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 13 kwietnia 2021 r.

SPIS TREŚCI

Europejska Rada Ochrony Danych

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"),

uwzględniając Porozumienie o Europejskim Obszarze Gospodarczym (zwanym dalej „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.[1],

uwzględniając art. 12 i art. 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. STRESZCZENIE

1. Komisja Europejska zatwierdziła swój projekt decyzji wykonawczej (zwany dalej „projektem decyzji") w sprawie odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie na podstawie RODO w dniu 19 lutego 2021 r.[2] Następnie Komisja Europejska rozpoczęła procedurę jego formalnego przyjęcia.

2. W tym samym dniu Komisja Europejska zwróciła się o opinię do Europejskiej Rady Ochrony Danych (zwanej dalej „EROD")[3]. EROD przeprowadziła ocenę odpowiedniego stopnia ochrony danych zapewnianego w Zjednoczonym Królestwie na podstawie analizy samego projektu decyzji, jak również na podstawie analizy dokumentacji udostępnionej przez Komisję Europejską.

3. EROD skupiła się na ocenie zarówno ogólnych aspektów RODO zawartych w projekcie decyzji, jak i na dostępie organów publicznych do danych osobowych przekazywanych z EOG do celów egzekwowania prawa i bezpieczeństwa narodowego, w tym na środkach ochrony prawnej dostępnych osobom fizycznym w EOG. EROD oceniła również, czy zabezpieczenia przewidziane w ramach prawnych Zjednoczonego Królestwa zostały wprowadzone i czy są skuteczne.

4. Jako główny punkt odniesienia dla tych prac EROD wykorzystała swój dokument dotyczący odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO[4], przyjęty

[1] Odniesienia do „państw członkowskich" zawarte w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Zob. komunikat prasowy Komisji Europejskiej, Ochrona danych: Komisja Europejska rozpoczyna procedurę dotyczącą przepływu danych osobowych do Wielkiej Brytanii, 19 lutego 2021 r., https://ec.europa.eu/commission/presscorner/detail/pl/ip_21_661.
[3] Tamże.
[4] Zob. Grupa Robocza Art. 29, dokument dotyczący odpowiedniego stopnia ochrony przekazywanych danych osobowych, przyjęty w dniu 28 listopada 2017 r., ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r., WP254 rev.01 (zatwierdzona przez EROD, zob. https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines); (zwany dalej „dokumentem dotyczącym odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO").

w lutym 2018 r., a także zalecenia EROD 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru[5].

[5] Zob. zalecenia EROD 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, przyjęte dnia 10 listopada 2020 r., https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_pl.

1.1. Obszary zbieżności

5. Podstawowym celem EROD jest przedstawienie Komisji Europejskiej opinii na temat odpowiedniego stopnia ochrony danych przyznanego osobom fizycznym w Zjednoczonym Królestwie. Należy zaznaczyć, że EROD nie oczekuje, aby ramy prawne Zjednoczonego Królestwa powielały europejskie przepisy o ochronie danych.

6. EROD przypomina jednak, że w art. 45 RODO oraz w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „TSUE") wymaga się, aby prawodawstwo państwa trzeciego było zgodne z istotą podstawowych zasad zapisanych w RODO, aby można je było uznać za zapewniające odpowiedni stopień ochrony. Ramy ochrony danych Zjednoczonego Królestwa są w dużej mierze oparte na unijnych ramach ochrony danych (w szczególności na RODO oraz dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680, zwanej dalej „dyrektywą (UE) 2016/680"), co wynika z faktu, że Zjednoczone Królestwo było państwem członkowskim UE do 31 stycznia 2020 r. Ponadto w ustawie o ochronie danych Zjednoczonego Królestwa z 2018 r., która weszła w życie w dniu 23 maja 2018 r. i uchyliła ustawę o ochronie danych Zjednoczonego Królestwa z 1998 r., oprócz transpozycji dyrektywy (UE) 2016/680, doprecyzowano stosowanie RODO w prawie Zjednoczonego Królestwa, jak również przyznano uprawnienia krajowemu organowi nadzorczemu ds. ochrony danych, którym jest Urząd Rzecznika Informacji Zjednoczonego Królestwa (ang. Information Commissioner's Office), i nałożono na niego obowiązki. W związku z tym EROD uznaje, że Zjednoczone Królestwo w dużej mierze odzwierciedliło RODO w swoich ramach ochrony danych.

7. **Oczywistym jest, że analizując prawo i praktykę państwa trzeciego, które do niedawna było państwem członkowskim UE, EROD uznała wiele aspektów za merytorycznie równoważne z unijnymi.**

8. W obszarze ochrony danych EROD zauważa, że istnieje duża zbieżność między ramami RODO a ramami prawnymi Zjednoczonego Królestwa w zakresie niektórych podstawowych przepisów, takich jak np. przepisy dotyczące definicji pojęć (np. „dane osobowe"; „przetwarzanie danych osobowych"; „administrator danych"); podstaw zgodnego z prawem i rzetelnego przetwarzania danych do prawnie uzasadnionych celów; ograniczania celu; jakości i proporcjonalności danych; zatrzymywania danych, ich bezpieczeństwa i poufności; przejrzystości; szczególnych kategorii danych; marketingu bezpośredniego; zautomatyzowanego podejmowania decyzji i profilowania.

1.2. Wyzwania

9. Zjednoczone Królestwo było do niedawna państwem członkowskim UE; w związku z tym, analizując jego prawo i praktykę, EROD uznała wiele aspektów za merytorycznie równoważne z unijnymi. Jednocześnie, mając na uwadze swoją rolę w procesie przyjmowania ustalenia odpowiedniego stopnia ochrony, a także ograniczenia czasowe, EROD postanowiła skupić swoją uwagę na tych aspektach, w przypadku których uważa, że istnieje potrzeba pogłębionej analizy i bardziej szczegółowej kontroli.

10. Wyzwania jednak pozostają, a EROD uważa, że następujące elementy powinny zostać poddane dalszej ocenie w celu zapewnienia, że przestrzegany jest merytorycznie równoważny stopień ochrony, i że powinny one być ściśle monitorowane w Zjednoczonym Królestwie przez Komisję Europejską.

1.2.1. Uwagi ogólne

11. Pierwsze wyzwanie o charakterze ogólnym wiąże się z monitorowaniem zmian systemu prawnego Zjednoczonego Królestwa w zakresie kompleksowej ochrony danych. Rząd Zjednoczonego Królestwa wyraził zamiar opracowania odrębnej i niezależnej polityki w zakresie ochrony danych, z ewentualną wolą odejścia od unijnych przepisów o ochronie danych. Takie deklaracje polityczne nie znalazły jeszcze odzwierciedlenia w ramach prawnych Zjednoczonego Królestwa. Ta ewentualna przyszła **rozbieżność może jednak stworzyć zagrożenia dla utrzymania odpowiedniego stopnia ochrony danych osobowych przekazywanych z UE. Wzywa się zatem Komisję Europejską do ścisłego monitorowania takich zmian po wejściu w życie decyzji stwierdzającej odpowiedni stopień ochrony oraz do podjęcia niezbędnych działań, w tym, w stosownych przypadkach, w drodze zmiany lub zawieszenia decyzji.**

1.2.2. Ogólne aspekty ochrony danych

12. Po pierwsze, tak zwane „**wyłączenie do celów imigracyjnych**" ustanowione na mocy **załącznika 2 do ustawy o ochronie danych z 2018 r., część 1**, ustęp 4, **jest sformułowane „szeroko"**. W szczególności wyłączenie to ma zastosowanie również w przypadku, gdy dane osobowe nie są gromadzone przez administratora do celów kontroli imigracyjnej, ale są przez niego udostępniane innemu administratorowi, który przetwarza takie dane osobowe do celów kontroli imigracyjnej.

13. EROD zachęca Komisję Europejską do sprawdzenia stanu postępowania Open Rights Group & Anor, R (On the Application Of) przeciwko Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), a w związku z tym, że wyrok ten nie jest ostateczny (powaga rzeczy osądzonej), sprawdzenia, czy wyrok instancji odwoławczej podtrzyma go czy też zmieni, uwzględniając wszelkie informacje do wykorzystania w tym zakresie oraz wyszczególniając je w decyzji. **EROD wzywa także Komisję Europejską do przedstawienia w decyzji stwierdzającej odpowiedni stopień ochrony dalszych informacji na temat wyłączenia do celów imigracyjnych[6], w szczególności w odniesieniu do konieczności i proporcjonalności tak szerokiego wyłączenia w prawie Zjednoczonego Królestwa, zwłaszcza biorąc pod uwagę szeroki zakres zastosowania zakresu podmiotowego.** Jednocześnie EROD zachęca Komisję Europejską do dalszego zbadania, czy w ramach prawnych Zjednoczonego Królestwa istnieją lub mogą zostać przewidziane dodatkowe zabezpieczenia, na przykład za pomocą prawnie wiążących instrumentów, które uzupełniłyby wyłączenie do celów imigracyjnych w drodze zwiększenia jego przewidywalności i zabezpieczeń dla osób, których dane dotyczą, umożliwiając również lepszą i szybką ocenę i monitorowanie wymogów konieczności i proporcjonalności.

14. Po drugie, chociaż EROD uznaje, że Zjednoczone Królestwo w większości odzwierciedliło rozdział V RODO w swoich ramach ochrony danych, EROD wskazała pewne aspekty ram prawnych Zjednoczonego Królestwa **dotyczące dalszego przekazywania danych**, które mogą osłabić stopień ochrony danych osobowych przekazywanych z EOG.

[6] Także wyniku trwającego przeglądu stosowania wyłączenia do celów imigracyjnych, o którym mowa na s. 5 ram wyjaśniających rządu Zjednoczonego Królestwa na potrzeby dyskusji na temat odpowiedniego stopnia ochrony, sekcja E3: załącznik 2 Ograniczenia, 13 marca 2020 r., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf.

15. Art. 44 RODO stanowi istotnie[7], że przekazanie i dalsze przekazanie danych osobowych następuje tylko, gdy nie został naruszony stopień ochrony osób fizycznych zagwarantowany w RODO. **Oznacza to nie tylko, że przepisy Zjednoczonego Królestwa są „merytorycznie równoważne" przepisom UE w odniesieniu do przetwarzania danych osobowych przekazywanych do Zjednoczonego Królestwa na podstawie przyszłej decyzji stwierdzającej odpowiedni stopień ochrony, lecz także, że przepisy obowiązujące w Zjednoczonym Królestwie w odniesieniu do dalszego przekazywania tych danych do państw trzecich gwarantują dalsze zapewnianie merytorycznie równoważnego stopnia ochrony.**

16. Chociaż EROD odnotowuje zdolność Zjednoczonego Królestwa — na podstawie jego ram prawnych — do uznawania terytoriów za zapewniające odpowiedni stopień ochrony w świetle ram ochrony danych Zjednoczonego Królestwa, EROD pragnie podkreślić, że terytoria te obecnie mogą nie korzystać z decyzji stwierdzającej odpowiedni stopień ochrony wydanej przez Komisję Europejską i zapewniającej, że stopień ochrony jest „merytorycznie równoważny" stopniowi gwarantowanemu w EOG. Może to prowadzić do potencjalnych zagrożeń w zakresie ochrony danych osobowych przekazywanych z EOG, zwłaszcza jeśli w przyszłości ramy ochrony danych Zjednoczonego Królestwa będą odbiegać od dorobku prawnego UE. Ponadto Zjednoczone Królestwo uznało już za odpowiednie państwa trzecie, w odniesieniu do których Komisja Europejska stwierdziła odpowiedni stopień ochrony na mocy dyrektywy 95/46/WE[8], chociaż Komisja Europejska wkrótce dokona przeglądu tych ustaleń, a wnioski z tego przeglądu nie są jeszcze znane.

17. **W powyższych sytuacjach Komisja Europejska powinna zatem pełnić swoją rolę monitorującą, a w przypadku, gdy stopień ochrony danych osobowych przekazywanych z EOG merytorycznie równoważny stopniowi przewidzianemu w EOG nie zostanie utrzymany, Komisja Europejska powinna rozważyć zmianę decyzji stwierdzającej odpowiedni stopień ochrony w celu wprowadzenia szczególnych zabezpieczeń w odniesieniu do danych przekazywanych z EOG lub zawieszenia decyzji stwierdzającej odpowiedni stopień ochrony.**

18. **W odniesieniu do umów międzynarodowych zawartych między Zjednoczonym Królestwem a państwami trzecimi** zachęca się Komisję Europejską do zbadania zależności między ramami ochrony danych Zjednoczonego Królestwa a jego zobowiązaniami międzynarodowymi, poza umową w sprawie dostępu do danych elektronicznych w celu zwalczania poważnej przestępczości zawartą między Zjednoczonym Królestwem a Stanami Zjednoczonymi (zwanymi dalej „USA")[9] (zwaną dalej „umową między Zjednoczonym Królestwem a USA dotyczącą ustawy CLOUD"), w szczególności w celu zapewnienia ciągłości stopnia ochrony, w przypadku gdy dane osobowe są przekazywane z UE

[7] „Przekazanie danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej, następuje tylko, gdy – z zastrzeżeniem innych przepisów niniejszego rozporządzenia – administrator i podmiot przetwarzający spełnią warunki określone w niniejszym rozdziale, w tym warunki dalszego przekazania danych z państwa trzeciego lub przez organizację międzynarodową do innego państwa trzeciego lub innej organizacji międzynarodowej. Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu."

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

[9] Zob. umowa między rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej a rządem Stanów Zjednoczonych w sprawie dostępu do danych elektronicznych w celu zwalczania poważnej przestępczości zawarta w dniu 3 października 2019 r. w Waszyngtonie, D.C., w Stanach Zjednoczonych, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

do Zjednoczonego Królestwa na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, a następnie przekazywane do innych państw trzecich; oraz do ciągłego monitorowania i podejmowania działań, w stosownych przypadkach, na wypadek gdyby zawarcie umów międzynarodowych między Zjednoczonym Królestwem a państwami trzecimi mogło podważyć stopnień ochrony danych osobowych przewidziany w UE.

19. Ponadto wzywa się Komisję Europejską do monitorowania, czy umowa między Zjednoczonym Królestwem a USA dotycząca ustawy CLOUD zapewnia odpowiednie dodatkowe zabezpieczenia, uwzględniające stopień wrażliwości kategorii danych, których dotyczy, oraz wyłączne wymogi dotyczące przekazywania elektronicznych materiałów dowodowych bezpośrednio przez dostawców usług, a nie między organami, oceniając również, w jakich okolicznościach zabezpieczenia mogą zostać zapewnione poprzez odpowiednie wdrożenie dostosowania umowy ramowej UE-USA[10].

20. Ponadto EROD zauważa, że dalsze przekazywanie danych może również odbywać się ze Zjednoczonego Królestwa do innego państwa trzeciego w oparciu o **narzędzia przekazywania zgodnie z obowiązującym w Zjednoczonym Królestwie prawodawstwem dotyczącym ochrony danych**[11]. W następstwie spraw Schrems II[12], EROD zwraca się do Komisji Europejskiej o zapewnienie w decyzji stwierdzającej odpowiedni stopień ochrony, że niezbędne zabezpieczenia zostaną skutecznie wprowadzone, biorąc również pod uwagę prawodawstwo odbierającego państwa trzeciego.

21. Jeżeli chodzi o brak w prawodawstwie Zjednoczonego Królestwa **ochrony przewidzianej w art. 48 RODO**, EROD zwraca się do Komisji Europejskiej o przedstawienie dalszych zapewnień i konkretnych odniesień do prawodawstwa Zjednoczonego Królestwa, które zagwarantują, że stopień ochrony wynikający z ram prawnych Zjednoczonego Królestwa będzie merytorycznie równoważny stopniowi ochrony gwarantowanemu w EOG.

22. W odniesieniu do **mechanizmów proceduralnych i egzekwowania,** EROD zauważa, że istnienie i skuteczne funkcjonowanie niezależnego organu nadzorczego; istnienie systemu zapewniającego odpowiedni poziom zgodności; oraz systemu dostępu do odpowiednich mechanizmów dochodzenia roszczeń, dzięki któremu osoby fizyczne w EOG mogą korzystać ze swoich praw i dochodzić roszczeń bez napotykania uciążliwych barier w dochodzeniu roszczeń na drodze administracyjnej i sądowej, to kluczowe elementy, jakimi muszą charakteryzować się ramy ochrony danych zgodne z europejskimi.

23. EROD przyjmuje do wiadomości, że Zjednoczone Królestwo odzwierciedliło w większości odpowiednie przepisy RODO w RODO Zjednoczonego Królestwa i w ustawie o ochronie danych z 2018 r; wzywa się jednak Komisję Europejską do stałego monitorowania wszelkich zmian w ramach prawnych Zjednoczonego Królestwa i w praktyce, które mogłyby mieć szkodliwy wpływ na te obszary.

[10] Zob. Umowa między USA a UE w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych, grudzień 2016 (zwana dalej „umową ramową UE-USA"), https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=LEGISSUM:3104_8&from=PL.
[11] Zob. art. 46 i 47 RODO Zjednoczonego Królestwa.
[12] Zob. Schrems II.

1.2.3. W sprawie dostępu organów publicznych do danych przekazywanych do Zjednoczonego Królestwa

24. EROD odnotowuje znaczące zmiany w ramach prawnych Zjednoczonego Królestwa mających zastosowanie do agencji bezpieczeństwa i wywiadu, zwłaszcza w odniesieniu do przechwytywania i pozyskiwania danych komunikacyjnych. EROD uznaje, że zmiany te są między innymi odpowiedzią na postępowania wszczęte przed TSUE i Europejskim Trybunałem Praw Człowieka oraz na ich ostatnie wyroki w tym kontekście.

25. W szczególności EROD z zadowoleniem przyjmuje fakt, że Zjednoczone Królestwo ustanowiło Trybunał ds. Uprawnień Dochodzeniowo-Śledczych (ang. Investigatory Powers Tribunal). Trybunał ds. Uprawnień Dochodzeniowo-Śledczych jest właściwy nie tylko do rozpatrywania spraw dotyczących korzystania z uprawnień dochodzeniowych przez organy ścigania, ale również przez służby wywiadowcze. W rozumieniu EROD Trybunał ds. Uprawnień Dochodzeniowo-Śledczych funkcjonuje zatem jako właściwy sąd w rozumieniu art. 47 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych UE").

26. Ponadto EROD pozytywnie odnotowuje wprowadzenie „komisarzy sądowych" (ang. Judicial Commissioners) w ustawie o uprawnieniach dochodzeniowo-śledczych z 2016 r. (ang. Investigatory Powers Act 2016, zwanej dalej „IPA 2016") jako znaczącą poprawę. EROD wnioskuje, że ważną funkcją komisarzy sądowych jest zatwierdzanie *ex ante* w poszczególnych przypadkach różnych środków nadzoru, w tym ukierunkowanego przechwytywania i masowego pozyskiwania danych komunikacyjnych (tzw. procedura „podwójnego zabezpieczenia").

27. Aby ocenić skuteczność tego dodatkowego poziomu nadzoru, EROD dostrzega jednak potrzebę dalszego wyjaśnienia scenariuszy, w których możliwe jest zgodne z prawem przechwytywanie danych bez zgody Komisarza ds. uprawnień dochodzeniowo-śledczych (ang. Investigatory Powers Commissioner) lub komisarzy sądowych, oraz wzywa Komisję Europejską do dalszej oceny i wykazania, że — nawet w przypadkach, w których procedura podwójnego zabezpieczenia nie ma zastosowania — ramy prawne Zjednoczonego Królestwa zapewniają odpowiednie zabezpieczenia, w tym dzięki skutecznemu nadzorowi *ex post* i możliwościom dochodzenia roszczeń dostępnym dla osób fizycznych, zapewniając tym samym stopień ochrony merytorycznie równoważny stopniowi zapewnianemu w UE.

28. Ponadto EROD wzywa Komisję Europejską do dalszej oceny warunków, na podstawie których można powołać się na pilny charakter sprawy, oraz do przedstawienia wyjaśnień dotyczących możliwych sposobów wykonywania praw przez osoby, których dane dotyczą, oraz ewentualnych możliwości dochodzenia roszczeń oferowanych im w kontekście działań polegających na ingerencji w urządzenia w celu pozyskania danych (ang. equipment interference), zwłaszcza w przypadku odstępstwa od procedury podwójnego zabezpieczenia.

29. EROD stwierdza również, że istnieje potrzeba dalszego wyjaśnienia i oceny masowego przechwytywania danych, w szczególności w odniesieniu do wyboru i stosowania selektorów (kryteriów wyszukiwania), w celu wyjaśnienia zakresu, w jakim dostęp do danych osobowych spełnia wymagania progowe określone przez TSUE, oraz jakie zabezpieczenia są stosowane w celu ochrony praw podstawowych osób fizycznych, których dane są przechwytywane w tym kontekście, w tym w odniesieniu do okresów zatrzymywania danych. Szczególnie przydatna byłaby niezależna ocena ze strony właściwych organów nadzorczych Zjednoczonego Królestwa. EROD podkreśla również, że tym istotniejszy wydaje się fakt, że „łączność międzynarodowa", która wchodzi w zakres praktyk masowego przechwytywania, wydaje się oznaczać, że dane mogłyby być bezpośrednio

przechwytywane i gromadzone masowo w UE przez Zjednoczone Królestwo, w tym w odniesieniu do danych przekazywanych między UE a Zjednoczonym Królestwem, które wchodziłyby w zakres projektu decyzji. Biorąc pod uwagę znaczenie tego aspektu, EROD wzywa Komisję Europejską do ścisłego monitorowania zmian w tym względzie.

30. Nadal w odniesieniu do masowego przechwytywania danych EROD podkreśla spójną ocenę Europejskiego Trybunału Praw Człowieka i TSUE oraz przypomina obawy wyrażone w odniesieniu do danych wtórnych, które powinny stanowić przedmiot szczególnych zabezpieczeń ze względu na ich wrażliwość. EROD wzywa zatem Komisję Europejską do starannej oceny, czy zabezpieczenia przewidziane w prawie Zjednoczonego Królestwa dla tej kategorii danych osobowych zapewniają stopień ochrony merytorycznie równoważny stopniowi gwarantowanemu w EOG.

31. W tym kontekście EROD jest świadoma faktu, że publiczne sprawozdanie komisji parlamentarnej do spraw wywiadu i bezpieczeństwa (ang. Intelligence and Security Committee) z 2016 r. w sprawie wykorzystania uprawnień dotyczących masowego operowania danymi[13] odnosi się do praktyk stosowanych w poprzednich ramach prawnych, które zostały następnie zastąpione przez IPA 2016. Dostrzega jednak potrzebę dalszej niezależnej oceny i nadzoru nad stosowaniem narzędzi do zautomatyzowanego przetwarzania danych przez właściwe organy nadzoru Zjednoczonego Królestwa i wzywa Komisję Europejską do dalszej oceny tej kwestii oraz zabezpieczeń, jakie w tym kontekście zostałyby lub mogłyby zostać zapewnione osobom w EOG, których dane dotyczą.

32. EROD podziela pogląd wyrażony przez Komisarza ds. uprawnień dochodzeniowo-śledczych, że konieczny jest dalszy przegląd i monitorowanie w celu zapewnienia, aby zabezpieczenia stosowane w praktyce przez właściwe organy w dziedzinie bezpieczeństwa narodowego i wywiadu w celu usunięcia niezgodności związanych ze stosowaniem odpowiedniego prawodawstwa zostały utrzymane i były nadal ulepszane. EROD z zadowoleniem przyjmuje również fakt, że w rezultacie Komisarz ds. uprawnień dochodzeniowo-śledczych przeprowadził w 2019 r. przegląd swojego podejścia do kontroli przechwytywania masowego, „który obejmował dokładny przegląd technicznie złożonych sposobów faktycznego wdrażania przechwytywania masowego" i zobowiązał się do włączenia „szczegółowej analizy selektorów i kryteriów wyszukiwania, o których wspomniał powyżej Europejski Trybunał Praw Człowieka" do kontroli przechwytywania masowego począwszy od 2020 r. Uwzględniając znaczenie tego aspektu, EROD wyraża zaniepokojenie faktem, że szczegółowa kontrola selektorów i kryteriów wyszukiwania nie została jeszcze przeprowadzona przez Komisarza ds. uprawnień dochodzeniowo-śledczych i wzywa Komisję Europejską do ścisłego monitorowania rozwoju sytuacji w tym zakresie, zwłaszcza że konkretna forma takiego nadzoru nie została jeszcze określona.

33. EROD podkreśla, że w przypadku ujawniania informacji za granicą zastosowanie wyłączenia dotyczącego bezpieczeństwa narodowego przewidzianego w prawie Zjednoczonego Królestwa może prowadzić do braku zabezpieczeń gwarantujących przestrzeganie zasad ograniczenia celu, konieczności (niezbędności) i proporcjonalności lub przewidujących, że w państwie trzecim przeznaczenia zostaną również zapewnione lub będą przestrzegane wystarczające prawa osób fizycznych, nadzór i możliwość dochodzenia roszczeń. EROD zaleca zatem, aby Komisja Europejska dokładniej zbadała ogólne zabezpieczenia przewidziane w prawie Zjednoczonego Królestwa

[13] Zob. sprawozdanie z przeglądu uprawnień dotyczących masowego operowania danymi sporządzone przez niezależnego kontrolera do spraw ustawodawstwa dotyczącego terroryzmu (ang. Independent Reviewer of Terrorism Legislation), sierpień 2016 r, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf.

w odniesieniu do ujawniania informacji za granicą, w szczególności w świetle stosowania wyłączeń dotyczących bezpieczeństwa narodowego.

