komisji z trzeciego przeglądu co do celu, jakim jest kontynuowanie rozmów z władzami USA[33].

2 ASPEKTY OGÓLNE OCHRONY DANYCH

2.1 Zasady dotyczące treści

[30] Roczne przeglądy: Tarcza Prywatności UE–USA – pierwszy roczny wspólny przegląd, WP 255, sprawozdanie Grupy Roboczej Art. 29 przyjęte w dniu 28 listopada 2017 r. (zwane dalej „sprawozdaniem z pierwszego wspólnego przeglądu"); Tarcza Prywatności UE–USA – drugi roczny wspólny przegląd, sprawozdanie EROD przyjęte w dniu 22 stycznia 2019 r. (zwane dalej „sprawozdaniem z drugiego wspólnego przeglądu"); Tarcza Prywatności UE–USA – trzeci roczny wspólny przegląd, sprawozdanie EROD przyjęte w dniu 12 listopada 2019 r. (zwane dalej „sprawozdaniem z trzeciego wspólnego przeglądu").

[31] Na przykład (i) zgodnie z brzmieniem sekcji III pkt 6 lit. f) załącznika I do projektu decyzji zasady DPF miałyby zastosowanie wyłącznie w przypadku, gdy podmiot „przechowuje, wykorzystuje lub ujawnia" otrzymane dane (tj. nie w przypadku innych operacji objętych terminem „przetwarzanie", takich jak gromadzenie, utrwalanie, modyfikowanie, pobieranie, przeglądanie, usuwanie), oraz (ii) zgodnie z sekcją II pkt 4 lit. a) załącznika I do projektu decyzji wymóg zapewnienia bezpieczeństwa danych miałby obowiązywać wyłącznie w odniesieniu do „tworzenia, przechowywania, wykorzystywania lub rozpowszechniania" danych osobowych.

[32] Sekcja I pkt 8 załącznika I do projektu decyzji.

[33] sprawozdanie z trzeciego wspólnego przeglądu, s. 5, 15–16 i 30; zob. również dokument roboczy służb Komisji towarzyszący dokumentowi Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie trzeciego rocznego przeglądu funkcjonowania Tarczy Prywatności, s. 17–18.

2.1.1 Pojęcia

40. Zgodnie z dokumentem w sprawie odpowiedniego stopnia ochrony na podstawie RODO w ramach prawnych państwa trzeciego powinny istnieć podstawowe pojęcia lub zasady ochrony danych. Nie muszą one wprawdzie odpowiadać terminologii RODO, ale powinny odzwierciedlać pojęcia zawarte w europejskich przepisach o ochronie danych osobowych i być z nimi spójne. Przykładowo RODO zawiera następujące istotne terminy: „dane osobowe", „przetwarzanie danych osobowych", „administrator danych", „podmiot przetwarzający dane", „odbiorca" i „dane wrażliwe". EROD z zadowoleniem przyjmuje fakt, że w DPF zawarto definicje terminów „dane osobowe", „przetwarzanie" i „administrator", podobnie jak to uczyniono w Tarczy Prywatności.

41. EROD zauważa, że w dalszym ciągu niejasny jest zakres, w jakim zasady DPF mają zastosowanie do podmiotów objętych DPF otrzymujących dane osobowe z UE do celów „zwykłego przetwarzania" (zwanych „przedstawicielami" lub „podmiotami przetwarzającymi"). W DPF nie dokonano rozróżnienia między zasadami DPF mającymi zastosowanie do przedstawicieli a zasadami DPF mającymi zastosowanie do administratorów, natomiast szereg obowiązków zawartych w zasadach DPF nie jest odpowiedni dla przedstawicieli/podmiotów przetwarzających. Na przykład przedstawiciel/podmiot przetwarzający nie powinien być w stanie przekazać osobom fizycznym wszystkich elementów pełnego powiadomienia zgodnie z zasadą powiadomienia (np. celów, w których gromadzi i wykorzystuje dotyczące ich dane osobowe)[34], ponieważ przedstawiciel/podmiot przetwarzający nie może samodzielnie określić środków i celów przetwarzania[35].

2.1.2 Zasada ograniczenia celu

42. W dokumencie w sprawie odpowiedniego stopnia ochrony na podstawie RODO wskazano – zgodnie z RODO – że dane osobowe powinny być przetwarzane w konkretnym celu, a następnie wykorzystywane wyłącznie w zakresie, w jakim jest to zgodne z tym celem przetwarzania.

43. Zasada integralności danych i ograniczenia celu stanowi, że podmiot nie może przetwarzać danych osobowych w sposób niezgodny z celami, w których zostały one zgromadzone lub na które dana osoba wyraziła następnie zgodę[36]. EROD zauważa, że w zasadach powiadomienia, wyboru oraz integralności danych i ograniczenia celu stosuje się różną terminologię. Jak zauważyła Grupa Robocza Art. 29, a także mimo użytecznych wyjaśnień w motywach projektu decyzji, terminy takie jak „inne cele", „znacząco różne" cele lub „sposób korzystania niezgodny z" są stosowane w DPF bez jasnej definicji tych pojęć w DPF i mogą prowadzić do niepewności prawa.

2.1.3 Prawo dostępu, prawo do sprostowania i usunięcia danych oraz prawo do sprzeciwu

44. W DPF prawa osób, których dane dotyczą, do dostępu, sprostowania i usunięcia danych są objęte zasadą dostępu[37].

45. Zasada dostępu pozostaje niezmieniona w porównaniu z Tarczą Prywatności. W związku z tym niektóre kwestie budzące obawy wyrażone w opinii Grupy Roboczej Art. 29 nr 01/2016 są nadal aktualne, jak opisano szczegółowo poniżej.

[34] Sekcja II pkt 1 lit. a) załącznika I do projektu decyzji.
[35] Zob. także opinia Grupy Roboczej Art. 29 nr 01/2016, s. 16.
[36] Sekcja II pkt 5 załącznika I do projektu decyzji.
[37] Sekcja II pkt 6 oraz sekcja III pkt 8 lit. a) ppkt (i) załącznika I do projektu decyzji.

46. Jeżeli chodzi o prawo dostępu osób fizycznych, EROD uważa za konieczne powtórzenie, że szczegóły dotyczące obowiązku udzielania odpowiedzi na wnioski osób fizycznych lepiej byłoby włączyć do głównego tekstu dotyczącego tej zasady (obecnie są one wciąż opisane wyłącznie w przypisie[38]).). Ponadto powinno być jasne, że dostęp ma być udzielany w zakresie, w jakim dany podmiot objęty DPF przetwarza dane osobowe, a nie tylko wtedy, gdy je „przechowuje"[39]. Zdaniem EROD obecne brzmienie mogłoby prowadzić do wąskiej interpretacji prawa dostępu.

47. Jeśli chodzi o wykaz wyjątków od prawa dostępu[40], niektóre z nich nadal przechylają szalę na korzyść interesów podmiotów objętych DPF. EROD w dalszym ciągu wyraża zaniepokojenie, ponieważ w tych przypadkach wydaje się, że nie ma wymogu uwzględniania praw i interesów osoby fizycznej[41].

48. Innym wyjątkiem, co do którego Grupa Robocza Art. 29 wyrażała już obawy[42] i który zdaniem EROD wydaje się zbyt szeroki, jest wyjątek od prawa dostępu do publicznie dostępnych informacji i informacji z rejestrów publicznych[43]. EROD wielokrotnie stwierdzała, że zgodnie z prawem UE osoby, których dane dotyczą, zawsze mają prawo dostępu do swoich danych niezależnie od tego, czy dane osobowe zostały opublikowane czy nie. Gdyby wnioski o dostęp były odrzucane ze względu na to, że dane zostały pozyskane z publicznie dostępnych źródeł lub z rejestrów publicznych, osoby fizyczne utraciłyby możliwość kontrolowania prawidłowości danych i przede wszystkim tego, czy dane zostały podane do wiadomości publicznej zgodnie z prawem.

49. EROD przypomina, że prawo dostępu jest zapisane w art. 8 ust. 2 Karty. Chociaż nie jest to prawo absolutne, ma ono podstawowe znaczenie dla prawa do ochrony danych osobowych, ponieważ ułatwia osobie, której dane dotyczą, wykonywanie pozostałych praw, takich jak prawo do poprawienia i usunięcia danych oraz prawo do sprzeciwu[44].

50. Oprócz prawa dostępu do danych i ich usuwania osoby, których dane dotyczą, powinny mieć prawo wniesienia w dowolnym momencie sprzeciwu wobec przetwarzania ich danych, z ważnych prawnie uzasadnionych powodów związanych z ich szczególną sytuacją, na szczególnych warunkach ustanowionych w ramach prawnych państwa trzeciego[45].

51. W ramach zasady wyboru w DPF przewiduje się prawo do wniesienia sprzeciwu (klauzulę opt-out) wobec ujawnienia danych osobowych osobie trzeciej lub wykorzystywania danych osobowych do celów znacząco różnych[46]. Ponadto osoby fizyczne korzystają w dowolnym momencie z prawa do wycofania zgody na wykorzystywanie ich danych osobowych do celów marketingu bezpośredniego[47]. Z wyjątkiem celów marketingu bezpośredniego, warunki, w szczególności terminy, korzystania z prawa do sprzeciwu nie są przedstawione szczegółowo. W związku z tym EROD zwraca się do Komisji o doprecyzowanie, w jaki sposób osoby fizyczne mogą korzystać z przysługującego im prawa do sprzeciwu.

[38] Sekcja III pkt 8 lit. a) ppkt (i) pppkt 1 załącznika I do projektu decyzji – przypis 14.
[39] Sekcja III pkt 8 lit. d) ppkt (ii) załącznika I do projektu decyzji.
[40] Sekcja III pkt 8 lit. e) załącznika I do projektu decyzji.
[41] Sekcja 2.2.5 opinii Grupy Roboczej Art. 29 nr 01/2016.
[42] Sekcja 2.2.9 opinii Grupy Roboczej Art. 29 nr 01/2016.
[43] Sekcja III pkt 15 lit. d)–e) załącznika I do projektu decyzji.
[44] Sekcja 2.2.5 opinii Grupy Roboczej Art. 29 nr 01/2016.
[45] Rozdział 3 część A pkt 8 dokumentu w sprawie odpowiedniego stopnia ochrony na podstawie RODO.
[46] Sekcja II pkt 2 lit. a) załącznika I do projektu decyzji.
[47] Sekcja III pkt 12 lit. a) załącznika I do projektu decyzji.

52. Jak stwierdzono w opinii Grupy Roboczej Art. 29 nr 01/2016, EROD uważa, że zwykłe odniesienie do istnienia tego prawa w polityce prywatności nie jest wystarczające. Indywidualna możliwość skorzystania z tego prawa powinna być oferowana nie tylko w przypadku ujawniania lub ponownego wykorzystywania danych osobowych. EROD podkreśla, że w DPF należy zapewnić ogólne prawo do sprzeciwu z ważnych prawnie uzasadnionych powodów związanych ze szczególną sytuacją osoby, której dane dotyczą. EROD zaleca, aby takie prawo do sprzeciwu było zagwarantowane w dowolnym momencie oraz aby nie było ono ograniczone do wykorzystywania danych do celów marketingu bezpośredniego[48].

53. W odniesieniu do danych dotyczących zasobów ludzkich EROD docenia doprecyzowanie przez Komisję kwestii stosowania zasad powiadomienia i wyboru w sytuacji, gdy certyfikowany podmiot amerykański zamierza wykorzystywać dane dotyczące zasobów ludzkich do innych celów niezwiązanych z zatrudnieniem, takich jak materiały marketingowe[49]. EROD utrzymuje jednak, że dalsze przetwarzanie danych dotyczących zasobów ludzkich do celów niezwiązanych z zatrudnieniem w większości przypadków zostanie uznane za niezgodne z pierwotnym celem oraz że zgoda udzielana w kontekście zatrudnienia rzadko będzie w pełni swobodna.

54. EROD przypomina również obawy Grupy Roboczej Art. 29 dotyczące wyłączenia z zasad powiadomienia i wyboru danych dotyczących zasobów ludzkich „[w] okresie i w stopniu, w którym będzie to niezbędne do uniknięcia negatywnego wpływu na zdolność podmiotu do dokonywania awansów, powoływania na stanowiska lub do podejmowania podobnych decyzji dotyczących zatrudnienia”[50], które to wyłączenie zdaniem EROD wydaje się szerokie i niejasne[51].

2.1.4 Ograniczenia dotyczące dalszego przekazywania danych

55. Dalsze przekazywanie danych osobowych przez pierwotnego odbiorcę pierwotnego przekazywania danych powinno być dozwolone tylko wtedy, gdy dalszy odbiorca (tj. odbiorca dalszego przekazywania) również podlega przepisom (w tym przepisom umownym) zapewniającym odpowiedni stopień ochrony i przestrzega odpowiednich instrukcji podczas przetwarzania danych w imieniu administratora danych. Dalsze przekazywanie danych nie może obniżać stopnia ochrony osób fizycznych, których dane są przekazywane. Pierwotny odbiorca danych przekazywanych z UE jest odpowiedzialny za zapewnienie odpowiednich zabezpieczeń w odniesieniu do dalszego przekazywania danych w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony. Takie dalsze przekazywanie danych powinno być prowadzone jedynie w ograniczonych i określonych celach oraz dopóki istnieje podstawa prawna takiego przetwarzania[52].

56. Zgodnie z zasadą odpowiedzialności za dalsze przekazywanie danych określoną w DPF dalsze przekazywanie może mieć miejsce wyłącznie w ograniczonym i określonym celu, na podstawie umowy między podmiotem objętym DPF a osobą trzecią (lub porównywalnego uzgodnienia w ramach grupy przedsiębiorstw) i tylko wtedy, gdy umowa ta zobowiązuje osobę trzecią do zapewnienia takiego samego stopnia ochrony jak ten gwarantowany przez zasady DPF[53].

[48] Sekcja 2.2.2 opinii Grupy Roboczej Art. 29 nr 01/2016.
[49] Sekcja III pkt 9 lit. b) ppkt (i) załącznika I do projektu decyzji oraz motyw 15 i przypis 27 projektu decyzji.
[50] Sekcja III pkt 9 lit. b) ppkt (iv) załącznika I do projektu decyzji.
[51] Sekcja 2.2.7 opinii Grupy Roboczej Art. 29 nr 01/2016.
[52] Rozdział 3 część A pkt 9 dokumentu w sprawie odpowiedniego stopnia ochrony na podstawie RODO.
[53] Sekcja II pkt 3 załącznika I do projektu decyzji.

57. EROD pragnie powtórzyć obawy wyrażone w opinii Grupy Roboczej Art. 29 nr 01/2016 dotyczące zwolnienia z obowiązku zawarcia umowy dotyczącej wewnątrzgrupowego przekazywania danych między administratorami[54]. W odniesieniu do danych dotyczących zasobów ludzkich EROD nadal nie rozumie uzasadnienia zwolnienia z obowiązku zawarcia umowy z administratorem będącym osobą trzecią w przypadku dalszego przekazywania danych w przypadku „sporadycznych, związanych z zatrudnieniem potrzeb operacyjnych”[55].

58. Ponadto EROD pragnie powtórzyć wniosek Grupy Roboczej Art. 29[56], aby podmioty związane ramami przed dalszym przekazaniem oceniały, czy obowiązkowe wymogi prawodawstwa krajowego państwa trzeciego mające zastosowanie do odbiorcy nie będą naruszać ciągłości ochrony osób, których dane są przekazywane[57].

59. EROD utrzymuje, że dalsze przekazywanie danych osobowych do państw trzecich może prowadzić do ingerencji w prawa podstawowe osób fizycznych, oraz zwraca się do Komisji o doprecyzowanie, że zabezpieczenia nałożone przez pierwotnego odbiorcę na podmiot odbierający dane w państwie trzecim muszą być skuteczne w świetle przepisów państwa trzeciego przed dalszym przekazaniem w kontekście DPF[58].

2.1.5 Zautomatyzowane podejmowanie decyzji i profilowanie

60. Decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach), w tym profilowaniu, które wywołują skutki prawne lub istotnie wpływają na osobę, której dane dotyczą, mogą być podejmowane jedynie pod pewnymi warunkami określonymi w ramach prawnych państwa trzeciego. W ramach europejskich warunki takie obejmują m.in. potrzebę uzyskania wyraźnej zgody osoby, której dane dotyczą, lub konieczność uzyskania takiej decyzji do celów zawarcia umowy. Jeżeli decyzja nie jest zgodna z takimi warunkami określonymi w ramach prawnych państwa trzeciego, osoba, której dane dotyczą, powinna mieć prawo do niepodlegania takiej decyzji. Przepisy państwa trzeciego powinny w każdym przypadku przewidywać niezbędne zabezpieczenia, w tym prawo do uzyskania informacji o konkretnych powodach podjęcia danej decyzji oraz o jej logice, prawo do skorygowania nieprawidłowych lub niekompletnych informacji oraz prawo do zakwestionowania decyzji, jeżeli została ona podjęta na podstawie błędnego stanu faktycznego[59].

---

[54] Sekcja III pkt 10 lit. b) ppkt (i) załącznika I do projektu decyzji, gdzie użyto sformułowania „lub inne instrumenty wewnątrzgrupowe (np. programy zgodności i kontroli)”, które to instrumenty – jak się wydaje – nie muszą być wiążące.

[55] Sekcja III pkt 9 lit. e) ppkt (i) załącznika I do projektu decyzji, gdzie podano przykłady takie jak wykupienie polisy ubezpieczeniowej.

[56] Sekcja 2.2.3 opinii Grupy Roboczej Art. 29 nr 01/2016, s. 21.

[57] W świetle wyroku w sprawie Schrems II EROD doprecyzowała obowiązki podmiotów przekazujących i podmiotów odbierających dane w odniesieniu do dalszego przekazywania danych w szeregu wytycznych i zaleceń: zob. EROD, Zalecenia 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych (wersja 2.0 przyjęta w dniu 18 czerwca 2021 r.); Zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru (przyjęte w dniu 10 listopada 2020 r.); Wytyczne 04/2021 dotyczące kodeksów postępowania jako narzędzi do przekazywania danych (wersja 2.0 przyjęta w dniu 22 lutego 2022 r.); Zalecenia 1/2022 dotyczące wniosku o zatwierdzenie oraz elementów i zasad, które powinny się znaleźć w wiążących regułach korporacyjnych dla administratora (przyjęte w dniu 14 listopada 2022 r.); Wytyczne 07/2022 dotyczące certyfikacji jako narzędzia do przekazywania danych (przyjęte po konsultacjach publicznych w dniu 14 lutego 2023 r.).

[58] Sekcja 2.2.3 opinii Grupy Roboczej Art. 29 nr 01/2016, s. 21.

[59] Rozdział 3 część B pkt 3 dokumentu w sprawie odpowiedniego stopnia ochrony na podstawie RODO.

61. W DPF nie przewiduje się żadnych szczególnych gwarancji prawnych w przypadku, gdy osoby fizyczne podlegają decyzjom, które wywołują skutki prawne lub mają na nie istotny wpływ oraz które oparte są wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych aspektów o charakterze osobistym dotyczących tych osób, jak np. wyniki osiągane w pracy, zdolność kredytowa, wiarygodność lub sposób zachowania.

62. Jak już wspomniano w opinii Grupy Roboczej Art. 29 nr 01/2016 oraz w poprzednich opiniach EROD w sprawie decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu do Japonii i Korei Południowej[60], EROD stwierdza, że w tym względzie szczególną uwagę należy zwrócić na szybkie zmiany w dziedzinie zautomatyzowanego podejmowania decyzji i profilowania, które w coraz większym stopniu realizuje się za pomocą technologii sztucznej inteligencji[61].

63. EROD przyjmuje do wiadomości argumenty Komisji, zgodnie z którymi brak przepisów szczegółowych dotyczących zautomatyzowanego podejmowania decyzji w DPF prawdopodobnie nie wpłynie na stopień ochrony danych osobowych gromadzonych w Unii (ponieważ wszelkie decyzje oparte na zautomatyzowanym przetwarzaniu byłyby zazwyczaj podejmowane przez administratora w Unii, który ma bezpośrednie relacje z daną osobą, której dane dotyczą)[62]. Zdaniem EROD nie można jednak wykluczyć, że zautomatyzowane podejmowanie decyzji mogłoby być wykorzystywane przez administratora danych z siedzibą w USA w odniesieniu do danych przekazywanych na podstawie projektu decyzji (np. w kontekście zatrudnienia, w celu oceny wyników w pracy, wykupienia ubezpieczenia, zapewnienia zamieszkania).

64. EROD z zadowoleniem przyjmuje odniesienia Komisji do szczególnych zabezpieczeń przewidzianych w odpowiednich przepisach prawa USA w różnych dziedzinach[63]. Wydaje się jej jednak, że stopień ochrony osób fizycznych różni się w zależności od tego, które przepisy sektorowe – o ile takie istnieją – mają zastosowanie do danej sytuacji. Istnieje ryzyko, że niektóre sytuacje nie będą objęte tymi przepisami, ponieważ nie wchodzą w zakres stosowania aktów, o których mowa. Ponadto treść praw indywidualnych związanych ze zautomatyzowanym podejmowaniem decyzji jest opisywana w różny sposób w tych poszczególnych aktach.

65. W związku z tym EROD uważa, że w DPF należy zawrzeć przepisy szczegółowe dotyczące zautomatyzowanego podejmowania decyzji, które zapewnią odpowiednie zabezpieczenia, w tym prawo osoby fizycznej do poznania logiki, zakwestionowania decyzji i uzyskania interwencji ludzkiej, w przypadku gdy dana decyzja ma na tę osobę istotny wpływ[64].

2.2 Mechanizmy proceduralne i mechanizmy egzekwowania prawa

66. EROD zauważa, że DPF nadal opierają się na systemie samocertyfikacji, nawet jeśli Komisja nazywa go systemem „certyfikacji".

[60] EROD, Opinia nr 28/2018 dotycząca projektu decyzji wykonawczej Komisji Europejskiej w sprawie odpowiedniej ochrony danych osobowych w Japonii, przyjęta w dniu 5 grudnia 2018 r.; EROD, Opinia nr 32/2021 na podstawie rozporządzenia (UE) 2016/679 dotycząca projektu decyzji wykonawczej Komisji Europejskiej w sprawie odpowiedniej ochrony danych osobowych w Republice Korei, przyjęta w dniu 24 września 2021 r.;
[61] Zob. między innymi sprawa C-634/21, OQ/Land Hesse (SCHUFA Holding i in.), wniosek o wydanie orzeczenia w trybie prejudycjalnym (w toku).
[62] Motywy 33 i 34 projektu decyzji.
[63] Motyw 35 projektu decyzji.
[64] Zob. również sprawozdanie z trzeciego wspólnego przeglądu, s. 76.

67. EROD przypomina o usprawnieniach osiągniętych w trakcie poprzednich wspólnych przeglądów. Na przykład w odniesieniu do roli DoC, procesu (ponownej) samocertyfikacji (...), monitorowania przestrzegania przez przedsiębiorstwa zasad DPF (np. za pomocą kontroli wyrywkowej, stosowania kwestionariuszy dotyczących zgodności) oraz wykrywania fałszywych oświadczeń dotyczących uczestnictwa w programie i podejmowania działań zaradczych (np. za pomocą wyszukiwań internetowych).

68. Jednocześnie Grupa Robocza Art. 29 i EROD wyraziły swoje zaniepokojenie w kwestii braku nadzoru nad spełnianiem wymogów Tarczy Prywatności w niektórych przypadkach[65]. W szczególności EROD zgadza się z ustaleniami Komisji po trzecim rocznym przeglądzie Tarczy Prywatności, zgodnie z którymi w ramach Tarczy Prywatności kontrole wyrywkowe przeprowadzane przez DoC ograniczały się do wymogów formalnych (np. brak odpowiedzi ze strony wyznaczonych punktów kontaktowych lub brak dostępu do polityki prywatności przedsiębiorstwa w internecie)[66]. EROD uważa, że kontrole zgodności w odniesieniu do bardziej zasadniczych wymogów są niezwykle ważne.

69. Ponadto EROD przypomina o znaczeniu skutecznego nadzoru (w tym nad spełnianiem zasadniczych wymogów) i egzekwowania DPF. Kwestie te będą ściśle monitorowane przez EROD, w tym w kontekście okresowych przeglądów.

70. W odniesieniu do egzekwowania prawa EROD przyjmuje do wiadomości odnowione zobowiązania zawarte w pismach FTC[67] i DoT[68] dotyczące priorytetowego traktowania postępowania w sprawie domniemanych naruszeń DPF, wszczynania stosownych postępowań w zakresie egzekwowania prawa przeciwko podmiotom składającym fałszywe lub wprowadzające w błąd oświadczenia dotyczące uczestnictwa w programie, monitorowania decyzji służących egzekwowaniu przepisów w sprawach naruszeń DPF i współpracy z unijnymi organami ochrony danych. W tym względzie EROD uznaje również, że FTC wskazała, iż oczekuje dalszego skoncentrowania swoich działań w zakresie egzekwowania prawa na istotnych naruszeniach DPF oraz że zamierza prowadzić postępowania (również) z własnej inicjatywy. Kwestie te będą ściśle monitorowane przez EROD, w tym w kontekście okresowych przeglądów.

2.3 Mechanizmy dochodzenia roszczeń

71. EROD z zadowoleniem przyjmuje wyraźne przedstawienie w projekcie decyzji siedmiu środków dochodzenia roszczeń zapewnionych osobom z UE, których dane dotyczą, w przypadku gdy ich dane osobowe są przetwarzane z naruszeniem DPF[69].

72. Te różne mechanizmy ochrony prawnej ustanawia się zgodnie z wymogami zasady ochrony prawnej, egzekwowania prawa oraz odpowiedzialności i zgodnie z zasadą uzupełniającą 11 dotyczącą

[65] Sprawozdanie z trzeciego wspólnego przeglądu, s. 7.
[66] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie trzeciego rocznego przeglądu funkcjonowania Tarczy Prywatności (23.10.2019 r., COM(2019) 495 final), s. 4.
[67] Załącznik IV do projektu decyzji.
[68] Załącznik V do projektu decyzji.
[69] Motyw 67 projektu decyzji.

rozstrzygania sporów i egzekwowania wydaną przez DoC i wspomnianą w załączniku I do projektu decyzji[70].

73. Jak podkreśliła Komisja w projekcie decyzji, „osobie, której dane dotyczą, należy zapewnić skuteczne administracyjne i sądowe środki zaskarżenia"[71]. Jest to zgodne z wymogiem określonym w art. 45 ust. 2 lit. a) RODO, aby Komisja przy dokonywaniu oceny odpowiedniości stopnia ochrony w państwie trzecim uwzględniała w szczególności „prawa osób, których dane dotyczą, których dane osobowe są przekazywane, do skutecznych administracyjnych i sądowych środków zaskarżenia"[72]. Wymóg ten został również przywołany w dokumencie w sprawie odpowiedniego stopnia ochrony na podstawie RODO[73].

74. EROD zauważa, że te mechanizmy dochodzenia roszczeń są takie same jak te, które zawarto w unieważnionej Tarczy Prywatności, i co do których Grupa Robocza Art. 29 przedstawiła swoje uwagi[74].

75. Jeśli chodzi o mechanizm arbitrażu, EROD zauważa, że opcja ta nie jest dostępna w odniesieniu do wyjątków od zasad DPF[75] i w związku z tym odsyła do uwagi przedstawionej w pkt 33.

76. W odniesieniu do dodatkowych sądowych środków zaskarżenia dostępnych na mocy prawa USA EROD z zadowoleniem przyjęłaby również dalsze szczegółowe informacje na temat wspomnianych przepisów[76] i odsyła do swojej uwagi przedstawionej w pkt21.

77. EROD ponadto z zadowoleniem przyjmuje pismo FTC, w którym opisuje ona swój zamiar prowadzenia ścisłej współpracy z unijnymi organami ochrony danych[77]. EROD z zadowoleniem przyjmuje również priorytetowe traktowanie skarg przez FTC, chociaż i to może nie dawać osobie, której dane dotyczą, pewności, że jej skargi będą rozpatrywane we wszystkich przypadkach.

78. Jeżeli chodzi o występującą w niektórych przypadkach możliwość składania skarg przez osoby fizyczne do unijnego organu ochrony danych, EROD byłaby wdzięczna za dalsze informacje na temat tego, (i) czy możliwość udzielania porad w sprawie środków naprawczych lub odszkodowawczych przez unijny organ ochrony danych może obejmować zalecenia dotyczące kar pieniężnych lub korzystania z uprawnień dochodzeniowych (w zakresie prowadzonych postępowań) oraz (ii) w jakim zakresie działania unijnego organu ochrony danych zostałyby uwzględnione jako dowody na potrzeby czynności w zakresie egzekwowania prawa podejmowanych przez FTC lub DoT[78].

79. EROD będzie ściśle monitorować skuteczność tych mechanizmów dochodzenia roszczeń, w tym w kontekście okresowych przeglądów.

[70] Sekcja II pkt 7 i sekcja III pkt 11 załącznika I do projektu decyzji oraz załącznik I do załącznika I do projektu decyzji.
[71] Motyw 64 projektu decyzji.
[72] Zob. także motyw 141 RODO w odniesieniu do art. 47 Karty praw podstawowych dotyczącego prawa do skutecznego środka prawnego w UE.
[73] Dokument w sprawie odpowiedniego stopnia ochrony na podstawie RODO, s. 8.
[74] Zob. w szczególności sekcja 2.2.6 lit. a) opinii Grupy Roboczej Art. 29 nr 01/2016.
[75] Część A załącznika I do załącznika I do projektu decyzji.
[76] Motyw 85 projektu decyzji.
[77] Załącznik IV do projektu decyzji.
[78] Sekcja III pkt 5 lit. b) ppkt (iii) załącznika I do projektu decyzji.

3 DOSTĘP DO DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UNII EUROPEJSKIEJ I ICH WYKORZYSTYWANIE PRZEZ ORGANY PUBLICZNE W USA

3.1 Dostęp do danych i ich wykorzystywanie do celów ścigania przestępstw

3.1.1 Dostęp organów ścigania do danych osobowych powinien opierać się na jasnych, precyzyjnych i dostępnych przepisach

80. EROD z zadowoleniem przyjmuje przewidziane w projekcie decyzji bardziej szczegółowe informacje i wyjaśnienia – w porównaniu z poprzednią decyzją stwierdzającą odpowiedni stopień ochrony – dotyczące dostępu do danych osobowych i ich wykorzystywania przez amerykańskie organy publiczne do celów ścigania przestępstw. W załączniku VI do projektu decyzji zawarto także pismo Wydziału Karnego amerykańskiego Departamentu Sprawiedliwości „przedstawiające krótki opis głównych narzędzi dochodzeniowych wykorzystywanych do pozyskiwania danych handlowych i innych informacji przechowywanych w rejestrach od korporacji w Stanach Zjednoczonych do celów ścigania przestępstw lub do celów interesu publicznego (na potrzeby organów administracji cywilnej i regulacyjnych), w tym ograniczeń dostępu określonych w aktach stanowiących podstawę prawną". Zgodnie z treścią tego pisma wszystkie opisane w nim pisma sądowe stosuje się do pozyskiwania informacji od korporacji w USA, niezależnie od narodowości czy miejsca zamieszkania osób, których dane dotyczą, przy czym pisma te wynikają bezpośrednio z konstytucji Stanów Zjednoczonych (czwartej poprawki), z prawa stanowionego i procesowego albo z wytycznych i strategii politycznych Departamentu Sprawiedliwości. W piśmie tym nie uwzględniono narzędzi dochodzeniowych do celów bezpieczeństwa narodowego stosowanych przez organy ścigania w dochodzeniach związanych z terroryzmem i innych dochodzeniach dotyczących bezpieczeństwa narodowego[79].

81. EROD zauważa, że w projekcie decyzji i w załączniku VI do tego projektu omówiono przede wszystkim federalne organy ścigania i organy regulacyjne[80] i nie odniesiono się konkretnie do ustaw obowiązujących w prawie stanowym, w których przewidziano takie procedury uzyskiwania informacji. W załączniku VI wspomniano również, że „istnieją inne podstawy prawne umożliwiające przedsiębiorstwom zaskarżenie wniosków o udostępnienie danych składanych przez agencje administracyjne w zależności od ich konkretnych sektorów i rodzajów danych, jakimi dysponują". Podano tam ponadto kilka niewyczerpujących przykładów, takich jak ustawa o tajemnicy bankowej i przepisy wykonawcze do niej[81], ustawa o rzetelnej sprawozdawczości kredytowej[82], ustawa o prawie do prywatności w kwestiach finansowych[83]. EROD zauważa, że podstawa prawna mająca zastosowanie do określonego wniosku o dostęp zależy od charakteru poszukiwanych danych, charakteru przedsiębiorstwa, charakteru procedur prawnych (karnych, administracyjnych, związanych z innym interesem publicznym) oraz charakteru podmiotu występującego o dostęp. Ponieważ wszystkie mające zastosowanie przepisy ograniczające dostęp organów ścigania do danych przekazywanych do USA opierają się na konstytucji, prawie stanowionym i przejrzystych strategiach politycznych Departamentu Sprawiedliwości, EROD uznaje dostępność tych przepisów i zwraca się do Komisji o uwzględnienie tego elementu w projekcie decyzji. Wynika to z załącznika VI: akty te mają

[79] Przypis 1 w załączniku VI do projektu decyzji.
[80] Zob. motywy 90–93 projektu decyzji.
[81] Tytuł 31 § 5318 U.S.C.; tytuł 31 rozdział X C.F.R.
[82] Tytuł 15 § 1681b U.S.C.
[83] Tytuł 12 §§ 3401–3423 U.S.C.

zastosowanie niezależnie od obywatelstwa lub miejsca zamieszkania osoby, której dane dotyczą, i zasadniczo zawierają wymogi określone w czwartej poprawce (chociaż często wykraczają one również poza ten zakres i obejmują dodatkowe środki ochrony).

82. Podsumowując, EROD odnotowuje bardziej szczegółową ocenę zawartą w projekcie decyzji w porównaniu z poprzednią decyzją stwierdzającą odpowiedni stopień ochrony w odniesieniu do dostępu organów ścigania na szczeblu federalnym. Jeśli chodzi o dostęp organów ścigania na szczeblu stanowym, EROD także odnotowuje, że zgodnie z załącznikiem VI środki ochrony na podstawie prawa stanowego muszą być co najmniej równoważne środkom przewidzianym w konstytucji Stanów Zjednoczonych, w tym między innymi w czwartej poprawce. EROD zwraca się do Komisji o dalszą ocenę elementu ochrony na podstawie prawa stanowego w przyszłych przeglądach.

3.1.2 Należy wykazać konieczność i proporcjonalność w odniesieniu do zamierzonych prawnie uzasadnionych celów

83. EROD odnotowuje, że wniosek o udzielenie dostępu do danych do celów egzekwowania prawa można zasadniczo uznać za służący realizacji prawnie uzasadnionego celu. Jednocześnie jednak tego rodzaju ingerencje są dopuszczalne tylko wtedy, gdy są konieczne i proporcjonalne[84].

84. Zgodnie z utrwalonym orzecznictwem TSUE zasada proporcjonalności wymaga, aby środki ustawodawcze wprowadzające możliwości ingerencji w prawo do życia prywatnego i prawo do ochrony danych osobowych „były odpowiednie do realizacji uzasadnionych celów, którym akty te służą, i nie wykraczały poza to, co jest konieczne do ich osiągnięcia”[85]. W związku z tym ocena konieczności i proporcjonalności odbywa się co do zasady zawsze w odniesieniu do konkretnego środka przewidzianego w przepisach.

85. Władze USA określają w załączniku VI, że prokuratorzy federalni i federalni agenci śledczy mogą uzyskać dostęp do dokumentów i innych informacji pochodzących od podmiotów w drodze „kilku rodzajów obowiązkowych pism sądowych, takich jak wezwania do stawienia się przed wielką ławą przysięgłych, wezwania administracyjne oraz nakazy przeszukania” oraz mogą pozyskiwać innego rodzaju informacje „na podstawie aktów stanowiących podstawę prawną na szczeblu federalnym do kontroli rozmów telefonicznych oraz instalowania urządzeń rejestrujących wybierane numery na gruncie prawa karnego”[86]. Agencje o kompetencjach cywilnych i regulacyjnych mogą ponadto wezwać podmioty do „przekazania dokumentacji dotyczącej prowadzonej działalności, informacji przechowywanych w formie elektronicznej lub innych przedmiotów materialnych”[87]. Same te pisma wyjaśniono także w motywach 90–93 projektu decyzji. EROD odnotowuje w tym względzie

[84] Zob. wyrok Trybunału Sprawiedliwości z dnia 6 października 2020 r., sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i inni, ECLI:EU:C:2020:791 (zwany dalej „wyrokiem TSUE w sprawie La Quadrature du Net”), pkt 140. Zob. również EIOD, „Assessing the necessity of measures that limit the fundamental right to the protection of personal data A toolkit” [„Zestaw narzędzi w zakresie oceny konieczności środków ograniczających podstawowe prawo do ochrony danych osobowych”], 11 kwietnia 2017 r. oraz „EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data” [„Wytyczne EIOD w sprawie oceny proporcjonalności środków ograniczających prawa podstawowe do prywatności i ochrony danych osobowych”], 19 grudnia 2019 r.

[85] Zob. wyrok Trybunału Sprawiedliwości z dnia 8 kwietnia 2014 r., sprawy połączone C-293/12 i C-594/12, Digital Rights Ireland Ltd, ECLI:EU:C:2014:238 (zwany dalej: „wyrokiem TSUE w sprawie Digital Rights Ireland”), pkt 46 i przytoczone tam orzecznictwo.

[86] Załącznik VI do projektu decyzji, s. 2.

[87] Załącznik VI do projektu decyzji, s. 4.

wspomniane w projekcie decyzji pozytywne zmiany w orzecznictwie USA w odniesieniu do informacji przechowywanych elektronicznie[88].

86. W załączniku VI określono ponadto, że te wszystkie postępowania sądowe są niedyskryminacyjne i wykorzystuje się je zasadniczo do pozyskiwania informacji od „korporacji" w USA, zarówno tych certyfikowanych zgodnie z ramami ochrony danych USA–UE, jak i nie, „niezależnie od narodowości czy miejsca zamieszkania osób, których dane dotyczą".

87. Co więcej, załącznik VI zawiera ustalenia dotyczące zabezpieczeń przewidzianych w czwartej poprawce do konstytucji Stanów Zjednoczonych, zgodnie z którą przeszukanie i zatrzymanie przez organy ścigania zasadniczo wymagają nakazu sądowego wydawanego po wykazaniu spełnienia wymogu dotyczącego prawdopodobieństwa winy i szczegółowości, a także odniesiono się w nim do faktu, że w wyjątkowych przypadkach, gdy wymóg nakazu nie ma zastosowania, organy ścigania podlegają analizie zasadności zgodnie z czwartą poprawką[89]. Osoba, której dotyczy przeszukanie lub której mienie jest przedmiotem przeszukania, może wystąpić o wyłączenie z postępowania dowodów uzyskanych w wyniku bezprawnego przeszukania lub pochodzących z takiego przeszukania, jeżeli dowody te zostały przedstawione przeciwko tej osobie w postępowaniu karnym[90].

88. Podsumowując, EROD odnotowuje, że system narzędzi dochodzeniowych wykorzystywanych do pozyskiwania danych handlowych i innych informacji przechowywanych w rejestrach od korporacji w USA do celów ścigania przestępstw lub do celów interesu publicznego – w tym ograniczeń i zabezpieczeń dostępu – zapewnia kompleksowy, ale również złożony system środków, odzwierciedlający m.in. federalny charakter rządu USA.

89. W związku z tym można uznać, że system środków dochodzeniowych organów ścigania w USA zasadniczo spełnia wymogi konieczności i proporcjonalności w odniesieniu do praw podstawowych do życia prywatnego i ochrony danych.

3.1.3 Powinien istnieć niezależny mechanizm nadzoru

90. EROD odnotowuje fakt, że większość procedur opisanych w projekcie decyzji i w załączniku VI zakłada konieczność wydania przez sąd odpowiedniej decyzji, zanim organy uzyskają dostęp do danych (np. nakazy sądowe dotyczące urządzeń rejestrujących wybierane numery oraz urządzeń śledzących[91], nakazy sądowe dotyczące objęcia obserwacją zgodnie z federalną ustawą o podsłuchach[92], nakazy przeszukania zgodnie z art. 41 federalnego kodeksu postępowania karnego[93]). Wydaje się jednak, że nie wszystkie z nich wymagają udziału sądu a priori. Na przykład organy administracji cywilnej i regulacyjne „mogą wydawać wezwania"[94]. W takich przypadkach istnieje jednak możliwość kontroli

[88] Zob. przypis 146 w projekcie decyzji. W wyroku z 2018 r. Sąd Najwyższy USA potwierdził, że nakaz przeszukania lub wyjątek od nakazu są również wymagane, w przypadku gdy organy ścigania chcą uzyskać dostęp do historycznych rejestrów danych dotyczących lokalizacji telefonów komórkowych, które zapewniają kompleksowy przegląd informacji o przemieszczaniu się użytkownika, a także że użytkownik może mieć uzasadnione oczekiwania co do ochrony prywatności w odniesieniu do takich informacji (Timothy Ivory Carpenter przeciwko Stanom Zjednoczonym Ameryki, sprawa nr 16-402, 585 U.S. (2018)).
[89] Zob. załącznik VI do projektu decyzji, s. 2.
[90] Zob. motyw 90 projektu decyzji.
[91] Zob. motyw 92 projektu decyzji.
[92] Zob. załącznik VI do projektu decyzji, s. 3.
[93] Zob. motyw 90 projektu decyzji i załącznik VI do tego projektu, s. 3.
[94] Zob. załącznik VI do projektu decyzji, s. 4, a także motyw 91 projektu decyzji.

sądowej *ex post* zasadności wezwania, ponieważ „odbiorca wezwania administracyjnego może zaskarżyć wykonanie tego wezwania do sądu”[95].

91. Ponadto w projekcie decyzji opisano nadzór organów ścigania na szczeblu federalnym sprawowany przez różne organy, od wewnętrznej kontroli sprawowanej przez urzędników ds. ochrony prywatności i wolności obywatelskich po kontrolę zewnętrzną sprawowaną przez inspektora generalnego i specjalne komisje Kongresu Stanów Zjednoczonych[96]. Komisja Europejska przedstawia zróżnicowane i szczegółowe informacje oraz zasadniczo dochodzi do kompleksowych wniosków. W związku z tym EROD powstrzymuje się od powtarzania w niniejszej opinii ustaleń faktycznych i ocen.

92. Na podstawie dostępnych informacji EROD zauważa, że jeżeli chodzi o dostęp organów ścigania do danych będących w posiadaniu przedsiębiorstw w USA, funkcjonuje dość solidny niezależny mechanizm nadzoru.

3.1.4 Skuteczne środki ochrony prawnej muszą być dostępne dla osób fizycznych

93. Zgodnie z orzecznictwem TSUE osoba fizyczna musi mieć możliwość skorzystania ze skutecznego środka prawnego w celu zaspokojenia swoich praw, jeżeli uzna, że nie są lub nie były one przestrzegane. W wyroku w sprawie Schrems I TSUE wyjaśnił, że „uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 [K]arty. Artykuł 47 akapit pierwszy [K]arty stanowi bowiem, że każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka prawnego przed sądem, zgodnie z warunkami przewidzianymi w tym artykule”[97].

94. Projekt decyzji[98] i załącznik VI do tego projektu zawierają dalsze informacje dotyczące możliwych środków prawnych wynikających z przepisów prawa stanowionego, które byłyby dostępne dla osób fizycznych w przypadku niezgodnego z prawem uzyskania przez organy publiczne dostępu do ich danych.

95. W tym względzie zdaniem Komisji[99] tytuł 5 § 702 U.S.C. (ustawy o postępowaniu administracyjnym (APA)) stanowi, że osoba doznająca krzywdy w świetle prawa w wyniku działania agencji, dotknięta negatywnymi skutkami takiego działania lub poszkodowana w wyniku takiego działania może wystąpić o kontrolę sądową tych działań.

96. Ponadto ustawa o przechowywanych danych przekazywanych za pomocą łączności elektronicznej (przyjęta jako tytuł II ustawy o ochronie danych w łączności elektronicznej) stanowi, że każda osoba poszkodowana w wyniku naruszenia przepisów tego rozdziału (przy czym czyn stanowiący naruszenie jest popełniany w sposób świadomy lub umyślny), może w ramach powództwa cywilnego dochodzić roszczeń od osoby lub podmiotu, innych niż Stany Zjednoczone, które dopuściły się takiego naruszenia, stosownie do przypadku[100]. Co więcej, każda osoba poszkodowana w wyniku umyślnego naruszenia przepisów tego rozdziału lub rozdziału 119 może wytoczyć powództwo przed sądem dystryktowym

[95] Zob. załącznik VI do projektu decyzji, s. 4, a także motyw 91 projektu decyzji.
[96] Zob. motywy 103–106 projektu decyzji.
[97] Wyrok TSUE w sprawie Schrems I, pkt 95.
[98] Zob. motywy 107–112 projektu decyzji.
[99] Zob. motyw 109 projektu decyzji.
[100] Tytuł 18 § 2707 U.S.C.