34. Ponadto EROD wyraża zaniepokojenie innymi formami wymiany i ujawniania informacji na podstawie innych instrumentów, w szczególności poszczególnych umów międzynarodowych zawartych przez Zjednoczone Królestwo z innymi państwami trzecimi, zwłaszcza w przypadkach, gdy instrumenty te pozostają niedostępne publicznie, takich jak umowa w sprawie wywiadu telekomunikacyjnego (ang. Communication Intelligence Agreement) między Zjednoczonym Królestwem a USA. Skutkiem takiej umowy mogłoby być obejście zabezpieczeń określonych w odniesieniu do dostępu do danych osobowych i wykorzystywania ich do celów bezpieczeństwa narodowego. EROD uważa, że zawarcie dwustronnych lub wielostronnych umów z państwami trzecimi w celu współpracy wywiadowczej, stanowiących podstawę prawną dla bezpośredniego przechwytywania i uzyskiwania danych osobowych lub przekazywania danych osobowych do tych państw, może również znacząco wpłynąć na warunki dalszego wykorzystania zebranych informacji, ponieważ umowy takie prawdopodobnie wpłyną na ramy prawne ochrony danych w Zjednoczonym Królestwie, które zostały poddane ocenie.

1.3. Wnioski

35. EROD uważa, że ocena odpowiedniego stopnia ochrony danych przez Zjednoczone Królestwo jest wyjątkowa ze względu na poprzedni status Zjednoczonego Królestwa jako państwa członkowskiego UE. Oprócz tego byłaby to też pierwsza decyzja stwierdzająca odpowiedni stopień ochrony zawierająca klauzulę wygaśnięcia.

36. W związku z tym EROD uznaje wiele obszarów zbieżności między ramami ochrony danych w Zjednoczonym Królestwie i w UE. Jednocześnie jednak, po wnikliwej analizie projektu decyzji Komisji Europejskiej oraz prawodawstwa Zjednoczonego Królestwa dotyczącego ochrony danych, EROD wskazała szereg wyzwań, które poddano w niniejszej opinii obszernej analizie. W tym kontekście EROD pragnie podkreślić pierwszoplanową rolę Komisji Europejskiej w zakresie monitorowania wszystkich istotnych zmian w Zjednoczonym Królestwie.

37. W świetle powyższego EROD zaleca Komisji Europejskiej podjęcie wyzwań, o których jest mowa w niniejszej opinii. EROD zachęca również Komisję Europejską do ścisłego monitorowania wszystkich istotnych zmian w Zjednoczonym Królestwie, które mogą mieć wpływ na niezbędną odpowiedniość stopnia ochrony danych osobowych oraz szybkiego podejmowania stosownych działań w razie potrzeby.

2. WPROWADZENIE

2.1. Ramy ochrony danych Zjednoczonego Królestwa

38. Ramy ochrony danych Zjednoczonego Królestwa są w dużej mierze oparte na unijnych ramach ochrony danych (w szczególności na RODO oraz dyrektywie (UE) 2016/680, co wynika z faktu, że Zjednoczone Królestwo było państwem członkowskim UE do 31 stycznia 2020 r. Co więcej, w ustawie o ochronie danych Zjednoczonego Królestwa z 2018 r., która weszła w życie w dniu 23 maja 2018 r. i uchyliła ustawę o ochronie danych Zjednoczonego Królestwa z 1998 r., oprócz transpozycji dyrektywy (UE 0 2016/680, doprecyzowano stosowanie RODO w prawie Zjednoczonego Królestwa, jak również przyznano uprawnienia krajowemu organowi nadzorczemu ds. ochrony danych, którym jest Urząd Rzecznika Informacji Zjednoczonego Królestwa, i nałożono na niego obowiązki.

39. Jak wspomniano w motywie 12 projektu decyzji Komisji Europejskiej, rząd Zjednoczonego Królestwa uchwalił Ustawę o wystąpieniu z Unii Europejskiej z 2018 r., na mocy której włączono bezpośrednio stosowane przepisy UE do prawa Zjednoczonego Królestwa. Na podstawie tej ustawy ministrowie Zjednoczonego Królestwa są uprawnieni do wprowadzania prawa wtórnego, za pomocą aktów prawnych, w celu dokonania niezbędnych zmian w utrzymanym prawie Unii po wystąpieniu Zjednoczonego Królestwa z UE, tak aby dostosować je do kontekstu krajowego.

40. W związku z tym odpowiednie ramy prawne mające zastosowanie w Zjednoczonym Królestwie po zakończeniu okresu przejściowego[14] obejmują:

- ogólne rozporządzenie o ochronie danych Zjednoczonego Królestwa (zwane dalej „rozporządzeniem o ochronie danych Zjednoczonego Królestwa"), włączone do prawa Zjednoczonego Królestwa na mocy Ustawy o wystąpieniu z Unii Europejskiej z 2018 r. i zmienione rozporządzeniami o ochronie danych, prywatności i komunikacji elektronicznej (zmiany itp.) (wystąpienie z UE) z 2019 r. (Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019);
- ustawę o ochronie danych z 2018 r., zmienioną rozporządzeniami o ochronie danych, prywatności i komunikacji elektronicznej z 2019 r., oraz rozporządzenia o ochronie danych, prywatności i komunikacji elektronicznej (zmiany itp.) (wystąpienie z UE) z 2020 r. (Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020) oraz
- IPA 2016.

(łącznie zwane „ramami ochrony danych Zjednoczonego Królestwa").

2.2. Zakres oceny przeprowadzonej przez EROD

41. Projekt decyzji Komisji Europejskiej jest wynikiem oceny ram ochrony danych Zjednoczonego Królestwa, która poprzedzała rozmowy z rządem Zjednoczonego Królestwa. Zgodnie z art. 70 ust. 1 lit. s) RODO od EROD oczekuje się przedstawienia niezależnej opinii na temat ustaleń Komisji Europejskiej, określenia ewentualnych niedociągnięć w ramach oceny odpowiedniego stopnia ochrony danych oraz podjęcia starań w celu przedstawienia propozycji zaradzenia takim niedociągnięciom.

42. Jak wspomniano w dokumencie dotyczącym odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO: „informacje dostarczone przez Komisję Europejską powinny być wyczerpujące i powinny umożliwić EROD dokonanie własnej oceny stopnia ochrony danych osobowych w państwie trzecim"[15].

43. W tym względzie należy zauważyć, że EROD jedynie częściowo otrzymała na czas dokumenty niezbędne do przeprowadzenia analizy ram prawnych Zjednoczonego Królestwa. EROD otrzymała większość przepisów Zjednoczonego Królestwa, o których mowa w projekcie decyzji, za pośrednictwem linków zamieszczonych w tym projekcie. Komisja Europejska nie była w stanie przedstawić EROD pisemnych wyjaśnień i zobowiązań Zjednoczonego Królestwa w odniesieniu do

[14] Okres przejściowy ustalono do dnia 31 grudnia 2020 r., po którym to terminie prawo Unii nie będzie już stosowane w Zjednoczonym Królestwie. Dodatkowy okres przejściowy (ang. „bridge period") został ustalony najpóźniej do dnia 30 czerwca 2021 r. i odnosi się do dodatkowego okresu, w którym przekazywanie danych osobowych z EOG do Zjednoczonego Królestwa nie jest uznawane za przekazywanie do państwa trzeciego.
[15] Zob. WP254 rev.01, s. 3.

wymiany informacji między władzami Zjednoczonego Królestwa a Komisją Europejską istotnych z punktu widzenia tego zadania[16].

44. Uwzględniając powyższe oraz z uwagi na ograniczony czas (2 miesiące) przyznany EROD na przyjęcie niniejszej opinii, EROD postanowiła skupić się na niektórych szczególnych elementach przedstawionych w projekcie decyzji i przedstawić swoją analizę i opinię na ich temat.

45. Oczywiste jest, że analizując prawo i praktykę państwa trzeciego, które do niedawna było państwem członkowskim UE, EROD uznała wiele aspektów za merytorycznie równoważne z unijnymi. Mając na uwadze swoją rolę w procesie przyjmowania ustaleń dotyczących zapewnienia odpowiedniego stopnia ochrony oraz liczbę przepisów prawa i praktyk, które należy przeanalizować, EROD postanowiła skupić swoją uwagę na tych aspektach, w przypadku których dostrzegła największą potrzebę dokładniejszej analizy. Ponadto, zgodnie z orzecznictwem TSUE, bardzo istotna część analizy obejmuje system prawny regulujący dostęp organów bezpieczeństwa narodowego do danych osobowych przekazywanych do Zjednoczonego Królestwa oraz praktykę aparatu bezpieczeństwa narodowego w Zjednoczonym Królestwie. Należy jednak pamiętać, że bezpieczeństwo narodowe stanowi w sposób oczywisty obszar prawa i praktyki, w którym prawodawstwo państw członkowskich nie jest zharmonizowane na szczeblu UE, a zatem mogą występować różnice.

46. EROD uwzględniła obowiązujące europejskie ramy ochrony danych osobowych, w tym art. 7, 8 i 47 Karty praw podstawowych Unii Europejskiej, 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 (zwanej dalej „EKPC") chroniący prawo do życia prywatnego i rodzinnego. Oprócz powyższego EROD wzięła pod uwagę wymogi RODO, jak również odpowiednie orzecznictwo.

47. Celem tego działania jest dostarczenie Komisji Europejskiej opinii dotyczącej oceny odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie. Pojęcie „odpowiedniego stopnia ochrony", które istniało już w ramach dyrektywy 95/46/WE, zostało rozwinięte przez TSUE. Należy przypomnieć normę ustanowioną przez TSUE w wyroku w sprawie Schrems I, zgodnie z którą – 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

[16] W odniesieniu do: art. 48 RODO (przypis 78 w projekcie decyzji); wzmocnionych zabezpieczeń i środków bezpieczeństwa stosowanych przez administratorów przy przetwarzaniu w kontekście bezpieczeństwa narodowego (przypis 64 w projekcie decyzji); wymogu, aby administrator rozważył, czy występuje konieczność stosowania wyłączeń w indywidualnych przypadkach, nawet w przypadku gdy wydano certyfikat bezpieczeństwa narodowego (motyw 126 i przypis 172 w projekcie decyzji); faktu, że ochrona przewidziana w umowie ramowej między UE a Stanami Zjednoczonymi będzie obowiązywała w stosunku do wszystkich danych osobowych wytworzonych lub zabezpieczanych na podstawie umowy między Zjednoczonym Królestwem a USA dotyczącej ustawy CLOUD, niezależnie od charakteru lub rodzaju organu wnioskującego w odniesieniu do szczegółów dotyczących konkretnego wdrożenia zabezpieczeń w zakresie ochrony danych, które są nadal przedmiotem dyskusji między Zjednoczonym Królestwem a Stanami Zjednoczonymi, potwierdzenia, że władze Zjednoczonego Królestwa zezwolą na wejście w życie tej umowy tylko po upewnieniu się, że jej wdrożenie jest zgodne z zawartymi w niej zobowiązaniami prawnymi, w tym jasności w zakresie zgodności ze standardami ochrony danych, w przypadku wszelkich danych, o które wnioskuje się w ramach tej umowy (motyw 153 projektu decyzji); sytuacji, w których dane przekazywane są z UE do Zjednoczonego Królestwa w zakresie objętym tym projektem decyzji oraz faktu, że zawsze występowałoby „połączenie Wysp Brytyjskich" oraz że wszelkie działania polegające na ingerencji w urządzenia w celu pozyskania takich danych podlegałoby zatem obowiązkowemu wymogowi uzyskania nakazu określonego w sekcji 13 ust. 1 IPA 2016 (motyw 206 projektu decyzji) oraz podanych przykładów celów operacyjnych (motyw 216 i przypis 369 w projekcie decyzji).

zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w Unii”[17]. W związku z tym celem nie jest dokładne powielanie prawodawstwa europejskiego, lecz ustalenie zasadniczych i podstawowych wymogów badanego prawodawstwa. Odpowiedni stopień ochrony danych można osiągnąć w drodze połączenia praw osób, których dane dotyczą, i obowiązków podmiotów, które przetwarzają dane lub sprawują kontrolę nad takim przetwarzaniem, oraz nadzoru 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 przekazywanych do państwa trzeciego lub organizacji międzynarodowej, ale także systemu wprowadzonego w celu zapewnienia skuteczności tych przepisów. Skuteczne mechanizmy egzekwowania prawa mają pierwszorzędne znaczenie dla skuteczności przepisów o ochronie danych[18].

2.3. Uwagi i zastrzeżenia ogólne

2.3.1 Zobowiązania międzynarodowe zaciągnięte przez Zjednoczone Królestwo

48. Zgodnie z art. 45 ust. 2 lit. c) RODO i dokumentem dotyczącym odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO[19], oceniając odpowiedni stopień ochrony danych w państwie trzecim, Komisja Europejska musi wziąć pod uwagę m.in. międzynarodowe zobowiązania państwa trzeciego lub inne obowiązki wynikające z jego udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych, a także realizację takich obowiązków. Ponadto należy wziąć pod uwagę przystąpienie państwa trzeciego do Konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (zwanej dalej „konwencją 108”)[20] oraz protokołu dodatkowego do tej konwencji[21].

49. **W tym względzie EROD z zadowoleniem przyjmuje fakt, że Zjednoczone Królestwo przystąpiło do EKPC i podlega jurysdykcji Europejskiego Trybunału Praw Człowieka. Ponadto Zjednoczone Królestwo przystąpiło również do konwencji 108 i protokołu dodatkowego do tej konwencji, a w 2018 r. podpisało konwencję 108+[22] i obecnie pracuje nad jej ratyfikacją.**

2.3.2 Możliwe przyszłe rozbieżności ram ochrony danych Zjednoczonego Królestwa

50. Jak wspomniano w motywie 281 projektu decyzji, Komisja Europejska musi wziąć pod uwagę, że wraz z końcem okresu przejściowego przewidzianego w umowie o wystąpieniu[23] Zjednoczone Królestwo stosuje i egzekwuje własny system ochrony danych oraz zarządza nim, a gdy tylko przestanie obowiązywać przepis przejściowy na podstawie art. FINPROV.10A umowy o handlu i współpracy

[17] Zob. wyrok TSUE z dnia 6 października 2015 r., Maximilian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, (zwany dalej „Schrems I”), pkt 73–74.
[18] Zob. WP254 rev.01, s. 2.
[19] Zob. WP254 rev.01, s. 2.
[20] Zob. Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, konwencja 108, 28 stycznia 1981 r.
[21] Zob. Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzorczych i transgranicznych przepływów danych, sporządzony w dniu 8 listopada 2001 r.
[22] Zob. Protokół zmieniający Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych („konwencja 108+”) z dnia 18 maja 2018 r.
[23] Zob. Umowa o wystąpieniu Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej z Unii Europejskiej i Europejskiej Wspólnoty Energii Atomowej (Dz.U. L 029 z 31.1.2020, s. 7).

między Zjednoczonym Królestwem a UE[24] może to w szczególności wiązać się z poprawkami lub zmianami ram ochrony danych ocenianych w projekcie decyzji, jak również innymi istotnymi zmianami.

51. Komisja Europejska postanowiła zatem włączyć do projektu decyzji klauzulę wygaśnięcia[25], ustalając datę wygaśnięcia decyzji na cztery lata po jej wejściu w życie.

52. Należy zauważyć, że możliwość wprowadzenia przez ministrów i sekretarza stanu Zjednoczonego Królestwa prawodawstwa wtórnego po zakończeniu dodatkowego okresu przejściowego może doprowadzić w przyszłości do znacznej rozbieżności między ramami ochrony danych Zjednoczonego Królestwa a ramami unijnymi.

53. Rząd Zjednoczonego Królestwa wskazał na swój zamiar opracowania odrębnych i niezależnych polityk dotyczących ochrony danych, co może następnie doprowadzić do rozbieżności z unijnymi przepisami o ochronie danych[26]. Zamiar ten obejmuje włączenie aspektów dotyczących danych osobowych do umów handlowych[27], praktykę, która niesie ze sobą ryzyko obniżenia stopnia ochrony danych osobowych zapewnianych przez Zjednoczone Królestwo[28].

---

[24] Zob. Umowa o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej, z jednej strony, a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej, z drugiej strony (Dz.U. L 444 z 31.12.2020, s. 14).

[25] Zob. art. 4 projektu decyzji. Zob. również motyw 282 projektu decyzji.

[26] W Narodowej strategii Zjednoczonego Królestwa w sprawie danych (ostatnia aktualizacja w dniu 9 grudnia 2020 r., https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy) zawarto m.in. następującą misję: „Wprowadzanie międzynarodowego przepływu danych. Przepływ danych przez granice dynamizuje międzynarodową działalność gospodarczą, łańcuchy dostaw i handel, wzmacniając wzrost gospodarczy na świecie. Odgrywa również szerszą rolę społeczną. Przekazywanie danych osobowych zapewnia wypłatę wynagrodzeń i pomaga ludziom kontaktować się z bliskimi osobami, które przebywają daleko. Oprócz tego, jak udowodniła pandemia koronawirusa, udostępnianie danych dotyczących zdrowia może wspomóc kluczowe badania naukowe w dziedzinie chorób i jednocześnie łączyć kraje w ramach reagowania na globalne sytuacje zagrożenia zdrowia. **Po opuszczeniu Unii Europejskiej Zjednoczone Królestwo będzie orędownikiem korzyści, jakie mogą zapewnić dane.** Będziemy upowszechniać najlepsze praktyki krajowe i współpracować z partnerami międzynarodowymi **w celu zapewnienia, aby dane nie były w sposób niewłaściwy ograniczane granicami krajowymi i rozdrobnionymi systemami regulacyjnymi**, tak aby można było w pełni wykorzystać potencjał tych danych.” (pogrubienie dodano).

[27] Ibidem: „Ułatwienie transgranicznych przepływów danych: **Będziemy pracować na arenie światowej na rzecz usunięcia niepotrzebnych barier dla międzynarodowych przepływów danych. W naszych negocjacjach handlowych ustalimy ambitne postanowienia dotyczące danych** i wykorzystamy nasze nowo uzyskane niezależne członkostwo w Światowej Organizacji Handlu, aby wywrzeć wpływ na udoskonalenie reguł handlu w odniesieniu do danych. **Usuniemy bariery hamujące międzynarodowe przekazywanie danych** wspierających wzrost i innowacje, w tym dzięki opracowaniu nowej zdolności Zjednoczonego Królestwa zapewniającej nowe i innowacyjne mechanizmy międzynarodowego przekazywania danych. Będziemy również pracować wspólnie z naszymi partnerami w ramach G20 na rzecz tworzenia interoperacyjności między krajowymi systemami danych, aby minimalizować komplikacje związane z przekazywaniem danych między krajami”. (pogrubienie dodano).

[28] Zob. rezolucję Parlamentu Europejskiego z dnia 12 grudnia 2017 r. „W kierunku strategii w zakresie handlu elektronicznego” (2017/2065(INI)), sekcję V, w której podkreślono, że „ochrona danych osobowych jest kwestią niepodlegającą negocjacjom w umowach handlowych [UE]”, dostępną pod adresem: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0488_PL.pdf Zob. także rezolucję Parlamentu Europejskiego z dnia 25 marca 2021 r. w sprawie sprawozdania Komisji z oceny wdrożenia ogólnego rozporządzenia o ochronie danych po dwóch latach jego stosowania, pkt 28, w którym stwierdza się: „popiera stosowaną przez Komisję praktykę rozdzielania kwestii ochrony danych i przepływu danych osobowych od umów handlowych”, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_PL.html

54. Ponadto od zakończenia okresu przejściowego Zjednoczone Królestwo nie tylko nie jest już związane orzecznictwem TSUE, ale również wydane już wyroki TSUE, uważane za zachowane orzecznictwo w ramach prawnych Zjednoczonego Królestwa, mogą nie być już wiążące dla Zjednoczonego Królestwa, zwłaszcza z uwagi na fakt, że Zjednoczone Królestwo ma możliwość zmiany zachowanego prawa Unii po zakończeniu dodatkowego okresu przejściowego, a jego Sąd Najwyższy nie jest związany żadnym zachowanym orzecznictwem UE[29].

55. **Mając na uwadze ryzyko związane z ewentualnymi rozbieżnościami między ramami ochrony danych Zjednoczonego Królestwa a dorobkiem prawnym UE po zakończeniu dodatkowego okresu przejściowego, EROD z zadowoleniem przyjmuje decyzję Komisji Europejskiej o wprowadzeniu do projektu decyzji czteroletniej klauzuli wygaśnięcia. EROD pragnie jednak podkreślić znaczenie monitorującej roli Komisji Europejskiej[30]. Komisja Europejska powinna monitorować na bieżąco i w sposób ciągły wszystkie istotne zmiany w Zjednoczonym Królestwie, które mogą mieć wpływ na niezbędną odpowiedniość stopnia ochrony danych osobowych przekazywanych na podstawie decyzji stwierdzającej odpowiedni stopień ochrony w Zjednoczonym Królestwie począwszy od momentu wejścia w życie tej decyzji. Ponadto Komisja Europejska powinna podjąć odpowiednie działania poprzez zawieszenie, zmianę lub uchylenie decyzji stwierdzającej odpowiedni stopień ochrony, stosownie do okoliczności, jeżeli po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony Komisja Europejska odnotuje sygnały świadczące o tym, że w Zjednoczonym Królestwie nie jest już zapewniony odpowiedni stopień ochrony.**

56. Ze swojej strony EROD dołoży wszelkich starań, aby informować Komisję Europejską o wszelkich istotnych działaniach podejmowanych przez organy nadzorczymi ds. ochrony danych w państwach członkowskich (zwane dalej „organami nadzorczymi"), w sektorze komercyjnym bądź publicznym, a w szczególności o skargach składanych przez osoby, których dane dotyczą, w EOG w zakresie przekazywania danych osobowych z EOG do Zjednoczonego Królestwa.

3. ASPEKTY OGÓLNE OCHRONY DANYCH

3.1. Zasady dotyczące treści

57. Rozdział 3 dokumentu dotyczącego odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO poświęcony jest „zasadom dotyczącym treści". System państwa trzeciego musi obejmować zasady dotyczące treści, aby jego stopień ochrony danych można było uznać za merytorycznie równoważny stopniowi gwarantowanemu w UE. EROD uznaje fakt, że Zjednoczone Królestwo nie posiada skodyfikowanej konstytucji, a zatem nie istnieje żaden jednolity dokument określający podstawowe zasady regulacyjne. Prawo do poszanowania życia prywatnego i rodzinnego (oraz prawo do ochrony danych w ramach tego prawa), a także prawo do rzetelnego procesu sądowego[31] zawarte są w ustawie o prawach człowieka z 1998 r., a konstytucyjną wartość tej ustawy uznały sądy Zjednoczonego Królestwa. Ustawa o prawach człowieka z 1998 r. faktycznie obejmuje prawa zawarte w EKPC[32]. Ponadto ustawa o prawach człowieka z 1998 r. zawiera bardzo ważne stwierdzenie, że wszelkie działanie organów publicznych musi być zgodne z EKPC[33].

[29] Zob. art. 6 ust. 3 do 6 umowy o wystąpieniu z UE z 2018 r.
[30] Zob. art. 45 ust. 4 RODO.
[31] Zob. art. 6 i 8 EKPC (Załącznik 1 do ustawy o prawach człowieka z 1998 r.).
[32] Więcej informacji można znaleźć w motywach 8–10 projektu decyzji.
[33] Zob. sekcję 6 ustawy o prawach człowieka z 1998 r.

58. Poza strukturalnymi i formalistycznymi różnicami między prawodawstwem Zjednoczonego Królestwa i UE, EROD zauważa, że jak można oczekiwać, podejście Zjednoczonego Królestwa do ochrony danych jest podobne do podejścia unijnego, co wynika z faktu, że Zjednoczone Królestwo było państwem członkowskim UE do 31 stycznia 2020 r. Stąd wiele zasad dotyczących treści jest zgodnych z zasadami RODO; a zatem zapewniają one stopień ochrony merytorycznie równoważny stopniowi ochrony gwarantowanemu w UE. EROD postanowiła nie rozwijać dalej analizy zasad dotyczących treści zgodnych z prawodawstwem UE i jest usatysfakcjonowana analizą przedstawioną przez Komisję Europejską w projekcie decyzji. Do takich zasad dotyczących treści należą na przykład m.in.: pojęcia (np. „dane osobowe"; „przetwarzanie danych osobowych"; „administrator danych"); podstawy zgodnego z prawem i rzetelnego przetwarzania danych do prawnie uzasadnionych celów; ograniczanie celu; jakość i proporcjonalność danych; zatrzymywanie danych, ich bezpieczeństwa i poufności; przejrzystość; szczególne kategorii danych; marketing bezpośredni; zautomatyzowane podejmowanie decyzji i profilowania. EROD zauważa dalej, że RODO Zjednoczonego Królestwa oraz ustawa o ochronie danych z 2018 r. zawierają zasady dotyczące treści idące dalej, niż wymogi zawarte w dokumencie dotyczącym odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO, i odzwierciedlają zasady zawarte w RODO; podwyższają zatem stopień ochrony przewidziany w Zjednoczonym Królestwie. Takie zasady dotyczące treści to na przykład zasady dotyczące zgłaszania naruszenia ochrony danych osobowych, inspektora ochrony danych, ocen skutków dla ochrony danych oraz uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

59. Jak wspomniano we wprowadzeniu, EROD pragnie jednak w niniejszej opinii zająć się pewnymi kwestiami, które budzą jej obawy i w sprawie których chciałaby zwrócić się do Komisji Europejskiej o wyjaśnienie.