Stanów Zjednoczonych przeciwko Stanom Zjednoczonym w celu uzyskania odszkodowania pieniężnego[101].

97. Projekt decyzji zawiera ponadto informacje na temat prawa wglądu do rejestrów prowadzonych przez agencję federalną wynikającego z ustawy o dostępie do informacji publicznej[102] oraz kilku innych ustaw, które przyznają osobom fizycznym prawo do wytoczenia powództwa przeciwko amerykańskiemu organowi lub urzędnikowi publicznemu w związku z przetwarzaniem ich danych osobowych, takich jak ustawa o podsłuchach, ustawa o oszustwach i nadużyciach komputerowych, federalna ustawa o roszczeniach z tytułu czynu niedozwolonego, ustawa o prawie do prywatności w kwestiach finansowych oraz ustawa o rzetelnej sprawozdawczości kredytowej[103].

98. EROD z zadowoleniem przyjmuje zatem wyjaśnienia Komisji dotyczące liczby prawnych środków dochodzenia roszczeń przez osoby fizyczne. EROD zwraca się również do Komisji o doprecyzowanie, czy te środki prawne umożliwiają osobom, których dane dotyczą, uzyskanie „dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych", zgodnie z wymogami TSUE.

3.1.5 Dalsze wykorzystywanie zebranych informacji

3.1.5.1 Dalsze wykorzystywanie przekazywanych danych, do których organy ścigania w USA mają dostęp

99. EROD z zadowoleniem odnotowuje, że w projekcie decyzji oceniono dalsze wykorzystywanie danych, do których organy ścigania w USA mają dostęp. EROD wyraża jednak ubolewanie, że podano tylko jeden przykład powodu, dla którego informacje mogą być dalej rozpowszechniane[104]. W związku z tym EROD zaleca Komisji uwzględnienie w projekcie decyzji dalszych wyjaśnień dotyczących zasad i zabezpieczeń mających zastosowanie do dalszego wykorzystywania danych, takich jak zasady i zabezpieczenia zawarte w ustawie o ochronie prywatności (tytuł 5 552a U.S.C.)[105].

3.1.5.2 Dalsze przekazywanie danych poza USA

100. Oprócz powyższego EROD zauważa, że Komisja Europejska odniosła się również do dalszego przekazywania danych przez organy ścigania w USA organom w państwach trzecich, ale ponownie jedynie w odniesieniu do ogólnych wytycznych prokuratora generalnego dotyczących krajowych operacji FBI[106]. Zdaniem EROD takie informacje i ocena są niezbędne, aby umożliwić kompleksową ocenę stopnia ochrony zapewnianej przez ramy legislacyjne i praktyki USA w odniesieniu do ujawniania i dalszego wykorzystywania informacji w skali międzynarodowej. Biorąc pod uwagę, że Komisja podała tylko jeden ograniczony przykład w odniesieniu ogólnie do kwestii dalszego przekazywania danych poza USA, EROD zwraca się do Komisji o dalsze doprecyzowanie mających zastosowanie przepisów i zabezpieczeń dotyczących dalszego przekazywania, dalszego wykorzystywania i ujawniania danych osobowych gromadzonych w USA do celów egzekwowania prawa, a następnie przekazywanych do państw trzecich, w tym w ramach umów międzynarodowych.

[101] Tytuł 18 § 2712 U.S.C.
[102] Zob. motyw 111 projektu decyzji.
[103] Zob. motyw 112 projektu decyzji.
[104] Zob. motyw 102 projektu decyzji.
[105] Zob. sekcja B pkt 1 lit. g) wytycznych prokuratora generalnego dotyczących krajowych operacji FBI, s. 36.
[106] Zob. motyw 102 projektu decyzji.

3.2 Dostęp do danych i ich wykorzystywanie do celów związanych z bezpieczeństwem narodowym

101. Tytułem uwagi ogólnej EROD przyznaje, że państwa posiadają szeroki margines swobody w kwestiach dotyczących bezpieczeństwa narodowego i potwierdził to również Europejski Trybunał Praw Człowieka. EROD przypomina również, że – jak podkreślono w zaktualizowanych zaleceniach dotyczących niezbędnych gwarancji europejskich dla środków nadzoru[107] – art. 6 ust. 3 Traktatu o Unii Europejskiej stanowi, że prawa podstawowe zagwarantowane w EKPC stanowią część prawa Unii jako zasady ogólne prawa. Jednak jak przypomina TSUE w swoim orzecznictwie, to jednak konwencja ta, do czasu przystąpienia do niej Unii, nie stanowi aktu prawnego formalnie obowiązującego w porządku prawnym Unii[108]. W związku z tym stopień ochrony praw podstawowych wymagany w art. 45 RODO należy określić na podstawie przepisów tego rozporządzenia w świetle praw podstawowych zawartych w Karcie praw podstawowych Unii Europejskiej. W związku z tym, zgodnie z art. 52 ust. 3 Karty praw podstawowych Unii Europejskiej, zawarte w niej prawa, które odpowiadają prawom zagwarantowanym w EKPC, mają takie samo znaczenie i zakres jak prawa przyznane przez tę konwencję. W rezultacie, jak przypomniał TSUE, orzecznictwo Europejskiego Trybunału Praw Człowieka dotyczące praw, które są również przewidziane w Karcie praw podstawowych UE, należy uwzględnić jako próg minimalnej ochrony w celu interpretacji odpowiadających im praw Karty praw podstawowych Unii Europejskiej[109]. Jednak zgodnie z art. 52 ust. 3 zdanie ostatnie Karty praw podstawowych Unii Europejskiej to „postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę".

102. Dlatego też w poniższej ocenie EROD uwzględniła orzecznictwo Europejskiego Trybunału Praw Człowieka w zakresie, w jakim Karta praw podstawowych Unii Europejskiej, zgodnie z wykładnią TSUE, nie przewiduje wyższego stopnia ochrony, który wymagałby spełnienia innych wymogów niż określone w orzecznictwie Europejskiego Trybunału Praw Człowieka.

103. W amerykańskich ramach prawnych szereg instrumentów prawnych przewiduje możliwość gromadzenia danych i ich dalszego udostępniania i przetwarzania przez amerykańskie agencje wywiadowcze.

104. Jak przypomniała Komisja Europejska w projekcie decyzji, „amerykańskie agencje wywiadowcze mogą ubiegać się o dostęp do danych osobowych, które zostały przekazane podmiotom mającym siedzibę w Stanach Zjednoczonych do celów związanych z bezpieczeństwem narodowym wyłącznie zgodnie z ustawą stanowiącą podstawę prawną, w szczególności zgodnie z ustawą o kontroli wywiadu lub przepisami prawa stanowionego zezwalającymi na dostęp z wykorzystaniem wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego"[110]. „Amerykańskie agencje wywiadowcze mają również możliwość gromadzenia danych osobowych poza Stanami Zjednoczonymi, przy czym może to obejmować dane osobowe, które są w tranzycie między Unią a Stanami Zjednoczonymi" na podstawie rozporządzenia wykonawczego 12333[111].

105. W odniesieniu do konkretnych systemów gromadzenia danych, w szczególności art. 702 ustawy o kontroli wywiadu i rozporządzenia wykonawczego 12333, w rozporządzeniu wykonawczym 14086

[107] Zob. Zalecenia 02/2020 EROD dotyczące niezbędnych gwarancji europejskich dla środków nadzoru.
[108] Zob. wyrok TSUE w sprawie Schrems II, pkt 98.
[109] Zob. wyrok TSUE w sprawie La Quadrature du Net, pkt 124.
[110] Zob. motyw 115 projektu decyzji.
[111] Zob. motyw 117 projektu decyzji.

przewiduje się obecnie nowe przepisy mające na celu wzmocnienie zabezpieczeń w odniesieniu do działań Stanów Zjednoczonych w obszarze rozpoznania radioelektronicznego. Te przepisy ogólne mają zastosowanie horyzontalnie i „muszą być wdrażane w ramach strategii politycznych i procedur agencji, które przekładają je na konkretne kierunki codziennej działalności”[112]. Rozporządzenie wykonawcze 14086 w znacznym stopniu zastąpiło poprzednią dyrektywę polityczną prezydenta nr 28 („PPD-28”)[113].

106. Aby ocenić ramy prawne mające zastosowanie do gromadzenia danych, dostępu do nich i ich dalszego przetwarzania do celów związanych z bezpieczeństwem narodowym, ważne jest zatem przeanalizowanie konkretnych ram prawnych regulujących gromadzenie danych w USA i poza nimi, tj. art. 702 ustawy o kontroli wywiadu i rozporządzenia wykonawczego 12333, które jako takie nie uległy zmianie od czasu poprzedniego przeglądu Tarczy Prywatności, biorąc pod uwagę fakt, że nowe rozporządzenie wykonawcze 14086 przewiduje zabezpieczenia, które należy wdrożyć również w kontekście gromadzenia danych na podstawie konkretnych tekstów prawnych, takich jak art. 702 ustawy o kontroli wywiadu i rozporządzenie wykonawcze 12333.

3.2.1 Gwarancja A – Przetwarzanie powinno być zgodne z prawem i oparte na jasnych, precyzyjnych i dostępnych zasadach

107. W celu dokonania oceny ogólnej struktury gromadzenia danych do celów związanych z bezpieczeństwem narodowym EROD pragnie przypomnieć pierwszą z czterech tzw. niezbędnych gwarancji europejskich, zgodnie z którą „przetwarzanie powinno opierać się na jasnych, precyzyjnych i dostępnych zasadach”[114].

108. Zgodnie z utrwalonym orzecznictwem TSUE wszelkie ograniczenia prawa do ochrony danych osobowych muszą być przewidziane ustawą, a podstawa prawna, która pozwala na ingerencję w to prawo, musi sama określać zakres ograniczenia wykonywania tego prawa[115]. Trybunał przypomniał także, że „[t]o uregulowanie musi być prawnie wiążące w prawie wewnętrznym”[116]. W tym względzie w orzecznictwie ETPC wyjaśniono, że termin „prawo” należy rozumieć w znaczeniu materialnym, a nie formalnym. Termin ten może obejmować wydane ustawy niższego rzędu oraz środki regulacyjne przyjęte przez organy regulacyjne ds. zawodów regulowanych w ramach niezależnych uprawnień do ustanawiania przepisów, nadanych im przez parlament, a także prawo niepisane. Aby być „prawem”, norma musi być co najmniej odpowiednio dostępna i sformułowana z wystarczającą precyzją[117].

[112] Zob. motyw 120 projektu decyzji.
[113] Rozporządzeniem wykonawczym uchylono PPD-28 z wyjątkiem sekcji 3 i 6 tej dyrektywy oraz załącznika niejawnego do tej dyrektywy, które pozostały w mocy. Zob. memorandum prezydenta w sprawie bezpieczeństwa narodowego z dnia 7 października 2022 r.
[114] Zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, przyjęte w dniu 10 listopada 2020 r. Zob. wyrok w sprawie Schrems II, pkt 175 i 180, a także opinia 1/15 (umowa dotycząca PNR między UE a Kanadą) z dnia 26 lipca 2017 r., pkt 139 i przytoczone tam orzecznictwo.
[115] Zob. wyrok TSUE w sprawie Schrems II, pkt 174–175 i przytoczone tam orzecznictwo. Zob. również – w odniesieniu do dostępu organów publicznych państw członkowskich – wyrok w sprawie C-623/17, Privacy International, ECLI:EU:C:2020:790 (zwany dalej „wyrokiem TSUE w sprawie Privacy International”), pkt 65; oraz wyrok TSUE w sprawie La Quadrature du Net, pkt 175.
[116] Wyrok TSUE w sprawie Privacy International, pkt 68.
[117] Wyrok ETPC w sprawie Sunday Times/Zjednoczone Królestwo (nr 1), z dnia 26 kwietnia 1979 r., CE:ECHR:1979:0426JUD000653874 (zwany dalej „wyrokiem ETPC w sprawie Sunday Times/Zjednoczone Królestwo nr 1”, pkt 49.

109. Wymagany stopień precyzji musi być mierzony w odniesieniu do zakresu ograniczenia danego prawa[118]. Ponadto w odniesieniu do „przewidywalności" przepisów prawa ETPC przypomniał w wyroku w sprawie Zakharov, że w kontekście niejawnych środków nadzoru takich jak przechwytywanie wiadomości „przewidywalność nie może oznaczać, że dana osoba powinna być w stanie przewidzieć, kiedy organy prawdopodobnie przechwycą jej wiadomości, tak aby mogła odpowiednio dostosować swoje zachowanie". Jasne i szczegółowe przepisy dotyczące niejawnych środków nadzoru są jednak niezbędne, aby zapobiec ryzyku arbitralności, w przypadku uprawnień organów wykonawczych realizowanych w sposób niejawny. „Prawo wewnętrzne musi być wystarczająco jasne, aby osoby fizyczne mogły uzyskać odpowiednie informacje na temat okoliczności i warunków, w których organy publiczne są uprawnione do stosowania tego rodzaju środków"[119].

110. Ponadto TSUE wyjaśnił, że ocena mającego zastosowanie prawa państwa trzeciego powinna koncentrować się na tym, czy osoby fizyczne mogą się na nie powoływać i przywoływać je przed sądem. Prawa przyznane osobom, których dane dotyczą, powinny być w szczególności egzekwowalne przed sądami, a osobom fizycznym należy zapewnić prawa egzekwowalne wobec organów publicznych[120], co nie miało miejsca w kontekście poprzedniej PPD-28. Rozporządzenie wykonawcze 14086, które – jak rozumie EROD – uznaje się za mające takie same skutki prawne w porządku prawnym USA jak PPD-28 (tj. wiążące dla władzy wykonawczej), przewiduje obecnie uprawnienia egzekwowalne wobec organów publicznych. Szczegółową ocenę nowych egzekwowalnych praw osób, których dane dotyczą, przedstawiono w sekcji dotyczącej środków dochodzenia roszczeń.

111. Motywy 114–152 projektu decyzji i załącznik VII zawierają podsumowanie niektórych aspektów obowiązujących ram prawnych, ograniczeń gromadzenia danych, ograniczeń zatrzymywania i rozpowszechniania danych, zgodności i nadzoru, przejrzystości i dochodzenia roszczeń. Amerykański system prawny dotyczący działań wywiadowczych składa się z szeregu różnych dokumentów, w tym sprawozdań, strategii politycznych i procedur poszczególnych agencji. W tym względzie ocena EROD koncentruje się na ograniczonej liczbie kwestii, które jej zdaniem mają kluczowe znaczenie.

112. Zgodnie z motywami 115–119 projektu decyzji dostęp amerykańskich organów bezpieczeństwa narodowego do przekazanych danych osobowych może mieć miejsce wyłącznie na podstawie ustawy o kontroli wywiadu, na podstawie innych przepisów prawa stanowionego (tytuł 12 § 3414 U.S.C., tytuł 15 § 1681u-1681v U.S.C. i tytuł 18 § 2709 U.S.C.) lub, w związku z danymi osobowymi będącymi w tranzycie, na podstawie rozporządzenia wykonawczego 12333. Z motywów 116 i 118 projektu decyzji wynika, że w odniesieniu do dostępu amerykańskich organów bezpieczeństwa narodowego do danych osobowych Komisja koncentruje swoją ocenę na art. 105, 302, 402, 501 i 702 ustawy o kontroli wywiadu (działania wywiadowcze ukierunkowane na osoby niebędące obywatelami ani rezydentami USA przebywające poza USA) oraz na rozporządzeniu wykonawczym 12333 (działania wywiadowcze dotyczące danych osobowych w tranzycie), które to przepisy uważa za najistotniejsze. Opinia EROD ogranicza się zatem do oceny tych przepisów dokonanej przez Komisję, z uwzględnieniem ograniczeń i zabezpieczeń określonych w rozporządzeniu wykonawczym 14086[121].

---

[118] Wyrok ETPC w sprawie Sunday Times/Zjednoczone Królestwo nr 1, pkt 49.

[119] Wyrok ETPC z dnia 4 grudnia 2015 r. w sprawie Zakharov/Rosja (zwany dalej „wyrokiem ETPC w sprawie Zakharov", pkt 229.

[120] Wyrok TSUE w sprawie Schrems II, pkt 181.

121 Rozporządzeniem wykonawczym uchylono PPD-28 z wyjątkiem sekcji 3 i 6 tej dyrektywy oraz załącznika niejawnego do tej dyrektywy, które pozostały w mocy. Zob. memorandum prezydenta w sprawie bezpieczeństwa narodowego z dnia 7 października 2022 r.

113. W tym względzie należy zauważyć, że wszystkie instrumenty prawne wymienione w projekcie decyzji są dostępne dla ogółu społeczeństwa (w USA i poza nimi) i udostępnione w internecie. Ponadto wymogi określone w rozporządzeniu wykonawczym są wiążące dla całej Wspólnoty Wywiadowczej[122] i mają zastosowanie przekrojowo do wszystkich działań służb wywiadowczych.

114. W rozporządzeniu wykonawczym 14086 nie zawarto definicji terminu „rozpoznanie radioelektroniczne". Rozporządzenie to zawiera odesłanie do definicji określonych w rozporządzeniu wykonawczym 12333 na potrzeby określenia zakresu wywiadu i kontrwywiadu, które są tam zdefiniowane szeroko. W tym względzie, choć twierdzono, że od czasu wprowadzenia ustawy o kontroli wywiadu rozporządzenie wykonawcze 12333 może być stosowane wyłącznie do gromadzenia danych poza terytorium USA, EROD przypomina, że samo rozporządzenie wykonawcze 12333, które pozostaje nienaruszone, nie zawiera wystarczająco szczegółowych przepisów dotyczących jego zakresu geograficznego, zakresu, w jakim dane mogą być gromadzone, zatrzymywane lub dalej rozpowszechniane, czy charakteru przestępstw, które mogą być przesłanką do rozpoczęcia działań nadzorczych, lub rodzaju informacji, które mogą być gromadzone lub wykorzystywane. Co do zasady wszelkie gromadzenie danych wywiadowczych wchodzące w zakres rozporządzenia wykonawczego 12333 może odbywać się wedle uznania Prezydenta USA[123]. W rozumieniu EROD głównym celem rozporządzenia wykonawczego 14086 jest jednak określenie ograniczeń w zakresie gromadzenia i przetwarzania danych osobowych w kontekście wywiadu, niezależnie od tego, z jakich programów nadzoru się korzysta i skąd pochodzą dane. EROD przyjmuje zatem, że dodatkowe zabezpieczenia przewidziane w rozporządzeniu wykonawczym 14086 mają również zastosowanie w kontekście programów nadzoru mających zastosowanie do danych osobowych będących w tranzycie, realizowanych zgodnie z rozporządzeniem wykonawczym 12333[124].

115. W związku z tym w rozporządzeniu wykonawczym 14086 wymieniono 12 prawnie uzasadnionych celów, którym powinno służyć gromadzenie danych w wyniku rozpoznania radioelektronicznego, oraz pięć celów, w odniesieniu do których nie wolno prowadzić gromadzenia danych w wyniku rozpoznania radioelektronicznego[125], a także sześć prawnie uzasadnionych celów dotyczących wykorzystania danych gromadzonych hurtowo[126]. Podczas gdy niektóre z nich są dość szczegółowe (np. „ratowanie zakładników"), inne mają bardziej ogólny charakter (np. „bezpieczeństwo globalne"). Rozporządzenie wykonawcze 14086 zawiera również wykaz zakazanych celów, który obejmuje w szczególności wyeliminowanie lub ograniczenie „prawnie uzasadnionych względów związanych z ochroną prywatności"[127]. W rozporządzeniu wykonawczym 14086 przewidziano również możliwość dodania przez Prezydenta Stanów Zjednoczonych do tego wykazu innych celów, w których gromadzenie danych jest dozwolone, przy czym na mocy decyzji Prezydenta cele te nie muszą zostać podane do wiadomości publicznej, jeżeli Prezydent uzna, że stanowiłoby to zagrożenie dla bezpieczeństwa narodowego Stanów Zjednoczonych[128]. Takie aktualizacje mogą być dozwolone wyłącznie „w świetle nowych wymogów bezpieczeństwa narodowego".

122 Zob. motyw 120 projektu decyzji.

123 Zgodnie z art. II konstytucji USA odpowiedzialność za zapewnienie bezpieczeństwa narodowego, w tym w szczególności gromadzenie danych wywiadowczych, spoczywa na Prezydencie, który pełni funkcję Zwierzchnika Sił Zbrojnych.

124 Zob. motyw 134 projektu decyzji.

125 Zob. sekcja 2 część b) pkt (ii) lit. A ppkt 1–5 rozporządzenia wykonawczego 14086.

126 Zob. motyw 134 projektu decyzji oraz sekcja 2 część c) pkt (ii) rozporządzenia wykonawczego 14086.

127 Zob. sekcja 2 część b) pkt (ii) lit. A ppkt 2 rozporządzenia wykonawczego 14086.

128 Zob. sekcja 2 część b) pkt (i) lit. B rozporządzenia wykonawczego 14086.

116. Agencje wywiadowcze nie mogą powoływać się na te cele same w sobie, aby uzasadnić gromadzenie danych w wyniku rozpoznania radioelektronicznego, lecz cele te muszą być dodatkowo poparte – w przypadku celów operacyjnych – bardziej konkretnymi priorytetami, w odniesieniu do których można gromadzić dane w wyniku rozpoznania radioelektronicznego. W rozporządzeniu wykonawczym 14086 szczegółowo określono procedurę zatwierdzania priorytetów, w odniesieniu do których można gromadzić dane w wyniku rozpoznania radioelektronicznego[129]. EROD rozumie, że proces określania zatwierdzonych priorytetów w zakresie wywiadu zasadniczo opiera się na decyzji Dyrektora Wspólnoty Wywiadowczej, i przyjmuje do wiadomości, że co do zasady proces ten powinien obejmować ocenę urzędnika ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych (CLPO), z którą to oceną dyrektor może się nie zgadzać, a wówczas „przy przedstawianiu Prezydentowi ram amerykańskich priorytetów wywiadowczych uwzględnia się ocenę urzędnika ds. ochrony wolności obywatelskich i opinie Dyrektora”[130].