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

60. Tzw. „wyłączenie do celów imigracyjnych" określone w **załączniku 2 do ustawy o ochronie danych z 2018 r. części 1** ust. 4 zezwala administratorom zajmującym się „kontrolą imigracyjną" na niestosowanie niektórych praw osób, których dane dotyczą, przewidzianych w ustawie o ochronie danych z 2018 r. w przypadku, gdy mogłoby to „stanąć na przeszkodzie utrzymaniu skutecznej kontroli imigracyjnej" lub „prowadzeniu dochodzeń w sprawie działań lub wykrywaniu działań osłabiających utrzymywanie skutecznej kontroli imigracyjnej".

61. Jak uznano w projekcie decyzji Komisji Europejskiej[34] i jak wspomniano w opinii Komisji LIBE Parlamentu Europejskiego w sprawie zawarcia w imieniu UE umowy o handlu i współpracy między UE a Zjednoczonym Królestwem,[35] wyłączenie to jest **sformułowane „szeroko"**. Dotyczy ono

[34] Zob. motywy 62–65 projektu decyzji.

[35] W tym względzie w odniesieniu do **szerokiego sformułowania** wyłączenia do celów imigracyjnych, zob. Opinia Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w sprawie zawarcia, w imieniu Unii, Umowy o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej, z jednej strony, a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej, z drugiej strony, oraz Umowy między Unią Europejską a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej w sprawie procedur bezpieczeństwa na potrzeby wymiany i ochrony informacji niejawnych (2020/0382(NLE)), 5 lutego 2021 r., https://www.europarl.europa.eu/doceo/document/LIBE-AL-680848_PL.pdf, pkt 10: „przypomina w związku z tym rezolucje Parlamentu z lutego i czerwca 2020 r., w których zwrócono uwagę na **ogólne i szerokie wyłączenie** przetwarzania danych osobowych do celów imigracyjnych z ustawy o ochronie danych w Zjednoczonym Królestwie" oraz pkt 11: „uważa, że przed wydaniem ważnej decyzji stwierdzającej odpowiedni poziom ochrony należy zmienić **ogólne i szerokie** wyłączenie przetwarzania danych osobowych do celów imigracyjnych z ustawy o ochronie danych w Zjednoczonym Królestwie" (pogrubienie dodano).

następujących praw: prawa do otrzymania informacji; prawa dostępu; prawa do usunięcia danych; prawa do ograniczenia przetwarzania; oraz prawa sprzeciwu.

62. Poza tym należy zwrócić uwagę, że wyłączenie to obowiązuje również w przypadku, gdy dane osobowe nie są zbierane przez administratora („administratora 1") w celu kontroli imigracyjnej, lecz są przez niego udostępniane innemu administratorowi („administratorowi 2"), który przetwarza te dane osobowe w celu kontroli imigracyjnej (np. Ministerstwu Spraw Wewnętrznych (Home Office) Zjednoczonego Królestwa)36.

63. W sprawie Open Rights Group i in., R (W sprawie stosowania) przeciwko Secretary of State for the Home Department i in. [2019] EWHC 2562 (Admin) (3 października 2019 r.), skarżący zakwestionowali legalność wyłączenia do celów imigracyjnych na podstawie tego, że jest ona sprzeczna z art. 23 RODO i niezgodna z prawami zagwarantowanymi w art. 7 i 8 Karty praw podstawowych Unii Europejskiej w odniesieniu do prywatności i ochrony danych osobowych. Sąd wyższej instancji (Anglia & Walia) (zwany dalej: „Sądem wyższej instancji") badał, czy wyłączenie do celów imigracyjnych zawartego w ustawie o ochronie danych z 2018 r. załącznik 2, część 1, pkt 4 jest zgodne z prawem.

64. Sąd wyższej instancji uznał w szczególności, że;

- "[…] Wyłączenie do celów imigracyjnych jest ewidentnie kwestią »ważnego interesu publicznego« i jest uzasadnione celem zgodnym z prawem.[…]", pkt 30;
- „Wyłączenie do celów imigracyjnych spełnia wymogi środka »zgodnego z prawem. […]«", pkt 38;
- „Na wyłączenie do celów imigracyjnych można powoływać się w przypadku i w zakresie w jakim zgodność z »wymienionymi przepisami RODO« **mogłaby przynieść szkodę** utrzymaniu skutecznej kontroli imigracyjnej lub prowadzeniu dochodzeń w sprawie działań lub wykrywaniu działań osłabiających utrzymywanie skutecznej kontroli imigracyjnej. Znaczenie słów „»mogłaby

---

[36] Zob. przykład podany w „Przewodniku dotyczącym rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO)" wydanym przez Urząd Rzecznika Informacji (Guide to the General Data Protection Regulation (GDPR)), wersja z dnia 1 stycznia 2021 r., s. 307 (pogrubienie dodano): „Prywatna organizacja (administrator 1) zawiadamia Ministerstwo Spraw Wewnętrznych (administratora 2) w sprawie pracownika, który rzekomo przedstawił w celu zdobycia pracy fałszywe dokumenty potwierdzające jego tożsamość i kwalifikacje. Pracodawca przekazuje Ministerstwu Spraw Wewnętrznych informacje mające znaczenie dla sprawy. Prawo osoby fizycznej do bycia poinformowaną, że jej dane osobowe przekazano Ministerstwu Spraw Wewnętrznych jest ograniczone, gdyż wykonanie tego prawa mogłoby stanąć na przeszkodzie dochodzeniu.
***Pracodawca nie ma zatem obowiązku informowania osoby fizycznej, że jej dane przekazano Ministerstwu Spraw Wewnętrznych**, a z kolei **Ministerstwo Spraw Wewnętrznych** nie ma obowiązku przekazania osobie fizycznej oświadczenia o ochronie prywatności, w którym informuje tę osobę, że obecnie przetwarza jej dane osobowe. Wyłączenie obejmuje obu administratorów w tym samym zakresie.*
*Pracownik zwraca się jednak do Ministerstwa Spraw Wewnętrznych, które obecnie bada jego dane osobowe, o ich kopię. **Ministerstwo Spraw Wewnętrznych może powołać się na wyłączenie** w celu nieujawniania części danych tej osoby, jeśli ujawnienie ich mogłoby stanąć na przeszkodzie dochodzeniu. W przypadku zwrócenia się pracownika z podobnym wnioskiem do **pracodawcy, ten ostatni również miałby prawo zastosować wyłączenie** w tym samym zakresie."*
Innymi słowy, jak wyjaśniono na s. 300: „W większości przypadków Ministerstwo Spraw Wewnętrznych, lub jedna z jego agencji i kontrahentów, będzie administratorem stosującym to wyłączenie. Należy jednak zauważyć, że stosowanie tego wyłączenia nie jest ograniczone tylko do Ministerstwa Spraw Wewnętrznych. Może ono również mieć znaczenie dla innych administratorów – takich jak pracodawcy, wyższe uczelnie i policja – którzy kontaktują się z Ministerstwem Spraw Wewnętrznych w kwestiach imigracyjnych."

przynieść szkodę«" w kontekście ustawy o ochronie danych z 1998 r. (która poprzedzała ustawę o ochronie danych z 2018 r.) zinterpretowano jako „»bardzo znaczącą i poważną możliwość zaszkodzenia określonemu interesowi publicznemu«. Stopień ryzyka musi być taki, że »może okazać się« przeszkodą dla tych interesów, nawet jeśli ryzyko daleko odbiega od bycia bardziej prawdopodobnym niż nieprawdopodobnym [...]", pkt 39 (pogrubienie dodano).

65. Należy zauważyć, że wyrok ten, według wiedzy EROD, nie jest ostateczny, i wniesiono od niego odwołanie.

66. Jak określono w wytycznych EROD dotyczących ograniczeń uregulowanych w art. 23 RODO („Wytyczne dotyczące art. 23 RODO")[37] „[...] w kontekście RODO ograniczenia **ustala się w drodze aktu prawnego**, dotyczą one **ograniczonej liczby praw osób, których dane dotyczą, lub obowiązków administratora** wymienionych w art. 23 RODO, **szanują istotę** omawianych podstawowych praw i wolności, stanowią w demokratycznym społeczeństwie **niezbędny i proporcjonalny środek** oraz służą jednemu z celów określonych w art. 23 ust. 1 RODO [...]"[38].

67. EROD przypomina również, że w motywie 41 RODO stwierdza się „[w] przypadku gdy w niniejszym rozporządzeniu jest mowa o **podstawie prawnej lub akcie prawnym**, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego. Taka podstawa prawna lub taki akt prawny powinny być **jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających** – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej [...] i Europejskiego Trybunału Praw Człowieka" (pogrubienie dodano).

68. Chociaż Europejski Trybunał Praw Człowieka określił, że „ponadto, jeżeli chodzi o wyrażenia »przewidziane przez ustawę« i »które określa ustawa«, które pojawiają się w art. 8–11 Konwencji, [EKPC] zauważa, że zawsze rozumiał termin »ustawa« w sensie »merytorycznym«, a nie »formalnym«; uwzględnił zarówno »prawo pisane« obejmujące 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, jak i prawo niepisane. »Prawo« należy rozumieć jako obejmujące zarówno prawo powszechne, **jak i »prawo precedensowe«**[39], w wytycznych dotyczących art. 23 RODO przypomina się, że „zgodnie z orzecznictwem TSUE, każdy **akt prawny** przyjęty na podstawie art. 23 ust. 1 [RODO] musi w szczególności **spełniać szczegółowe wymogi określone w art. 23 ust. 2 RODO**. Art. 23 ust. 2 [RODO] stanowi, że akty prawne ograniczające prawa osób, których dane dotyczą, oraz obowiązki administratorów muszą zawierać – w stosownym przypadku – **szczegółowe przepisy w odniesieniu do szeregu kryteriów opisanych poniżej**. **Akt prawny nakładający ograniczenia na mocy art. 23 RODO powinien co do zasady zawierać wszystkie wymogi opisane szczegółowo poniżej**."[40].

[37]Zob. Wytyczne EROD 10/2020 dotyczące ograniczeń uregulowanych w art. 23 RODO, wersja 1.0 przyjęte dnia 15 grudnia 2020 r., które są obecnie na etapie finalizacji po konsultacjach publicznych, https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-102020-restrictions-under-article-23_en

[38] Zob. wytyczne dotyczące art. 23 RODO, pkt 9, s. 5.

[39] Zob. Europejski Trybunał Praw Człowieka, *Sanoma Uitgevers B.V. przeciwko Niderlandy*, 14 września 2010 r., EC:ECHR:2010:0914JUD003822403, pkt 83 (pogrubienie dodano).

[40]Zob. wytyczne dotyczące art. 23 RODO, pkt 45 i 46, s. 11. Zgodnie z art. 52 ust. 3 Karty praw podstawowych Unii Europejskiej „[w] zakresie, w jakim niniejsza Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, ich

69. Można zaobserwować w tym względzie, że w samym **wyłączeniu do celów imigracyjnych nie wyszczególniono następujących elementów, o których mowa w art. 23 ust. 2 RODO**:

- „zabezpiecze[ń] zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu (lit. d);
- „określeni[a] administratora lub kategorii administratorów (lit. e)[41];
- „ryzyka naruszenia praw i wolności osoby, której dane dotyczą" (lit. g);
- „praw[a] osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia" (lit. h).

70. „Przewodnik dotyczący rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO)"[42], wydany przez Urząd Rzecznika Informacji nie zawiera wyjaśnień dotyczących „wyłączenia do celów imigracyjnych", lecz **nie może** sam w sobie określić wiążących zasad uzupełniających to wyłączenie. Ponadto kwestia „jakości prawa" jest szczególnie istotna ze względu na wagę ograniczanych praw oraz rozszerzenie wyłączenia[43].

---

znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję. Niniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę." Jeżeli chodzi o pojęcie „**przewidziane ustawą**" zawarte w art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, kryteria ustalone przez Europejski Trybunał Praw Człowieka należy stosować w sposób sugerowany w kilku opiniach rzecznika generalnego TSUE, zob. np. opinie w sprawach połączonych C-203/15 i C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:572, pkt 137–154, oraz w sprawie C-70/10, Scarlet Extended, ECLI:EU:C:2011:255, pkt 88–114. Można zatem odwołać się m.in. do wyroku Europejskiego Trybunału Praw Człowieka w sprawie Weber i Saravia przeciwko Niemcom, pkt 84: *„Trybunał ponownie stwierdza, że wyrażenie »**przewidziane przez ustawę**« w rozumieniu art. 8 ust. 2 [EKPC] wymaga, po pierwsze, aby zaskarżony akt opierał się w pewnej mierze na **prawie krajowym**; wyrażenie to odnosi się również do **jakości przedmiotowego prawa**, wymagając, aby było ono dostępne dla osoby, której sprawa dotyczy, która musi ponadto być zdolna do przewidzenia konsekwencji tego prawa dla siebie, i musi być zgodne z praworządnością."* (pogrubienie dodano).
Zob. również motyw 41 RODO: „Taka podstawa prawna lub taki akt prawny powinny być **jasne** i **precyzyjne**, a ich zastosowanie **przewidywalne dla osób im podlegających** – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej [...] i Europejskiego Trybunału Praw Człowieka" (pogrubienie dodano).

[41]Zob. wspomnianą wyżej sprawę High Court, pkt 54: „Moim zdaniem nie ma niczego niezgodnego z prawem w tym, aby wyłączenie do celów imigracyjnych było dostępne dla **wszystkich administratorów danych** przetwarzających dane w określonych celach. Jak podkreślają pozwani bez pkt 4(3)–(4) wyłączenie do celów imigracyjnych stałoby się nieskuteczne do celów utrzymania skutecznej kontroli imigracyjnej w przypadkach uzyskania danych od stron trzecich (takich jak władze lokalne lub administracja podatkowa i celna (HM Revenue and Customs))." (pogrubienie dodano), co potwierdza **powszechne** stosowanie ograniczeń.

[42]„Przewodnik dotyczący rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO)" wydany przez Urząd Rzecznika Informacji, wersja z dnia 1 stycznia 2021 r., s. 299–307.

[43] Zob. punkt 57 sprawy High Court, o której mowa powyżej: „Pan Knight poinformował mnie, że Rzecznik kończy opracowywanie wytycznych dotyczących wyłączenia, lecz będą one miały status „ustawy" tylko w takim sensie, że wydawane są na mocy uprawnień Rzecznika wynikających z art. 57 ust. 1 RODO. *Nie będą one miały żadnego statusu prawnego na mocy ustawy o ochronie danych z 2018 r.."*
O uzasadnieniu dla wprowadzenia prawnie wiążących wytycznych, wspieranych przez Urząd Rzecznika Informacji, mowa jest w szczególności w pkt 56–60 wyroku:
„56. Odnoszę się na koniec do twierdzenia Rzecznika, że bez towarzyszących wytycznych ustawowych zapewniających zabezpieczenia w odniesieniu do znaczenia i stosowania wyłączenia do celów imigracyjnych,

71. Tym bardziej „**test stawania na przeszkodzie**” nie daje zabezpieczeń zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu, które mogłyby być wdrożone na przykład przez Ministerstwo Spraw Wewnętrznych.

72. W świetle wszystkich powyższych argumentów EROD zauważa, że potrzebne są dalsze wyjaśnienia w kwestii stosowania wyłączenia do celów imigracyjnych.

73. Ponadto EROD zauważa brak prawnie wiążącego dokumentu precyzującego wyłączenie do celów imigracyjnych w celu rozważenia, czy jest ono merytorycznie równoważne art. 23 RODO oraz art. 7 i 8 Karty praw podstawowych Unii Europejskiej. EROD uważa jednocześnie, że Komisja Europejska powinna wykazać, przedstawiając dowody, konieczność i proporcjonalność szerokiego zakresu podmiotowego wyłączenia do celów imigracyjnych.

---

wyłączenie nie stanowiłoby proporcjonalnego stosowania art. 23 ust. 1 RODO. Pan Knight twierdzi, że przepis ten, uzupełniony takimi wytycznymi, jest proporcjonalny.

57. Pan Knight poinformował mnie, że Rzecznik kończy opracowywanie wytycznych dotyczących wyłączenia, lecz będą one miały status »ustawy« tylko w takim sensie, że wydawane są na mocy uprawnień Rzecznika wynikających z art. 57 ust. 1 RODO. Nie będą one miały żadnego statusu prawnego na mocy ustawy o ochronie danych z 2018 r. „Wiem również, że Ministerstwo Spraw Wewnętrznych opracowało projekt wewnętrznych wytycznych dla pracowników dotyczących wyłączenia do celów imigracyjnych (zob. pkt 22 powyżej). W praktyce wytyczne wydane przez Rzecznika są wpływowe niezależnie od ich podstawy prawnej. Rzecznik nie ma jednak prawa wydawania tego rodzaju „wiążących” wytycznych, o jakie chodziło Sądowi Najwyższemu w sprawie *Christian Institute (pkt 101 i 107).* Wydaje się, że konieczne byłoby prawo pierwotne, gdyby uznano za konieczne istnienie wytycznych dotyczących wyłączenia do celów imigracyjnych o takim samym statusie jak kodeksy praktyk przewidziane obecnie w *ppkt 121–124 ustawy o ochronie danych z 2018 r*.

58. *W swojej argumentacji na rzecz wytycznych ustawowych pan Knight twierdzi, że kontekst w którym pojawi się stosowanie wyłączenia do celów imigracyjnych siłą rzeczy nasuwa obawy w zakresie konieczności i proporcjonalności jego istnienia i stosowania.* W kontekście prawnym zwrócił on uwagę w szczególności na dwie kwestie. Po pierwsze, dane osobowe do których stosuje się wyłączenie do celów imigracyjnych z natury mogą obejmować szczególnych kategorii danych w rozumieniu art. 9 ust. 1 RODO (tj. dane »ujawniające pochodzenie rasowe lub etniczne«).Dane takie wskazano w RODO ponieważ wymagają one większego stopnia ochrony (*Opinia 1/15 [2019] 3 C.M.L.R. 25 pkt 141). Po drugie, podstawowym założeniem przepisów o ochronie danych jest w szczególności to, że prawo dostępu osób, których dane dotyczą, jest ogromnie ważne, gdyż jest on niezbędne do wykonywania innych praw przyznanych tym osobom (zob. YS przeciwko Minister voor Immigratie, Integratie en Asiel (C-141/12) EU:C:2014:2081; [2015] 1 C.M.L.R. 18 pkt 44).*

59. Pan Knight wskazuje na cztery kwestie natury praktycznej. Po pierwsze, gdy administratorzy nie wyjaśniają osobom, których dane dotyczą, że powołali się na wyłączenie ustawowe, ani nie przekazują ogólnego wyjaśnienia przyczyn takiego działania, osoba, której dane dotyczą będzie nieświadoma, że zastosowano wyłączenie, a zatem nie będzie mogła go skutecznie zakwestionować. Po drugie, osoby, których dane dotyczą, będą szczególnie uzależnione od administratorów, aby stosowali oni wyłączenie ze starannością i tylko niezbędnym zakresie. Każda osoba, której dane dotyczą, ma prawo złożyć do Rzecznika skargę dotyczącą stosowania wyłączenia lub wszcząć postępowanie sądowe, jest jednak prawdopodobne, że osoba, której dane dotyczą, nie będzie świadoma swoich praw i nie będzie miała środków na podjęcie kroków prawnych w okolicznościach, w których występuje potrzeba szybkiego i dokładnego przestrzegania praw do ochrony danych. Po trzecie, jako imigrant, osoba, której dane dotyczą, może być w trudnej sytuacji. Po czwarte, nie jest to abstrakcyjna kwestia w świetle dowodów pozwanych dotyczących stosowania wyłączenia do celów imigracyjnych (zob. pkt 4 powyżej).

60. Pan Knight sugeruje, że istnieje silna analogia między obecnym zakwestionowaniem wyłączenia do celów imigracyjnych a rozumowaniem sądu w sprawie *Christian Institute [2016] UKSC 51* . Podobnie jak w sprawie *Christian Institute* twierdzi on, że wyłączenie do celów imigracyjnych jest szerokie, użyto w nim nieokreślonych wyrażeń, ma niski próg stosowania, podlega kontrolom, które nie wynikają bezpośrednio z tego przepisu i obowiązuje w odniesieniu do bardzo szerokiego spektrum okoliczności i praw. W odróżnieniu od sprawy *Christian Institute* w przypadku wyłączenia do celów imigracyjnych nie ma ogólnodostępnych wytycznych, a tym bardziej dokumentu o statusie ustawy, które należy uwzględniać.”

74. **Podsumowując, EROD zachęca Komisję Europejską do sprawdzenia stanu postępowania Open Rights Group & Anor, R (On the Application Of) przeciwko Secretary of State for the Home Department & Anor [2019] EWHC 2562 (Admin), o którym mowa powyżej, a w związku z tym, że wyrok ten nie jest ostateczny (powaga rzeczy osądzonej), sprawdzenia, czy wyrok instancji odwoławczej podtrzyma go czy też zmieni, do uwzględnienia wszelkich najnowszych informacji w tym względzie oraz wyszczególnienia ich w decyzji stwierdzającej odpowiedni stopień ochrony. EROD wzywa także Komisję Europejską do przekazania dalszych informacji dotyczących konieczności i proporcjonalności wyłączenia do celów imigracyjnych, w szczególności uwzględniając szeroki zakres stosowania zakresu podmiotowego.**

75. **EROD zachęca jednocześnie Komisję Europejską do dalszego badania, czy w ramach prawnych Zjednoczonego Królestwa istnieją dodatkowe zabezpieczenia lub czy można by przewidzieć, że będą istnieć, na przykład w postaci prawnie wiążących instrumentów, które uzupełniałyby wyłączenie do celów imigracyjnych, zwiększając w odniesieniu do osób, których dane dotyczą, jego przewidywalność i zabezpieczenia, a także umożliwiając lepszą i szybszą ocenę i monitorowanie wymogów w zakresie konieczności i proporcjonalności.**

3.1.2 Ograniczenia dotyczące dalszego przekazywania danych

76. Art. 44 RODO stanowi, że przekazanie i dalsze przekazanie danych osobowych następuje tylko wtedy, gdy nie zostaje naruszony stopień ochrony osób fizycznych zagwarantowany w RODO. Dane osobowe przekazywane z EOG do Zjednoczonego Królestwa na podstawie decyzji stwierdzającej odpowiedni stopień ochrony będą zatem objęte stopniem ochrony merytorycznie równoważnym stopniowi ochrony zapewnionemu na podstawie unijnych ram ochrony danych. **Oznacza to nie tylko, że przepisy Zjednoczonego Królestwa są „merytorycznie równoważne" przepisom UE w odniesieniu do przetwarzania danych osobowych przekazywanych do Zjednoczonego Królestwa na podstawie projektu decyzji, lecz także, że przepisy obowiązujące w Zjednoczonym Królestwie w odniesieniu do dalszego przekazywania tych danych do państw trzecich gwarantują dalsze zapewnianie merytorycznie równoważnego stopnia ochrony.**

77. W efekcie istotne jest, aby wszelkie dalsze przekazywanie ze Zjednoczonego Królestwa do innego państwa trzeciego danych osobowych pochodzących z EOG było należycie chronione za pomocą zabezpieczeń lub dokonywane zgodnie z przepisami dotyczącymi odstępstw[44], aby zapewnić ciągłość ochrony zapewnianej przez przepisy UE. **Jeżeli nie można zapewnić takiej ochrony, dalsze przekazywanie danych osobowych pochodzących z EOG nie powinno mieć miejsca.**

78. EROD uznaje, że w RODO Zjednoczonego Królestwa (art. 44–49) i w ustawie o ochronie danych z 2018 r. Zjednoczone Królestwo odzwierciedliło w głównej mierze rozdział V RODO[45]. **EROD wskazała jednak na pewne aspekty ram legislacyjnych Zjednoczonego Królestwa dotyczące dalszego przekazywania danych, które mogą osłabić stopień ochrony danych osobowych przekazywanych z EOG.**

79. **Pierwsze wyzwanie**, jakie zidentyfikowała EROD, odnosi się do uznawania przez Zjednoczone Królestwo państw trzecich, organizacji międzynarodowych lub terytoriów[46] jako adekwatnych odbiorców na podstawie procedury opisanej w ustawie o ochronie danych z 2018 r. W istocie dalsze przekazywanie ze Zjednoczonego Królestwa do innych państw trzecich danych osobowych

[44] Zob. art. 49 RODO Zjednoczonego Królestwa
[45] Zob. sekcje 17A, 17B, 17C i 18 ustawy o ochronie danych z 2018 r.
[46] Zob. sekcję 17 A ustawy o ochronie danych z 2018 r.

pochodzących z EOG będzie mogło odbywać się na podstawie ewentualnego przyszłego rozporządzenia Zjednoczonego Królestwa stwierdzającego odpowiedni stopień ochrony[47].

80. W szczególności, jak wyjaśniono w motywie 77 projektu decyzji, sekretarz stanu Zjednoczonego Królestwa jest uprawniony do uznania państwa trzeciego (lub terytorium lub sektora w państwie trzecim), organizacji międzynarodowej lub opisu takiego państwa, terytorium, sektora lub organizacji za zapewniające odpowiedni stopień ochrony danych osobowych, po konsultacji z Urzędem Rzecznika Informacji[48]. Oceniając, czy stopień ochrony jest odpowiedni, sekretarz stanu Zjednoczonego Królestwa musi uwzględnić te same elementy, które Komisja Europejska ma obowiązek ocenić na podstawie art. 45 ust. 2 lit. a)–c) RODO, interpretowanego łącznie z motywem 104 RODO i zachowanym orzecznictwem UE. Oznacza to, że przy ocenie, czy stopień ochrony w państwie trzecim jest odpowiedni, właściwym standardem będzie ocenienie, czy dane państwo trzecie zapewnia stopień ochrony „merytorycznie równoważny" stopniowi gwarantowanemu w Zjednoczonym Królestwie. Chociaż EROD odnotowuje zdolność Zjednoczonego Królestwa – w ramach RODO Zjednoczonego Królestwa – do uznawania terytoriów za zapewniającą odpowiedni stopień ochrony w świetle ram ochrony danych Zjednoczonego Królestwa, EROD pragnie podkreślić, że terytoria te mogą do tej pory nie korzystać z decyzji stwierdzającej odpowiedni stopień ochrony wydanej przez Komisję Europejską, uznającej stopień ochrony za „merytorycznie równoważny" stopniowi gwarantowanemu w UE. Może to prowadzić do potencjalnych zagrożeń w zakresie ochrony danych osobowych przekazywanych z EOG, zwłaszcza jeśli w przyszłości ramy ochrony danych Zjednoczonego Królestwa miałyby odbiegać od dorobku prawnego UE. Należy zauważyć, że w lipcu 2020 r. precedensowa sprawa TSUE „Schrems II"[49] doprowadziła do unieważnienia decyzji w sprawie Tarczy Prywatności UE-USA, ponieważ zdaniem TSUE nie można było uznać, że ramy prawne Stanów Zjednoczonych zapewniają stopień ochrony merytorycznie równoważny ramom UE. Jednakże wydane już wyroki TSUE, uważane za zachowane orzecznictwo w brytyjskich ramach prawnych, mogą nie być już wiążące dla Zjednoczonego Królestwa, zwłaszcza z uwagi na fakt, że Zjednoczone Królestwo ma możliwość zmiany zachowanego prawa Unii po zakończeniu dodatkowego okresu przejściowego, a jego Sąd Najwyższy nie jest związany żadnym utrwalonym orzecznictwem UE[50].

81. **EROD zachęca Komisję Europejską do ścisłego monitorowania procesu oceny odpowiedniego stopnia ochrony oraz kryteriów stosowanych przez organy Zjednoczonego Królestwa wobec innych państw trzecich, a w szczególności w odniesieniu do państw trzecich, które nie zostały uznane przez UE za zapewniające odpowiedni stopień ochrony na podstawie RODO. W przypadku gdy Komisja Europejska stwierdzi, że państwo trzecie uznane przez Zjednoczone Królestwo za zapewniające odpowiedni stopień ochrony nie zapewnia stopnia ochrony merytorycznie równoważnego stopniowi gwarantowanemu w UE, EROD wzywa Komisję Europejską do podjęcia wszelkich niezbędnych kroków, takich jak na przykład zmiana decyzji stwierdzającej odpowiedni stopień ochrony w Zjednoczonym Królestwie w celu wprowadzenia konkretnych zabezpieczeń dla danych osobowych pochodzących z EOG, lub rozważenie zawieszenia decyzji stwierdzającej odpowiedni stopień ochrony w Zjednoczonym Królestwie, jeżeli dane osobowe przekazywane z EOG do Zjednoczonego Królestwa podlegają dalszemu przekazywaniu do danego państwa**

[47] Odpowiednik Zjednoczonego Królestwa decyzji stwierdzającej odpowiedni stopień ochrony na mocy RODO.
[48] Zob. sekcję 182 ust. 2 ustawy o ochronie danych z 2018 r. Zob. również protokół ustaleń w sprawie roli Urzędu Rzecznika Informacji w odniesieniu do nowych ocen odpowiedniości stopnia ochrony w Zjednoczonym Królestwie, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/
[49] Zob. Schrems II.
[50] Zob. sekcję 6 ust. 3–6 umowy o wystąpieniu z UE z 2018 r.

trzeciego na podstawie przepisów Zjednoczonego Królestwa dotyczących odpowiedniego stopnia ochrony.

82. **Drugie wyzwanie** odnosi się do nadchodzącego przeglądu istniejących decyzji stwierdzających odpowiedni stopień ochrony wydanych przez Komisję Europejską na mocy dyrektywy 95/46/WE. W następstwie tego przeglądu Komisja Europejska może postanowić, że niektóre państwa, które do tej pory korzystały z decyzji stwierdzającej odpowiedni stopień ochrony, nie zapewniają już merytorycznie równoważnego stopnia ochrony przy uwzględnieniu obecnych przepisów UE oraz niedawnego orzecznictwa. Na podstawie przepisu ustawy o ochronie danych z 2018 r. załącznik 21 pkt 4 Zjednoczone Królestwo uznało już jednak te państwa za zapewniające odpowiedni stopień ochrony. Chociaż sekretarz stanu Zjednoczonego Królestwa musi co cztery lata przeprowadzać przegląd tych ustaleń dotyczących odpowiedniego poziomu ochrony, Komisja Europejska zauważa w swoim projekcie decyzji, że te ustalenia dotyczące odpowiedniego poziomu stopnia nie przestaną automatycznie istnieć w przypadku, gdyby sekretarz stanu Zjednoczonego Królestwa nie przeprowadził wymaganego przeglądu w przewidzianym terminie czterech lat[51].

83. **EROD zachęca Komisję Europejską do monitorowania po zakończeniu unijnego przeglądu istniejących decyzji stwierdzających odpowiedni stopień ochrony, czy państwo uznane za niezapewniające odpowiedniego stopnia ochrony jest nadal uznawane przez Zjednoczone Królestwo jako państwo zapewniające taki stopień ochrony. W takim przypadku EROD wzywa Komisję Europejską, na podstawie motywów 277–280 projektu decyzji, do podjęcia wszelkich kroków niezbędnych do zaradzenia sytuacji, takich jak na przykład zmiana decyzji stwierdzającej odpowiedni stopień ochrony w celu wprowadzenia konkretnych zabezpieczeń dla danych osobowych pochodzących z EOG, lub zawieszenie decyzji stwierdzającej odpowiedni stopień ochrony, jeżeli dane osobowe przekazywane z EOG do Zjednoczonego Królestwa podlegają dalszemu przekazywaniu do danego państwa trzeciego. EROD wzywa Komisję Europejską do kontynuowania tego procesu monitorowania przez okres obowiązywania decyzji Zjednoczonego Królestwa stwierdzającej odpowiedni stopień ochrony.**

84. **Trzecie wyzwanie** dotyczy dalszego przekazywania danych osobowych pochodzących z EOG do państw niezapewniających odpowiedniego stopnia ochrony przy użyciu narzędzi przekazywania określonych w art. 46 i 47 RODO Zjednoczonego Królestwa. Chociaż RODO Zjednoczonego Królestwa przewiduje te same narzędzia przekazywania co RODO, EROD podkreśla potrzebę zapewnienia, aby zawarte w nich zabezpieczenia zapewniały skuteczną ochronę w państwie trzecim, zwłaszcza w świetle wyroku w sprawie Schrems II.

85. Po wyroku w sprawie Schrems II, w którym TSUE przypomniał, że ochrona przyznana danym osobowym w UE musi towarzyszyć tym danym w każdym miejscu, do którego są przekazywane, EROD przyjęła już wstępne zalecenia dotyczące środków uzupełniających[52], aby w stosownych przypadkach wesprzeć podmioty przekazujące dane w zakresie zapewnienia osobom, których dane dotyczą, stopnia ochrony merytorycznie równoważnego stopniowi gwarantowanemu w UE.

86. Według TSUE do podmiotów przekazujących dane należy sprawdzenie w każdym konkretnym przypadku i – gdy ma to zastosowanie – we współpracy z podmiotem odbierającym te dane

[51] Zob. motyw 82 projektu decyzji.

[52] Zob. Zalecenia EROD 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych przyjęte w dniu 10 listopada 2020 r., które są obecnie finalizowane po konsultacjach publicznych, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pl.pdf.

w państwie trzecim, czy prawo lub praktyki państwa trzeciego mają negatywny wpływ na skuteczność odpowiednich zabezpieczeń zawartych w narzędziach przekazywania z art. 46 RODO[53]. W takich przypadkach podmioty przekazujące dane powinny wdrożyć środki uzupełniające, które wypełniłyby luki w ochronie i podniosłyby ją do stopnia wymaganego przez prawo UE.

87. **W celu zapewnienia ciągłości ochrony EROD wzywa Komisję Europejską do wprowadzenia do projektu decyzji gwarancji, aby w przypadku korzystania przez podmioty przekazujące dane w Zjednoczonym Królestwie z narzędzi przekazywania przewidzianych w art. 46 i 47 RODO Zjednoczonego Królestwa do celów dalszego przekazywania do innych państw trzecich danych przekazanych z EOG, podmioty te oceniały w każdym konkretnym przypadku ramy ochrony danych obowiązujące w tym państwie trzecim; a w razie potrzeby wprowadzały stosowne środki w celu zapewnienia skutecznego przestrzegania zabezpieczeń zawartych w wybranym narzędziu przekazywania w celu zapewnienia stopnia ochrony merytorycznie równoważnego stopniowi gwarantowanemu w UE. EROD podkreśla, że bez tych gwarancji istnieje ryzyko, że stopień ochrony merytorycznie równoważny stopniowi ochrony zapewnianemu w UE zostanie osłabiony przez dalsze przekazywanie danych ze Zjednoczonego Królestwa.**

88. **Czwarte wyzwanie** dotyczące dalszego przekazywania odnosi się do umów międzynarodowych, które zostały lub zostaną w przyszłości zawarte przez Zjednoczone Królestwo – i możliwego bezpośredniego dostępu władz państwa trzeciego (państw trzecich) będącego (będących) stroną tych umów do danych osobowych pochodzących z EOG. EROD wyraża silne zaniepokojenie w związku z już zawartą umową między Zjednoczonym Królestwem i USA dotyczącą ustawy CLOUD, a Komisja Europejska uznaje to wyzwanie, podkreślając, że „ewentualne wejście w życie tej umowy może mieć wpływ na stopień ochrony oceniany w niniejszej decyzji”[54]. Istotnie na podstawie tej umowy, po jej wejściu w życie, dane osobowe przekazywane z EOG do Zjednoczonego Królestwa zgodnie z projektem decyzji podlegałyby następnie postanowieniom tej umowy określającej warunki bezpośredniego dostępu władz Stanów Zjednoczonych, wpływającej na ramy ochrony danych Zjednoczonego Królestwa, w tym postanowieniom dotyczącym dalszego przekazywania. W związku z tym postanowienia umowy zawartej ze Stanami Zjednoczonymi mogą mieć istotny wpływ na stopień ochrony zapewniany w odniesieniu do danych przekazywanych z EOG oraz wpływ na stopień ochrony takich danych. EROD zauważa w tym kontekście, że w motywie 153 projektu decyzji Komisja Europejska odnosi się do wyjaśnień udzielonych przez władze Zjednoczonego Królestwa bez cytowania ani podawania jakiegokolwiek zapewnienia na piśmie ani zobowiązania, ani też wskazania konkretnych przepisów prawa Zjednoczonego Królestwa, które nadawałyby skuteczność tym wyjaśnieniom.

89. EROD wyraziła już wcześniej te obawy w piśmie z dnia 15 czerwca 2020 r. skierowanym do Parlamentu Europejskiego[55]. EROD podkreśliła, że w oparciu o „dorobek prawny UE w dziedzinie ochrony danych, w szczególności RODO i dyrektywę (UE) 2016/680”, ma ona zastrzeżenia, czy zabezpieczenia określone w umowie dotyczące dostępu do danych osobowych w Zjednoczonym Królestwie obowiązywałyby w pewnych okolicznościach powodujących obowiązek ujawnienia

[53] Zob. *Schrems II*, pkt 134.
[54] Zob. motyw 153 projektu decyzji.
[55] Zob. odpowiedź EROD na pismo posłów do Parlamentu Europejskiego Sophie in’t Veld i Moritza Körnera w kwestii umowy między Stanami Zjednoczonymi a Zjednoczonym Królestwem w ramach amerykańskiej ustawy CLOUD, zawartej w dniu 15 czerwca 2020 r., https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out_2020-0054-uk-usagreement.pdf.

Stanom Zjednoczonym, a także czy zabezpieczenia te są wystarczające w świetle standardów unijnych, aby nie osłabiać stopnia ochrony zapewnianego w UE.

90. Postanowienia umowy między Zjednoczonym Królestwem a Stanami Zjednoczonymi dotyczące ustawy CLOUD mogą mieć istotny wpływ na warunki merytoryczne i proceduralne, na podstawie których władze Stanów Zjednoczonych mogą uzyskiwać bezpośredni dostęp do danych osobowych przechowywanych przez administratorów lub podmioty przetwarzające w Zjednoczonym Królestwie, wpływając w ten sposób na stopień ochrony gwarantowany w ramach prawa Zjednoczonego Królestwa. Aby zapewnić stopień ochrony merytorycznie równoważny stopniowi ochrony gwarantowanemu w świetle prawa Unii, na przykład „kluczowym jest, aby zabezpieczenia określone w tej umowie obejmowały obowiązkowe uprzednie zezwolenie sądu, jako niezbędną gwarancję w przypadku dostępu do metadanych i danych dotyczących treści. Na podstawie oceny wstępnej EROD, odnotowując, że umowa odnosi się do stosowania prawa krajowego, nie była w stanie wskazać wyraźnego postanowienia o takiej treści w umowie zawartej między Zjednoczonym Królestwem a Stanami Zjednoczonymi”[56].

91. Chociaż Komisja Europejska podkreśla, że dane uzyskane na podstawie tej umowy podlegałyby ochronie równoważnej tej określonej w szczególnych zabezpieczeniach określonych w tzw. „Umowie ramowej między UE i Stanami Zjednoczonymi”, EROD ma obawy, czy włączenie tych zabezpieczeń do umowy między Zjednoczonym Królestwem a USA dotyczącej ustawy CLOUD tylko poprzez odniesienie obowiązujące na zasadzie *mutatis mutandis* spełniłoby kryteria jasnych, precyzyjnych i dostępnych reguł, jeżeli chodzi o dostęp do danych osobowych, lub czy wystarczająco ugruntowałoby te zabezpieczenia, aby były one skuteczne i wykonywalne w ramach prawa Zjednoczonego Królestwa.

92. **EROD zaleca zatem, aby Komisja Europejska wyjaśniła, w jaki sposób i na podstawie jakiego instrumentu prawnego nadano by skuteczność ochronie równoważnej wobec szczególnych zabezpieczeń przewidzianych w umowie ramowej między UE a Stanami Zjednoczonymi i miałaby ona wiążący charakter na mocy prawa Zjednoczonego Królestwa.**

93. EROD zauważa również, że postanowienia umowy między Zjednoczonym Królestwem a USA dotyczącej ustawy CLOUD, w związku z sekcją 3 amerykańskiej ustawy CLOUD[57], rodzą pytania dotyczące faktycznego stosowania zabezpieczeń przewidzianych w umowie w odniesieniu do dostępu organów ścigania Stanów Zjednoczonych do danych osobowych w Zjednoczonym Królestwie przetwarzanych przez dostawców usług łączności elektronicznej lub zdalnych usług przetwarzania danych (zwanych dalej „CSP”) podlegających jurysdykcji Stanów Zjednoczonych. W istocie, jeżeli tego typu dostawca znajdujący się w Zjednoczonym Królestwie podlega prawu Stanów Zjednoczonych (np. dlatego, że jest spółką zależną spółki amerykańskiej), należy upewnić się, czy władze Stanów Zjednoczonych zobowiązane byłyby do powoływania się na umowę między Zjednoczonym Królestwem a USA dotyczącą ustawy CLOUD, aby uzyskać te dane. Komisja Europejska podkreśla, że „szczególna uwaga będzie poświęcona stosowaniu i adaptacji zabezpieczeń przewidzianych w umowie ramowej do szczególnego rodzaju przekazywania danych objętego umową między Zjednoczonym Królestwem a Stanami Zjednoczonymi”, EROD podkreśla, że, na podstawie dokonanej przez nią oceny wstępnej, nie jest jasne, czy zabezpieczenia zawarte w umowie między Zjednoczonym Królestwem a USA dotyczącej ustawy CLOUD, a zatem te przewidziane w umowie ramowej między UE a Stanami Zjednoczonymi, obowiązywałyby wobec wszystkich

[56] Zob. pismo EROD, o którym mowa powyżej.
[57] Zob. ustawę CLOUD Stanów Zjednoczonych,https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

wniosków o dostęp do danych w Zjednoczonym Królestwie składanych przez władze Stanów Zjednoczonych w ramach amerykańskiej ustawy CLOUD.

94. Zjednoczone Królestwo może w przyszłości podpisać inne umowy międzynarodowe lub zobowiązania z państwami trzecimi, które miałyby zastosowanie do danych osobowych przekazywanych z EOG do Zjednoczonego Królestwa w ramach projektu decyzji[58]. W zależności od postanowień tych umów międzynarodowych oraz stosowania szczególnych klauzul ochronnych, umowy te mogą również wywierać istotny wpływ na merytoryczne i formalne warunki dostępu organów państw trzecich do danych osobowych w Zjednoczonym Królestwie poprzez wpływ na ramy ochrony danych w Zjednoczonym Królestwie. Ma to miejsce w szczególności w przypadku projektu drugiego protokołu dodatkowego do Konwencji Rady Europy o cyberprzestępczości (dalej „Konwencja o cyberprzestępczości"), który obecnie negocjują strony tej konwencji, wśród których jest kilka państw niebędących członkami UE. Projekt protokołu obejmuje istotnie klauzule, które strony mogą uruchamiać dyskrecjonalnie, np. dotyczące zgody na udzielenie dostępu do danych dotyczących treści lub braku takiej zgody. Wszystkie państwa członkowskie UE uruchamiałyby te klauzule zgodnie z unijnymi przepisami o ochronie danych, nie przedstawiono jednak gwarancji dotyczącej Zjednoczonego Królestwa, które mogłoby w istotnej mierze odstąpić od stopnia ochrony, który byłby wtedy oferowany w obrębie UE. Innym przykładem kwestii przedstawionych powyżej jest kompleksowa umowa o partnerstwie gospodarczym między Zjednoczonym Królestwem a Japonią[59] („CEPA"), pierwsza umowa handlowa Zjednoczonego Królestwa po brexicie, która weszła w życie w dniu 1 stycznia 2021 r.[60] i która zawiera postanowienia dotyczące danych osobowych[61]. EROD zauważa ponadto, że w dniu 1 lutego 2021 r. Zjednoczone Królestwo formalnie ogłosiło również swój wniosek o przystąpienie do kompleksowego i progresywnego partnerstwa transpacyficznego („CPTPP"), które obejmuje porozumienie o partnerstwie transpacyficznym („TPP")[62].

95. EROD zauważa, że poza umową między Zjednoczonym Królestwem a USA dotyczącą ustawy CLOUD w projekcie decyzji nie uwzględniono wspomnianych wyżej umów międzynarodowych.

96. **EROD zachęca Komisję Europejską, aby:**

- **zbadała zależności między ramami ochrony danych Zjednoczonego Królestwa a jego zobowiązaniami międzynarodowymi, poza umową między Zjednoczonym Królestwem a USA dotyczącą ustawy CLOUD, w szczególności w celu zapewnienia ciągłości stopnia ochrony w przypadku dalszego przekazywania do innych państw trzecich danych osobowych przekazanych z EOG do Zjednoczonego Królestwa na podstawie decyzji stwierdzającej odpowiedni stopień ochrony w Zjednoczonym Królestwie oraz aby stale monitorowała**

[58] Zob. sekcja 2.3.3 powyżej.

[59] Zob. Zjednoczone Królestwo/Japonia: kompleksowa umowa o partnerstwie gospodarczym [CS Japonia nr 1/2020], https://www.gov.uk/government/publications/ukjapan-agreement-for-a-comprehensive-economic-partnership-cs-japan-no12020.

[60] Zob. wytyczne rządu Zjednoczonego Królestwa w sprawie umów handlowych Zjednoczonego Królestwa z państwami niebędącymi członkami UE, https://www.gov.uk/guidance/uk-trade-agreements-with-non-eu-countries.

[61] Zgodnie z art. 8.80 ust. 5 CEPA strony zobowiązują się zachęcać do opracowywania mechanizmów promowania zgodności między ich różnymi podejściami prawnymi do ochrony danych (osobowych). Zgodnie z art. 8.84 strony zobowiązują się, że nie będą zabraniać ani ograniczać transgranicznego przekazywania informacji drogą elektroniczną, w tym danych osobowych, jeśli czynność ta służy prowadzeniu działalności przez osobę objętą umową w rozumieniu CEPA.

[62] Zgodnie z art. 14.11 ust. 2 TPP każda ze stron zezwala na transgraniczne przekazywanie informacji drogą elektroniczną, w tym danych osobowych, jeśli czynność ta służy prowadzeniu działalności przez osobę objętą porozumieniem.

sytuację i w razie potrzeby podejmowała działania w odniesieniu do zawierania innych umów międzynarodowych między Zjednoczonym Królestwem a państwami trzecimi, które mogą podważyć stopień ochrony danych osobowych przewidziany w UE;

- **przekazała EROD pisemne zobowiązania władz Zjednoczonego Królestwa i wskazała konkretne przepisy prawa Zjednoczonego Królestwa odnoszące się do wyjaśnienia związanego z możliwym stosowaniem i wdrożeniem umowy między Zjednoczonym Królestwem a USA dotyczącej ustawy CLOUD, o której mowa w motywie 153 projektu decyzji;**
- **monitorowała w tym kontekście, czy oprócz zabezpieczeń, które można zapewnić poprzez odpowiednie wdrożenie dostosowania umowy ramowej między UE a Stanami Zjednoczonymi, w umowie między Zjednoczonym Królestwem a Stanami Zjednoczonymi dotyczącej ustawy CLOUD zapewniono odpowiednie dodatkowe zabezpieczenia, w których uwzględniono poziom wrażliwości kategorii odnośnych danych, oraz wyjątkowe wymogi związane z przekazywaniem dowodów elektronicznych bezpośrednio przez dostawców usług łączności elektronicznej lub usług przetwarzania danych (CSP), a nie między organami;**
- **oceniła wpływ i potencjalne zagrożenia wynikające z przepisów dotyczących danych osobowych zawartych w umowach międzynarodowych podpisanych ostatnio przez Zjednoczone Królestwo, takich jak CEPA.**

97. **Piąte wyzwanie**, na które wskazano, dotyczy stosowania odstępstw w zakresie przekazywania danych osobowych do państwa trzeciego. Chociaż odstępstwa przewidziane w RODO Zjednoczonego Królestwa są takie same jak odstępstwa przewidziane w RODO, ważne jest, aby wykładnia Urzędu Rzecznika Informacji w zakresie korzystania z tych odstępstw była obecnie i w przyszłości zgodna z wykładnią EROD. W przeciwnym razie, lub gdyby w przyszłości Zjednoczone Królestwo odeszło od tej wykładni, zaistniałoby ryzyko osłabienia stopnia ochrony danych przekazywanych z EOG do państw trzecich przez Zjednoczone Królestwo.

98. **EROD zachęca Komisję Europejską, aby w ramach swojego zadania związanego z monitorowaniem sprawdziła, czy wykładnia Zjednoczonego Królestwa dotycząca stosowania odstępstw pozostaje zgodna z wykładnią UE. Gdyby jednak Zjednoczone Królestwo stosowało inną wykładnię korzystania z odstępstw, która osłabiałaby stopień ochrony, istotne jest, aby Komisja Europejska podjęła niezbędne działania, zmieniając decyzję stwierdzającą odpowiedni stopień ochrony, dzięki którym stopień ochrony danych osobowych pochodzących z EOG przekazywanych do Zjednoczonego Królestwa nie zostanie osłabiony, gdy dane te będą dalej przekazywane ze Zjednoczonego Królestwa do państw trzecich na podstawie innej wykładni odstępstw.**

99. **Szóste wyzwanie,** będące ostatnim wyzwaniem w tej sekcji, odnosi się do braku ochrony zapewnianej na podstawie art. 48 RODO w ramach ochrony danych Zjednoczonego Królestwa.