117. EROD zauważa jednak również, że zgodnie z definicją „zatwierdzonego priorytetu wywiadowczego” taki priorytetowy status oznacza w przypadku „większości amerykańskich działań związanych z gromadzeniem danych w wyniku rozpoznania radioelektronicznego”[131] priorytet zatwierdzony zgodnie z sekcją 2 część b) pkt (iii) rozporządzenia wykonawczego (jak opisano w poprzednim punkcie). Proces zatwierdzenia może w niektórych przypadkach różnić się od tego procesu w „ograniczonych okolicznościach”, w którym to przypadku Prezydent lub szef jednej z jednostek Wspólnoty Wywiadowczej może ustalić priorytet „w zakresie, w jakim jest to możliwe”, zgodnie z kryteriami określonymi w tej samej sekcji 2 część b) pkt (iii) lit. A ppkt 1–3, która zawiera wymóg odpowiedniego uwzględnienia ochrony prywatności i wolności obywatelskich wszystkich osób, ale bez udziału urzędnika ds. ochrony wolności obywatelskich.

118. W rozporządzeniu wykonawczym 14086 podkreśla się ponadto, że „działania związane z gromadzeniem danych w wyniku rozpoznania radioelektronicznego powinny być w możliwie największym stopniu dostosowane” do realizacji zatwierdzonego priorytetu wywiadowczego oraz że „Wspólnota Wywiadowcza ocenia dostępność, wykonalność i stosowność innych, mniej inwazyjnych źródeł”, a także określa ogólne wymogi dotyczące konieczności i proporcjonalności[132].

119. Ponadto zgodnie z sekcją 5 część h) rozporządzenie wykonawcze 14086 uprawnia do wniesienia do CLPO kwalifikujących się skarg oraz do uzyskania kontroli decyzji CLPO przez Sąd Odwoławczy ds. Ochrony Danych zgodnie z mechanizmem dochodzenia roszczeń ustanowionym w sekcji 3 tego rozporządzenia.

120. Tekst ustawy o kontroli wywiadu wydaje się jaśniejszy i bardziej precyzyjny niż tekst rozporządzenia wykonawczego 12333 w odniesieniu do rodzaju operacji wywiadowczych, które mogą być dozwolone. Obecnie ustawa o kontroli wywiadu i rozporządzenie wykonawcze 12333 muszą być stosowane w świetle rozporządzenia wykonawczego 14086, w szczególności z uwzględnieniem między innymi zasad konieczności i proporcjonalności.

121. Wymogi określone w rozporządzeniu wykonawczym 14086 muszą być wdrażane w ramach strategii politycznych i procedur agencji, które przekładają je na konkretne kierunki codziennej działalności. W tym względzie rozporządzenie wykonawcze 14086 zapewnia amerykańskim agencjom

[129] Zob. motyw 129 projektu decyzji.
[130] Zob. sekcja 2 część b) pkt (iii) lit. B rozporządzenia wykonawczego 14086.
[131] Zob. sekcja 4 część n) rozporządzenia wykonawczego 14086.
[132] Zob. sekcja 2 część c) pkt (i) lit. A i B rozporządzenia wykonawczego 14086.

wywiadowczym maksymalnie rok na aktualizację ich obowiązujących strategii politycznych i procedur (tj. do 7 października 2023 r.) w celu dostosowania ich do wymogów tego rozporządzenia wykonawczego. Takie zaktualizowane strategie polityczne i procedury muszą być opracowywane w porozumieniu z Prokuratorem Generalnym, CLPO i Radą Nadzoru nad Ochroną Prywatności i Wolnościami Obywatelskimi (PLCOB) oraz w możliwie najszerszym zakresie podawane do wiadomości publicznej[133].

122. EROD z zadowoleniem przyjęłaby uzależnienie nie tylko wejścia w życie, ale również przyjęcia decyzji od m.in. przyjęcia przez wszystkie amerykańskie agencje wywiadowcze zaktualizowanych strategii politycznych i procedur wdrażania rozporządzenia wykonawczego 14086. EROD zaleca Komisji przeprowadzenie oceny tych zaktualizowanych strategii politycznych i procedur oraz przekazanie tej oceny EROD.

123. Ponadto w odniesieniu do zatrzymywania przekazywanych danych gromadzonych do celów związanych z bezpieczeństwem narodowym EROD zauważa, że rozporządzenie wykonawcze 14086 zapewnia, aby przepisy mające zastosowanie do danych osobowych osób będących obywatelami lub rezydentami USA miały również zastosowanie do danych osobowych osób niebędących obywatelami ani rezydentami USA[134]. Z projektu decyzji wynika, że przepisy te są przewidziane w art. 309 ustawy o zatwierdzeniu działań wywiadowczych na rok budżetowy 2015[135], w której ustanowiono maksymalny okres zatrzymywania informacji o niepublicznej łączności telefonicznej lub elektronicznej uzyskanych bez zgody danej osoby, wynoszący co do zasady pięć lat. EROD zaleca w tym względzie, aby Komisja zapewniła w decyzji większą jasność co do dokonanej w decyzji oceny przepisów dotyczących zatrzymywania mających zastosowanie do danych osobowych osób będących obywatelami lub rezydentami USA.

3.2.2 Gwarancja B – Należy wykazać konieczność i proporcjonalność w odniesieniu do prawnie uzasadnionych zamierzonych celów

3.2.2.1 Horyzontalne zabezpieczenia przewidziane w nowym rozporządzeniu wykonawczym 14086 – konieczność i proporcjonalność

124. Nowe rozporządzenie wykonawcze 14086, które zasadniczo zastępuje PPD-28, ma na celu zapewnienie przepisów służących wzmocnieniu zabezpieczenia w odniesieniu do działań Stanów Zjednoczonych w obszarze rozpoznania radioelektronicznego, które mają być dalej wdrażane przez jednostki Wspólnoty Wywiadowczej w ich wewnętrznych strategiach politycznych i procedurach.

125. Rozporządzeniem wykonawczym 14086 wprowadza się w prawie amerykańskim dwa nowe wymogi, które są zgodne z wymogami przypomnianymi przez TSUE w wyroku w sprawie Schrems II, a mianowicie, aby działania w obszarze rozpoznania radioelektronicznego były prowadzone wyłącznie w zakresie niezbędnym do gromadzenia danych w ramach zatwierdzonego priorytetu wywiadowczego oraz wyłącznie takim w zakresie i w taki sposób, który będzie proporcjonalny do zatwierdzonego priorytetu wywiadowczego[136].

126. EROD rozumie, że elementy te uwzględniono w celu odzwierciedlenia przewidzianych w prawie UE oraz w orzecznictwie TSUE i ETPC zasad konieczności i proporcjonalności, których celem jest

[133] Zob. sekcja 2 część c) pkt (iv) lit. B i C rozporządzenia wykonawczego 14086.
[134] Motyw 150 projektu decyzji.
[135] Przypis 272 w projekcie decyzji.
[136] Zob. sekcja 2 część a) pkt (ii) lit. A i B rozporządzenia wykonawczego 14086.

zapewnienie, aby gromadzenie i przetwarzanie danych ograniczało się do tego, co jest konieczne i proporcjonalne.

127. W tym względzie EROD przypomina o procesie przewidzianym w odniesieniu do zatwierdzania priorytetów wywiadowczych, a także o możliwym odstępstwie (zob. pkt 116 i 117).

128. Ponadto EROD zauważa, że te zasady konieczności i proporcjonalności przewidziane w rozporządzeniu wykonawczym będą musiały w ciągu roku zostać wdrożone i wprowadzone w życie w strategiach politycznych i procedurach każdej jednostki Wspólnoty Wywiadowczej[137].

3.2.2.2 Szczególne zabezpieczenia dotyczące gromadzenia danych w wyniku rozpoznania radioelektronicznego

129. EROD zauważa również, że w rozporządzeniu wykonawczym 14086 przewiduje się ograniczenia dotyczące celów, do których dane osobowe mogą i nie mogą być gromadzone w kontekście gromadzenia danych w wyniku rozpoznania radioelektronicznego[138].

130. EROD z zadowoleniem przyjmuje fakt, że w rozporządzeniu wykonawczym przewidziano, iż ukierunkowane gromadzenie danych powinno mieć większy priorytet niż hurtowe gromadzenie danych[139]. W kontekście gromadzenia danych w wyniku rozpoznania radioelektronicznego w rozporządzeniu wykonawczym przedstawiono wykaz 12 celów, do których można gromadzić dane i które muszą być dodatkowo uzasadnione priorytetami wywiadowczymi (zob. pkt 117), a także wykaz pięciu celów, do których nie wolno prowadzić działań związanych z gromadzeniem danych w wyniku rozpoznania radioelektronicznego[140]. Zasadniczo przepisy te stanowią gwarancję, że gromadzenie danych będzie realizowane tylko wówczas, gdy będzie konieczne.

131. Mimo to EROD przypomina, że w rozporządzeniu wykonawczym 14086 przewidziano również możliwość dodania przez Prezydenta Stanów Zjednoczonych do tego wykazu innych celów (zob. pkt 114 i 115)[141].

3.2.2.3 Szczególne zabezpieczenia dotyczące hurtowego gromadzenia danych

132. W wyroku w sprawie Schrems I TSUE podkreślił, że „ochrona prawa podstawowego do poszanowania życia prywatnego na poziomie Unii wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne”[142] i orzekł, że „uregulowanie pozwalające władzom publicznym na uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za naruszenie zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego, wynikającego z art. 7 [K]arty”.

133. W sprawie Schrems II[143], w odniesieniu do analizy hurtowego gromadzenia danych w związku ze skorelowanym brzmieniem rozporządzenia wykonawczego 12333 i PPD-28, a w szczególności w pkt 183–185, Trybunał podkreślił, jak przypomniano powyżej, że możliwość hurtowego gromadzenia danych, „która oznacza w ramach programów nadzoru mających podstawę w rozporządzeniu wykonawczym nr 12333 udzielenie dostępu do danych, które są »w tranzycie« w kierunku terytorium

[137] Zob. sekcja 2 część c) pkt (iv) lit. B rozporządzenia wykonawczego 14086.
[138] Zob. sekcja 2 część b) pkt (i) lit. A ppkt 1–12 rozporządzenia wykonawczego 14086.
[139] Zob. sekcja 2 część c) pkt (ii) lit. A rozporządzenia wykonawczego 14086.
[140] Zob. sekcja 2 część b) pkt (ii) lit. A ppkt 1–5 rozporządzenia wykonawczego 14086.
[141] Zob. sekcja 2 część b) pkt (i) lit. B rozporządzenia wykonawczego 14086.
[142] Wyrok TSUE w sprawie Schrems I, pkt 92.
[143] Zob. wyrok TSUE w sprawie Schrems II.

Stanów Zjednoczonych, przy czym dostęp ten nie jest przedmiotem jakiegokolwiek nadzoru sądowego, w żadnym razie nie stanowi uregulowania w sposób wystarczająco jasny i precyzyjny zakresu takiego »hurtowego« gromadzenia danych osobowych".

134. EROD zauważa zatem, że TSUE zasadniczo nie wykluczył hurtowego gromadzenia, ale uznał w wyroku w sprawie Schrems II, że aby takie hurtowe gromadzenie było zgodne z prawem, muszą istnieć wystarczająco jasne i precyzyjne ograniczenia, które pozwolą określić zakres takiego hurtowego gromadzenia.

135. EROD uznaje również, że oprócz zastąpienia PPD-28 rozporządzenie wykonawcze 14086 przewiduje nowe zabezpieczenia i ograniczenia gromadzenia i wykorzystywania danych gromadzonych poza USA, ponieważ ograniczenia wynikające z ustawy o kontroli wywiadu lub innych bardziej szczegółowych przepisów USA nie mają zastosowania.

136. W odniesieniu do hurtowego gromadzenia danych EROD przyjmuje do wiadomości, że zgodnie z rozporządzeniem wykonawczym 14086 hurtowe gromadzenie danych jest nadal dozwolone. EROD podkreśla, że definicja hurtowego gromadzenia danych pozostaje taka sama jak w nieobowiązującej już PPD-28, tj: „»hurtowe« gromadzenie danych w wyniku rozpoznania radioelektronicznego oznacza uprawnione gromadzenie dużych ilości danych z rozpoznania radioelektronicznego, które ze względów technicznych lub operacyjnych są pozyskiwane bez zastosowania wyróżników (na przykład bez użycia konkretnych identyfikatorów lub terminów umożliwiających selekcję)"[144].

137. Od czasu wydania wyroku w sprawie Schrems II Trybunał nie sprecyzował dokładnie zabezpieczeń wymaganych do hurtowego gromadzenia. EROD przypomina jednak, że ETPC wydał ważne decyzje dotyczące hurtowego gromadzenia i odpowiednich zabezpieczeń w tym kontekście.

138. EROD przypomina, że ponieważ hurtowe gromadzenie danych umożliwia gromadzenie dużych ilości danych bez zastosowania wyróżników, stwarza większe ryzyko dla osób fizycznych[145] niż ukierunkowane gromadzenie, w związku z czym wymaga wprowadzenia dodatkowych zabezpieczeń.

139. EROD zauważa również, że TSUE wypracował dalsze orzecznictwo dotyczące zatrzymywania danych o ruchu i danych dotyczących lokalizacji, a następnie dostępu do tych danych zatrzymywanych przez operatorów telekomunikacyjnych, w tym do celów związanych z bezpieczeństwem narodowym, które – choć nie można uznać, że mają bezpośrednie zastosowanie w tym kontekście – mogą być do pewnego stopnia istotne w odniesieniu do obecnej oceny hurtowego gromadzenia danych w kontekście rozporządzenia wykonawczego 12333.

1) <u>Ograniczenie celu</u>

140. Rozporządzenie wykonawcze stanowi, że hurtowe gromadzenie danych powinno odbywać się wyłącznie po ustaleniu, że „informacje niezbędne do realizacji zatwierdzonego priorytetu wywiadowczego nie mogą być w racjonalny sposób uzyskane w ramach gromadzenia ukierunkowanego"[146] oraz że „jednostka Wspólnoty Wywiadowczej musi stosować zasadne metody i środki techniczne w celu ograniczenia gromadzonych danych wyłącznie do tego, co jest konieczne do

[144] Zob. sekcja 4 część b) rozporządzenia wykonawczego 14086.

[145] Zob. np. wyrok ETPC (wielka izba) z dnia 25 maja 2021 r., Big Brother Watch i inni/Zjednoczone Królestwo (zwany dalej „wyrokiem ETPC w sprawie Big Brother Watch"), motyw 363, w którym ETPC – jak twierdzi – „nie jest przekonany, że pozyskiwanie powiązanych danych z łączności w ramach masowego przechwytywania jest siłą rzeczy mniej inwazyjne niż pozyskiwanie treści".

[146] Sekcja 2 część c) pkt (ii) lit. A rozporządzenia wykonawczego 14086.

realizacji zatwierdzonego priorytetu wywiadowczego, przy jednoczesnym ograniczeniu do minimum gromadzenia informacji nieistotnych”[147]. Oprócz tych zabezpieczeń EROD uznaje również, że wykorzystywanie hurtowo gromadzonych danych ma służyć do realizacji co najmniej jednego z sześciu wymienionych celów[148]. EROD podkreśla ponadto, że choć cele te są bardziej szczegółowe niż cele określone w nieobowiązującej już PPD-28, zasadniczo zastąpionej przez rozporządzenie wykonawcze 14086, skala takich możliwości gromadzenia danych pozostaje potencjalnie szeroka, tj. obejmuje duże ilości danych.

141. W tym miejscu EROD ponownie przypomina, że w rozporządzeniu wykonawczym 14086 przewidziano również możliwość dodania przez Prezydenta Stanów Zjednoczonych do tego wykazu innych celów (zob. pkt 115)[149].

2) Uprzednie niezależne zezwolenie

142. EROD podkreśla, że ETPC przywiązuje dużą wagę do uzyskania uprzedniego niezależnego zezwolenia w kontekście hurtowego gromadzenia danych do celów związanych z bezpieczeństwem narodowym. ETPC orzekł bowiem w szczególności, że „aby zminimalizować ryzyko nadużywania możliwości masowego przechwytywania, ETPC uważa, że proces ten musi podlegać »zabezpieczeniom typu 'end-to-end'«, co oznacza, że na szczeblu krajowym należy dokonać oceny konieczności i proporcjonalności podejmowanych środków na każdym etapie procesu, że takie masowe przechwytywanie powinno podlegać wymogowi uzyskania niezależnego zezwolenia już na początkowym etapie, gdy określa się przedmiot i zakres operacji, oraz że operacja powinna podlegać nadzorowi i niezależnemu przeglądowi *ex post*. Zdaniem ETPC są to podstawowe zabezpieczenia, które będą stanowić główny element każdego zgodnego z art. 8 systemu masowego przechwytywania”[150].

143. EROD odnotowuje również następujący punkt tego wyroku wielkiej izby, w którym ETPC podkreśla ponadto, że „przychyla się do stanowiska izby, że zezwolenie sądowe stanowi »ważne zabezpieczenie przed arbitralnością«, ale nie jest »niezbędnym wymogiem« (zob. pkt 318–320 wyroku izby). Niemniej jednak masowe przechwytywanie podlega zezwoleniu wydanemu przez niezależny organ; tj. organ niezależny od władzy wykonawczej”[151].

144. W tym kontekście EROD zauważa, że rozporządzenie wykonawcze nie przewiduje takiego niezależnego uprzedniego zezwolenia na hurtowe gromadzenie oraz że nie jest to również przewidziane w rozporządzeniu wykonawczym 12333 (zob. sekcja poniżej dotycząca rozporządzenia wykonawczego 12333).

3) Przepisy dotyczące zatrzymywania

145. EROD przypomina, że innym ważnym zestawem zabezpieczeń są przepisy dotyczące okresu gromadzenia i zatrzymywania danych. W tym względzie ETPC podkreślił, że „prawo krajowe powinno określać ograniczenie czasu trwania przechwytywania, procedurę analizowania, wykorzystywania i przechowywania pozyskanych danych, środki ostrożności, które należy stosować przy przekazywaniu danych innym stronom, oraz okoliczności, w których przechwycone dane mogą lub muszą zostać

[147] Sekcja 2 część c) pkt (ii) lit. A rozporządzenia wykonawczego 14086.
[148] Sekcja 2 część c) pkt (ii) lit. B rozporządzenia wykonawczego 14086.
[149] Zob. sekcja 2 część c) pkt (ii) lit. C rozporządzenia wykonawczego 14086.
[150] Zob. wyrok ETPC w sprawie Big Brother Watch, pkt 350.
[151] Zob. wyrok ETPC w sprawie Big Brother Watch, pkt 351.

usunięte lub zniszczone”[152], ponieważ zabezpieczenia te „są równie istotne w przypadku masowego przechwytywania”[153].

146. W tym względzie EROD rozumie, że rozporządzenie wykonawcze ustanawia przepisy dotyczące zatrzymywania danych osobowych gromadzonych w wyniku rozpoznania radioelektronicznego, w tym gromadzonych hurtowo[154]. EROD zauważa, że zgodnie z sekcją 2 część c) pkt (iii) lit. A rozporządzenia wykonawczego 14086 każda jednostka Wspólnoty Wywiadowczej, która przetwarza dane osobowe zgromadzone w wyniku rozpoznania radioelektronicznego, ustanawia i stosuje strategie polityczne i procedury mające na celu ograniczenie do minimum rozpowszechniania i zatrzymywania danych osobowych gromadzonych w wyniku rozpoznania radioelektronicznego. Przepisy te nie przewidują jednak konkretnego okresu zatrzymywania danych, lecz odnoszą się zasadniczo do tych samych mających zastosowanie przepisów w zakresie zatrzymywania danych dotyczących osób będących obywatelami lub rezydentami USA oraz do sytuacji, w których nie dokonano ostatecznego ustalenia dotyczącego zatrzymywania danych. W związku z tym EROD jest zaniepokojona faktem, że te okresy zatrzymywania, podobnie jak w przypadku ukierunkowanego gromadzenia danych (zob. pkt 122), nie są jasno określone we wspomnianym rozporządzeniu wykonawczym w odniesieniu do danych gromadzonych hurtowo. Wzywa Komisję do tego, by udostępniła swoją ocenę konieczności i proporcjonalności okresów zatrzymywania danych mających zastosowanie do osób będących obywatelami lub rezydentami USA oraz dostępne informacje dotyczące okresów zatrzymywania stosowanych w praktyce, w przypadku gdy w prawie USA nie dokonano ostatecznego ustalenia dotyczącego zatrzymywania danych, ponieważ w obecnym stanie projekt decyzji ogranicza się do przypomnienia tej ogólnej zasady w jednym krótkim akapicie[155] i w przypisie[156], co nie pozwala na ustalenie, czy te okresy zatrzymywania danych są konieczne i proporcjonalne. Ponieważ, jak podkreślił ETPC, jest to kluczowe zabezpieczenie dla osób, których dane dotyczą, aby mogły one wykonywać swoje prawa w kontekście, w którym w celu gromadzenia ich danych stosuje się szczególnie inwazyjny środek, EROD wzywa Komisję Europejską do dalszego doprecyzowania poszczególnych okresów zatrzymywania danych w praktyce.

4) <u>Zabezpieczenia dotyczące „rozpowszechniania”</u>

147. EROD przypomina ponadto, że z myślą o zapewnieniu skuteczności w kwestii konieczności i proporcjonalności oraz zasady ograniczenia celu ETPC uznał również znaczenie przepisów prawa dotyczących dalszego rozpowszechniania gromadzonych danych, w tym w kontekście hurtowego gromadzenia danych[157].

148. Sekcja 2 część c) pkt (iii) lit. A ppkt 1 lit. c) rozporządzenia wykonawczego 14086 stanowi, że informacje dotyczące osób niebędących obywatelami ani rezydentami USA, które zostały zgromadzone w ramach działań w obszarze rozpoznania radioelektronicznego, mogą być rozpowszechniane wyłącznie wtedy, gdy upoważniona i odpowiednio przeszkolona osoba ma uzasadnione przekonanie, że dane osobowe będą odpowiednio chronione i że ich odbiorca ma dostęp do informacji zgodnie z zasadą ograniczonego dostępu.

[152] Zob. wyrok ETPC w sprawie Big Brother Watch, pkt 348.
[153] Zob. wyrok ETPC w sprawie Big Brother Watch, pkt 348.
[154] Zob. sekcja 2 część c) pkt (iii) lit. A ppkt 2 lit. a)–c) rozporządzenia wykonawczego 14086.
[155] Zob. pkt 150 projektu decyzji.
[156] Zob. przypis 271 w projekcie decyzji.
[157] Zob. wyrok ETPC w sprawie Big Brother Watch, pkt 348.