100. Komisja Europejska faktycznie wyjaśnia w swoim projekcie decyzji, że w przypadku braku uregulowań dotyczących odpowiedniości lub odpowiednich zabezpieczeń przekazanie może nastąpić wyłącznie na podstawie odstępstw określonych w art. 49 RODO Zjednoczonego Królestwa „z wyjątkiem art. 48 rozporządzenia (UE) 2016/679, którego Zjednoczone Królestwo postanowiło nie włączać do RODO Zjednoczonego Królestwa”[63]. Brak przepisu merytorycznie równoważnego z art. 48 RODO zapisanego w ramach ochrony danych Zjednoczonego Królestwa w odniesieniu do przekazywania lub ujawniania danych w następstwie wyroku sądu lub trybunału lub decyzji organu administracyjnego z innego państwa trzeciego może powodować niepewność prawa co do tego, czy

[63] Zob. przypis 78 w projekcie decyzji.

stopień ochrony danych osobowych przekazywanych z EOG do Zjednoczonego Królestwa na podstawie projektu decyzji zostałby znacząco naruszony.

101. W swoim dokumencie dotyczącym odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO EROD zwraca uwagę, że jeśli chodzi o dalsze przekazywanie, „na dalsze przekazywanie danych osobowych przez pierwotnego odbiorcę pierwotnego przekazania danych należy zezwolić tylko wówczas, gdy podczas przetwarzania danych w imieniu administratora danych dalszy odbiorca również podlega przepisom zapewniającym odpowiedni stopień ochrony i stosuje się do odpowiednich instrukcji”[64]. Ponadto EROD podkreśla, że „pierwotny odbiorca danych przekazywanych z UE ponosi odpowiedzialność za zapewnienie odpowiednich zabezpieczeń w odniesieniu do dalszego przekazywania danych w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony. Takie dalsze przekazywanie danych powinno odbywać się wyłącznie w ograniczonych i określonych celach i dopóki istnieje podstawa prawna takiego przetwarzania”[65]. Jako część rozdziału V RODO art. 48 musi być w pełni uwzględniony przy ocenie, czy ramy prawne Zjednoczonego Królestwa zapewniają w tym względzie merytorycznie równoważny stopień ochrony[66].

102. EROD podkreśla w tym kontekście orzecznictwo TSUE dotyczące ryzyka nadużycia lub niezgodnego z prawem dostępu do danych i ich wykorzystania, stwierdzając w szczególności, że „[j]eśli chodzi o gwarantowany w Unii stopień ochrony podstawowych praw i wolności, uregulowania Unii stanowiące ingerencję w prawa podstawowe gwarantowane w art. 7 i 8 karty muszą, zgodnie z utrwalonym orzecznictwem Trybunału, zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane osobowe zostają dotknięte ingerencją, miały wystarczające gwarancje rzeczywistej ochrony ich danych przed ryzykiem nadużyć oraz uzyskaniem do nich bezprawnego dostępu i ich wykorzystywaniem. Konieczność zapewnienia takich gwarancji ma znaczenie tym większe, że dane osobowe przetwarzane są automatycznie i istnieje znaczne ryzyko bezprawnego uzyskania dostępu do nich”[67].

103. EROD zauważa w tym względzie, że na podstawie informacji dostępnych w projekcie decyzji ramy ochrony danych Zjednoczonego Królestwa nie stanowią wyraźnie, że wyrok sądu lub trybunału oraz decyzja organu administracyjnego państwa trzeciego wymagające od administratora lub podmiotu przetwarzającego przekazania lub ujawnienia danych osobowych mogą zostać uznane lub być egzekwowalne wyłącznie, gdy opierają się na umowie międzynarodowej obowiązującej między wnioskującym państwem trzecim a Zjednoczonym Królestwem. Art. 48 RODO jest zasadniczym przepisem rozdziału V RODO, ponieważ zawiera wymóg, aby przekazanie lub ujawnienie danych osobowych w następstwie wyroku lub decyzji sądu/trybunału lub organu administracyjnego państwa trzeciego mogły zostać uznane lub być egzekwowalne wyłącznie, gdy opierają się na umowie międzynarodowej obowiązującej między wnioskującym państwem trzecim a Unią lub państwem członkowskim, bez uszczerbku dla innych podstaw przekazania na mocy rozdziału V RODO. EROD przypomina, że „wniosek organu zagranicznego nie stanowi sam w sobie podstawy prawnej do przekazania. Nakaz może zostać uznany, »gdy opiera się na umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, obowiązującej między wnioskującym państwem trzecim

[64] Zob. WP254 rev.01, s. 6.
[65] Zob. WP254 rev.01, s. 6.
[66] Zob. art. 44 zdanie ostatnie RODO, w szczególności: „Wszystkie przepisy niniejszego rozdziału należy stosować z myślą o zapewnieniu, by nie został naruszony stopień ochrony osób fizycznych zagwarantowany w niniejszym rozporządzeniu”.
[67] Zob. Schrems I, pkt 91.

a Unią lub państwem członkowskim«"[68]. Kluczowe znaczenie ma zatem możliwość określenia merytorycznie równoważnych przepisów w prawie Zjednoczonego Królestwa.

104. W projekcie decyzji Komisja Europejska przedstawia wyjaśnienia władz Zjednoczonego Królestwa, zgodnie z którymi na podstawie prawa precedensowego lub ustaw orzeczenie sądu zagranicznego zawierające wniosek o przekazanie danych jest niewykonalne w Zjednoczonym Królestwie bez umowy międzynarodowej, a każde przekazanie danych na wniosek zagranicznego sądu lub organu administracyjnego wymaga narzędzia przekazywania, takiego jak uregulowanie dotyczące odpowiedniości lub odpowiednie zabezpieczenia, chyba że zastosowanie ma odstępstwo na podstawie art. 49 RODO Zjednoczonego Królestwa. EROD nie poinformowano jednak o wymianie informacji między Komisją Europejską a władzami Zjednoczonego Królestwa[69] w tym zakresie, a zatem nie jest ona w stanie przeanalizować i niezależnie ocenić, czy gwarancje przedstawione przez władze Zjednoczonego Królestwa są wystarczające, aby zapewnić merytorycznie równoważny stopień ochrony w odniesieniu do zabezpieczeń zawartych w art. 48 RODO.

105. **EROD zachęca Komisję Europejską do przedstawienia dalszych zapewnień i konkretnych odniesień do prawodawstwa Zjednoczonego Królestwa, które zagwarantują, że stopień ochrony wynikający z ram prawnych Zjednoczonego Królestwa jest merytorycznie równoważny stopniowi ochrony gwarantowanemu w EOG. W związku z tym EROD zachęca Komisję Europejską do przedstawienia pisemnych wyjaśnień i zobowiązań władz Zjednoczonego Królestwa w odniesieniu do wdrażania ochrony merytorycznie równoważnej ochronie przewidzianej w art. 48 RODO.**

106. **EROD uważa, że określenie przepisów prawa Zjednoczonego Królestwa zapewniających merytorycznie równoważny stopień ochrony w stosunku do zabezpieczeń zawartych w art. 48 RODO jest tym istotniejsze w świetle wcześniej wyrażonych obaw dotyczących wniosków o dostęp do danych w Zjednoczonym Królestwie składanych przez organy Stanów Zjednoczonych lub innych państw trzecich oraz biorąc pod uwagę, że zgodnie z decyzją stwierdzającą odpowiedni stopień ochrony dane osobowe mogą być przekazywane z EOG do Zjednoczonego Królestwa bez żadnej dalszej gwarancji lub żadnego wiążącego zobowiązania ze strony odbiorcy w odniesieniu do wniosków o dostęp do danych składanych przez organy innych państw trzecich.**

3.2. Mechanizmy proceduralne i mechanizmy egzekwowania prawa

107. Na podstawie kryteriów określonych w dokumencie dotyczącym odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO EROD przeanalizowała następujące aspekty ram ochrony danych Zjednoczonego Królestwa objęte projektem decyzji: istnienie i skuteczne funkcjonowanie niezależnego organu nadzorczego; istnienie systemu zapewniającego odpowiedni poziom zgodności oraz system dostępu do odpowiednich mechanizmów dochodzenia roszczeń, dzięki któremu osoby fizyczne w UE mogą korzystać ze swoich praw i dochodzić roszczeń bez napotykania uciążliwych barier w dochodzeniu roszczeń na drodze administracyjnej i sądowej.

3.2.1 Właściwy niezależny organ nadzorczy

108. EROD z zadowoleniem przyjmuje starania Komisji Europejskiej zmierzające do kompleksowej analizy ustanowienia, funkcjonowania i uprawnień organu nadzorczego Zjednoczonego Królestwa w rozdziale 2.6. projektu decyzji. W Zjednoczonym Królestwie zadaniem komisarza ds. informacji jest

[68] Zob. załącznik do wspólnej odpowiedzi EROD-EIOD dla komisji LIBE w sprawie wpływu amerykańskiej ustawy CLOUD na europejskie ramy prawne ochrony danych osobowych, przyjęty w dniu 10 lipca 2019 r., https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_pl

[69] Zob. przypis 78 w projekcie decyzji.

nadzorowanie i egzekwowanie zgodności z RODO Zjednoczonego Królestwa i ustawą o ochronie danych z 2018 r. Zgodnie z załącznikiem 12 do ustawy o ochronie danych z 2018 r. Rzecznik Informacji jest „pojedynczą osobą prawną", tj. odrębnym podmiotem prawnym, który tworzy jedna osoba, wspieranym przez Urząd Rzecznika Informacji.

109. W odniesieniu do niezależności komisarza ds. informacji EROD podkreśla, że art. 51 RODO Zjednoczonego Królestwa nie zawiera wyraźnego wyjaśnienia, że Rzecznik Informacji jest niezależnym organem publicznym, jak stwierdzono w art. 51 RODO w odniesieniu do organów nadzorczych. EROD przyznaje jednak, że RODO Zjednoczonego Królestwa odzwierciedla w podobny sposób w art. 52 odpowiednie zasady dotyczące niezależności, jak określono w art. 52 ust. 1–3 RODO.

110. Ponadto EROD zwraca uwagę, że art. 52 RODO Zjednoczonego Królestwa nie zawiera obowiązków odpowiadających art. 52 ust. 4–6 RODO, które wyraźnie zapewniają, by odpowiedni organ nadzorczy dysponował zasobami niezbędnymi do skutecznego wypełniania swoich zadań i wykonywania swoich uprawnień. EROD uznaje jednak, że ustawa o ochronie danych z 2018 r. zawiera przepisy, których celem jest zapewnienie odpowiedniego finansowania Urzędu Rzecznika Informacji[70], a także okoliczność, że Urząd Rzecznika Informacji jest obecnie jednym z największych organów nadzorczych w porównaniu z organami nadzorczymi w UE/EOG. Ponieważ stały przydział odpowiednich zasobów, zwłaszcza w odniesieniu do personelu i budżetu[71], jest niezbędny, aby zapewnić właściwe funkcjonowanie organu nadzorczego w zakresie wypełniania wszystkich powierzonych mu zadań, co Parlament Europejski również uznał ostatnio za niezwykle istotne[72], EROD uważa, że należy zwrócić szczególną uwagę na przyszłe zmiany w tej dziedzinie.

111. **W związku z tym EROD zachęca Komisję Europejską do obserwowania wszelkich zmian w zakresie przyznawania zasobów na rzecz Urzędu Rzecznika Informacji, które to zmiany mogłyby być szkodliwe dla właściwego wypełniania zadań Urzędu Rzecznika Informacji.**

3.2.2. Istnienie systemu ochrony danych zapewniającego odpowiedni poziom zgodności

112. W projekcie decyzji podjęto się kompleksowego zbadania uprawnień, w które wyposażono Urząd Rzecznika Informacji na podstawie art. 58 RODO Zjednoczonego Królestwa i ustawy o ochronie danych z 2018 r., w celu zapewnienia monitorowania i egzekwowania przepisów. EROD przyznaje, że art. 58 RODO Zjednoczonego Królestwa odzwierciedla ściśle odpowiednie zasady dotyczące uprawnień organów nadzorczych, jak określono w art. 58 RODO. Jeśli chodzi o uprawnienie do nakładania administracyjnych kar pieniężnych w zależności od okoliczności każdego indywidualnego przypadku, art. 83 RODO Zjednoczonego Królestwa zawiera podobne przepisy i maksymalne kwoty, jak określono w art. 83 RODO. W związku z tym EROD uważa, że ramy prawne Zjednoczonego Królestwa w tej dziedzinie są obecnie zgodne z normami określonymi w odpowiednich przepisach UE. W tym względzie EROD podkreśla jednak, że istnienie *skutecznych* sankcji odgrywa ważną rolę w zapewnianiu przestrzegania zasad[73].

[70] Zob. art. 137, 138, 182 i załącznik 12 pkt 9 ustawy o ochronie danych z 2018 r.
[71] Zob. WP254 rev.01, s. 7.
[72] Rezolucja Parlamentu Europejskiego z dnia 25 marca 2021 r. w sprawie sprawozdania Komisji z oceny wdrożenia ogólnego rozporządzenia o ochronie danych po dwóch latach jego stosowania, pkt 15, https://www.europarl.europa.eu/doceo/document/B-9-2021-0211_PL.html
[73] Zob. WP254 rev.01, s. 7.

113. **W związku z powyższym EROD zachęca Komisję Europejską do monitorowania skuteczności sankcji i odpowiednich środków ochrony prawnej określonych w ramach ochrony danych Zjednoczonego Królestwa.**

3.2.3. System ochrony danych musi zapewniać wsparcie i pomoc osobom, których dane dotyczą, w wykonywaniu przysługujących im praw i korzystaniu z odpowiednich mechanizmów dochodzenia roszczeń

114. Skuteczny mechanizm nadzoru umożliwiający niezależne rozpatrywanie skarg w celu wykrywania i karania naruszeń praw osób, których dane dotyczą, w praktyce, jak również skuteczne administracyjne i sądowe środki zaskarżenia (w tym odszkodowanie za szkody poniesione w wyniku niezgodnego z prawem przetwarzania danych osobowych osób, których dane dotyczą), są kluczowymi elementami oceny, czy system ochrony danych zapewnia odpowiedni stopień ochrony.

115. EROD z zadowoleniem przyjmuje fakt, że Urząd Rzecznika Informacji udostępnia na swojej stronie internetowej kompleksowe informacje i wytyczne, których celem jest zwiększenie świadomości administratorów i podmiotów przetwarzających na temat ich zobowiązań i obowiązków, a także wspieranie osób, których dane dotyczą, w uzyskiwaniu informacji o ich prawach dotyczących danych osobowych oraz dochodzeniu ich indywidualnych praw na podstawie RODO Zjednoczonego Królestwa i ustawy o ochronie danych z 2018 r.

116. **Niezależnie od obecnej sytuacji EROD zachęca Komisję Europejską do stałego obserwowania poziomu wsparcia, jakie Urząd Rzecznika Informacji udziela w szczególności osobom fizycznym, których dane osobowe przekazano do Zjednoczonego Królestwa na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, aby pomóc im w korzystaniu z praw przysługujących im na podstawie systemu ochrony danych Zjednoczonego Królestwa.**

4. DOSTĘP DO DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UE PRZEZ ORGANY PUBLICZNE W ZJEDNOCZONYM KRÓLESTWIE I ICH WYKORZYSTYWANIE

4.1. Dostęp organów publicznych Zjednoczonego Królestwa do danych na potrzeby ścigania przestępstw i wykorzystywanie tych danych przez te organy w tym samym celu

4.1.1. Podstawy prawne i właściwe ograniczenia/zabezpieczenia

117. Jeśli chodzi o ocenę przeprowadzoną przez Komisję Europejską i udokumentowaną w motywach 132 i nast. projektu decyzji **w sprawie dostępu na potrzeby ścigania przestępstw**, 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 większości ustaleń faktycznych i ocen. Istnieją jednak pewne przypadki, w których przedstawienie faktów lub wyjaśnienie wniosków nie wystarczą do przyjęcia ich przez EROD.

4.1.1.1. Wykorzystanie zgody

118. EROD odnotowuje, że Komisja Europejska stwierdza w motywie 184 projektu decyzji[74], że **wykorzystanie zgody** nie jest istotne w scenariuszu dotyczącym odpowiedniego stopnia ochrony,

[74] Zob. s. 37 w projekcie decyzji.

ponieważ w sytuacjach przekazywania danych organ ścigania Zjednoczonego Królestwa nie zbiera danych bezpośrednio od osoby, której dane dotyczą, na podstawie zgody. W związku z tym Komisja Europejska nie ocenia wykorzystania zgody jako podstawy prawnej w działaniach policyjnych.

119. W tym względzie EROD przypomina, że art. 45 ust. 2 lit. a) RODO zawiera wymóg, aby w ocenie uwzględniono szeroki wachlarz elementów, które nie ograniczają się do sytuacji przekazywania danych, w tym „praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie [...] prawa karnego".

120. EROD zauważa, również na podstawie informacji przedstawionych przez Komisję Europejską w motywie 38 projektu decyzji wykonawczej na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie odpowiedniego stopnia ochrony danych osobowych w Zjednoczonym Królestwie (zwanego dalej „projektem decyzji stwierdzającej odpowiedni stopień ochrony na podstawie dyrektywy (UE) 2016/680"), że wykorzystanie zgody, tak jak zostało to ujęte w systemie Zjednoczonego Królestwa w kontekście ścigania przestępstw, zawsze wymagałoby podstawy prawnej, na którą można by się powołać. Oznacza to, że nawet jeśli policja posiada ustawowe uprawnienia do przetwarzania danych w celu prowadzenia dochodzenia, w pewnych szczególnych okolicznościach (np. w celu pobrania próbki DNA) może ona uznać za stosowne zwrócenie się o zgodę osoby, której dane dotyczą.

121. **EROD zachęca Komisję Europejską do wprowadzenia do decyzji stwierdzającej odpowiedni stopień ochrony danych analizy dotyczącej możliwości wykorzystania zgody w kontekście ścigania przestępstw przewidzianej w projekcie decyzji stwierdzającej odpowiedni stopień ochrony dyrektywy (UE) 2016/680**.

4.1.1.2. Nakazy przeszukania i nakazy wydania dowodów

122. Chociaż EROD nie ma uwag na temat pozyskiwania dowodów przez policję na podstawie nakazów przeszukania i nakazów wydania dowodów ogółem, z motywu 136 projektu decyzji wynika, że Komisja Europejska skoncentrowała się w swoich rozważaniach dotyczących dostępu organów ścigania na policji, a w mniejszym stopniu przeanalizowała przetwarzanie danych osobowych przez inne organy ścigania.

123. Na przykład w „Ramach wyjaśniających Zjednoczonego Królestwa na potrzeby dyskusji na temat odpowiedniego stopnia ochrony", w sekcji F dotyczącej ścigania przestępstw[75] na s. 11 zasugerowano, że **Krajowa Agencja ds. Przestępczości** (ang. National Crime Agency, zwana dalej „NCA") mogłaby być szczególnie istotnym organem ścigania, który między innymi pełni szerszą funkcję w zakresie wywiadu kryminalnego. NCA określa swoją misję jako gromadzenie danych wywiadowczych z różnych źródeł w celu zmaksymalizowania możliwości analizy, ocen i możliwości taktycznych, w tym w ramach technicznego przechwytywania komunikacji oraz od partnerów zajmujących się ściganiem przestępstw w Zjednoczonym Królestwie i za granicą, agencji bezpieczeństwa i wywiadu[76]. NCA jest również jednym z głównych podmiotów w kontaktach

[75] Zob. rząd Zjednoczonego Królestwa, „Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement" [„Ramy wyjaśniające na potrzeby dyskusji na temat odpowiedniego stopnia ochrony, sekcja F: ściganie przestępstw"], 13 marca 2020 r., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

[76] Zob. strona internetowa NCA, „Intelligence: enhancing the picture of serious organised crime affecting the UK" [„Wywiad: poprawa obrazu sytuacji w zakresie poważnej przestępczości zorganizowanej dotykającej

z międzynarodowymi partnerami w dziedzinie ścigania przestępstw i odgrywa kluczową rolę w wymianie danych wywiadowczych dotyczących przestępstw[77].

124. EROD odnotowuje ponadto fakt, że Centrala Łączności Rządowej (ang. Government Communications Headquarters, zwana dalej „GCHQ"), której działania zwykle są objęte zakresem części 4 ustawy o ochronie danych z 2018 r., tj. dotyczącej bezpieczeństwa narodowego, przyjmuje również aktywną rolę w ograniczaniu szkód społecznych i finansowych, jakie poważna i zorganizowana przestępczość wyrządza w Zjednoczonym Królestwie, ściśle współpracując z Ministerstwem Spraw Wewnętrznych (Home Office), NCA, Królewskim Urzędem Podatkowym i Celnym (ang. HM Revenue and Customs, HMRC) i innymi departamentami rządowymi[78]. Jej działalność dotyczy zwalczania niegodziwego traktowania dzieci w celach seksualnych; nadużyć finansowych; innych rodzajów przestępstw gospodarczych, w tym prania pieniędzy; przestępczego wykorzystywania technologii; cyberprzestępczości; nielegalnej migracji o znamionach przestępczości zorganizowanej, w tym handlu ludźmi, oraz handlu narkotykami, bronią palną i innych nielegalnych działań przemytniczych.

125. **EROD wzywa Komisję Europejską do uzupełnienia jej analizy o analizę agencji działających w dziedzinie ścigania przestępstw, które, jak się wydaje, uczyniły gromadzenie i analizę danych, w tym danych osobowych, centralnym punktem swoich codziennych działań, w szczególności NCA. Ponadto EROD zachęca Komisję Europejską, aby bliżej przyjrzała się agencjom takim jak GCHQ, których działalność wchodzi w zakres zarówno ścigania przestępstw, jak i bezpieczeństwa narodowego, oraz podlega ramom prawnym mającym do nich zastosowanie w odniesieniu do przetwarzania danych osobowych.**

4.1.1.3. Uprawnienia dochodzeniowo-śledcze na potrzeby ścigania przestępstw

126. W rozdziale 4 dokumentu dotyczącego odpowiedniego stopnia ochrony przekazywanych danych osobowych na podstawie RODO „Niezbędne gwarancje w **państwach trzecich dotyczące dostępu do danych w celu egzekwowania prawa** i ze względów bezpieczeństwa narodowego mające na celu ograniczenie ingerencji w prawa podstawowe" EROD przypomina, że „[w] tym kontekście Trybunał zauważył również krytycznie, że poprzednia decyzja w sprawie »bezpiecznej przystani« »nie zawiera żadnego stwierdzenia dotyczącego istnienia w Stanach Zjednoczonych reguł o charakterze ogólnopaństwowym służących do ograniczenia ewentualnych ingerencji w prawa podstawowe osób,

Zjednoczone Królestwo"], https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk

[77] Chociaż nie wszystkie dane wywiadowcze przetwarzane przez NCA są danymi osobowymi, znaczna ich część może stanowić takie dane, a opisane w tej części działania różnią się od klasycznych działań policyjnych, a zatem ocena dostępu do danych osobowych przez organy ścigania w Zjednoczonym Królestwie nie byłaby kompletna bez dokładnej oceny działań NCA. Rozsądne wydaje się dopilnowanie, aby zasady ochrony danych były interpretowane w taki sam sposób we wszystkich właściwych organach ścigania, co pozwoliłoby rzucić światło na agencję, której działalność w szczególności opiera się na danych, jaką jest NCA. Ponadto w sekcji dotyczącej przyszłych działań przedstawiono ciąg dalszy wyjaśnienia: „[n]ieustannie poszukujemy nowych możliwości gromadzenia, rozwijania i wzmacniania tradycyjnych zdolności w celu zwiększenia ilości i jakości danych wywiadowczych dostępnych do wykorzystania zarówno w Zjednoczonym Królestwie, jak i za granicą. W ramach tych działań rozwijamy nową Krajową Zdolność Wykorzystywania Danych, wykorzystując uprawnienia nadane agencji na mocy ustawy o zwalczaniu przestępczości i sądach, na potrzeby uzyskiwania dostępu do informacji przechowywanych przez różne departamenty rządu oraz łączenia ich i wykorzystywania. [...] Wszystkie te działania pozwolą zwiększyć naszą sprawność i elastyczność, aby reagować na nowe zagrożenia i działać w sposób proaktywny, gromadzić i analizować informacje i dane wywiadowcze na temat pojawiających się zagrożeń, abyśmy mogli działać, zanim zagrożenia się zmaterializują".

[78] Zob. strona internetowa GCHQ, sekcja poświęcona misjom w zakresie zwalczania poważnej i zorganizowanej przestępczości, https://www.gchq.gov.uk/section/mission/serious-crime

których dane zostały przekazane z Unii do Stanów Zjednoczonych**, ingerencji, które organy państwowe tego kraju mogłyby dokonywać przy okazji dążenia do realizacji uzasadnionego prawem celu**, takiego jak bezpieczeństwo narodowe«."[79]. W dokumencie tym EROD stwierdza, że aby **cztery europejskie niezbędne gwarancje**[80] **zostały uznane za odpowiednie, muszą być jednak przestrzegane przez wszystkie państwa trzecie w odniesieniu do dostępu do danych**, zarówno ze względów bezpieczeństwa narodowego, jak i **do celów egzekwowania prawa**: w szczególności **należy wykazać konieczność i proporcjonalność w odniesieniu do zamierzonych prawnie uzasadnionych celów.**

127. W tej części projektu decyzji Komisja Europejska stwierdza (motyw 139) „ponieważ uprawnienia dochodzeniowo-śledcze przewidziane w ustawie o uprawnieniach dochodzeniowo-śledczych z 2016 r. są takie same jak te, którymi dysponują krajowe agencje bezpieczeństwa, warunki, ograniczenia i zabezpieczenia mające zastosowanie do takich uprawnień zostały szczegółowo omówione w sekcji dotyczącej dostępu organów publicznych Zjednoczonego Królestwa do danych osobowych na potrzeby bezpieczeństwa narodowego i wykorzystywania tych danych przez te organy w tym samym celu". Wynika to jednak z orzecznictwa TSUE, który po poddaniu prawodawstwa państw członkowskich zezwalających na zatrzymywanie danych osobowych i dostęp do nich przez organy publiczne analizie konieczności i proporcjonalności stwierdził, że uzasadnione cele, takie jak bezpieczeństwo narodowe lub zwalczanie poważnych przestępstw, są różne, a zatem jeden z nich może uzasadnić pewien rodzaj ingerencji, podczas gdy drugi nie[81].

128. **W związku z tym EROD z zadowoleniem przyjmie określoną w decyzji szczegółową ocenę konieczności i proporcjonalności warunków, ograniczeń i zabezpieczeń opisanych w motywie 174 i następnych – czyli w części poświęconej środkom służącym celom bezpieczeństwa narodowego – w przypadku zastosowania tych warunków, ograniczeń i zabezpieczeń w kontekście środka służącego celom związanym ze ściganiem przestępstw. Zwraca się zatem do Komisji Europejskiej o dalsze wyjaśnienie, czy opisane zatrzymywanie danych osobowych i dostęp do nich na potrzeby ścigania przestępstw są wystarczająco ograniczone, by zapewnić stopień ochrony merytorycznie równoważny temu gwarantowanemu w UE.**

4.1.2. Dalsze wykorzystywanie informacji zgromadzonych na potrzeby ścigania przestępstw (motywy 140–154)

129. EROD zauważa, że ramy ochrony danych w Zjednoczonym Królestwie przewidują podobne zabezpieczenia i ograniczenia jak te przewidziane w prawie Unii w odniesieniu do dalszego wykorzystywania informacji zgromadzonych na potrzeby ścigania przestępstw.

4.1.2.1. Dalsze wykorzystywanie do innych celów w zakresie ścigania przestępstw

130. W ustawie o ochronie danych z 2018 r. przewidziano, że dane osobowe zgromadzone przez właściwy organ na potrzeby ścigania przestępstw mogą być dalej przetwarzane (przez pierwotnego administratora lub innego administratora) do jakichkolwiek innych celów w zakresie ścigania przestępstw, pod warunkiem że administrator jest upoważniony na mocy prawa do przetwarzania danych w tym innym celu, a przetwarzanie jest niezbędne i proporcjonalne do tego celu. Komisja Europejska zauważa, że wszystkie zabezpieczenia przewidziane w części 3 ustawy o ochronie danych z 2018 r. mają zastosowanie do przetwarzania prowadzonego przez organ otrzymujący. EROD

[79] Zob. WP254 rev.01, s. 9.
[80] Zob. Zalecenia 02/2020 EROD dotyczące niezbędnych gwarancji europejskich dla środków nadzoru.
[81] Zob. wyrok TSUE, sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in., z dnia 6 października 2020 r., ECLI:EU:C:2020:791.

podkreśla jednak, że w części 3, art. 44 ust. 4, art. 45 ust. 4, art. 48 ust. 3 i art. 68 ust. 7, ustawy o ochronie danych z 2018 r. przewidziano możliwość ograniczenia praw osoby, której dane dotyczą, a w art. 79 przewidziano możliwość wydawania certyfikatów poświadczających, że ograniczenie jest niezbędnym i proporcjonalnym środkiem służącym ochronie bezpieczeństwa narodowego. **EROD zaleca zatem, aby Komisja Europejska przeprowadziła dalszą ocenę ewentualnego wpływu takich ograniczeń na stopień ochrony danych osobowych w odniesieniu do dalszego wykorzystywania zgromadzonych informacji. Należy również przedstawić dalsze wyjaśnienia na temat faktu, że ramy prawne Zjednoczonego Królestwa dopuszczają takie dalsze udostępnianie, w szczególności ustawa o gospodarce cyfrowej z 2017 r., jak również ustawa o zwalczaniu przestępczości i sądach z 2013 r., która dopuszcza udostępnianie informacji NCA.**

4.1.2.2. Dalsze wykorzystywanie do innych celów niż ściganie przestępstw w Zjednoczonym Królestwie

131. Ustawa o ochronie danych z 2018 r. stanowi również, że dane osobowe zebrane w jakimkolwiek celu związanym ze ściganiem przestępstw mogą być przetwarzane w celu, który nie jest celem związanym ze ściganiem przestępstw, jeżeli prawo dopuszcza takie przetwarzanie. W tym przypadku podstawą prawną upoważniającą do takiego udostępniania jest art. 19 ustawy o zwalczaniu terroryzmu z 2008 r. W tym względzie EROD zauważa, że zakres i przepisy art. 19 ustawy o zwalczaniu terroryzmu nie zostały w pełni uwzględnione w ocenie Komisji Europejskiej i mogą sugerować dalsze wykorzystywanie o szerszym charakterze, w szczególności w odniesieniu do art. 19 ust. 2, który stanowi, że „[i]nformacje uzyskane przez którąkolwiek ze służb wywiadu w związku z wykonywaniem którejkolwiek z jej funkcji mogą być wykorzystane przez tę służbę w związku z wykonywaniem którejkolwiek z jej innych funkcji".

132. EROD zauważa również, że stwierdzenie Komisji Europejskiej, iż właściwe organy są organami publicznymi, które muszą działać zgodnie z EKPC, w tym z jej art. 8, zapewniając w ten sposób zgodność wszelkiej wymiany danych pomiędzy organami ścigania a służbami wywiadowczymi z prawodawstwem dotyczącym ochrony danych oraz z EKPC, można by dodatkowo uzasadnić poprzez wskazanie odpowiednich aktów i ustaw należących do porządku prawnego Zjednoczonego Królestwa, które jasno i precyzyjnie określają takie ograniczenia.

4.1.2.3. Dalsze wykorzystywanie w kontekście dalszego przekazywania danych poza Zjednoczone Królestwo

133. Chociaż Komisja Europejska odniosła się do faktu, że umowa między Zjednoczonym Królestwem a USA dotycząca ustawy CLOUD może mieć wpływ na dalsze przekazywanie danych do Stanów Zjednoczonych przez dostawcę usług łączności elektronicznej lub usług przetwarzania danych (CSP) w Zjednoczonym Królestwie, EROD podkreśla również, że wejście w życie tej umowy może mieć również wpływ na wykorzystywanie zebranych danych poprzez ich dalsze przekazywanie przez organy ścigania w Zjednoczonym Królestwie, w szczególności w odniesieniu do wydawania i przekazywania nakazów zgodnie z art. 5 tej umowy.

134. Szerzej rzecz ujmując, EROD uważa, że zawarcie w przyszłości dwustronnych umów z państwami trzecimi w celu współpracy w zakresie ścigania przestępstw, stanowiących podstawę prawną przekazywania danych osobowych do tych państw, może również w znacznym stopniu wpłynąć na warunki dalszego wykorzystywania zgromadzonych informacji, ponieważ – jak oceniono – takie umowy mogą mieć wpływ na ramy ochrony danych Zjednoczonego Królestwa. EROD zaleca zatem, aby Komisja Europejska dokonała dalszej oceny tej kwestii, ustalając, czy takie umowy międzynarodowe istnieją, oraz wyjaśniła, czy postanowienia tych umów mogą mieć wpływ na stosowanie przepisów o ochronie danych Zjednoczonego Królestwa, a także aby zapewniła dalsze ograniczenia lub wyłączenia w odniesieniu do dalszego wykorzystywania i ujawniania za granicą

informacji zebranych do celów ścigania przestępstw. EROD uważa, że takie informacje i ocena są niezbędne, aby umożliwić kompleksową ocenę stopnia ochrony zapewnianej przez ramy legislacyjne i praktyki Zjednoczonego Królestwa w odniesieniu do ujawniania i dalszego wykorzystywania informacji za granicą.

4.1.3. Nadzór

135. EROD zauważa, że nadzór nad organami ścigania w sprawach karnych jest zapewniany przez połączenie funkcji kilku różnych komisarzy, w tym Urzędu Rzecznika Informacji. W projekcie ustaleń dotyczących zapewnienia odpowiedniego stopnia ochrony wymieniono Komisarza ds. uprawnień dochodzeniowo-śledczych, Komisarza ds. zatrzymywania i wykorzystywania materiału biometrycznego (Commissioner for the Retention and Use of Biometric Material) oraz Komisarza ds. kamer monitorujących (Surveillance Camera Commissioner). W tym kontekście należy zauważyć, że TSUE wielokrotnie podkreślał potrzebę zapewnienia niezależnego nadzoru. Komisarz ds. uprawnień dochodzeniowo-śledczych ma szczególne znaczenie dla kwestii dostępu do danych osobowych przekazywanych do Zjednoczonego Królestwa. EROD sądzi, że Komisarz ds. uprawnień dochodzeniowo-śledczych jest tak zwanym komisarzem sądowym działającym podobnie jak inni komisarze sądowi, o których należy mówić w kontekście rozdziału dotyczącego bezpieczeństwa narodowego, oraz że ci komisarze sądowi korzystają z niezawisłości sędziów również podczas pełnienia funkcji komisarza. Jeśli chodzi o urząd Komisarza ds. uprawnień dochodzeniowo-śledczych, Komisja Europejska wyjaśnia w motywie 245 projektu decyzji, że funkcjonuje on jako organ niezależny, ale jest finansowany przez Ministerstwo Spraw Wewnętrznych (Home Office).

136. EROD nie stwierdziła w projekcie decyzji dalszych wskazówek pozwalających ocenić niezależność komisarza ds. zatrzymywania i wykorzystywania materiału biometrycznego oraz komisarza ds. kamer monitorujących.

137. **Komisję Europejską wzywa się do przeprowadzenia dalszej oceny niezależności komisarzy sądowych, także w przypadkach, w których komisarz nie pełni (już) funkcji sędziego, a także do przeprowadzenia oceny niezależności komisarza ds. zatrzymywania i wykorzystywania materiału biometrycznego oraz komisarza ds. kamer monitorujących.**

4.2. Ogólne ramy prawne w zakresie ochrony danych w dziedzinie bezpieczeństwa narodowego

4.2.1. Certyfikaty bezpieczeństwa narodowego

138. Zgodnie z art. 111 ustawy o ochronie danych z 2018 r. administratorzy mogą ubiegać się o certyfikaty bezpieczeństwa narodowego wydawane przez ministra, członka gabinetu, prokuratora generalnego lub rzecznika generalnego ds. Szkocji, poświadczające, że wyłączenia z obowiązków i praw zapisanych w częściach 4–6 ustawy o ochronie danych z 2018 r. są niezbędnym i proporcjonalnym środkiem ochrony bezpieczeństwa narodowego. Certyfikaty te mają na celu zapewnienie administratorom większej pewności prawa i będą stanowiły rozstrzygający dowód na to, że przy przetwarzaniu danych osobowych uwzględniane są kwestie dotyczące bezpieczeństwa narodowego. Należy jednak wspomnieć, że certyfikaty te nie są wymagane w celu powołania się na wyłączenia dotyczące bezpieczeństwa narodowego, lecz stanowią środek zapewniania przejrzystości[82].

[82] Zob. Ministerstwo Spraw Wewnętrznych (Home Office), ustawa o ochronie danych z 2018 r., wytyczne dotyczące certyfikatów bezpieczeństwa narodowego, sierpień 2020 r., s. 3 pkt 4,

139. EROD wnioskuje na podstawie pkt 17 i 18 załącznika 20 do ustawy o ochronie danych z 2018 r., że certyfikat bezpieczeństwa narodowego wydany na podstawie ustawy o ochronie danych osobowych z 1998 r. (zwany dalej „starym certyfikatem") miał przedłużony okres obowiązywania na potrzeby przetwarzania danych osobowych na podstawie ustawy o ochronie danych z 2018 r. do dnia 25 maja 2019 r. Do tego dnia stare certyfikaty, o ile nie zostały zastąpione lub cofnięte, były traktowane tak, jakby zostały wydane na podstawie ustawy o ochronie danych z 2018 r.

140. EROD wnioskuje jednak, że w przypadku braku wyraźnego wskazania daty wygaśnięcia ważności na certyfikacie bezpieczeństwa narodowego wydanym na podstawie ustawy o ochronie danych z 1998 r. taki certyfikat będzie nadal obowiązywać w odniesieniu do przetwarzania danych zgodnie ustawą o ochronie danych z 1998 r., chyba że zostanie cofnięty lub unieważniony[83]. Mimo że ochrona zapewniana przez te stare certyfikaty ogranicza się do przetwarzania danych osobowych na podstawie ustawy o ochronie danych z 1998 r., EROD odnotowuje, że nowe certyfikaty bezpieczeństwa narodowego mogą być wydawane na mocy ustawy o ochronie danych z 1998 r. w odniesieniu do danych osobowych, które były przetwarzane na podstawie ustawy o ochronie danych z 1998 r.[84]

141. **W celu zarysowania pełnego obrazu sytuacji EROD zwraca się do Komisji Europejskiej o doprecyzowanie w projekcie decyzji, że certyfikaty bezpieczeństwa narodowego mogą być nadal wydawane na podstawie ustawy o ochronie danych z 1998 r. EROD zwraca się również do Komisji Europejskiej o przedstawienie w projekcie decyzji opisu mechanizmu dochodzenia roszczeń i mechanizmu nadzoru w odniesieniu do certyfikatów wydanych na podstawie ustawy o ochronie danych z 1998 r. Ponadto EROD zwraca się do Komisji Europejskiej o uwzględnienie w projekcie decyzji liczby istniejących certyfikatów wydanych na podstawie ustawy o ochronie danych z 1998 r. oraz do uważnego monitorowania tego aspektu.**

4.2.2. Prawo do sprostowania i usunięcia danych

142. Jeżeli chodzi o prawo do sprostowania i usunięcia danych, EROD zauważa, że zgodnie z art. 100 i art. 149 ustawy o ochronie danych z 2018 r. osoby, których dane dotyczą, mają możliwość powołania się na Sąd wyższej instancji (Szkocja, naczelny sąd cywilny), aby nakazać administratorowi sprostowanie lub usunięcie ich danych bez zbędnej zwłoki.

143. **EROD podkreśla, że należy skutecznie zapewnić wykonywanie praw osób, których dane dotyczą; dlatego zwraca się do Komisji Europejskiej o opisanie w projekcie decyzji, jak w praktyce działa art. 100 ustawy o ochronie danych z 2018 r., oraz o ścisłe monitorowanie stosowania tego artykułu.**

4.2.3. Wyłączenia ze względu na bezpieczeństwo narodowe

144. EROD pragnie zwrócić uwagę na art. 110 ustawy o ochronie danych z 2018 r., a w szczególności na załącznik 11, w którym określono konkretne cele, w których służby wywiadowcze mogą odstąpić od niektórych zasad ochrony danych, w tym w odniesieniu do praw osób, których dane dotyczą, i nie są

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf

[83] Zob. Ministerstwo Spraw Wewnętrznych (Home Office), ustawa o ochronie danych z 2018 r., wytyczne dotyczące certyfikatów bezpieczeństwa narodowego, sierpień 2020 r., s. 5.

[84] Zob. Ministerstwo Spraw Wewnętrznych (Home Office), ustawa o ochronie danych z 2018 r., wytyczne dotyczące certyfikatów bezpieczeństwa narodowego, sierpień 2020 r., s. 5 pkt 8.

zobowiązane do informowania Urzędu Rzecznika Informacji o naruszeniach ochrony danych osobowych[85].

145. **EROD wzywa Komisję Europejską do dalszego wyjaśnienia zakresu wyłączeń, ponieważ zastanawia się, czy wszystkie wyłączenia określone w załączniku 11 do ustawy o ochronie danych z 2018 r. są istotne dla pracy służb wywiadowczych oraz czy w równoważnym stopniu zapewniają poszanowanie zasady konieczności i proporcjonalności**. W szczególności **EROD wzywa Komisję Europejską o przedstawienie dodatkowych wyjaśnień na temat okoliczności, w których służba wywiadowcza mogłaby powołać się na pkt 10 załącznika 11 do ustawy o ochronie danych z 2018 r., który stanowi, że „wymienione przepisy nie mają zastosowania do danych osobowych, które składają się z zapisów intencji administratora w odniesieniu do wszelkich negocjacji z osobą, której dane dotyczą, w zakresie, w jakim zastosowanie wymienionych przepisów prawdopodobnie przyniosłoby szkodę negocjacjom".**

4.3. Dostęp organów publicznych Zjednoczonego Królestwa do danych w celach związanych z bezpieczeństwem narodowym i wykorzystywanie przez nie tych danych w celach związanych z bezpieczeństwem narodowym

146. 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[86] – 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[87]. 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[88]. Jednak zgodnie z ostatnim zdaniem art. 52 ust. 3 Karty praw podstawowych Unii Europejskiej „[n]iniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę".

147. Dlatego też w poniższej ocenie EROD uwzględniła orzecznictwo Europejskiego Trybunału Praw Człowieka w zakresie, w jakim Karta praw podstawowych Unii Europejskiej, zgodnie z wykładnią

[85] Do celów tych należą: zapobieganie i wykrywanie „przestępczości", „informacje, których ujawnienie jest wymagane na mocy prawa lub w związku z postępowaniem sądowym", „przywilej parlamentarny", „postępowanie sądowe", „zaszczyty i tytuły koronne", „siły zbrojne", „dobrobyt gospodarczy", „prawnicza tajemnica zawodowa", „negocjacje", „poufne referencje udzielone przez administratora", „arkusze egzaminacyjne i oceny z egzaminów", „badania naukowe i statystyka" oraz „archiwizacja w interesie publicznym".

[86] Zob. Zalecenia 02/2020 EROD dotyczące niezbędnych gwarancji europejskich dla środków nadzoru.

[87] Zob. Schrems II, pkt 98.

[88] Zob. wyrok TSUE, sprawy połączone C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in., z dnia 6 października 2020 r., ECLI:EU:C:2020:791, pkt 124.

TSUE, nie przewiduje wyższego stopnia ochrony, który wymagałby spełnienia innych wymogów niż określone w orzecznictwie Europejskiego Trybunału Praw Człowieka.

4.3.1. Podstawy prawne, ograniczenia i zabezpieczenia – uprawnienia dochodzeniowo-śledcze wykonywane w kontekście bezpieczeństwa narodowego

4.3.1.1. Uwagi ogólne

148. EROD przypomina, że ustawę o uprawnieniach dochodzeniowo-śledczych z 2016 r. uchwalono niedawno i zmieniono nią szereg przepisów ustawy o służbach wywiadowczych z 1994 r. Określono w niej zakres, w którym można wykorzystywać niektóre uprawnienia dochodzeniowo-śledcze do ingerencji w prywatność[89]. Pomimo dwóch sprawozdań Komisarza ds. uprawnień dochodzeniowo-śledczych, w których przedstawiono użyteczne informacje na temat stosowania tych nowych ram prawnych, nadal nie zbadano niektórych aspektów, w szczególności dotyczących selektorów i stosowanych kryteriów wyszukiwania.

149. Ponadto tytułem uwagi ogólnej dotyczącej ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. i zakresu jej stosowania EROD zwraca uwagę na następujące cztery kwestie:

150. W odniesieniu do **pierwszej kwestii, na którą należy zwrócić uwagę**, dotyczącej elementów ustawy, EROD pragnie podkreślić dwa aspekty:

151. Po pierwsze, EROD zauważa, że przepisy odnoszą się do szerokich celów stosowania procedur przewidzianych w ustawie o uprawnieniach dochodzeniowo-śledczych z 2016 r. a nie do kategorii osób fizycznych, których może dotyczyć gromadzenie danych na podstawie części 2–7 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. W tym względzie EROD przypomina, że aby można było określić zakres podmiotowy ustawy, powinien istnieć związek między kategoriami osób fizycznych, które mogą zostać objęte środkami nadzoru, a celami prawodawstwa.

152. Ponadto EROD podkreśla, że również definicje „operatorów telekomunikacyjnych", „usługi telekomunikacyjnej" i „systemu telekomunikacyjnego", które określają zakres zastosowania ustawy, są bardzo szerokie i do pewnego stopnia niejasne. EROD wskazuje, że pojęcia te, w kontekście ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r., należy rozumieć w sposób znacznie szerszy niż wynika to z prawodawstwa telekomunikacyjnego, np. z definicji zawartych w Europejskim kodeksie łączności elektronicznej[90]. EROD zauważa, że zawarte w ustawie definicje „usługi telekomunikacyjnej" i „systemu telekomunikacyjnego" są celowo szerokie, aby pozostały aktualne na potrzeby nowych technologii. Również definicja operatora telekomunikacyjnego jest bardzo szeroka i mogłaby na przykład obejmować gry *online* z funkcją czatu lub inne strony internetowe składające się jedynie z takich okien czatu[91].

---

[89] Zob. art. 1 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.

[90] Zob. art. 2 pkt 5 Europejskiego kodeksu łączności elektronicznej, w którym zdefiniowano na przykład „usługę łączności interpersonalnej" jako „usługę zazwyczaj świadczoną za wynagrodzeniem, która umożliwia bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci łączności elektronicznej między skończoną liczbą osób, w ramach której osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, natomiast nie obejmuje ona usług, które umożliwiają interpersonalną i interaktywną komunikację wyłącznie jako podrzędną funkcję dodatkową, która jest nieodłącznie związana z inną usługą".

[91] Zob. Ministerstwo Spraw Wewnętrznych (Home Office), Kodeks postępowania w zakresie przechwytywania komunikacji, marzec 2018 r., pkt 2.5 i następne, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

153. Ponadto chociaż zasadniczo określono procedury i nadzór dotyczące oceny konieczności i proporcjonalności gromadzenia danych i dostępu do nich, w samej ustawie nie określono kryteriów przeprowadzenia takiej oceny. Dodatkowe informacje można znaleźć w innych dokumentach, takich jak kodeksy postępowania.

154. Jednak jak przypomniano w zaleceniach EROD 02/2020 dotyczących niezbędnych gwarancji europejskich dla środków nadzoru, TSUE wskazał, że „wymóg, zgodnie z którym wszelkie ograniczenia korzystania z praw podstawowych muszą być przewidziane ustawą, oznacza, że podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa”[92]. Ściślej rzecz ujmując, TSUE wyjaśnił, że aby spełnić wymóg proporcjonalności, „uregulowanie musi zawierać jasne i precyzyjne przepisy regulujące zakres i sposób stosowania rozpatrywanego środka oraz ustanawiające minimalne wymogi służące temu, aby osoby, o których dane osobowe chodzi, miały wystarczające gwarancje pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć. Uregulowanie musi być prawnie wiążące w prawie krajowym, a w szczególności powinno ono wskazywać, w jakich okolicznościach i pod jakimi warunkami może zostać przyjęty środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja będzie ograniczona do tego, co ściśle konieczne”[93].

155. Również Europejski Trybunał Praw Człowieka podkreślił znaczenie jasności prawa, aby osoby fizyczne mogły uzyskać odpowiednie informacje na temat okoliczności i warunków, w których organy publiczne są uprawnione do stosowania tego rodzaju środków[94].

156. **W związku z tym EROD wzywa Komisję Europejską do dalszej oceny wskazanych aspektów dotyczących precyzyjności, jasności i wyczerpującego charakteru przedmiotowej ustawy oraz do przedstawienia dalszych informacji w celu wykazania, że zapewnia ona stopień ochrony merytorycznie równoważny z tym gwarantowanym w UE w odniesieniu do elementów tej ustawy. EROD podkreśla również, że szerokie definicje należy oceniać również w odniesieniu do proporcjonalności środków dotyczących przechwytywania.**

157. Ponadto chociaż w szeregu wewnętrznych kodeksów właściwych organów służb wywiadowczych częściowo rozwinięto niektóre z tych elementów, na przykład w odniesieniu do oceny konieczności i proporcjonalności gromadzenia danych, EROD podkreśla, że wymogi TSUE dotyczące charakteru prawa oznaczają, że podstawowe elementy, w tym możliwość powoływania się na nie przez osoby fizyczne w kontekście dochodzenia roszczeń, muszą być określone w przepisach gwarantujących prawa, które mogą być egzekwowalne[95]. W pkt 6 załącznika 7 do ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. rzeczywiście stwierdzono, że sądy (i organy nadzorcze) „biorą pod uwagę możliwość nieuwzględnienia przez osobę kodeksu przy rozstrzyganiu kwestii w każdym takim postępowaniu”, nie wyjaśniając, czy osoby fizyczne mogą powoływać się na naruszenie kodeksów przed sądami (lub organami nadzorczymi). Ponadto elementy przedstawione dotychczas w projekcie decyzji odnoszą się albo do uznania przez Europejski Trybunał Praw Człowieka

[92] Zob. *Schrems II*, pkt 175; oraz przytoczone orzecznictwo, a także wyrok TSUE w sprawie C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs i in., z dnia 6 października 2020 r., ECLI:EU:C:2020:790 (dalej „Privacy International”), pkt 65.