149. Mając to na uwadze, EROD rozumie, że przepisy dotyczące rozpowszechniania określone w rozporządzeniu wykonawczym 14086 nie przewidują wyraźnego zakazu rozpowszechniania do celów innych niż związane z bezpieczeństwem narodowym w przypadku rozpowszechniania wśród amerykańskich właściwych organów[158]. EROD wzywa Komisję do doprecyzowania mających zastosowanie przepisów i zabezpieczeń w tym przypadku.

150. W związku z powyższym EROD jest zaniepokojona faktem, że dane uzyskane przez właściwe organy Wspólnoty Wywiadowczej mogłyby być następnie rozpowszechniane wśród właściwych organów USA do celów zwalczania przestępczości, w tym poważnych przestępstw, w kontekście postępowań w sprawach karnych, co jest równoważne z zapewnieniem organom ścigania, bez żadnych dalszych szczególnych ograniczeń, możliwości pozyskania danych, których nie mogłyby gromadzić bezpośrednio, i wzywa Komisję do dalszej oceny tej kwestii.

151. W szczególnym kontekście dalszego przekazywania danych (rozpowszechniania wśród odbiorców spoza rządu Stanów Zjednoczonych, w tym do rządu innego państwa lub organizacji międzynarodowej[159]) EROD przypomina, że jej zdaniem należy utrzymać ochronę danych również w kontekście dalszego przekazywania, w tym w dziedzinie bezpieczeństwa narodowego[160].

152. W tym względzie rozporządzenie wykonawcze przewiduje pewne zabezpieczenia, a mianowicie wymóg należytego uwzględnienia przed rozpowszechnieniem danych celu rozpowszechniania – choć nie wymaga się wyraźnie, by celem rozpowszechniania była również ochrona bezpieczeństwa narodowego – charakteru i zakresu rozpowszechnianych danych osobowych oraz potencjalnego szkodliwego wpływu na daną osobę lub dane osoby.

153. Chociaż EROD przyznaje, że niektóre z tych zabezpieczeń, w szczególności uwzględnienie „potencjalnego szkodliwego wpływu”[161] na osoby, których dane dotyczą, odzwierciedlają niektóre wymogi ETPC, podkreśla ona również, że ETPC wymaga ponadto, aby prawnie wiążący obowiązek „analizowania i ustalania, czy zagraniczny odbiorca danych wywiadowczych zapewnia akceptowalny minimalny poziom zabezpieczeń”[162], którego EROD nie stwierdza wyraźnie w przepisach rozporządzenia wykonawczego dotyczących rozpowszechniania danych wśród odbiorców zagranicznych. Wobec tego EROD zwraca się do Komisji o dalszą ocenę tej kwestii.

154. EROD odnotowuje również, że Komisja Europejska nie uwzględniła w swojej ocenie faktu istnienia umów międzynarodowych zawartych z państwami trzecimi lub organizacjami międzynarodowymi, które to umowy mogą zawierać postanowienia szczegółowe dotyczące międzynarodowego przekazywania danych osobowych państwom trzecim przez służby wywiadowcze. EROD uważa, że zawarcie dwustronnych lub wielostronnych umów z państwami trzecimi w celu współpracy wywiadowczej prawdopodobnie wpłynie na oceniane ramy prawne ochrony danych.

155. EROD zwraca się zatem do Komisji Europejskiej o wyjaśnienie, czy takie umowy istnieją, na jakich warunkach można je zawrzeć, a także o ocenę, czy postanowienia umów międzynarodowych mogą wpływać na stopień ochrony danych osobowych przekazywanych z EOG zapewniony przez ramy

[158] Zob. sekcja 2 część c) pkt (iii) lit. A ppkt 1 rozporządzenia wykonawczego 14086.
[159] Zob. w szczególności sekcja 2 część c) pkt (iii) lit. A ppkt 1 lit. d) rozporządzenia wykonawczego 14086.
[160] Zob. np. EROD, Opinia 14/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia (UE) 2016/679 w sprawie odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie, przyjęta w dniu 13 kwietnia 2021 r., sekcje 4.3.2.1 i 4.3.2.2.
[161] Zob. sekcja 2 część c) pkt (iii) lit. A ppkt 1 lit. d) rozporządzenia wykonawczego 14086.
[162] Zob. wyrok ETPC (wielka izba) z dnia 25 maja 2021 r., w sprawie Centrum För Rättvisa/Szwecja, pkt 326.

legislacyjne i praktyki ustawodawcze w odniesieniu do dalszego przekazywania danych do celów związanych z bezpieczeństwem narodowym.

5) Tymczasowe hurtowe gromadzenie danych w celu wsparcia początkowej fazy technicznej ukierunkowanego gromadzenia

156. EROD przypomina, że w kontekście ostatniego wspólnego przeglądu Tarczy Prywatności dyskusje koncentrowały się głównie na interpretacji i stosowaniu dodatkowej podstawy (sytuacji/scenariusza) hurtowego gromadzenia przewidzianych w pierwszym zdaniu przypisu 5 w sekcji 2 PPD-28, w którym stwierdzono, że „ograniczenia zawarte w tej sekcji nie mają zastosowania do danych z rozpoznania radioelektronicznego, które są tymczasowo pozyskiwane w celu ułatwienia ukierunkowanego gromadzenia". Władze USA wyjaśniły wówczas znaczenie „danych z rozpoznania radioelektronicznego, które są tymczasowo pozyskiwane w celu ułatwienia ukierunkowanego gromadzenia". Na podstawie tych dyskusji EROD zrozumiała, że przypis ten oznacza, iż dane mogą być gromadzone hurtowo – i niezależnie od przewidzianych sześciu celów – jeżeli są gromadzone tymczasowo, w celu ustalenia identyfikatora dla określonego celu. Stanowiłoby to zatem dodatkową podstawę do hurtowego gromadzenia danych i w tym przypadku nadal obowiązywałyby jedynie ogólne zasady określone w sekcji 1 PPD-28. Jak przypomniano powyżej, w wyroku w sprawie Schrems II TSUE uznał, że łącznie rozporządzenie wykonawcze 12333 i PPD-28 w odniesieniu do hurtowego gromadzenia danych nie stanowią „uregulowania w sposób wystarczająco jasny i precyzyjny zakresu takiego »hurtowego« gromadzenia danych osobowych"[163].

157. EROD zauważa, że odstępstwo umożliwiające tego rodzaju hurtowe gromadzenie jest nadal przewidziane w rozporządzeniu wykonawczym 14086[164]; z zadowoleniem przyjmuje jednak fakt, że odstępstwo to zostało zawężone w porównaniu z tym, co przewidziano w PPD-28, oraz że w rozporządzeniu wykonawczym 14086 przewidziano dodatkowe zabezpieczenia.

158. EROD rozumie, że w nowym rozporządzeniu wykonawczym 14086 przewiduje się zabezpieczenia, które nadal mają zastosowanie w kontekście tego rodzaju tymczasowego hurtowego gromadzenia na potrzeby fazy technicznej, w szczególności ogólne zasady konieczności i proporcjonalności w odniesieniu do zatwierdzonego priorytetu wywiadowczego, gdy dane są pozyskiwane bez zastosowania wyróżników przed ukierunkowanym gromadzeniem (sekcja 2 część a)–b) i sekcja 2 część c) pkt (i) rozporządzenia wykonawczego 14086). EROD rozumie również, że takie hurtowe gromadzenie danych na potrzeby późniejszego ukierunkowanego gromadzenia danych w wyniku rozpoznania radioelektronicznego podlega także dodatkowym zabezpieczeniom przewidzianym w podsekcji 2 część c) pkt (iii) i następnych[165].

159. EROD przypomina jednak również – zob. pkt 117 powyżej – że w definicji „zatwierdzonego priorytetu wywiadowczego" przewiduje się procedurę odstępstwa bez udziału urzędnika ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych.

160. EROD w dalszym ciągu zauważa jednak, że zabezpieczenia zawarte w podsekcji dotyczącej hurtowego gromadzenia danych nie mają zastosowania do tymczasowego hurtowego gromadzenia danych wykorzystywanych do wsparcia początkowej fazy technicznej ukierunkowanego gromadzenia danych w wyniku rozpoznania radioelektronicznego, jak określono w sekcji 2 część c) pkt (ii) lit. D rozporządzenia wykonawczego 14086, co w szczególności oznacza, że w tym kontekście dane

[163] Wyrok TSUE w sprawie Schrems II, pkt 183.
[164] Zob. sekcja 2 część c) pkt (ii) lit. D rozporządzenia wykonawczego 14086 oraz przypis 226 w projekcie decyzji.
[165] Więcej informacji na temat poszczególnych elementów tych przepisów można znaleźć w poprzednich sekcjach.

gromadzone hurtowo mogą być wykorzystywane do celów innych niż wymienione w podsekcji 2 część c) pkt (ii). EROD z zadowoleniem przyjęłaby doprecyzowanie w projekcie decyzji celów, do których można wykorzystać dane gromadzone hurtowo w tym kontekście, a także kwestii stosowania ograniczeń określonych w podsekcji 2 część c) pkt (i) w odniesieniu do gromadzenia danych w wyniku rozpoznania radioelektronicznego w ujęciu ogólnym (tj. wyłącznie do prawnie uzasadnionych celów wymienionych w tym przepisie) w kontekście tymczasowego hurtowego gromadzenia danych, o którym mowa w projekcie decyzji.

161. Podsumowując, EROD podkreśla także, że to odstępstwo dotyczące tymczasowego hurtowego gromadzenia danych na potrzeby ukierunkowanego gromadzenia oraz pozostałych zabezpieczeń, które należy stosować, pozostaje niejasne, w szczególności w kwestii tego, jakie zabezpieczenia przewidziane w rozporządzeniu wykonawczym 14086 i na którym etapie miałyby zastosowanie (hurtowego gromadzenia, dalszego ukierunkowanego gromadzenia), oraz wzywa Komisję do dalszej oceny tych elementów, a także do oceny tych aspektów w praktyce w przyszłych wspólnych przeglądach.

162. Ponadto EROD ubolewa również nad tym, że choć termin „tymczasowo" został nieco bardziej doprecyzowany w rozporządzeniu wykonawczym, niż to miało miejsce w PPD-28, w opinii EROD nadal – jak się wydaje – oznacza on, że dopóki namierzana osoba nie zostanie zidentyfikowana, można kontynuować hurtowe gromadzenie danych. W tym względzie EROD przypomina o konieczności ustanowienia jasnych i precyzyjnych przepisów, a także podkreśla w tym miejscu, że takie przepisy stanowią kluczowe zabezpieczenie dla osób, których dane dotyczą.

163. Podsumowując, w odniesieniu do zabezpieczeń mających zastosowanie do hurtowego gromadzenia danych EROD jest nadal zaniepokojona faktem, że choć w rozporządzeniu wykonawczym 14086 przewidziano dodatkowe zabezpieczenia, w dalszym ciągu dopuszcza się możliwość hurtowego gromadzenia danych, tj. bez zastosowania wyróżników, przy braku kluczowych zabezpieczeń takich jak uprzednia zgoda na gromadzenie tych danych – w tym w przypadku tymczasowego gromadzenia danych na potrzeby fazy technicznej – biorąc również pod uwagę potrzebę dalszych wyjaśnień i wyrażone obawy dotyczące ścisłego ograniczenia celu w odniesieniu do późniejszego dostępu do danych, jasnych i rygorystycznych przepisów dotyczących zatrzymywania danych oraz bardziej rygorystycznych zabezpieczeń dotyczących rozpowszechniania danych gromadzonych hurtowo, w tym w kontekście dalszego przekazywania danych.

164. Co do zasady EROD podkreśla, że wspomniane powyżej orzeczenie ETPC jest kolejnym potwierdzeniem znaczenia kompleksowego nadzoru ze strony niezależnych organów nadzorczych. EROD zaznacza, że niezależny nadzór na wszystkich etapach procesu dostępu organów rządowych do celów związanych z bezpieczeństwem narodowym stanowi ważne zabezpieczenie przed arbitralnymi środkami nadzoru, a tym samym służy ocenie odpowiedniego stopnia ochrony danych. Gwarancja niezależności organów nadzorczych w rozumieniu art. 8 ust. 3 Karty ma na celu zapewnienie efektywnego i rzetelnego monitorowana zgodności z przepisami dotyczącymi ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych. Ma to zastosowanie w szczególności w sytuacji, gdy ze względu na charakter niejawnego nadzoru określona osoba nie może wnieść o kontrolę ani bezpośrednio uczestniczyć w jakimkolwiek postępowaniu odwoławczym przed zastosowaniem lub w trakcie stosowania środka nadzoru.

165. EROD przypomina, że jej zdaniem ocena odpowiedniości zależy od wszystkich okoliczności sprawy, w szczególności od skuteczności nadzoru *ex post* i środków dochodzenia roszczeń przewidzianych w ramach prawnych.

3.2.2.4 Ramy prawne regulujące specjalne gromadzenie danych do celów związanych z bezpieczeństwem narodowym przez jednostki Wspólnoty Wywiadowczej na terytorium USA i poza nim

166. W wyroku w sprawie Schrems II TSUE podkreślił w odniesieniu do art. 702 ustawy o kontroli wywiadu, że z jego treści „nie można w żaden sposób wyprowadzić wniosku o istnieniu jakichś ograniczeń ustanowionego w nim uprawnienia odnoszącego się do wdrażania programów nadzoru do celów wywiadu zagranicznego, ani też gwarancji przysługujących potencjalnie objętym tymi programami osobom nieposiadającym obywatelstwa amerykańskiego”[166]. Skłoniło to Trybunał do stwierdzenia, że „w tych okolicznościach [...] za pomocą tego uregulowania nie można zapewnić stopnia ochrony merytorycznie równoważnego temu gwarantowanemu w [K]arcie [...], zgodnie z którą podstawa prawna umożliwiająca ingerencje w prawa podstawowe powinna – aby spełniać wymóg proporcjonalności – sama określić zakres ograniczenia wykonywania danego prawa oraz przewidywać jasne i precyzyjne zasady dotyczące zakresu i stosowania danego środka oraz ustanawiać pewne wymogi minimalne.”[167].

167. Trybunał zauważył, że rozporządzenie wykonawcze 12333 „nie przyznaje praw, które mogłyby być egzekwowalne wobec władz amerykańskich przed sądami”[168], oraz stwierdził, że „w ramach programów nadzoru mających podstawę w rozporządzeniu wykonawczym nr 12333 udzielenie dostępu do danych, które są »w tranzycie« w kierunku terytorium Stanów Zjednoczonych, przy czym dostęp ten nie jest przedmiotem jakiegokolwiek nadzoru sądowego, [możliwość ta] w żadnym razie nie stanowi uregulowania w sposób wystarczająco jasny i precyzyjny zakresu takiego »hurtowego« gromadzenia danych osobowych”[169], przy czym opierał się na analizie warunków, na jakich hurtowe gromadzenie danych może się odbywać zgodnie z tym rozporządzeniem w połączeniu z PPD-28.

168. W odniesieniu do tych konkretnych systemów gromadzenia danych w rozporządzeniu wykonawczym 14086 przewiduje się obecnie nowe przepisy.

3.2.2.4.1 Gromadzenie danych do celów związanych z bezpieczeństwem narodowym na podstawie art. 702

169. EROD przypomina, że w ostatnim sprawozdaniu PCLOB z zadowoleniem przyjęto ustalenia dotyczące art. 702 ustawy o kontroli wywiadu[170], zgodnie z którymi „w praktyce »osoby niebędące obywatelami ani rezydentami USA« również korzystają z ograniczeń dostępu i zatrzymywania wymaganych w ramach procedur minimalizacji danych lub ukierunkowania gromadzenia stosowanych przez poszczególne agencje ze względu na koszty i trudności związane z identyfikowaniem i usuwaniem informacji o osobach będących obywatelami lub rezydentami USA w przypadku dużej ilości danych, co oznacza, że zazwyczaj cały zbiór danych jest przetwarzany zgodnie z wyższymi standardami amerykańskimi w zakresie danych”.

170. Zgodnie z tymi ustaleniami „w ramach programu wiadomości nie są przechwytywane hurtowo”. Ustalenia te potwierdzono w sprawozdaniach z przejrzystości statystycznej za lata 2014 i 2021 wydanych przez Urząd Dyrektora Krajowych Służb Wywiadowczych. Ponadto, jak wynika ze

[166] Zob. wyrok TSUE w sprawie Schrems II, pkt 180.
[167] Zob. wyrok TSUE w sprawie Schrems II, pkt 180.
[168] Zob. wyrok TSUE w sprawie Schrems II, pkt 182.
[169] Zob. wyrok TSUE w sprawie Schrems II, pkt 183.
[170] Zob. sprawozdanie PCLOB w sprawie programu nadzoru prowadzonego na podstawie art. 702 ustawy o kontroli wywiadu, s. 100.

sprawozdania PCLOB, do ukierunkowania nadzoru stosuje się „określone selektory", takie jak adres e-mail lub numer telefonu.

171. EROD przypomina jednak również, że jednocześnie w kontekście art. 702 wyjaśniono podczas ostatniego przeglądu Tarczy Prywatności, że określenie „osoba", odnoszące się do przyszłej namierzanej osoby, może obejmować kilka osób korzystających z tego samego identyfikatora, pod warunkiem że wszystkie te osoby są osobami niebędącymi obywatelami ani rezydentami USA i spełniają mające zastosowanie kryteria dotyczące ukierunkowywania na nie działań w tym zakresie. EROD przypomina również, że podczas trzeciego rocznego wspólnego przeglądu Tarczy Prywatności w 2019 r. wezwano do przedstawienia dalszych wyjaśnień w kontekście programu UPSTREAM, aby wykluczyć, że masowy i bezkrytyczny dostęp do danych osobowych osób niebędących obywatelami ani rezydentami USA ma miejsce[171].

172. Ponadto EROD przypomina, że fakt, iż gromadzenie danych na podstawie art. 702 ustawy o kontroli wywiadu jest uzasadnione tym, że „istotnym celem gromadzenia informacji jest pozyskanie zagranicznych informacji wywiadowczych", nadal pozostawia pewną niepewność co do ograniczenia celu i konieczności. EROD zauważa jednak, że zgodnie z sekcją 2 część a) lit. A i B rozporządzenia wykonawczego 14086 działania w obszarze rozpoznania radioelektronicznego mogą być prowadzone wyłącznie po ustaleniu, że działania te są niezbędne do realizacji zatwierdzonego priorytetu i wyłącznie takim w zakresie i w taki sposób, który będzie proporcjonalny do takiego priorytetu, oraz że działania te muszą być w możliwie największym stopniu dostosowane do realizacji zatwierdzonego priorytetu, z należytym uwzględnieniem istotnych czynników, takich jak inwazyjność gromadzenia danych czy wrażliwość danych, i nie mogą w nieproporcjonalny sposób wpływać na ochronę prywatności i wolności obywatelskich. EROD oczekuje jednak doprecyzowania, w jaki sposób zostanie to konkretnie wdrożone i wprowadzone w życie, w tym w kontekście stosowania art. 702 ustawy o kontroli wywiadu.

173. W związku z tym, wobec braku bezpośredniego dostępu do tych informacji dla EROD, EROD wezwała do przeprowadzenia niezależnej oceny konieczności i proporcjonalności definicji terminu „namierzane osoby" oraz pojęcia wywiadu w rozumieniu art. 702 ustawy o kontroli wywiadu (w tym w kontekście programu UPSTREAM) po jego odnowieniu. EROD uważa, że jej poprzednie wezwanie do dalszej niezależnej oceny procesu stosowania selektorów w konkretnych przypadkach („określanie selektorów"), a także do przedstawienia dalszych wyjaśnień w kontekście programu UPSTREAM jest w dalszym ciągu ważne. W związku z tym, biorąc pod uwagę nowe rozporządzenie wykonawcze 14086, EROD wzywa do przedstawienia dodatkowych informacji, aby również móc ocenić i monitorować, w jaki sposób i w jakim stopniu nowo wprowadzone zasady konieczności i proporcjonalności będą stosowane w praktyce w tym kontekście, a także oczekuje, że zostanie to również ocenione w kontekście przyszłych wspólnych przeglądów.

174. EROD z zadowoleniem przyjmuje fakt, że w pełni funkcjonalna Rada Nadzoru nad Ochroną Prywatności i Wolnościami Obywatelskimi (PCLOB), jako niezależna agencja nadzoru, podjęła decyzję o przeprowadzeniu „projektu kontroli w celu zbadania programu nadzoru realizowanego przez struktury władzy wykonawczej zgodnie z art. 702 ustawy o kontroli wywiadu w oczekiwaniu na datę wygaśnięcia art. 702 w grudniu 2023 r. oraz zbliżającą się debatę publiczną i kongresową w sprawie

[171] Zob. sprawozdanie z trzeciego wspólnego przeglądu, pkt 83, s. 17.

jego odnowienia”[172]. EROD z zadowoleniem przyjmuje również fakt, że „przegląd obejmuje wybrane cele szczegółowe dochodzenia, w tym m.in. zapytania osób będących obywatelami lub rezydentami USA o informacje zgromadzone na podstawie art. 702 oraz gromadzenie danych a ramach programu UPSTREAM na podstawie art. 702”[173], a także „obejmuje ocenę przeszłej i prognozowanej wartości i skuteczności programu, jak również adekwatności istniejących zabezpieczeń w zakresie ochrony prywatności i wolności obywatelskich”[174]. W związku z tym EROD podkreśla, że dostęp do ustaleń PCLOB zawartych w tym sprawozdaniu dotyczącym art. 702 jest konieczny do odpowiedniej i kompleksowej oceny zabezpieczeń prywatności zapewnianych i stosowanych w kontekście tego programu nadzoru.

175. Biorąc pod uwagę nowe rozporządzenie wykonawcze 14086, EROD wzywa ponadto do przedstawienia dodatkowych informacji, aby również móc ocenić i monitorować, w jaki sposób i w jakim stopniu nowo wprowadzone zasady konieczności i proporcjonalności, a także pozostałe zabezpieczenia przewidziane w tym akcie będą stosowane w praktyce w tym kontekście.

3.2.2.4.2 Gromadzenie danych do celów związanych z bezpieczeństwem narodowym na podstawie rozporządzenia wykonawczego 12333

176. Jak stwierdził TSUE w wyroku w sprawie Schrems II, analiza przepisów państwa trzeciego, w odniesieniu do których rozważana jest odpowiedniość, nie powinna ograniczać się do przepisów i praktyk umożliwiających nadzór w granicach fizycznych tego państwa, ale powinna również obejmować analizę podstaw prawnych w prawie tego państwa trzeciego, które umożliwiają mu prowadzenie nadzoru poza jego terytorium w odniesieniu do danych UE. Niezbędne ograniczenia dostępu organów rządowych do danych powinny obejmować dane osobowe „w tranzycie” do danego państwa, w odniesieniu do których stwierdzono odpowiedni stopień ochrony.

177. EROD z zadowoleniem przyjmuje ogólne sprawozdanie publiczne wydane przez PCLOB w sprawie rozporządzenia wykonawczego 12333 i opublikowane w kwietniu 2021 r., zauważa jednak, że sprawozdanie to pozostaje ogólne, ponieważ większość ustaleń jest niejawna.

178. W tym kontekście ponownie, biorąc pod uwagę brak pewności i jasności co do sposobu stosowania rozporządzenia wykonawczego 12333 oraz znaczenie wyjaśnienia, w jaki sposób będzie on stosowany w świetle nowego rozporządzenia wykonawczego 14086, EROD podkreśla znaczenie wyczekiwanych sprawozdań PCLOB dotyczących tekstu tego aktu[175]. Rozumie jednak, że większość treści sprawozdania prawdopodobnie pozostanie niejawna, w związku z czym żadne dalsze informacje na temat konkretnego funkcjonowania rozporządzenia wykonawczego 12333 oraz jego konieczności i proporcjonalności nie zostaną udostępnione ani opinii publicznej, ani EROD.

179. W związku z tym EROD z zadowoleniem przyjęłaby w szczególności, gdyby sprawozdanie PCLOB w sprawie stosowania rozporządzenia wykonawczego 14086 nie było niejawne, ale w pełni dostępne po jego ukończeniu, w tym w części poświęconej ocenienie tego, w jaki sposób zabezpieczenia przewidziane w rozporządzeniu wykonawczym 14086 będą stosowane do gromadzenia danych na

[172] Zob. ZAWIADOMIENIE O PROJEKCIE KONTROLI PCLOB W CELU ZBADANIA STOSOWANIA ART. 702 USTAWY O KONTROLI WYWIADU (FISA).

[173] Zob. powyżej.

[174] Zob. powyżej.

[175] Ogólne sprawozdanie dotyczące rozporządzenia wykonawczego 12333 pozostało w większości niejawne – jedynie krótka wersja publiczna została podana do wiadomości publicznej, a także sprawozdanie i zalecenia dotyczące prowadzonych przez CIA działań w zakresie zwalczania terroryzmu zgodnie z rozporządzeniem wykonawczym 12333, które również pozostają częściowo niejawne.

podstawie rozporządzenia wykonawczego 12333. EROD zwraca się również do Komisji o poświęcenie tej kwestii szczególnej uwagi w kontekście przyszłych wspólnych przeglądów.

180. Zasadniczo, jeśli chodzi o poszczególne instrumenty prawne w amerykańskich ramach prawnych przewidujące możliwość gromadzenia danych i ich dalszego udostępniania i przetwarzania przez amerykańskie agencje wywiadowcze, EROD z zadowoleniem przyjęłaby doprecyzowanie ich współzależności z nowym rozporządzeniem wykonawczym 14086 oraz oczekuje zagwarantowania, że wcześniejsze obawy wyrażone w poprzednich opiniach EROD w tym względzie zostaną rozwiane przez przyjęcie tych nowych zabezpieczeń.

181. EROD wzywa Komisję do poświęcenia również tym aspektom szczególnej uwagi w kontekście przyszłych wspólnych przeglądów.

3.2.2.4.3 Sprawozdanie PCLOB

182. EROD z zadowoleniem przyjmuje fakt, że w rozporządzeniu wykonawczym 14086 przewiduje się także wymóg sporządzenia przez PCLOB sprawozdania dotyczącego wdrożenia tego rozporządzenia. EROD podkreśla, że sprawozdanie to powinno zawierać ocenę tej konkretnej możliwości, jaką oferuje rozporządzenie wykonawcze w zakresie gromadzenia danych do celów wymienionych w przypadku ukierunkowanego gromadzenia, a także hurtowego gromadzenia danych, w tym ze względów technicznych, w celu lepszego zrozumienia kluczowych warunków przewidzianych w rozporządzeniu wykonawczym 14086 oraz tego, jak są one w praktyce rozumiane i stosowane w poszczególnych programach nadzoru. Sprawozdanie to byłoby również niezbędne do oceny wdrażania rozporządzenia wykonawczego w wewnętrznych procedurach i strategiach politycznych jednostek Wspólnoty Wywiadowczej.

3.2.3 Gwarancja C – Nadzór

3.2.3.1 Wprowadzenie

183. Działania wywiadowcze Stanów Zjednoczonych podlegają wielopoziomowemu procesowi nadzoru. Strukturę nadzorczą w Stanach Zjednoczonych można podzielić na nadzór wewnętrzny i zewnętrzny. Wszystkie jednostki Wspólnoty Wywiadowczej wyznaczają swoich urzędników odpowiedzialnych za nadzór i przestrzeganie przepisów, którzy prowadzą okresowy nadzór nad działaniami w obszarze rozpoznania radioelektronicznego, w tym urzędników ds. ochrony prywatności i wolności obywatelskich i inspektorów generalnych. Ponadto istnieją zewnętrzne organy nadzoru, takie jak Rada Nadzoru nad Ochroną Prywatności i Wolnościami Obywatelskimi (PCLOB) oraz Rada ds. Nadzoru nad Służbami Wywiadowczymi.

184. EROD przypomina, że ingerencja ma miejsce w chwili gromadzenia danych, ale również w chwili uzyskania dostępu do danych przez organ publiczny w celu dalszego przetwarzania. ETPC wielokrotnie stwierdzał w swoim orzecznictwie, że wszelkie ingerencje w prawo do prywatności i ochrony danych powinny podlegać skutecznemu, niezależnemu i bezstronnemu systemowi nadzoru, który musi być zapewniony albo przez sędziego, albo przez inny niezależny organ[176] (np. organ administracji lub organ parlamentarny).

[176] Wyrok ETPC z dnia 6 września 1978 r. w sprawie Klass i inni/Niemcy (zwany dalej „wyrokiem ETPC w sprawie Klass"), pkt 17 i 51.

185. Choć ETPC opowiedział się za tym, by to sędzia był odpowiedzialny za utrzymanie nadzoru, nie wykluczył możliwości odpowiedzialności innego organu w tym zakresie, „pod warunkiem że organ ten jest wystarczająco niezależny od władzy wykonawczej”[177] i „od organów prowadzących nadzór oraz powierzono mu wystarczające uprawnienia i kompetencje, aby mógł sprawować skuteczną i ciągłą kontrolę”[178].

186. ETPC dodał, że przy ocenie niezależności należy wziąć pod uwagę „sposób mianowania i status prawny członków organu nadzorczego”[179].

187. ETPC stwierdził również, że należy zbadać, czy działalność organu nadzorczego podlega kontroli publicznej. Taka kontrola może na przykład mieć formę praktyki, w której organ nadzorczy składa rządowi coroczne sprawozdania, a te publiczne sprawozdania są przedkładane Parlamentowi i przez niego omawiane[180].

188. Niezależny nadzór nad wdrażaniem środków nadzoru został również uwzględniony przez TSUE w wyroku w sprawie Schrems II, w którym Trybunał stwierdził, że „[…] kontrola sprawowana przez FISC ma zatem na celu sprawdzenie, czy te programy nadzoru są odpowiednie do realizacji celu polegającego na pozyskiwaniu zagranicznych informacji wywiadowczych, lecz nie dotyczy kwestii tego, »czy osoby fizyczne są odpowiednio namierzane do celów pozyskiwania zagranicznych informacji wywiadowczych«”[181].

3.2.3.2 Nadzór wewnętrzny

3.2.3.2.1 Inspektorzy generalni

189. EROD uznaje, że inspektorom generalnym powierza się szeroki zakres uprawnień niezbędnych do monitorowania działań wywiadowczych. W szczególności inspektorzy generalni mają dostęp do wszystkich informacji niezbędnych do oceny ogólnej zgodności pracy agencji z przepisami, w tym między innymi z przepisami dotyczącymi ochrony prywatności i ochrony danych, oraz mogą wydawać wezwania i przyjmować oświadczenia z mocą przysięgi od każdej osoby w związku z dochodzeniem prowadzonym przez inspektorów generalnych.

190. W związku z powyższym EROD uważa, że inspektorzy generalni mają zasadniczo szerokie uprawnienia dochodzeniowe. Nie dysponują jednak żadnymi wiążącymi uprawnieniami zaradczymi i wydają jedynie niewiążące zalecenia[182].

191. EROD uznaje, że co do zasady inspektorom generalnym nie zabrania się ani nie uniemożliwia inicjowania, przeprowadzania lub finalizowania kontroli lub dochodzenia, ani też nie zabrania się ani nie uniemożliwia wydawania wezwań w trakcie kontroli lub dochodzenia[183]. W tym kontekście EROD zauważa jednak, że inspektorzy generalni podlegają zwierzchnictwu, kierownictwu i kontroli

[177] Wyrok ETPC w sprawie Zakharov, pkt 258; wyrok ETPC z dnia 10 lutego 2009 r. w sprawie Iordachi i inni/Mołdawia, pkt 40 i 51; wyrok ETPC z dnia 26 kwietnia 2007 r. w sprawie Dumitru Popescu/Rumunia, pkt 70–73.
[178] Wyrok ETPC w sprawie Klass, pkt 56.
[179] Wyrok ETPC w sprawie Zakharov, pkt 278.
[180] Wyrok ETPC w sprawie Zakharov, pkt 283; wyrok ETPC z dnia 9 czerwca 1990 r. w sprawie L./Norwegia; wyrok ETPC z dnia 18 maja 2010 r. w sprawie Kennedy/Zjednoczone Królestwo, pkt 166.
[181] Wyrok TSUE w sprawie Schrems II, pkt 179.
[182] Motyw 105 projektu decyzji.
[183] § 3 lit. a) ustawy o inspektorze generalnym z 1978 r.

właściwego kierownika departamentu, który może zakazać im dostępu do informacji, wszczęcia dochodzenia oraz między innymi wydawania wezwań, w przypadku gdy kierownik wydziału stwierdzi, że taki zakaz jest niezbędny do ochrony interesów narodowych. Kierownik departamentu musi jednak informować właściwe komisje Kongresu USA o wykonywaniu tego uprawnienia[184].

192. EROD zauważa, że inspektorów generalnych może odwołać wyłącznie prezydent USA, który musi poinformować Kongres o powodach takiego odwołania.

193. EROD zauważa, że od czasu wydania opinii przez Grupę Roboczą Art. 29, a następnie EROD, nie wprowadzono istotnych zmian w mechanizmie nadzoru wewnętrznego. W związku z tym EROD stwierdza, zgodnie z opinią 01/2016 Grupy Roboczej Art. 29[185], że zasadniczo istnieją wystarczające mechanizmy nadzoru wewnętrznego.

3.2.3.3 Nadzór zewnętrzny

194. EROD zauważa, że oprócz organów wymienionych poniżej działalność amerykańskich agencji wywiadowczych nadzorują różne inne organy rządu Stanów Zjednoczonych, takie jak Rada ds. Nadzoru nad Służbami Wywiadowczymi lub komisje Kongresu. Te ostatnie mogą prowadzić własne dochodzenia i sporządzać sprawozdania.

3.2.3.3.1 Rada Nadzoru nad Ochroną Prywatności i Wolnościami Obywatelskimi (PCLOB)

195. EROD uznaje kompleksową rolę nadzorczą PCLOB w odniesieniu do nowego mechanizmu dochodzenia roszczeń i wdrożenia rozporządzenia wykonawczego 14086.

196. Po pierwsze, jej nowe funkcje obejmują konsultacje z prokuratorem generalnym w sprawie mianowania sędziów Sądu Odwoławczego ds. Ochrony Danych i specjalnych rzeczników. Po drugie, PCLOB będzie co roku dokonywać przeglądu procesu dochodzenia roszczeń, tj. rozpatrywania kwalifikujących się skarg w ramach mechanizmu dochodzenia roszczeń. Obejmuje to kontrolę, czy CLPO i Sąd Odwoławczy ds. Ochrony Danych terminowo rozpatrują kwalifikujące się skargi, czy uzyskują pełny dostęp do niezbędnych informacji i czy działają zgodnie z rozporządzeniem wykonawczym 14086, a także czy Wspólnota Wywiadowcza przestrzega ustaleń dokonanych przez CLPO i DPRC.

197. Co więcej, z PCLOB należy się konsultować w kontekście aktualizacji przez agencje wywiadowcze ich wewnętrznych strategii politycznych i procedur w celu wdrożenia rozporządzenia wykonawczego 14086. PCLOB przeprowadzi ponadto przegląd zaktualizowanych strategii politycznych i procedur oraz oceni ich zgodność z rozporządzeniem wykonawczym 14086[186]. Choć ustalenia PCLOB nie są wiążące sensu stricto, szef każdej z jednostek Wspólnoty Wywiadowczej ma obowiązek starannie rozważyć i wdrożyć wszystkie zalecenia zawarte w każdym takim przeglądzie lub w inny sposób zastosować się do nich, zgodnie z obowiązującym prawem[187]. EROD zwraca się do Komisji o zwrócenie w przyszłych

[184] Zob. np. w ustawie o inspektorze generalnym z 1978 r.: § 8 (w odniesieniu do Departamentu Obrony); § 8E (w odniesieniu do DoJ), § 8G lit. d) pkt 2 lit. A) i B) (w odniesieniu do krajowego organu ds. bezpieczeństwa); tytuł 50 § 403q lit. b) U.S.C. (w odniesieniu do CIA); art. 405 lit. f) ustawy o zatwierdzeniu działań wywiadowczych na rok budżetowy 2010 (w odniesieniu do Wspólnoty Wywiadowczej).
[185] Opinia Grupy Roboczej Art. 29 nr 01/2016.
[186] Sekcja 2 część c) pkt (iv) i sekcja 2 część c) pkt (v) rozporządzenia wykonawczego 14086.
[187] Sekcja 2 część c) pkt (v) lit. B rozporządzenia wykonawczego 14086.

przeglądach szczególnej uwagi na to, czy i w jaki sposób zalecenia PCLOB zostały wdrożone na poziomie agencji, jeżeli projekt decyzji zostanie przyjęty.

198. EROD przypomina, że PCLOB, jako niezależny organ, jest „zachęcana", ale nie jest zobowiązana do przeprowadzania przeglądu, czy zabezpieczenia ustanowione w rozporządzeniu wykonawczym 14086 są należycie uwzględniane i czy Wspólnota Wywiadowcza w pełni spełnia wymogi procesu dochodzenia roszczeń. W rozumieniu EROD PCLOB stwierdziła jednak w swoim dodatkowym wyjaśnieniu dla EROD, jak również publicznie[188], że przyjmie rolę przewidzianą w rozporządzeniu wykonawczym 14086.

199. EROD z zadowoleniem przyjmuje ponadto fakt, że wyniki sprawozdań PCLOB mają być podawane do wiadomości publicznej. Biorąc pod uwagę, że poszczególne organy w ramach mechanizmu dochodzenia roszczeń i organy Wspólnoty Wywiadowczej muszą co do zasady wdrożyć zalecenia zawarte w sprawozdaniach PCLOB lub w inny sposób je uwzględnić, EROD uznaje, że zalecenia te odgrywają ważną rolę w zabezpieczeniach prywatności.

200. EROD zwraca uwagę, że dostęp PCLOB do informacji jest ograniczony, jeżeli Prezydent USA zatwierdzi przeprowadzenie „działań niejawnych"[189] przez departamenty, agencje lub podmioty rządu Stanów Zjednoczonych[190].

201. Zgodnie ze swoimi wcześniejszymi opiniami EROD uważa, że PCLOB jako niezależny organ, którego zalecenia stanowią istotny wkład w reformy w USA i którego sprawozdania są szczególnie pomocne w zrozumieniu funkcjonowania poszczególnych programów nadzoru, stanowi zasadniczy element struktury nadzoru.

202. W trzecim rocznym wspólnym przeglądzie unieważnionej Tarczy Prywatności UE-USA EROD wyraziła jednak ubolewanie, że PCLOB przekazała EROD tylko te same informacje, które są dostępne dla ogółu społeczeństwa. Niefortunny był ponadto fakt, że PCLOB nie wydała dalszych sprawozdań dotyczących PPD-28 w ramach działań następczych w związku ze swoim pierwszym sprawozdaniem w celu dostarczenia dodatkowych rozważań dotyczących sposobu stosowania zabezpieczeń przewidzianych w PPD-28, a także ogólnego zaktualizowanego sprawozdania dotyczącego art. 702 ustawy o kontroli wywiadu.

203. W związku z tym EROD z zadowoleniem przyjmuje skierowaną do niej zapowiedź PCLOB, że w najbliższej przyszłości można się spodziewać opublikowania sprawozdania uzupełniającego dotyczącego art. 702 ustawy o kontroli wywiadu. Ponadto EROD odnotowuje, że PCLOB poinformowała o swoim zobowiązaniu do umożliwienia publikacji swoich sprawozdań dotyczących rozporządzenia wykonawczego 14086. EROD przypomina jednak, że ujawnienie sprawozdań jawnych jest regulowane prawem USA i musi odbywać się w koordynacji z agencjami Wspólnoty Wywiadowczej, a więc PCLOB nie może o tym decydować z własnej inicjatywy.

204. W związku z tym, jeżeli projekt decyzji zostanie przyjęty, EROD przypomina, że w przyszłych przeglądach ram ochrony danych UE–USA odpowiednio sprawdzeni eksperci EROD powinni mieć

[188] https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf

[189] Zgodnie z tytułem 50 § 3093 lit. e) pkt 1 U.S.C. termin „działanie niejawne" oznacza działanie lub działania rządu Stanów Zjednoczonych mające na celu wywieranie wpływu na warunki polityczne, gospodarcze lub wojskowe za granicą, w przypadku gdy zgodnie z założeniami udział rządu Stanów Zjednoczonych nie będzie oczywisty lub uznany publicznie, przy czym nie obejmuje to 1) działań, których głównym celem jest pozyskiwanie danych wywiadowczych, tradycyjnych działań kontrwywiadowczych [...].

[190] Tytuł 42 § 2000ee lit. g) pkt 5) U.S.C.; tytuł 50 § 3093 lit. a) U.S.C.

możliwość przeglądu dodatkowych dokumentów i omówienia dodatkowych elementów niejawnych, w stosownych przypadkach, aby zapewnić odpowiednią ocenę informacji zawartych w sprawozdaniach, przy jednoczesnym uwzględnieniu odpowiednich interesów bezpieczeństwa narodowego i mającej zastosowanie ochrony prywatności.

205. EROD z zadowoleniem przyjmuje niezależność PCLOB i jej nadzór nad krajową Wspólnotą Wywiadowczą, która musi stosować się do zaleceń PCLOB lub w inny sposób je uwzględniać, co zostanie wskazane w sprawozdaniu PCLOB dla Kongresu Stanów Zjednoczonych.

206. Biorąc pod uwagę określone przez ETPC wymogi dotyczące kontroli publicznej[191], zgodnie z którymi sprawozdania organu nadzorczego muszą być przedkładane Parlamentowi i omawiane przez Parlament, EROD uważa za wystarczające, aby PCLOB przedkładała swoje sprawozdania co najmniej raz na pół roku Prezydentowi Stanów Zjednoczonych, a w szczególności komisjom Kongresu Senatu i Izby Reprezentantów[192], które są organami parlamentarnymi USA.

3.2.3.3.2 Sąd ds. Kontroli Wywiadu (FISC)

207. Sąd ds. Kontroli Wywiadu jest odpowiedzialny za nadzór nad gromadzeniem danych osobowych na podstawie art. 702 ustawy o kontroli wywiadu[193], a od decyzji FISC można się odwołać do Sądu Apelacyjnego ds. Kontroli Wywiadu (FISCR).

208. FISC sprawuje nadzór nad procesem certyfikacji gromadzenia informacji wywiadowczych zgodnie z art. 702 ustawy o kontroli wywiadu i zatwierdza działania w zakresie nadzoru elektronicznego, przeszukania oraz inne środki dochodzeniowe do celów wywiadu[194]. FISC zatwierdza również procedury ukierunkowania gromadzenia danych, minimalizowania danych i wglądu do certyfikatów, które to procedury są prawnie wiążące dla amerykańskich agencji wywiadowczych[195]. Jeżeli FISC stwierdzi, że wymogi nie zostały spełnione, może odmówić wydania certyfikatu w całości lub w części i zażądać zmiany procedur.

209. W przypadku stwierdzenia naruszeń procedur ukierunkowywania gromadzenia danych FISC może nakazać odpowiedniej agencji wywiadowczej podjęcie działań zaradczych[196]. Działania takie mogą mieć różne formy: od pojedynczych środków, np. zakończenia uzyskiwania danych i usunięcia nielegalnie pozyskanych danych, po środki strukturalne, w tym zmianę praktyki gromadzenia, m.in. pod względem wytycznych i szkolenia dla pracowników.

210. EROD przyznaje, że rozporządzenie wykonawcze 14086 stanowi, że CLPO i DPRC mają zgłaszać naruszenia asystentowi prokuratora generalnego ds. bezpieczeństwa narodowego, który zgłasza te naruszenia do FISC[197].

211. Jak zauważył TSUE w decyzji w sprawie Schrems II, FISC nie jest uprawniony do zatwierdzania poszczególnych środków nadzoru; może jednak zatwierdzać programy nadzoru[198]. W związku z tym

[191] Wyrok ETPC w sprawie Zakharov, pkt 283, wyrok ETPC z dnia 9 czerwca 1990 r. w sprawie L./Norwegia; wyrok ETPC z dnia 18 maja 2010 r. w sprawie Kennedy/Zjednoczone Królestwo, pkt 166.
[192] Tytuł 42 § 2000ee lit. e) U.S.C.
[193] Tytuł 50 1881 lit. a) U.S.C.
[194] www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court
[195] Tytuł 50 § 1881a lit. i) U.S.C.
[196] Tytuł 50 § 1803 lit. h) U.S.C.
[197] Sekcja 3 część c) pkt (i) lit. D rozporządzenia wykonawczego 14086; sekcja 3 część d) pkt (i) lit. F rozporządzenia wykonawczego 14086.
[198] Wyrok TSUE w sprawie Schrems II, pkt 179.