[93] Zob. Privacy International, pkt 68.

[94] Zob. Europejski Trybunał Praw Człowieka, Zakharov/Rosja, z dnia 4 grudnia 2015 r., CE:ECHR:2015:1204JUD004714306, pkt 229.

[95] W tym względzie TSUE uznał na przykład, że amerykańska dyrektywa PPD 28 nie spełnia warunków, mimo że przewiduje również pewne ograniczenia w odniesieniu do masowego gromadzenia danych, zob. Schrems II, pkt 181.

przewidywalności zasad określonych[96] w tych kodeksach, a nie do „możliwości egzekwowania" ich przed sądem, jak wymaga tego TSUE, albo do faktu, że sądy Zjednoczonego Królestwa w niektórych przypadkach powoływały się na kodeksy, podczas gdy w żadnej z wymienionych spraw nie przedstawiono możliwości egzekwowania przez osoby fizyczne praw wynikających z kodeksów. **W przypadku stwierdzenia, że w prawie Zjednoczonego Królestwa nie wskazano w sposób wystarczający okoliczności i warunków, w jakich można przyjąć dany środek, oraz że elementy te w istocie zawarto w wewnętrznych kodeksach organów służ wywiadowczych**, **EROD wezwie Komisję Europejską do dalszej oceny, czy osoby fizyczne mogą egzekwować przed sądem ograniczenia i zabezpieczenia przewidziane w poszczególnych wewnętrznych kodeksach organów służb wywiadowczych**.

158. **Druga kwestia, na którą należy zwrócić uwagę,** dotyczy faktu, że przepisy z jednej strony odnoszące się do ukierunkowanego pozyskiwania i zatrzymywania danych komunikacyjnych, a z drugiej strony do masowego gromadzenia danych, które zawarto w ustawie o uprawnieniach dochodzeniowo-śledczych z 2016 r. lub w innych aktach prawnych, takich jak ustawa o służbach wywiadowczych z 1994 r. lub ustawa regulująca uprawnienia dochodzeniowo-śledcze z 2000 r. (dalej ustawa „RIPA"), będą miały zastosowanie również do danych przekazywanych z UE do Zjednoczonego Królestwa. Jeśli chodzi o masowe gromadzenie danych, EROD podkreśla, że odpowiednie przepisy prawa Zjednoczonego Królestwa pozwalają na gromadzenie danych poza Zjednoczonym Królestwem; co może obejmować dane przekazywane z EOG do Zjednoczonego Królestwa na podstawie decyzji stwierdzającej odpowiedni stopień ochrony[97]. Ponadto EROD zauważa, że Komisja Europejska wskazuje, iż „należy zauważyć, że zatrzymywanie i pozyskiwanie danych komunikacyjnych zwykle nie dotyczy danych osobowych osób z UE przekazywanych na podstawie niniejszej decyzji do Zjednoczonego Królestwa. Obowiązek zatrzymania lub ujawnienia danych komunikacyjnych wynikający z części 3 i 4 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. obejmuje dane gromadzone przez operatorów telekomunikacyjnych w Zjednoczonym Królestwie bezpośrednio od użytkowników usługi telekomunikacyjnej"[98]. Niemniej jednak EROD podkreśla brak jasności w kwestii faktu, że tylko jednostki organizacyjne tych operatorów znajdujące się w Zjednoczonym Królestwie mogą otrzymywać wnioski od właściwych organów Zjednoczonego Królestwa, ponieważ definicja operatora telekomunikacyjnego zawarta w art. 261 ust.10 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. wymaga, aby „operatorem telekomunikacyjnym była osoba, która oferuje lub świadczy usługi telekomunikacyjne osobom w Zjednoczonym Królestwie lub która kontroluje lub zapewnia system telekomunikacyjny, który (w całości lub częściowo) znajduje się w Zjednoczonym Królestwie lub jest kontrolowany ze Zjednoczonego Królestwa". W związku z tym mogłoby to w rezultacie dotyczyć danych osobowych osób, których dane dotyczą, z EOG, na przykład w przypadku danych gromadzonych lub wytwarzanych przez jednostkę organizacyjną operatora telekomunikacyjnego ze Zjednoczonego Królestwa znajdującą się na terenie EOG, przekazywanych do jednostki organizacyjnej tego samego operatora znajdującej się w Zjednoczonym Królestwie na

[96] Zob. Europejski Trybunał Praw Człowieka, Big Brother Watch i in./Zjednoczone Królestwo, z dnia 13 września 2018 r., ECLI:CE:ECHR:2018:0913JUD005817013 (dalej „Big Brother Watch"), pkt 325: „Ponieważ Kodeks praktyk dotyczących przechwytywania komunikacji jest dokumentem publicznym, podlegającym zatwierdzeniu przez obie izby parlamentu, i musi być brany pod uwagę zarówno przez osoby wykonujące obowiązki w zakresie przechwytywania, jak i przez sądy i trybunały, Trybunał jednoznacznie przyjął, że przepisy w nim zawarte mogą być brane pod uwagę przy ocenie przewidywalności systemu określonego w ustawie regulującej uprawnienia dochodzeniowo-śledcze (ustawa RIPA)".

[97] Zob. pkt 183 i następne wyroku Schrems II dotyczące oceny prawodawstwa przewidującego dostęp do danych, które są „w tranzycie" między UE a państwem trzecim, w kontekście decyzji stwierdzającej odpowiedni stopień ochrony.

[98] Zob. motyw 196 projektu decyzji.

podstawie decyzji stwierdzającej odpowiedni stopień ochrony (w celach handlowych), a następnie gromadzonych, na terenie Zjednoczonego Królestwa, przez właściwe organy publiczne.

159. **EROD jest zatem zdania, że ocena tych przepisów ma również znaczenie dla oceny odpowiedniego stopnia ochrony zapewnianego w ramach prawnych Zjednoczonego Królestwa, i wzywa Komisję Europejską do wyjaśnienia tego aspektu oraz do dokonania dalszej oceny skali tego zjawiska. W szczególności EROD wzywa Komisję Europejską do wyjaśnienia, jak rozumie zakres tych przepisów, w tym co obejmuje pojęcie „użytkowników usług telekomunikacyjnych" oraz czy możliwe jest żądanie danych od jednostek organizacyjnych operatorów telekomunikacyjnych poza Zjednoczonym Królestwem w zakresie, w jakim dotyczą one danych osób z EOG, biorąc pod uwagę bardzo szeroką definicję operatorów telekomunikacyjnych.**

160. **Trzecia kwestia, na którą należy zwrócić uwagę**, dotyczy procedury „podwójnego zabezpieczenia". EROD zauważa, że w ustawie o uprawnieniach dochodzeniowo-śledczych z 2016 r. wprowadzono nową procedurę „podwójnego zabezpieczenia". Niemniej jednak EROD uważa również, że nawet jeśli co do zasady gromadzenie lub dostęp do danych na potrzeby bezpieczeństwa narodowego lub działań wywiadowczych może odbywać się wyłącznie na podstawie nakazu zatwierdzonego przez komisarza sądowego, ustawa o uprawnieniach dochodzeniowo-śledczych z 2016 r. przewiduje, że „w konkretnych ograniczonych przypadkach możliwe jest zgodne z prawem przechwytywanie bez nakazu i konieczne jest jedynie uprzednie upoważnienie samych właściwych organów służb wywiadowczych [zob. podsekcja dotycząca nadzoru], w tym w przypadku przechwytywania na podstawie wniosków zagranicznych (art. 52 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.)". Jak podkreślono poniżej, zbiega się to również z obawami EROD dotyczącymi, w szczególności, ujawniania informacji za granicą. Ponadto EROD zauważa również, że także w przypadku ingerencji w urządzenia w celu pozyskania danych, czy to ingerencji ukierunkowanej, czy masowej, możliwe jest odstępstwo od procedury podwójnego zabezpieczenia oraz że komisarz sądowy jest uprawniony do zatwierdzania jedynie odnowienia nakazów masowych, po okresie początkowym wynoszącym maksymalnie 6 miesięcy. **EROD wzywa Komisję Europejską do dalszej oceny i wykazania, że — nawet w przypadkach, w których procedura podwójnego zabezpieczenia nie ma zastosowania — ramy prawne Zjednoczonego Królestwa przewidują odpowiednie zabezpieczenia, w tym dzięki skutecznemu nadzorowi *ex post* i możliwościom dochodzenia roszczeń dostępnym dla osób fizycznych, które zapewniają, aby gwarantowany stopień ochrony był merytorycznie równoważny stopniowi gwarantowanemu w UE (zob. również podsekcja 4.3.3 dotycząca nadzoru.**

161. Ponadto chociaż w ustawie o uprawnieniach dochodzeniowo-śledczych z 2016 r. rzeczywiście wprowadzono procedurę „podwójnego zabezpieczenia", EROD nadal wyraża zaniepokojenie niektórymi elementami nowych przepisów. Po przedstawieniu odpowiednich sekcji projektu decyzji EROD przeanalizowała następujące rodzaje gromadzenia i dostępu do danych w tej samej kolejności, w jakiej przedstawiła je Komisja Europejska. W związku z tym kolejność elementów ocenionych w dalszej części niniejszego dokumentu nie ma związku ze stopniem zainteresowania ze strony EROD.

4.3.1.2. Ukierunkowane pozyskiwanie i zatrzymywanie danych komunikacyjnych

162. EROD odnotowuje, że ukierunkowane upoważnienia do pozyskiwania danych komunikacyjnych mogą wydawać dwaj urzędnicy: urzędnik zatwierdzający w biurze ds. upoważnień dotyczących danych komunikacyjnych (ang. Office for Communications Data Authorisations), wyznaczony urzędnik wyższego szczebla (osoba zajmująca określone stanowisko lub posiadająca określoną rangę w odpowiednim organie publicznym), poza zatwierdzeniem przez komisarza sądowego w określonych przypadkach. EROD nadal nie ma jednak jasności, który dokładnie urzędnik, w świetle

prawa i odpowiedniego kodeksu, upoważnia do jakiego rodzaju ukierunkowanego pozyskiwania danych komunikacyjnych, oraz w jakim stopniu wyznaczony urzędnik byłby wystarczająco niezależny[99].

163. **W związku z tym EROD wzywa Komisję Europejską do dalszej oceny tego aspektu i przedstawienia dokładniejszych wyjaśnień na temat tych elementów.**

164. Jeżeli chodzi o wezwanie do zatrzymania danych komunikacyjnych, EROD zauważa również, że takie wezwania mogą być kierowane do „operatorów zgodnych z opisem". Pojęcie to wydaje się oznaczać, że do zatrzymania danych można jednocześnie wezwać kilku operatorów. Ukierunkowany charakter pozyskania nie odnosi się zatem do liczby operatorów, ale do nazwiska lub opisu osób, organizacji, miejsca lub grupy osób stanowiących „cel", opisu charakteru dochodzenia oraz opisu działań, do których wykorzystywany jest sprzęt. EROD podkreśla zatem, że w zależności od liczby operatorów, którzy „są zgodni z opisem", wezwanie może mieć szerszy zakres niż mogłoby to wynikać z procedury ukierunkowanego zatrzymywania. **EROD zwraca się do Komisji Europejskiej o przeprowadzenie dalszej oceny tego aspektu oraz do dodatkowego zagwarantowania, że nawet jeśli wezwania będą kierowane do szeregu operatorów, pozostaną one ograniczone do tego, co jest ściśle konieczne i proporcjonalne.**

4.3.1.3. Ingerencja w urządzenia

165. EROD zauważa, że jeżeli sprawa ma charakter pilny, dokonując „ingerencji w urządzenia" (ang. equipment interference) można odstąpić od procedury podwójnego zabezpieczenia[100]. EROD jest zatem zaniepokojona faktem, że cele, które mogą wymagać takiej ingerencji w urządzenia, mają charakter ogólny, a kryteria określające pilny charakter sprawy (gdy komisarz sądowy nie jest zobowiązany do wydania upoważnienia *ex ante* po dokonaniu oceny konieczności i proporcjonalności ingerencji w urządzenia) pozostają niejasne. Ponieważ w tym drugim przypadku „nakaz traci moc i nie można go odnowić" jeżeli komisarz sądowy nie zatwierdzi *ex post* ingerencji w urządzenia, EROD uznaje, że dane zgromadzone do tego momentu pozostają zgromadzone zgodnie z prawem. Usunięcie tych danych wymaga wydania przez komisarza sądowego specjalnego zarządzenia[101].

166. **EROD wzywa Komisję Europejską do dalszej oceny warunków, na podstawie których można powołać się na pilny charakter sprawy, oraz do przedstawienia wyjaśnień dotyczących możliwych sposobów wykonywania praw przez zainteresowane osoby, których dane dotyczą, oraz ewentualnych możliwości dochodzenia roszczeń oferowanych im w kontekście działań związanych z ingerencją w urządzenia, zwłaszcza jeżeli będą miały miejsce w sytuacji o charakterze pilnym, prowadzącej do zastosowania odstępstwa od procedury podwójnego zabezpieczenia.**

4.3.1.4. Masowe przechwytywanie danych z przewodów światłowodowych

167. Jak opisano w sprawozdaniu z przeglądu uprawnień dotyczących masowego operowania danymi[102] „masowe przechwytywanie zazwyczaj obejmuje pobieranie wiadomości, gdy przepływają przez określone przewody światłowodowe (łącza komunikacyjne)". W oficjalnej nocie informacyjnej

[99] Zob. również poniższa sekcja dotycząca oceny procedury podwójnego zabezpieczenia i niezależności komisarza sądowego.
[100] Zob. art. 109 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.
[101] Zob. art. 110 ust. 3 lit. b) ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.
[102] Zob. sprawozdanie z przeglądu uprawnień dotyczących masowego operowania danymi sporządzone przez niezależnego kontrolera do spraw ustawodawstwa dotyczącego terroryzmu (Independent Reviewer of Terrorism Legislation), sierpień 2016 r.

dotyczącej ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. opisano „masowe przechwytywanie" jako „proces polegający na pobieraniu dużej liczby wiadomości, a następnie na wybraniu konkretnych wiadomości do przeczytania, przejrzenia lub odsłuchania, gdy jest to konieczne i proporcjonalne". EROD zauważa, że „masowe przechwytywanie" danych w rzeczywistości oznacza gromadzenie danych jeszcze przed jakimkolwiek filtrowaniem przez selektorów (albo przed prostym filtrowaniem, w przypadku monitorowania osób już uznanych za zagrożenie, albo przed filtrowaniem złożonym, w przypadku rozpoznawania nowych zagrożeń i nieznanych wcześniej osób będących obiektem zainteresowania).

168. Pozyskiwanie dużych ilości danych komunikacyjnych stanowiło również jedno z zagadnień zbadanych przez TSUE w sprawie dotyczącej Privacy International, która zakończyła się wyrokiem wielkiej izby ogłoszonym w dniu 6 października 2020 r. (oprócz tego zbadano, czy takie gromadzenie danych odbywało się w kontekście prawa Unii, nawet w celach związanych z bezpieczeństwem narodowym). Ustawa o uprawnieniach dochodzeniowo-śledczych z 2016 r. zastąpiła przepisy, których ten wyrok dotyczył.

169. EROD zauważa, że wraz z wprowadzeniem ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. do prawa Zjednoczonego Królestwa, obowiązek uzyskania nakazu dotyczy obecnie również masowego przechwytywania danych. Procedura wydania tego nakazu wymaga określenia „celów operacyjnych". Wykaz tych celów operacyjnych ustalają szefowie służb wywiadowczych, a następnie zatwierdza go sekretarz stanu. Decyzję w tej sprawie zatwierdza niezależny komisarz sądowy, który musi sprawdzić, czy nakaz jest konieczny i proporcjonalny w stosunku do celów operacyjnych. EROD wnioskuje, że komisarz sądowy nie posiada uprawnień do oceny samych celów operacyjnych, lecz do określenia, czy nakaz jest konieczny i proporcjonalny do celów operacyjnych wymienionych w nakazie. Komisja parlamentarna ds. wywiadu i bezpieczeństwa co trzy miesiące otrzymuje kopię wykazu, a premier co najmniej raz w roku dokonuje przeglądu wykazu tych celów operacyjnych.

170. Trudno jest jednak ocenić na podstawie informacji przedstawionych w projekcie decyzji przez Komisję Europejską, jaki jest zakres celów operacyjnych wymienionych w wykazie i czy gromadzenie danych, które umożliwiają, jest zgodne z progiem określonym przez TSUE (np. ograniczenie gromadzenia danych do obszaru geograficznego może dotyczyć zarówno obszaru obejmującego kilka ulic, jak również może oznaczać gromadzenie danych z całego EOG).

171. Ponadto EROD wskazuje, że dane gromadzone na masową skalę mogą być zatrzymywane przez długi czas (aby można było je poddawać dalszej analizie). EROD zauważa, że art. 150 ust. 5 i 6 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. przewiduje tylko zniszczenie kopii zgromadzonych danych i tylko wtedy, gdy ich zatrzymanie nie jest konieczne z punktu widzenia interesów bezpieczeństwa narodowego lub prawdopodobnie nie stanie się konieczne z punktu widzenia interesów bezpieczeństwa narodowego lub z innych powodów objętych zakresem art. 138 ust. 2 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r., lub gdy zatrzymanie nie jest konieczne do szeregu innych celów[103]. EROD podkreśla, że powody te wydają się bardzo szerokie, a niezależnie od sytuacji odniesiono się tylko do kopii pozyskanych danych.

172. Ponadto EROD zauważa również, że w sprawach pilnych ustawa o uprawnieniach dochodzeniowo-śledczych z 2016 r. dopuszcza również wprowadzanie zmian w nakazach bez uprzedniej zgody komisarza sądowego oraz że w takim przypadku, jeżeli komisarz sądowy, z którym skonsultowano się *ex post* w ciągu trzech dni roboczych po wprowadzeniu takiej zmiany, odmówi zatwierdzenia zmiany, nakaz powinien obowiązywać w takiej formie, jakby zmiana nie miała miejsca, ale dane zgromadzone

[103] Zob. art. 150 ust. 3 i 6 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.

do tego momentu pozostają zgromadzone zgodnie z prawem[104]. Usunięcie tych danych wymaga wydania przez komisarza sądowego specjalnego zarządzenia[105].

173. **EROD wzywa zatem Komisję Europejską do złożenia dodatkowych wyjaśnień i przeprowadzenia oceny masowego przechwytywania danych, w szczególności w odniesieniu do wyboru i stosowania selektorów (kryteriów wyszukiwania) w kontekście tych procedur masowego przechwytywania danych, w celu wyjaśnienia zakresu, w jakim dostęp do danych osobowych spełnia wymagania progowe określone przez TSUE (zob. również poniższa sekcja 4.3.1.7, a w szczególności nadzór nad selektorami), oraz jakie zabezpieczenia są stosowane w celu ochrony praw podstawowych osób fizycznych, których dane są przechwytywane w tym kontekście, w tym w odniesieniu do okresów zatrzymywania danych. Szczególnie przydatna byłaby niezależna ocena ze strony właściwych organów nadzorczych Zjednoczonego Królestwa.**

174. **EROD podkreśla również, że tym istotniejszy wydaje się fakt, że „łączność międzynarodowa", która wchodzi w zakres praktyk masowego przechwytywania, wydaje się oznaczać, że dane mogłyby być bezpośrednio przechwytywane i gromadzone masowo w EOG przez Zjednoczone Królestwo, w tym w odniesieniu do danych przekazywanych między EOG a Zjednoczonym Królestwem, które wchodziłyby w zakres projektu decyzji (zob. poniżej sekcja 4.3.2 dotycząca dalszego wykorzystywania informacji zgromadzonych na potrzeby bezpieczeństwa narodowego oraz ujawniania informacji za granicą).**

4.3.1.5. Ochrona i zabezpieczenia dotyczące danych wtórnych

175. EROD jest również zaniepokojona faktem, że odpowiednie przepisy Zjednoczonego Królestwa związane z masowym przechwytywaniem nie zapewniają takiego samego stopnia ochrony wszystkim danym komunikacyjnym. „Dane wtórne", które można uzyskać za pomocą nakazu masowego, to zgodnie z art. 137 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. zarówno „dane systemowe", „które stanowią część wiadomości, są w niej zawarte, są do niej dołączone lub są z nią w logiczny sposób powiązane (niezależnie od tego, czy przez nadawcę, czy w inny sposób)", jak i „dane identyfikujące", „które stanowią część wiadomości, są w niej zawarte, są do niej dołączone lub są z nią w logiczny sposób powiązane (niezależnie od tego, czy przez nadawcę, czy w inny sposób), można je logicznie oddzielić od pozostałej części wiadomości, i w przypadku takiego oddzielenia nie ujawniłyby niczego, co można by racjonalnie uznać za znaczenie wiadomości (jeśli takie istnieje), z pominięciem wszelkiego znaczenia wynikającego z faktu komunikowania się lub z jakichkolwiek danych dotyczących przekazywania wiadomości"[106].

176. EROD zauważa, że te „dane wtórne", znane również jako „metadane"[107], gromadzone masowo, wydają się nie korzystać z takich samych zabezpieczeń co dane gromadzone na podstawie ukierunkowanego nakazu, ale również z takich zabezpieczeń, które chronią dane dotyczące treści

[104] Zob. art. 147 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. (część 6, rozdział I).
[105] Zob. art. 181 ust. 3 lit. b) ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.
[106] „Dane systemowe" i „dane identyfikujące" zdefiniowane w art. 263 ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.
[107] Zob. sprawozdanie z przeglądu uprawnień dotyczących masowego operowania danymi sporządzone przez niezależnego kontrolera do spraw ustawodawstwa dotyczącego terroryzmu (Independent Reviewer of Terrorism Legislation), sierpień 2016 r.
[108] Zob. art. 152 ust. 1 lit. c) oraz art. 152 ust. 3 i nast. ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.

gromadzone masowo. EROD zauważa wręcz, że wybór jakiejkolwiek przechwyconej treści jest objęty większą liczbą zabezpieczeń[108] niż wybór danych wtórnych[109].

177. EROD podkreśla również, że zarówno Europejski Trybunał Praw Człowieka[110], jak i TSUE[111] zakwestionowały pogląd, że takie dane są mniej wrażliwe niż inne, a w szczególności niż dane dotyczące treści. W kodeksie postępowania dotyczącym przechwytywania danych przedstawiono jako przykłady „danych wtórnych" zarówno „dane systemowe", takie jak konfiguracje routerów, adresy e-mail czy identyfikatory użytkowników; ale również identyfikatory kont alternatywnych, jak również „dane identyfikujące", takie jak lokalizacja spotkania zapisana w kalendarzu, informacje dotyczące zdjęcia, takie jak godzina, data i miejsce, w którym je zrobiono. **EROD podkreśla zatem spójną ocenę Europejskiego Trybunału Praw Człowieka i TSUE oraz przypomina obawy wyrażone w odniesieniu do danych wtórnych, które powinny stanowić przedmiot szczególnych zabezpieczeń ze względu na ich wrażliwość. EROD wzywa zatem Komisję Europejską do starannej oceny, czy zabezpieczenia przewidziane w prawie Zjednoczonego Królestwa dla tej kategorii danych osobowych zapewniają stopień ochrony merytorycznie równoważny stopniowi gwarantowanemu w UE.**

4.3.1.6 Automatyczne przetwarzanie danych komunikacyjnych

178. EROD zauważa, że organy służb wywiadowczych korzystają nie tylko z prostych lub złożonych selektorów do filtrowania danych uzyskanych masowo, lecz mogą również polegać na innych narzędziach do zautomatyzowanego przetwarzania danych do analizy „dużych ilości informacji, co pozwala agencjom na znalezienie również powiązań, wzorców, związków lub zachowań, które mogą wskazywać na poważne zagrożenie wymagające dochodzenia", według sprawozdania Komisji ds. wywiadu i bezpieczeństwa (Intelligence and Security Committee) z 2015 r.[112]. **EROD jest świadoma**

[108] Zob. art. 152 ust. 1 lit. c) oraz art. 152 ust. 3 i nast. ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.

[109] Zob. art. 152 ust. 1 lit. a) i b) ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r.

[110] Zob. Europejski Trybunał Praw Człowieka, Big Brother Watch, pkt 357, w sekcji dotyczącej przedłożenia sprawy wielkiej izbie. „W związku z tym, chociaż Trybunał nie ma wątpliwości, że powiązane dane komunikacyjne stanowią istotne narzędzie służb wywiadowczych w walce z terroryzmem i poważną przestępczością, nie uważa, aby władze zachowały sprawiedliwą równowagę między konkurującymi interesami publicznymi i prywatnymi, w całości wyłączając te dane z zabezpieczeń mających zastosowanie do przeszukiwania i badania treści. Chociaż Trybunał nie sugeruje, że powiązane dane komunikacyjne powinny być dostępne wyłącznie w celu ustalenia, czy dana osoba fizyczna przebywa na Wyspach Brytyjskich, ponieważ takie rozwiązanie wymagałoby zastosowania względem powiązanych danych komunikacyjnych bardziej rygorystycznych standardów niż te, które mają zastosowanie do treści, to jednak powinny istnieć zabezpieczenia wystarczające do zagwarantowania, że wyłączenie powiązanych danych komunikacyjnych z wymogów art. 16 ustawy RIPA jest ograniczone do zakresu niezbędnego do ustalenia, czy dana osoba fizyczna przebywa w danym momencie na Wyspach Brytyjskich".