EROD podtrzymuje swoje obawy, że FISC nie zapewnia skutecznej kontroli sądowej nad ukierunkowywaniem gromadzenia danych na osoby niebędące obywatelami ani rezydentami USA, co – jak się wydaje – nie zostało rozstrzygnięte w nowym rozporządzeniu wykonawczym 14086.

212. W odniesieniu do uprzedniego niezależnego zezwolenia[199] na nadzór na podstawie art. 702 ustawy o kontroli wywiadu EROD wyraża ubolewanie, że – jak rozumie EROD na podstawie projektu decyzji[200] i wyjaśnień przedstawionych przez rząd Stanów Zjednoczonych – FISC nie wydaje się związany dodatkowymi zabezpieczeniami przewidzianymi w rozporządzeniu wykonawczym 14086 przy certyfikowaniu programów zezwalających na ukierunkowywanie gromadzenia danych na osoby niebędące obywatelami ani rezydentami USA. Zdaniem EROD dodatkowe zabezpieczenia zawarte w tym rozporządzeniu powinny jednak zostać uwzględnione w tym kontekście. EROD przypomina, że szczególnie przydatne do oceny sposobu wdrożenia zabezpieczeń zawartych w rozporządzeniu wykonawczym 14086 oraz sposobu stosowania tych zabezpieczeń w przypadku gromadzenia danych na podstawie art. 702 ustawy o kontroli wywiadu byłyby sprawozdania PCLOB.

3.2.4 Gwarancja D – Skuteczne środki ochrony prawnej muszą być dostępne dla osób fizycznych

213. EROD przypomina, że skuteczne i egzekwowalne przed sądami prawa osób fizycznych mają zasadnicze znaczenie dla ustalenia odpowiedniego stopnia ochrony danych w państwie trzecim. Osoby, których dane dotyczą, muszą mieć możliwość skorzystania ze skutecznego środka prawnego w celu zaspokojenia swoich praw, jeżeli uznają, że te nie są lub nie były przestrzegane. W wyrokach w sprawie Schrems I i Schrems II TSUE wyjaśnił, że „uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 [K]arty”[201].

214. Amerykański system sądowych środków ochrony prawnej zawiera istotne ograniczenie, które bardzo utrudnia wszczynanie przed sądami powszechnymi postępowań sądowych przeciwko środkom nadzoru stosowanym przez rząd USA. Konstytucja Stanów Zjednoczonych wymaga od osoby fizycznej wykazania legitymacji procesowej, tj. ustalenia „konkretnej, szczegółowej i rzeczywistej lub nieuchronnej szkody”[202]. W sprawach dotyczących nadzoru wymóg taki wydaje się unieważniony przez brak powiadamiania osób objętych nadzorem nawet po zakończeniu stosowania tych środków.

215. W tym kontekście EROD z zadowoleniem przyjmuje fakt, że rozporządzenie wykonawcze 14086 ustanawia specjalny mechanizm dochodzenia roszczeń w celu rozpatrywania i rozstrzygania skarg od osób niebędących obywatelami ani rezydentami Stanów Zjednoczonych, które to skargi dotyczą działań Stanów Zjednoczonych w obszarze rozpoznania radioelektronicznego. W ramach tego nowego mechanizmu wymóg wykazania legitymacji procesowej nie ma zastosowania: zgodnie z sekcją 4 część k) pkt (ii) rozporządzenia wykonawczego 14086 skarżący nie musi wykazać, że jego dane były faktycznie przedmiotem rozpoznania radioelektronicznego USA. Osoby, których dane dotyczą, mogą zatem powołać się na zabezpieczenia określone w rozporządzeniu wykonawczym 14086, w tym zabezpieczenia przewidziane w innych odpowiednich prawach i przepisach, o których mowa w sekcji 4

[199] EROD obawia się, że w przypadku hurtowego gromadzenia danych na podstawie rozporządzenia wykonawczego 12333, gdy FISC nie jest właściwy, nie istnieje procedura uprzedniego zezwolenia na hurtowe gromadzenie danych (zob. również część poświęconą gwarancji B).
[200] Motyw 165 projektu decyzji.
[201] Wyrok TSUE w sprawie Schrems I, pkt 95; wyrok TSUE w sprawie Schrems II, pkt 187.
[202] Wyrok w sprawie Clapper przeciwko Amnesty International USA, 568 U.S. 398 (2013) II, s. 10.

część d) pkt (iii) rozporządzenia wykonawczego 14086[203]. W tym względzie nowy mechanizm oferuje dodatkowy środek dochodzenia roszczeń, który w przeciwnym razie nie istniałby.

216. Nowy mechanizm obejmuje dwa etapy: na pierwszym etapie osoby fizyczne mogą złożyć skargę do urzędnika ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych (CLPO). Na drugim etapie osoby fizyczne mają możliwość odwołania się od decyzji CLPO do nowo utworzonego organu, tzw. Sądu Odwoławczego ds. Ochrony Danych (DPRC). W poniższych sekcjach skupiono się przede wszystkim na tym drugim etapie mechanizmu dochodzenia roszczeń. EROD uważa, że CLPO, jako pełniący obowiązki urzędnika państwowego, nie jest wystarczająco niezależny od władzy wykonawczej, a zatem nie może sam w sobie odpowiednio spełniać wymogów wynikających z art. 47 Karty. Ocena ta została kilkukrotnie potwierdzona przez Komisję.

3.2.4.1 Czy samo ustanowienie DPRC na podstawie rozporządzenia wykonawczego może być wystarczające?

217. DPRC nie jest sądem powszechnym ustanowionym przez Kongres na podstawie art. III konstytucji Stanów Zjednoczonych, lecz powołanym na podstawie rozporządzenia wykonawczego wydanego przez Prezydenta USA. Chociaż EROD dostrzega i ogólnie z zadowoleniem przyjmuje podstawową argumentację, a mianowicie unikanie wymogu wykazania legitymacji procesowej (zob. również pkt 215), rodzi to fundamentalne pytanie: czy taki mechanizm dochodzenia roszczeń może (w ogóle) spełniać wymogi art. 47 Karty? Zgodnie z tym artykułem każdy, kogo prawa i wolności zagwarantowane przez prawo Unii zostały naruszone, ma prawo do skutecznego środka odwoławczego przed sądem uprzednio ustanowionego prawem.

218. Podczas gdy w angielskim brzmieniu art. 47 Karty odniesiono się do „tribunal" (trybunał), w innych wersjach językowych częściej stosuje się słowo „sąd"[204]. W wyroku w sprawie Schrems II TSUE powtórzył, że osobom, których dane dotyczą, „powinna przysługiwać możliwość skorzystania przed niezawisłym i bezstronnym sądem ze środków prawnych w celu uzyskania dostępu do dotyczących ich danych osobowych lub spowodowania korekty lub usunięcia takich danych"[205]. Jednak w tym samym kontekście oceny odpowiedniości stopnia ochrony danych TSUE uważa, że skuteczna ochrona sądowa przed tego rodzaju ingerencjami może być zapewniona nie tylko przez sąd, ale również przez organ, który zapewnia zabezpieczenia merytorycznie równoważne wymaganym art. 47 Karty[206]. Podobnie europejska konwencja praw człowieka („EKPC") stanowi, że „[k]ażdy, kogo prawa i wolności […] zostały naruszone, ma prawo do skutecznego środka odwoławczego do właściwego organu państwowego"[207], który zgodnie z niejednokrotnie podtrzymywanym orzecznictwem ETPC niekoniecznie musi być organem sądowym[208]. Uprawnienia i gwarancje proceduralne, którymi dysponuje organ, w szczególności to, czy jest on niezależny od władzy wykonawczej i czy zapewnia bezstronność postępowania, mają raczej znaczenie dla oceny skuteczności środka prawnego przed tym organem[209]. Wydaje się, że TSUE i ETPC nie opierają swojej oceny na kryteriach czysto formalistycznych, lecz uznają materialne zabezpieczenia za decydujące.

---

[203] W sekcji 5 część h) rozporządzenia wykonawczego 14086 wyraźnie uprawniono osoby, których dane dotyczą, do składania skarg zgodnie w ramach mechanizmu dochodzenia roszczeń.

[204] Na przykład „Gerich" w niemieckiej wersji językowej.

[205] Wyrok TSUE w sprawie Schrems II, pkt 194.

[206] Zob. wyrok TSUE w sprawie Schrems II, pkt 197.

[207] Art. 13 EKPC.

[208] Wyrok ETPC w sprawie Klass, pkt 67; wyrok ETPC w sprawie Big Brother Watch, pkt 359.

[209] Wyrok ETPC w sprawie Klass, pkt 67; wyrok ETPC w sprawie Big Brother Watch, pkt 359.

219. W sprawie Schrems II TSUE zwrócił szczególną uwagę na skuteczne możliwości zaskarżenia w obszarze dostępu do danych osobowych na potrzeby bezpieczeństwa narodowego. EROD przyjmuje do wiadomości, że czyniąc to, TSUE nie omówił jednak elementu „wcześniej ustanowionego ustawą", o którym mowa w art. 47 Karty, mimo że mechanizm ochrony prawnej przez Rzecznika ds. Tarczy Prywatności również nie opierał się na amerykańskim prawie stanowionym. Zamiast zająć się tą kwestią, TSUE ocenił różne aspekty swojej analizy odpowiedniości, takie jak brak uprawnień zaradczych. W związku z tym wyrok w sprawie Schrems II nie zawiera żadnych wskazówek dotyczących oceny tego, czy środek jest „poprzednio ustanowiony ustawą" zgodnie z art. 47 Karty. Istnieją jednak inne orzeczenia, w których TSUE wypowiedział się w tej kwestii. Powtarzając utrwalone orzecznictwo ETPC w tym względzie, TSUE przypomniał w sprawach C-487/19 i C-132/20, że celem wprowadzenia wyrażenia „uprzednio ustanowionego ustawą" jest uniknięcie sytuacji, w której organizacja systemu sądownictwa w społeczeństwie demokratycznym zostałaby pozostawiona uznaniu władzy wykonawczej, oraz zapewnienie, by kwestia ta była regulowana ustawą uchwaloną przez władzę ustawodawczą w sposób zgodny z normami regulującymi wykonywanie jej kompetencji[210]. Jak wynika z tego stwierdzenia, prawo dostępu do sądu uprzednio ustanowione ustawą jest ściśle powiązane z gwarancją niezależności.

220. W tym względzie EROD stwierdza, że w kontekście oceny odpowiedniości stopnia ochrony konkretny mechanizm dochodzenia roszczeń utworzony na mocy rozporządzenia wykonawczego 14086 – w przeciwieństwie do dochodzenia roszczeń w sądach na podstawie art. III – nie jest sam w sobie niewystarczający. Analiza stopnia ochrony w tym zakresie zależy od tego, czy zabezpieczenia przewidziane w rozporządzeniu wykonawczym 14086 i uzupełnione zarządzeniem prokuratora generalnego w wystarczającym stopniu zapewniają niezależność DPRC od pozostałych władz.

221. Komisja powinna stale monitorować, czy zasady określone w rozporządzeniu wykonawczym 14086 i jego przepisy uzupełniające, w szczególności mające na celu zwiększenie niezależności DPRC, są w pełni wdrażane i skutecznie funkcjonują w praktyce. Ponadto wszelkie zmiany ram należy dokładnie przeanalizować pod kątem wpływu na ocenę Komisji zgodnie z projektem decyzji. W tym względzie EROD zauważa, że zmiany w rozporządzeniu wykonawczym 14086 i zarządzeniu prokuratora generalnego mogą spowodować przyjęcie mających natychmiastowe zastosowanie aktów wykonawczych powodujących zawieszenie, uchylenie lub zmianę decyzji stwierdzającej odpowiedni stopień ochrony[211].

3.2.4.2 Wystarczająca niezależność od władzy wykonawczej

222. W wyroku w sprawie Schrems II TSUE podkreślił, że należy zapewnić niezależność odpowiedniego sądu lub organu, zwłaszcza od władzy wykonawczej, wraz ze wszystkimi niezbędnymi gwarancjami, w tym w odniesieniu do warunków odwołania lub unieważnienia powołania. Dokładniej rzecz ujmując, TSUE skrytykował fakt, że Rzecznik ds. Tarczy Prywatności był wyznaczany przez sekretarza stanu i podlegał bezpośrednio sekretarzowi stanu. Rzecznik stanowił integralną część Departamentu Stanu Stanów Zjednoczonych. TSUE stwierdził również, że nie było szczególnych gwarancji towarzyszących odwołaniu Rzecznika lub unieważnieniu jego powołania, co podważało jego niezależność w stosunku władzy wykonawczej.

[210] Zob. wyrok TSUE z dnia 6 października 2021 r. w sprawie C-487/19, W.Ż, ECLI:EU:C:2021:798, pkt 129 oraz wyrok TSUE z dnia 29 marca 2022 r. w sprawie C-132/20, Getin Noble Bank S.A., ECLI:EU:C:2022:235, pkt 121.
[211] Motyw 212 projektu decyzji.

223. EROD przyznaje, że przepisy rozporządzenia wykonawczego 14086 i uzupełniającego go zarządzenia prokuratora generalnego nie nakładają na DPRC obowiązku sprawozdawczego wobec prokuratora generalnego, jak miałoby to miejsce w przypadku relacji między przełożonymi a podległymi. DPRC nie podlega również „codziennemu nadzorowi" prokuratora generalnego[212]. Zabezpieczenia te stanowią znaczną poprawę w stosunku do tego, co przewidziano w Tarczy Prywatności. DPRC jest jednak ustanowiony w ramach władzy wykonawczej, a mianowicie w Departamencie Sprawiedliwości. Z tego powodu w szczególności wdrożenie i skuteczne funkcjonowanie zabezpieczeń w praktyce będzie miało kluczowe znaczenie dla ustalenia, czy DPRC – który wprawdzie nie stanowi integralnej części Departamentu Sprawiedliwości, ale jest podmiotem znajdującym się jednak w strukturach władzy wykonawczej – można uznać za wystarczająco niezależny w praktyce. EROD wzywa Komisję do uważnego monitorowania, czy zabezpieczenia te są w pełni odzwierciedlone w praktyce. Ponadto EROD sugeruje doprecyzowanie terminu „codzienny nadzór", aby można było ostatecznie stwierdzić, czy „sędziowie" DPRC nie podlegają żadnemu nadzorowi. Komisja potwierdziła, że termin „codzienny nadzór" należy rozumieć w tym sensie.

224. Oprócz omówionych powyżej zabezpieczeń w DPF UE–USA przewiduje się pewne gwarancje dotyczące powoływania i odwoływania „sędziów" DPRC. Chociaż są oni powoływani przez prokuratora generalnego, ich powołanie opiera się na kryteriach stosowanych do oceny kandydatów na stanowiska sędziowskie na szczeblu federalnym i wymaga konsultacji z PCLOB. Odwołanie „sędziów" przed upływem ich kadencji lub z toczącego się postępowania jest możliwe jedynie w ściśle określonych okolicznościach, które – jak rozumie EROD – są wzorowane na przepisach mających zastosowanie do sędziów federalnych[213]. Stosowanie tych przepisów stanowi kolejny krok w kierunku wzmocnienia niezależnej pozycji DPRC. EROD ponownie podkreśla, że kluczowe znaczenie będzie miało wdrożenie w praktyce. Z projektu decyzji jako takiego nie wynika jednak jasno, czy i w jaki sposób zgodność z tymi wymogami będzie przestrzegana w Stanach Zjednoczonych. Z dodatkowych wyjaśnień przedstawionych przez Komisję i rząd USA EROD rozumie, że PCLOB może odnieść się do wyżej wymienionych przepisów w swoim rocznym przeglądzie procesu dochodzenia roszczeń oraz że odpowiedzialność za monitorowanie i zapewnianie zgodności ze wszystkimi wymogami prawnymi inspektora generalnego w Departamencie Sprawiedliwości obejmuje wymogi zawarte w rozporządzeniu wykonawczym 14086 oraz rozporządzeniu ustanawiającym DPRC. EROD zachęca Komisję do doprecyzowania tego aspektu w projekcie decyzji. W związku z tym Komisja powinna uwzględnić te zabezpieczenia przy monitorowaniu rzeczywistej praktyki przetwarzania danych osobowych ocenianego w projekcie decyzji.

225. W projekcie decyzji nie odniesiono się do kwestii, czy, a jeśli tak, to na jakich warunkach, Prezydent Stanów Zjednoczonych jest uprawniony do odwołania lub unieważnienia powołania „sędziów" DPRC. EROD rozumie, że nie ma takiego uprawnienia, jak wyjaśniła Komisja Europejska i potwierdzili przedstawiciele rządu Stanów Zjednoczonych. EROD proponuje doprecyzowanie tego aspektu w decyzji stwierdzającej odpowiedni stopień ochrony.

226. „Sędziowie" DPRC są powoływani na czteroletnią odnawialną kadencję i w chwili ich pierwotnego powołania nie mogą mieć historii zatrudnienia w strukturach władzy wykonawczej w ciągu ostatnich dwóch lat[214]. Podczas kadencji na stanowiskach „sędziów" DPRC nie mogą oni pełnić żadnych innych

[212] § 201 ust. 7 lit. d) zarządzenia prokuratora generalnego.
[213] Sekcja 3 część d) pkt (iv) rozporządzenia wykonawczego 14086; § 201 ust. 7 zarządzenia prokuratora generalnego.
[214] § 201 ust. 3 lit. a) zarządzenia prokuratora generalnego.

oficjalnych funkcji ani nie mogą być zatrudnieni w rządzie USA[215]. W przeciwieństwie do amerykańskich sędziów federalnych mogą oni jednak uczestniczyć w działalności pozasądowej, w tym w działalności gospodarczej, działalności finansowej, działalności charytatywnej nienastawionej na zysk, działalności powierniczej oraz działalności prawniczej, jeżeli taka działalność nie zakłóca bezstronnego wykonywania ich obowiązków ani skuteczności lub niezależności DPRC[216]. Niezawisłość sądów wynika nie tylko z wolności od poleceń, ale również z niezależności osobistej. W tym kontekście istotne są takie czynniki jak kadencja, możliwość ponownego mianowania i możliwość wystąpienia konfliktu interesów. Okres czterech lat przewidziany w rozporządzeniu wykonawczym 14086 i odpowiednio w zarządzeniu prokuratora generalnego jest krótszy niż np. kadencja sędziów TSUE (sześć lat z możliwością ponownego powołania) i ETPC (dziewięć lat bez możliwości ponownego mianowania), ale jako taki nie budzi poważnych obaw. EROD nie zna żadnego orzecznictwa nakładającego w tym względzie minimalną kadencję[217]. EROD uznaje również, że możliwość prowadzenia działalności pozasądowej jest uzależniona od warunku, że – mówiąc prosto – nie prowadzi ona do konfliktu interesów zagrażającego obowiązkom nałożonym na DPRC. EROD wnioskuje z dodatkowych wyjaśnień rządu Stanów Zjednoczonych, że wymogi te podlegają również przeglądowi i monitorowaniu przez PCLOB oraz inspektora generalnego Departamentu Sprawiedliwości (zob. pkt 226 powyżej). Sposób, w jaki wymóg ten będzie stosowany i wykazany w praktyce, należy również uwzględnić w ramach wspólnych przeglądów.

227. Zgodnie z sekcją 3 część d) pkt (i) lit. B rozporządzenia wykonawczego 14086 wszyscy „sędziowie" DPRC muszą mieć poświadczenia bezpieczeństwa, aby móc uzyskać dostęp do informacji niejawnych, tj. wykonywać swoją funkcję orzekania w sprawach dotyczących bezpieczeństwa narodowego[218]. Z kolei niektóre europejskie przepisy ustawowe i wykonawcze dotyczące poświadczenia bezpieczeństwa zwalniają sędziów z wymogu poświadczenia bezpieczeństwa w zakresie, w jakim wykonują oni obowiązki sędziów, ponieważ taka szczegółowa kontrola może być sprzeczna z niezależnością sądów[219]. Zgodnie z wyjaśnieniami rządu Stanów Zjednoczonych kandydat ubiegający się o powołanie na stanowisko sędziego w sądzie amerykańskim przechodzi dokładną weryfikację, jednak po powołaniu go na stanowisko sędziego federalnego w sądzie amerykańskim sędzia federalny nie musi uzyskać poświadczenia bezpieczeństwa w celu uzyskania dostępu do dokumentów niejawnych istotnych dla danej sprawy.

228. Zdaniem EROD okoliczności przedstawione powyżej częściowo ujawniają różnice między stanowiskiem i statusem amerykańskiego sędziego federalnego a „sędziego" DPRC. Przewidziane zabezpieczenia nie dają jednak podstaw do wątpliwości co do niezależności DPRC. EROD wzywa Komisję, aby w przypadku przyjęcia projektu decyzji wyżej wymienione zabezpieczenia były priorytetem podczas pierwszego wspólnego przeglądu DPF UE–USA. EROD oczekuje ponadto, że Komisja podejmie działania następcze w związku ze swoim zobowiązaniem do zawieszenia, uchylenia lub zmiany decyzji, jeżeli ta zostanie przyjęta, w przypadku gdy organ wykonawczy USA zdecyduje o ograniczeniu zabezpieczeń zawartych w rozporządzeniu wykonawczym[220].

[215] § 201 ust. 3 lit. c) zarządzenia prokuratora generalnego.
[216] § 201 ust. 7 lit. c) zarządzenia prokuratora generalnego.
[217] Zob. również *mutatis mutandis* wyrok ETPC (wielka izba) z dnia 25 maja 2021 r., w sprawie Centrum För Rättvisa/Szwecja, pkt 346.
[218] Zob. również § 201 ust. 11 lit. b) zarządzenia prokuratora generalnego i motyw 177 projektu decyzji.
[219] Na przykład § 2 ust. 3 niemieckiej ustawy o poświadczeniu bezpieczeństwa.
[220] Motyw 212 projektu decyzji.

3.2.4.3 Uprawnienia DPRC

3.2.4.3.1 Dostęp do informacji

229. Skuteczna ochrona prawna wymaga, aby sąd dysponował wystarczającymi uprawnieniami dochodzeniowymi do kontroli zaskarżonego środka. W sprawie Kadi II TSUE orzekł w odniesieniu do art. 47 Karty, że sądy Unii Europejskiej muszą zapewnić, aby decyzja opierała się na wystarczająco solidnej podstawie faktycznej[221]. TSUE stwierdza, że „sąd Unii ma obowiązek przeprowadzić to badanie, zwracając się w razie potrzeby do właściwego organu Unii o przedstawienie informacji lub dowodów, poufnych lub nie, mających znaczenie dla takiego badania"[222], przy czym „nie można powołać się na tajemnicę lub poufność [...] informacji lub dowodów"[223].

230. Zgodnie z motywem 181 projektu decyzji DPRC dokonuje kontroli ustaleń dokonanych przez CLPO na podstawie co najmniej protokołu dochodzenia prowadzonego przez CLPO, jak również wszelkich informacji i uwag przedstawionych przez skarżącego, specjalnego rzecznika lub agencję wywiadowczą. W projekcie decyzji stwierdza się ponadto, że DPRC ma dostęp do wszystkich niezbędnych informacji, które może uzyskać za pośrednictwem CLPO. Opiera się to na przepisie § 201 ust. 9 lit. b) zarządzenia prokuratora generalnego, który upoważnia DPRC do „zwrócenia się do CLPO Urzędu Dyrektora Krajowych Służb Wywiadowczych o uzupełnienie rejestru o szczegółowe wyjaśnienia lub dodatkowe informacje oraz o dokonanie przez CLPO Urzędu Dyrektora Krajowych Służb Wywiadowczych w razie potrzeby dodatkowych ustaleń faktycznych, aby umożliwić panelowi DPRC przeprowadzenie kontroli". EROD przyjmuje zatem, że ocena przeprowadzona przez DPRC nie ogranicza się w żaden sposób do ustaleń dokonanych przez CLPO na pierwszym poziomie nowego mechanizmu dochodzenia roszczeń. Wręcz przeciwnie, DPRC może zarówno pozyskiwać dodatkowe informacje prawne, jak i, co ważne, ustalać dalsze okoliczności faktyczne w celu zbadania, czy doszło do naruszenia objętego zakresem. Jednocześnie EROD zauważa także, że te zasadniczo szerokie uprawnienia dochodzeniowe nie obejmują bezpośredniego dostępu do przechowywanych danych osoby fizycznej. Komisja wyjaśniła, że CLPO będzie zawsze działać jako pośrednik, gdy DPRC będzie potrzebował dalszych informacji. W związku z tym dostęp DPRC do informacji niezbędnych do niezależnego rozpatrzenia wniosku o wszczęcie procedury odwoławczej opiera się w pewnym stopniu na przekazaniu przez CLPO niezbędnych informacji. EROD uznaje, że CLPO ma obowiązek „zapewnienia wszelkiego niezbędnego wsparcia" DPRC, a agencje wywiadowcze są zobowiązane do zapewnienia CLPO dostępu do informacji niezbędnych do przeprowadzenia kontroli przez DPRC[224]. EROD zauważa jednak również, że sam CLPO nie jest niezależny i że prowadzi wstępne postępowanie wyjaśniające w sprawie skargi na pierwszym etapie procedury odwoławczej. W związku z tym EROD z zadowoleniem przyjmuje fakt, że podczas corocznych przeglądów mechanizmu dochodzenia roszczeń PCLOB zweryfikuje, czy DPRC uzyskał pełny dostęp do wszystkich niezbędnych informacji[225]. EROD zachęca ponadto Komisję do uwzględnienia tego aspektu we wspólnych przeglądach, jeżeli projekt decyzji zostanie przyjęty, aby zbadać implikacje tego systemu w praktyce.

[221] Wyrok TSUE z dnia 18 lipca 2013 r. w sprawach połączonych C-584/10 P, C-593/10 P i C-595/10 P, Komisja Europejska i inni/Yassin Abdullah Kadi (zwany dalej „wyrokiem TSUE w sprawie Kadi II"), pkt 119.
[222] Wyrok TSUE w sprawie Kadi II, pkt 120.
[223] Wyrok TSUE w sprawie Kadi II, pkt 125.
[224] Sekcja 3 część c) pkt (i) lit. H i sekcja 3 część d) pkt (iii) rozporządzenia wykonawczego 14086.
[225] Sekcja 3 część e) pkt (i) rozporządzenia wykonawczego 14086.

3.2.4.3.2 Uprawnienia zaradcze

231. Jednym z głównych braków w Tarczy Prywatności, które doprowadziły do jej unieważnienia przez TSUE w sprawie Schrems II, był brak wiążących uprawnień zaradczych Rzecznika ds. Tarczy Prywatności. TSUE stwierdził, że nie ma „żadnego elementu świadczącego o tym, że jest on uprawniony do podejmowania decyzji wiążących te służby”[226]. Samo (polityczne) zobowiązanie rządu amerykańskiego do doprowadzenia do tego, by Wspólnota Wywiadowcza podjęła działania naprawcze w związku z wszelkimi wykrytymi przez Rzecznika naruszeniami obowiązujących przepisów, nie wystarczyło do zapewnienia stopnia ochrony zasadniczo odpowiadającego stopniowi gwarantowanemu w art. 47 Karty.

232. Natomiast w ramach nowego mechanizmu dochodzenia roszczeń decyzje podjęte przez CLPO i DPRC mają moc wiążącą[227]. EROD uznaje, z jednej strony, że uprawnienie to nie ogranicza się do konkretnych środków, ale umożliwia stosowanie „odpowiednich środków zaradczych” w celu „pełnego dochodzenia roszczeń” w odniesieniu do stwierdzonego naruszenia objętego zakresem. W szczególności w sekcji 4 część a) rozporządzenia wykonawczego 14086 wyraźnie wspomniano o usunięciu danych zgromadzonych niezgodnie z prawem. Z drugiej strony EROD zauważa, że brzmienie sekcji 4 część a) rozporządzenia wykonawczego 14086 stwarza pewną niepewność co do procesu określania takich „odpowiednich środków zaradczych”. Chociaż środek powinien być skonstruowany w taki sposób, aby w pełni naprawić naruszenie, należy również rozważyć „sposób, w jaki zwyczajowo naprawiano naruszenia takie jak zidentyfikowane naruszenie”[228]. Znaczenie i skutki takiego wymogu są niejasne. W związku z tym EROD zwraca się do Komisji o ścisłe monitorowanie środków zaradczych przyjętych w praktyce.

3.2.4.4 Wniesienie skargi w ramach nowego mechanizmu dochodzenia roszczeń

233. Mechanizm dochodzenia roszczeń ustanowiony na mocy rozporządzenia wykonawczego 14086 ma zastosowanie wyłącznie do kwalifikujących się skarg przekazywanych przez właściwy organ publiczny w kwalifikującym się państwie, dotyczących działań Stanów Zjednoczonych w obszarze rozpoznania radioelektronicznego w związku z ewentualnym naruszeniem objętym zakresem[229]. W związku z tym, aby móc skorzystać z tej ochrony prawnej, szereg warunków musi być spełnionych.

3.2.4.4.1 Wskazanie państwa jako kwalifikującego się

234. Przede wszystkim państwo lub regionalna organizacja integracji gospodarczej, z których dane zostały przekazane do Stanów Zjednoczonych, muszą przed przekazaniem danych, których dotyczy skarga, zostać wskazane jako kwalifikujące się[230]. Oczywiście istotne jest, aby przewidziany mechanizm dochodzenia roszczeń był dostępny w chwili rozpoczęcia stosowania decyzji stwierdzającej odpowiedni stopień ochrony. W związku z tym motyw 196 projektu decyzji stanowi, że wejście w życie decyzji jest uzależnione między innymi od wskazania Unii jako kwalifikującego się podmiotu do celów mechanizmu dochodzenia roszczeń. Jak się w istocie wydaje, Komisja zakłada, że wskazanie nastąpi przed przyjęciem decyzji, ponieważ w projekcie decyzji znajduje się miejsce na takie wskazanie UE

[226] Wyrok TSUE w sprawie Schrems II, pkt 196.
[227] Odpowiednio sekcja 3 część c) pkt (ii) i sekcja 3 część d) pkt (ii) rozporządzenia wykonawczego 14086.
[228] Sekcja 4 część a) rozporządzenia wykonawczego 14086.
[229] Sekcja 3 część a) rozporządzenia wykonawczego 14086.
[230] Sekcja 4 część d) pkt (i) oraz sekcja 4 część k) pkt (i) rozporządzenia wykonawczego 14086.

przez Prokuratora Generalnego[231] (w przeciwieństwie do włączenia wskazania jako warunku zawieszającego do części normatywnej projektu decyzji).

3.2.4.4.2 Negatywny wpływ na interesy w zakresie ochrony prywatności i wolności obywatelskich oraz „legitymację procesową"

235. „Kwalifikująca się skarga" musi opierać się na domniemanym „naruszeniu objętym zakresem", co z kolei wymaga, aby naruszenie negatywnie wpływało na indywidualne interesy skarżącego w zakresie ochrony prywatności i wolności obywatelskich[232]. EROD rozumie, w oparciu o dodatkowe wyjaśnienia Komisji, że „niekorzystny wpływ" nie oznacza żadnego ograniczenia dopuszczalności skargi. Jak stwierdziła Komisja, taki niekorzystny wpływ odnosiłby się raczej do każdej skargi dotyczącej przetwarzania danych osobowych do celów działań w obszarze rozpoznania radioelektronicznego z naruszeniem przepisów, o których mowa w sekcji 4 część d) pkt (iii), np. dotyczących zabezpieczeń określonych w rozporządzeniu wykonawczym 14086. EROD wyraża ubolewanie, że nie zostało to sprecyzowane w tekście projektu decyzji, i zwraca się do Komisji o doprecyzowanie pojęcia „niekorzystnego wpływu" w celu zapewnienia, aby wszelkie naruszenia praw osób, których dane dotyczą, były oceniane i naprawiane oraz aby nie trzeba było wykazywać „wagi", aby mieć dostęp do środków dochodzenia roszczeń i odpowiednich środków zaradczych.

236. Jak już wspomniano, skarga na podstawie rozporządzenia wykonawczego 14086 nie wymaga od skarżącego wykazania legitymacji procesowej (zob. pkt 215)[233]. EROD z zadowoleniem przyjmuje wyjaśnienie zawarte w sekcji 4 część k) rozporządzenia wykonawczego 14086, zgodnie z którym stosowane będzie „kryterium przekonania" i nie jest konieczne wykazanie, że do danych skarżącego faktycznie uzyskano dostęp w wyniku działań w obszarze rozpoznania radioelektronicznego. Ustanowienie mechanizmu dochodzenia roszczeń jest ważnym krokiem, ponieważ wymóg dotyczący legitymacji procesowej sprawia, że bardzo trudno jest zaskarżyć środki nadzoru przed sądami powszechnymi w Stanach Zjednoczonych.

237. W związku z powyższym EROD nie rozważa możliwości odwołania się do sądów powszechnych, do których również odniesiono się w projekcie decyzji[234], w celu zapewnienia odpowiedniego stopnia ochrony[235]. W tym względzie EROD przypomina o swoich wielokrotnie już wyrażanych obawach w związku z wymogiem legitymacji procesowej przed sądami powszechnymi[236]. Ponadto na podstawie dodatkowych oświadczeń rządu Stanów Zjednoczonych EROD rozumie, że choć rozporządzenie wykonawcze 14086 nie wyklucza możliwości odwołania się do sądów powszechnych, nie ma pewności, w jaki sposób taki sąd zastosowałby to rozporządzenie. Kwestię tę można by dokładniej zbadać w przyszłych przeglądach, jeżeli projekt decyzji zostanie przyjęty.

3.2.4.4.3 Postępowanie w sprawie skargi

238. EROD zasadniczo popiera procedurę kierowania skargi do organów nadzorczych państw członkowskich i nadal uważa, że identyfikacja skarżącego powinna mieć miejsce na terytorium UE. Podobnie jednak jak w przypadku mechanizmu ochrony prawnej przez Rzecznika ds. Tarczy Prywatności projekt decyzji stanowi, że osoba, której dane dotyczą, chcąca złożyć taką skargę, musi złożyć ją do organu

[231] Przypis 320 w projekcie decyzji.
[232] Sekcja 4 część k) pkt (i) oraz sekcja 4 część d) pkt (ii) rozporządzenia wykonawczego 14086.
[233] Wyrok w sprawie Clapper przeciwko Amnesty International USA, 568 U.S. 398 (2013) II, s. 10.
[234] Motyw 187 i nast. projektu decyzji.
[235] Zob. również wyrok TSUE w sprawie Schrems II, pkt 191 i 192.
[236] Zob. opinia Grupy Roboczej Art. 29 nr 01/2016, s. 43.

nadzorczego w państwie członkowskim UE właściwego w sprawach nadzoru nad służbami bezpieczeństwa narodowego lub przetwarzania danych osobowych przez organy publiczne[237] W tym względzie EROD przypomina o swoich obawach wyrażonych już w opinii Grupy Roboczej Art. 29 w sprawie Tarczy Prywatności, na przykład co do potencjalnych trudności dla osób fizycznych w określeniu właściwego organu, biorąc pod uwagę różnorodność mechanizmów nadzoru nad służbami bezpieczeństwa narodowego w państwach członkowskich[238]. Mając na uwadze zaangażowanie krajowych organów ochrony danych w stosowanie DPF UE–USA i nadzór nad nimi, właściwsze jest przekazywanie skarg za ich pośrednictwem.

3.2.4.5 Decyzja DPRC

239. Po zakończeniu kontroli na wniosek skarżącego DPRC nie może ujawnić, czy skarżący podlegał działaniom USA w obszarze rozpoznania radioelektronicznego. Zamiast tego informuje się skarżącego, że „kontrola nie wykazała żadnych naruszeń objętych zakresem albo Sąd Odwoławczy ds. Ochrony Danych wydał decyzję wymagającą odpowiednich środków zaradczych"[239]. Ta standardowa odpowiedź służy zasadniczo prawnie uzasadnionemu celowi, jakim jest ochrona informacji szczególnie chronionych dotyczących działalności wywiadowczej USA. EROD obawia się jednak, że rozporządzenie wykonawcze 14086 nie przewiduje żadnych odstępstw od standardowej odpowiedzi DPRC.

240. W sprawie Kadi II TSUE musiał zająć się z jednej strony sprzecznymi interesami związanymi z tajemnicą państwową, a z drugiej strony sprawiedliwym i w miarę możliwości kontradyktoryjnym postępowaniem. TSUE orzekł, że w okolicznościach, w których nadrzędne względy dotyczące bezpieczeństwa narodowego stoją na przeszkodzie powiadomieniu zainteresowanej osoby o informacjach lub dowodach, to na sądzie jednak ciąży obowiązek zastosowania w ramach wykonywanej przez niego kontroli sądowej metod pozwalających na pogodzenie prawnie uzasadnionych względów bezpieczeństwa dotyczących charakteru i źródeł informacji oraz konieczności zagwarantowania stronie w wystarczającym stopniu przestrzegania jej uprawnień procesowych, takich jak prawo do bycia wysłuchanym oraz zasada kontradyktoryjności[240] TSUE uściślił ponadto, że sąd Unii, przeprowadzając analizę całości okoliczności prawnych lub faktycznych przedstawionych przez właściwy organ Unii, ma obowiązek sprawdzić zasadność powodów, na które powołuje się wspomniany organ, aby sprzeciwić się takiemu powiadomieniu[241]. Jeżeli okaże się, że powody, na które powołuje się właściwy organ Unii, rzeczywiście stoją na przeszkodzie powiadomieniu zainteresowanej osoby o informacjach lub dowodach, nadal konieczne jest wyważenie w sposób odpowiedni wymogów związanych z prawem do skutecznej ochrony sądowej oraz wymogów wynikających z bezpieczeństwa narodowego[242]. W celu takiego wyważenia dozwolone jest skorzystanie z możliwości takich jak powiadomienie o streszczeniu zawartości rozpatrywanych informacji lub dowodów[243]. Chociaż ustalenia sądu nie nakładają wymogów dotyczących orzeczenia wydanego przez sąd, lecz odnoszą się raczej do decyzji właściwego organu i przebiegu postępowania sądowego, dostarczają one wskazówek co do wyważenia wspomnianych powyżej interesów w kontekście prawa do skutecznej ochrony prawnej. W celu uzyskania dalszych wskazówek można

[237] Motyw 169 projektu decyzji.
[238] Opinia Grupy Roboczej Art. 29 nr 01/2016, s. 48 i 49.
[239] Sekcja 3 część d) pkt (i) lit. H rozporządzenia wykonawczego 14086. W sekcji rozporządzenia wykonawczego 14086 określono tę odpowiedź również w odniesieniu do CLPO.
[240] Wyrok TSUE w sprawie Kadi II, pkt 125.
[241] Wyrok TSUE w sprawie Kadi II, pkt 126.
[242] Wyrok TSUE w sprawie Kadi II, pkt 128.
[243] Wyrok TSUE w sprawie Kadi II, pkt 129.

również odnieść się do sprawy Big Brother Watch, w której ETPC, nawiązując do rzetelności postępowania, a w szczególności do zasady kontradyktoryjności, orzekł, że orzeczenia organu sądowego lub innego niezależnego organu powinny być uzasadnione[244].

241. EROD uznaje, że decyzje DPRC są rzeczywiście uzasadnione. DPRC jest wyraźnie zobowiązany do wydania pisemnej decyzji określającej jego ustalenia i określającej wszelkie odpowiednie środki zaradcze[245]. Ponadto EROD zauważa, że osoba fizyczna zostanie powiadomiona, jeżeli informacje dotyczące kontroli przeprowadzonej przez DPRC zostaną odtajnione[246]. EROD uznaje również funkcję specjalnych rzeczników przewidzianą w nowym mechanizmie dochodzenia roszczeń, która obejmuje opowiadanie się w interesie skarżącego w sprawie[247]. W świetle przedstawionych powyżej skutków orzecznictwa TSUE i ETPC oraz biorąc pod uwagę, że od decyzji DPRC nie można się odwołać i jest ona ostateczna[248], EROD ma jednak wątpliwości co do ogólnego stosowania standardowej odpowiedzi DPRC. EROD przypomina, że PCLOB dokona niezależnego przeglądu funkcjonowania nowego mechanizmu dochodzenia roszczeń i zwraca się do Komisji o zwrócenie szczególnej uwagi na tę kwestię, w tym na wszelkie oceny tego aspektu przez PCLOB, podczas przyszłych przeglądów decyzji, jeżeli zostanie ona przyjęta.

4 WDROŻENIE I MONITOROWANIE PROJEKTU DECYZJI

242. Jeżeli chodzi o monitorowanie i przegląd projektu decyzji, EROD zauważa, że zgodnie z orzecznictwem TSUE „w związku z tym, że poziom ochrony zapewniony w państwie trzecim może zmieniać się w czasie, do Komisji należy, po przyjęciu decyzji na podstawie [art. 45 RODO], okresowe badanie, czy przy uwzględnieniu stanu faktycznego i prawnego ustalenia poczynione co do odpowiedniego stopnia ochrony zapewnionego przez dane państwo trzecie są nadal zasadne. Takie badanie należy przeprowadzić w każdym razie wówczas, gdy wyjdą na jaw okoliczności mogące wzbudzić co do tego wątpliwości”[249].

243. Ponadto EROD zauważa, że w piśmie DoC przewidziano, że DoC i inne agencje USA, w stosownych przypadkach, będą odbywać okresowe spotkania z Komisją, zainteresowanymi unijnymi organami ochrony danych i odpowiednimi przedstawicielami EROD[250].

244. EROD uważa, że w kolejnych przeglądach okresowych szczególnej uwagi będą wymagały następujące kwestie: ochrona na podstawie prawa stanowionego w odniesieniu do dostępu organów ścigania, odstępstwo dotyczące tymczasowego hurtowego gromadzenia danych w związku z ukierunkowanym gromadzeniem danych przez amerykańskie organy bezpieczeństwa narodowego, stosowanie w praktyce nowo wprowadzonych zasad konieczności i proporcjonalności, w tym w kontekście programu UPSTREAM, wzajemne powiązania między rozporządzeniem wykonawczym 14086 a poszczególnymi amerykańskimi instrumentami prawnymi umożliwiającymi agencjom wywiadowczym USA gromadzenie i dalsze przetwarzanie danych osobowych, wdrażanie wewnętrznych strategii politycznych i procedur, sposób, w jaki zabezpieczenia te będą również uwzględniane w kontekście nadzoru prowadzonego przez FISC, oraz sposób skutecznego

[244] Wyrok ETPC w sprawie Big Brother Watch, pkt 359.
[245] § 201 ust. 9 lit. g) zarządzenia prokuratora generalnego.
[246] Sekcja 3 część d) pkt (v) rozporządzenia wykonawczego 14086.
[247] § 201 ust. 8 lit. g) zarządzenia prokuratora generalnego.
[248] § 201 ust. 9 lit. g) zarządzenia prokuratora generalnego.
[249] Wyrok TSUE w sprawie Schrems I, pkt 76. Zob. również art. 3 ust. 4 projektu decyzji.
[250] Załącznik III do projektu decyzji.

funkcjonowania mechanizmu dochodzenia roszczeń, a także kwestia dalszego przekazywania danych, zautomatyzowanych decyzji, merytorycznego i skutecznego nadzoru i egzekwowania zasad DPF, a także skutecznego mechanizmu dochodzenia roszczeń.

245. EROD zauważa, że przegląd ustaleń dotyczących zapewnienia odpowiedniego stopnia ochrony będzie miał miejsce po upływie jednego roku od daty powiadomienia państw członkowskich o decyzji stwierdzającej odpowiedni stopień ochrony, a następnie co najmniej co cztery lata [251]. W celu dalszego wzmocnienia ciągłego monitorowania decyzji stwierdzającej odpowiedni stopień ochrony EROD wzywa Komisję do przeprowadzania kolejnych przeglądów co najmniej raz na trzy lata.

246. Jeżeli chodzi o praktyczne zaangażowanie EROD i jej przedstawicieli w przygotowanie i przebieg przyszłych przeglądów okresowych, EROD powtarza, że wszelkie istotne dokumenty należy przekazywać EROD na piśmie, w tym korespondencję, z odpowiednim wyprzedzeniem przed przeglądami. Podobnie jak w przypadku przeglądów przeprowadzanych w odniesieniu do Tarczy Prywatności EROD zaleca, aby najpóźniej trzy miesiące przed dokonaniem przeglądu Komisja, administracja USA i EROD ustaliły i uzgodniły warunki przeglądu.

247. Ponadto EROD zauważa i z zadowoleniem przyjmuje fakt, że w motywie 212 projektu decyzji przedstawiono przykłady zmian obniżających stopień ochrony, które mogą uzasadniać wszczęcie „procedury uchylenia w sytuacji wyjątkowej", przy czym skoncentrowano się na możliwych zmianach rozporządzenia wykonawczego 14086 i powiązanego zarządzenia prokuratora generalnego.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

[251] Art. 3 ust. 4 projektu decyzji.