[111] Zob. TSUE, Privacy International, pkt 71: „Ingerencję w prawo ustanowione w art. 7 karty, jaką stanowi transmitowanie danych o ruchu i danych o lokalizacji służbom wywiadu i bezpieczeństwa, należy uważać za szczególnie poważną, biorąc pod uwagę między innymi okoliczność, że z danych tych mogą wynikać informacje szczególnie chronione, a zwłaszcza możliwość sporządzenia na ich podstawie profilu osób, których dane dotyczą, zaś taka informacja jest w tym samym stopniu szczególnie chroniona jak sama treść komunikacji. Ponadto może ona wywoływać u osób, których dane dotyczą, wrażenie, że ich prywatne życie podlega ciągłej obserwacji (zob. analogicznie wyroki: z dnia 8 kwietnia 2014 r., Digital Rights Ireland i in., C-293/12 i C-594/12, EU:C:2014:238, pkt 27, 37; a także z dnia 21 grudnia 2016 r., Tele2, C-203/15 i C-698/15, EU:C:2016:970, pkt 99, 100)."

[112] Zob. Komisja parlamentarna ds. wywiadu i bezpieczeństwa, Prywatność i bezpieczeństwo: nowoczesne i przejrzyste ramy prawne, 2015, pkt 18, s. 13, https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf.

faktu, że to publiczne sprawozdanie odnosi się do praktyk stosowanych w poprzednich ramach prawnych, które zostały następnie zastąpione przez ustawę o uprawnieniach dochodzeniowo-śledczych z 2016 r. Dostrzega jednak potrzebę dalszej niezależnej oceny i nadzoru nad stosowaniem narzędzi do zautomatyzowanego przetwarzania danych przez właściwe organy nadzoru Zjednoczonego Królestwa i wzywa Komisję Europejską do dalszej oceny tej kwestii oraz zabezpieczeń, jakie w tym kontekście zostałyby lub mogłyby zostać zapewnione osobom z EOG, których dane dotyczą.

4.3.1.7 Ryzyko braku zgodności i niezgodne z przepisami praktyki właściwych organów służb wywiadowczych

179. EROD zauważa, że dostępne są szczegółowe sprawozdania z nadzoru. Zawierają one cenne elementy dotyczące praktyk, które ocenia jako pozytywne praktyki w zakresie zgodności, oraz dotyczące stwierdzonych rodzajów ryzyka braku zgodności i praktyk niezgodnych z przepisami.

180. W tym względzie, zgodnie ze sprawozdaniem Komisarza ds. uprawnień dochodzeniowo-śledczych za 2019 r., szereg elementów dotyczących stosowania ram prawnych przez poszczególne właściwe organy ujawniło pewne (ryzyko) niezgodności z przepisami działań właściwych organów.

181. Po pierwsze, EROD zauważyła, że wydaje się, iż kryteria klasyfikacji zbioru danych jako masowy zbiór danych osobowych lub jako dane ukierunkowane nie zawsze są jasne dla samych MI5 (Służba Bezpieczeństwa Zjednoczonego Królestwa) i SIS, w szczególności dla MI5, co może prowadzić do braku stosowania wobec tych danych odpowiednich zabezpieczeń[113]. W sprawozdaniu z 2019 r. Komisarz ds. uprawnień dochodzeniowo-śledczych zasugerował, że „rozwiązanie tej kwestii powinno stanowić priorytet”[114]. W odniesieniu do masowych zbiorów danych EROD odnotowuje również, że choć klasyfikacja masowych zbiorów danych osobowych wydaje się satysfakcjonować GCHQ (ale ma jeszcze zostać objęta audytem Komisarza ds. uprawnień dochodzeniowo-śledczych), w marcu 2019 r. przegląd nakazów przeprowadzony przez specjalny zespół w ramach wewnętrznej kontroli zgodności wzbudził poważne zaniepokojenie, gdyż ponad 50% uzasadnień nakazów pozyskiwania danych masowych badanych przez zespół ds. zgodności GCHQ nie spełniało wymaganego standardu. Według Komisarza ds. uprawnień dochodzeniowo-śledczych zespół ds. zgodności podjął pracę nad zbadaniem tego problemu i ponownym przeszkoleniem personelu, aby poprawić zakres spełniania wymaganego standardu. Szkolenie przypominające dotyczące przepisów ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. oraz dodatkowe szkolenie przeprowadzone w ramach sieci ds. polityki i zgodności doprowadziły do poprawy zgodności GCHQ z przepisami w tym obszarze. Komisarz ds. uprawnień dochodzeniowo-śledczych nie oczekuje pogorszenia w zakresie spełniania

[113]Zob. Roczne sprawozdanie Komisarza ds. uprawnień dochodzeniowo-śledczych z 2019 r., 15 grudnia 2020, pkt 8.39, https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf: „Zaobserwowaliśmy pozytywny rozwój [panelu nadzoru nad danymi masowymi] i odnotowujemy jego wpływ w zakresie zarządzania wewnętrzną zgodnością z przepisami. Nadal dążymy do większej jasności procesów stosowanych przez MI5 do przeprowadzania wstępnego badania nowych zbiorów danych, aby lepiej rozumieć decyzje w sprawie klasyfikacji zbioru danych jako masowego zbioru danych osobowych lub na przykład jako danych ukierunkowanych. Nasze zastrzeżenia wzbudziło jedno nierozwiązane działanie, ujęte w protokole panelu nadzoru nad danymi masowymi, dotyczące usunięcia rozbieżności między podziałem masowych danych osobowych między MI5 a SIS. Ze względu na różne wykorzystanie danych oraz różne wycinki przechowywanych danych byłoby możliwe, aby obie agencje przechowywały ten sam zbiór danych, lub jego wersje, i mógłby on zgodnie z prawem zostać zaklasyfikowany przez jedną z nich jako »dane masowe«, a przez drugą jako »dane ukierunkowane«. Istnieje ryzyko, że jeżeli jedna z agencji nieprawidłowo zaklasyfikuje przechowywane dane jako »ukierunkowane«, dane te będą przechowywane bez odpowiedniego nakazu i mogą nie podlegać odpowiednim zabezpieczeniom.”

[114] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 8.39.

tego standardu przy przyszłych kontrolach, lecz będzie nadal ściśle monitorować ten obszar[115]. **W związku z tym EROD podziela pogląd, że potrzebne są dalsze przeglądy i monitorowanie wspomnianych elementów przez Komisję Europejską w ramach oceny stopnia ochrony, aby zapewnić podwyższenie tego standardu, jak podkreślono w sprawozdaniu Komisarza ds. uprawnień dochodzeniowo-śledczych, i przypomina, że przy ocenie zasadniczej odpowiedniości państwa trzeciego uwzględniane będzie także wdrożenie i konkretne stosowanie ram prawnych, jak przewidziano w art. 45 RODO.**

182. -Ogólnie rzecz ujmując, EROD podkreśla kwestie zasługujące na uwagę opisane przez Komisarza ds. uprawnień dochodzeniowo-śledczych dotyczące „wyszukiwań opartych na zadaniach" przeprowadzanych przez oficerów MI5 – które pozwalają osobie prowadzącej dochodzenie na przeprowadzenie większej liczby wyszukiwań w ramach udostępnionych jej masowych zbiorów danych osobowych, oraz „poważnego ryzyka braku zgodności związanego z pewnymi środowiskami technologicznymi, z których korzysta MI5", w odniesieniu do miejsca przechowywania danych w tym środowisku, osób mających do nich dostęp, zakresu ich kopiowania lub udostępniania, stosowanych wobec nich procesów usuwania oraz okresów zatrzymywania. Chociaż Komisarz ds. uprawnień dochodzeniowo-śledczych wskazuje, że podjęto działania i wprowadzono zabezpieczenia, niektóre z nich są nadal ręczne i wprowadzane indywidualnie przez człowieka, podkreśla on, że kluczowe jest, aby „MI5 nadal utrzymywała te nowe procesy i zapewniało dostateczne zasoby na ich skuteczne funkcjonowanie. Jeżeli MI5 zidentyfikuje zwiększenie liczby zachowań niezgodnych z przepisami[116]". Komisarz ds. uprawnień dochodzeniowo-śledczych oczekuje jak najszybszego zwrócenia mu uwagi na takie zachowania. **EROD wzywa zatem Komisję Europejską do ścisłego monitorowania w przyszłości tych aspektów**.

183. W kwestii GCHQ EROD również wnosi ze sprawozdania Komisarza ds. uprawnień dochodzeniowo-śledczych, że w przypadku operacji prowadzonych w ramach nakazów dotyczących danych masowych „jakość wniosków o zatwierdzenie wewnętrzne była różna i zaobserwowaliśmy, że istnieje możliwość udoskonalenia układu tych wniosków"[117] oraz że w przypadku ukierunkowanej ingerencji w urządzenia w celu pozyskiwania danych uzasadnienia dotyczące stosowania ogólnych deskryptorów były niekiedy zbyt ogólne i nieprecyzyjne[118]. EROD zauważyła też, że w kontekście masowej ingerencji w urządzenia Komisarz ds. uprawnień dochodzeniowo-śledczych zaleca, aby „aplikacje konsekwentnie i wyraźnie rejestrowały związek między celem a celem ustawowym oraz wymogami wywiadowczymi"[119], aby „wszystkie aplikacje powinny wyraźnie uwzględniać możliwość nieintencjonalnego naruszenia prywatności osób trzecich przy zbieraniu materiału dowodowego oraz odnośne środki ograniczające ten potencjał w ramach oceny proporcjonalności"[120], a Komisarz ds. uprawnień dochodzeniowo-śledczych podkreślił, że mimo postępu „nadal istnieje możliwość poprawy w tym zakresie"[121], a w przyszłości będzie również konieczne poświęcenie dalszej uwagi tej kwestii.

184. W związku z systemem przechwytywania danych masowych na mocy ustawy regulującej uprawnienia dochodzeniowo-śledcze z 2000 r. (dalej „ustawa RIPA 2000"), która została od tego czasu zastąpiona przepisami ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r., EROD

[115] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.48.
[116] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 8.52.
[117] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.2.
[118] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.16 i 10.17.
[119] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.23.
[120] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.23.
[121] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.23.

przypomina, że niedostateczny nadzór, zarówno nad wyborem nośników internetowych na potrzeby wychwytywania i filtrowania, wyszukiwaniem i selekcją przechwyconych komunikatów w celu ich zbadania, był jednym z kluczowych aspektów uznanych przez Europejski Trybunał Praw Człowieka za niezgodne z art. 8 EKPC w związku z poprzednimi przepisami o uprawnieniach dochodzeniowo-śledczych władz Zjednoczonego Królestwa w kontekście bezpieczeństwa narodowego w sprawie Big Brother Watch, obecnie przekazanej do wielkiej izby. **EROD zachęca Komisję Europejską do sprawdzenia stanu postępowania, do uwzględnienia tych elementów, oraz do wyszczególnienia ich w decyzji stwierdzającej odpowiedni stopień ochrony, jeżeli Komisja Europejska podejmie taką decyzję.**

185. W tym przypadku Europejski Trybunał Praw Człowieka: „Nie był przekonany, że zabezpieczenia regulujące wybór nośników w celu przechwytywania oraz wybór przechwyconego materiału do badania są dostatecznie solidne, aby zapewnić dostateczne gwarancje przeciwko nadużyciom. Największe obawy budzi jednak brak solidnego niezależnego nadzoru nad selektorami oraz kryteriami wyszukiwania stosowanymi do filtrowania przechwyconych komunikatów”[122]. Jak podkreślił Komisarz ds. uprawnień dochodzeniowo-śledczych „ustalenie to było powtórzeniem podobnego zalecenia zawartego w dokumencie komisji ds. wywiadu i bezpieczeństwa pt. „Prywatność i bezpieczeństwo: Nowoczesne i jasne ramy prawne, sprawozdania z marca 2015 r.”[123]. **EROD z zadowoleniem przyjmuje fakt, że w rezultacie Komisarz ds. uprawnień dochodzeniowo-śledczych przeprowadził w 2019 r. przegląd swojego podejścia do kontroli masowego przechwytywania, „który obejmował dokładny przegląd technicznie złożonych sposobów faktycznego wdrażania masowego przechwytywania”[124] i zobowiązał się do włączenia „szczegółowej analizy selektorów i kryteriów wyszukiwania, o których wspomniał powyżej Europejski Trybunał Praw Człowieka”[125] do kontroli przechwytywania masowego począwszy od 2020 r. Uwzględniając znaczenie tego aspektu, EROD wyraża zaniepokojenie faktem, że szczegółowa kontrola selektorów i kryteriów wyszukiwania przez Komisarza ds. uprawnień dochodzeniowo-śledczych nie została jeszcze przeprowadzona i wzywa Komisję Europejską do ścisłego monitorowania rozwoju sytuacji w tym zakresie, zwłaszcza że konkretna forma takiego nadzoru nie została jeszcze określona[126].**

4.3.2 Dalsze wykorzystywanie informacji zgromadzonych na potrzeby bezpieczeństwa narodowego oraz ujawnianie informacji za granicą

186. Jeżeli chodzi o dalsze wykorzystywanie informacji zgromadzonych na potrzeby bezpieczeństwa narodowego, Komisja Europejska w swojej ocenie odnosi się do sekcji 87 ust. 1 ustawy o ochronie danych z 2018 r., która faktycznie przewiduje, że „dane osobowe zgromadzone w ten sposób nie mogą być przetwarzane w sposób niezgodny z celem, w którym zostały zebrane”. EROD wskazuje jednak, że przepis ten może podlegać wyłączeniom dotyczącym bezpieczeństwa narodowego, o których mowa w sekcji 110 ustawy o ochronie danych z 2018 r. EROD zauważa ponadto, że zarówno w przypadku ukierunkowanego przechwytywania i badania, ukierunkowanego pozyskiwania i zatrzymywania danych komunikacyjnych, ukierunkowanej ingerencji w urządzenia lub

[122] Zob. ETPC, *Big Brother Watch*, pkt 347.
[123] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.28.
[124] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.28.
[125] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.28.
[126] Zob. Roczne sprawozdanie Komisarza ds. Uprawnień Dochodzeniowo-Śledczych z 2019 r., pkt 10.28: „dokładna forma tej kontroli musi jeszcze zostać ustalona”.

przechwytywania masowego i masowej ingerencji w urządzenia, prawodawstwo przewiduje możliwość ujawniania informacji za granicą.

4.3.2.1 Dalsze wykorzystywanie, ujawnianie informacji za granicą oraz ramy prawne obowiązujące w Zjednoczonym Królestwie

187. Komisja Europejska wskazała część 4 ustawy o ochronie danych z 2018 r., a w szczególności sekcję 109 tej ustawy, jako istotne przepisy określające szczegółowe wymogi w zakresie dalszego wykorzystywania zgromadzonych informacji, a zwłaszcza międzynarodowego przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym przez służby wywiadowcze. EROD odnotowuje jednak, że w sekcji 110 ustawy o ochronie danych z 2018 r. przewidziano wyłączenie dotyczące bezpieczeństwa narodowe stanowiące, że niektóre przepisy ustawy o ochronie danych z 2018 r. nie mają zastosowania, jeżeli wyłączenie z tych przepisów jest wymagane na potrzeby zabezpieczenia bezpieczeństwa narodowego. Odpowiednie przepisy, które mogą nie mieć zastosowania, obejmują ustawę o ochronie danych z 2018 r., część 4, rozdział 2, w odniesieniu do zasad ochrony danych, w tym ograniczenia celu, a także ustawę o ochronie danych z 2018 r. część 4, rozdział 3 w odniesieniu do praw osoby, której dane dotyczą. Sekcja 109 ustawy o ochronie danych z 2018 r. w związku z sekcją 110 tej ustawy oraz warunki, w których ma ona zastosowanie, może prowadzić do przypadków międzynarodowego przekazywania danych osobowych państwom trzecim przez służby wywiadowcze bez stosowania przepisów dotyczących zasad ochrony danych i praw osób, których dane dotyczą.

188. Jak wskazała Komisja Europejska, wyłączenie takie należy oceniać w każdym konkretnym przypadku i można się na nie powoływać tylko w zakresie, w jakim zastosowanie określonego przepisu powodowałoby negatywne konsekwencje dla bezpieczeństwa narodowego. W istocie wydanie służbom wywiadowczym Zjednoczonego Królestwa certyfikatu krajowego ma na celu poświadczenie, że wymagane jest wyłączenie w odniesieniu do określonych danych osobowych przetwarzanych w celu zabezpieczenia bezpieczeństwa narodowego. EROD zauważa jednak, że w swoich wytycznych dotyczących certyfikatu bezpieczeństwa narodowego na mocy ustawy o ochronie danych z 2018 r. Ministerstwo Spraw Wewnętrznych Zjednoczonego Królestwa wyjaśnia, że „należy zwrócić uwagę na samym początku, że certyfikat nie jest wymagany w celu powołania się na wyłączenie dotyczące bezpieczeństwa narodowego; faktycznie, w większości przypadków, administratorzy sami ustalą, czy wyłączenie dotyczące bezpieczeństwa narodowego ma zastosowanie.” [127] W wytycznych Ministerstwa Spraw Wewnętrznych Zjednoczonego Królestwa zauważa się, że „certyfikaty bezpieczeństwa narodowego mogą mieć zastosowanie do danych osobowych, które można konkretnie wskazać, lub mogą obejmować szerszą kategorię danych osobowych. Certyfikaty mogą być wydawane wcześniej jak również retrospektywnie.”[128] Wyłączenie dotyczące bezpieczeństwa narodowego może zatem mieć zastosowanie w odniesieniu do międzynarodowego przekazywania danych osobowych przez służby wywiadowcze do państw trzecich przy braku certyfikatu bezpieczeństwa narodowego.

189. EROD odnotowuje ponadto, że w certyfikacie bezpieczeństwa narodowego DPA/S27/Security Service[129] przewidziano, że do 24 lipca 2024 r. dane osobowe przetwarzane „dla, w imieniu, na

[127] Zob. Ministerstwo Spraw Wewnętrznych (Home Office), ustawa o ochronie danych z 2018 r., wytyczne dotyczące certyfikatów bezpieczeństwa narodowego, sierpień 2020 r., s. 3 pkt 3.
[128] Zob. Ministerstwo Spraw Wewnętrznych (Home Office), ustawa o ochronie danych z 2018 r., wytyczne dotyczące certyfikatów bezpieczeństwa narodowego, sierpień 2020 r., s. 5 pkt 4.
[129] Zob. DPA/S27/Security Service, sekcja 27 ustawy o ochronie danych z 2018 r., Certyfikat sekretarza stanu, 24 lipca 2019 r., https://ico.org.uk/media/about-the-ico/documents/nscs/2615660/nsc-part-2-mi5-201908.pdf.

wniosek lub z pomocą Służby Bezpieczeństwa (Security Service)" lub „oraz gdy przetwarzanie takie jest niezbędne w celu ułatwienia należytego wypełnienia funkcji Służby Bezpieczeństwa, opisanych w sekcji 1 ustawy o Służbie Bezpieczeństwa z 1989 r." wyłączone są z przepisów prawa Zjednoczonego Królestwa odpowiadających rozdziałowi V RODO w zakresie przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym. Inne ogólnodostępne certyfikaty bezpieczeństwa narodowego nie przewidują wyłączenia z przepisów sekcji 109 ustawy o ochronie danych z 2018 r., należy jednak przypomnieć, że publikacja całości lub części tekstu certyfikatu bezpieczeństwa narodowego może zostać wstrzymana, jeśli jego publikacja byłaby wbrew interesom bezpieczeństwa narodowego, sprzeczna z interesem publicznym lub mogłaby zagrozić bezpieczeństwu jakiejkolwiek osoby.

190. Ogólnie rzecz biorąc, przy ocenie projektu decyzji w odniesieniu do tych przepisów EROD stwierdza, że zabezpieczenia w zakresie tych ujawnień obejmują jedynie wymóg, aby odbiorca danych przestrzegał wymogów dotyczących bezpieczeństwa danych, ograniczenia zakresu ujawnienia do tego, co niezbędne, zatrzymywania danych oraz ograniczenia dostępu do nich do ograniczonej liczby osób. **EROD podkreśla zatem, że w przypadku ujawniania informacji za granicą zastosowanie wyłączenia dotyczącego bezpieczeństwa narodowego przewidzianego w prawie Zjednoczonego Królestwa może prowadzić do sytuacji, w których zabezpieczenia gwarantujące przestrzeganie zasady ograniczenia celu, konieczności i proporcjonalności lub przewidujące przestrzeganie praw osób fizycznych, nadzór i możliwość dochodzenia roszczeń nie będą w pełni zapewnione lub przestrzegane w docelowym państwie trzecim. EROD zaleca zatem, aby Komisja Europejska dokładniej zbadała ogólne zabezpieczenia przewidziane w prawie Zjednoczonego Królestwa w odniesieniu do ujawniania informacji za granicą, w szczególności w świetle stosowania wyłączeń dotyczących bezpieczeństwa narodowego.**

4.3.2.2 Ujawnianie danych za granicą i udostępnianie danych wywiadowczych w ramach współpracy międzynarodowej

191. EROD odnotowuje również, że Komisja Europejska nie uwzględniła w ramach swojej oceny odpowiedniego stopnia ochrony danych istniejących umów międzynarodowych zawartych między Zjednoczonym Królestwem a państwami trzecimi lub organizacjami międzynarodowymi, które mogą określać przepisy szczegółowe lub dotyczące międzynarodowego przekazywania danych osobowych państwom trzecim przez służby wywiadowcze.

192. EROD podkreśla również, że ocena Komisji Europejskiej opiera się głównie na ocenie części 4 ustawy o ochronie danych z 2018 r., i jest zaniepokojona zwłaszcza tym, że ustawa o uprawnieniach dochodzeniowo-śledczych z 2016 r. koncentruje się na „wnioskach" w sprawie wymiany danych wywiadowczych z partnerami zagranicznymi, a nie zajmuje się innymi formami wymiany danych wywiadowczych. EROD zauważa w tym względzie, że projekt decyzji Komisji Europejskiej nie odnosi się do połączenia między ramami legislacyjnymi Zjednoczonego Królestwa a „umową w sprawie wywiadu telekomunikacyjnego między Zjednoczonym Królestwem a USA" (ang. UK-US CI Agreement) ani nie ocenia tego połączenia. W niedawnym oświadczeniu z okazji 75. rocznicy podpisania tej umowy Agencja Bezpieczeństwa Narodowego Stanów Zjednoczonych (dalej „NSA") wspomniała, że partnerstwo to „umożliwia jak najdalej idącą wymianę informacji między agencjami z minimalnymi ograniczeniami" oraz że „ten przełomowy dokument określił polityki i procedury pozwalające specjalistom wywiadu Zjednoczonego Królestwa lub USA na udostępnianie

komunikatów, tłumaczeń, analiz i informacji w zakresie łamania szyfrów”[130]. Umowa ta stała się również fundamentem innego partnerstwa wywiadowczego z Australią, Kanadą i Nową Zelandią.

193. Tajny charakter tej umowy i jej przepisów szczegółowych stanowią poważne wyzwanie w zakresie jasności i przewidywalności prawa w odniesieniu do dalszego wykorzystywania i ujawniania za granicą informacji zgromadzonych przez władze Zjednoczonego Królestwa na potrzeby bezpieczeństwa narodowego. EROD przypomina w tym kontekście, że jeśli chodzi o gwarantowany w Unii stopień ochrony, TSUE podkreślił, że przepisy Unii stanowiące ingerencję w podstawowe prawo do ochrony danych osobowych muszą „zawierać jasne i dokładne reguły dotyczące zakresu i sposobu stosowania rozpatrywanych środków, a także ustanawiać minimalne zabezpieczenia służące temu, aby osoby, których dane osobowe zostają dotknięte ingerencją, miały wystarczające gwarancje rzeczywistej ochrony ich danych przed ryzykiem nadużyć oraz uzyskaniem do nich bezprawnego dostępu i ich wykorzystywaniem. Konieczność zapewnienia takich gwarancji ma znaczenie tym większe, że dane osobowe przetwarzane są automatycznie i istnieje znaczne ryzyko bezprawnego uzyskania dostępu do nich”[131]. EROD uważa zatem, że w ramach oceny odpowiedniego stopnia ochrony danych Komisja Europejska powinna rozważyć wpływ umowy w sprawie wywiadu telekomunikacyjnego między Zjednoczonym Królestwem a USA.

194. W sekcji pierwszej wyroku z dnia 13 września 2018 r. w sprawie Big Brother Watch Europejski Trybunał Praw Człowieka ocenił system udostępniania przez Zjednoczone Królestwo danych wywiadowczych, a w szczególności Umowę o przekazywaniu danych wywiadowczych między Zjednoczonym Królestwem a Stanami Zjednoczonymi. Europejski Trybunał Praw Człowieka istotnie stwierdził, że „ramy ustawowe, które zezwalają służbom wywiadowczym Zjednoczonego Królestwa na zwracanie się do zagranicznych agencji wywiadowczych o przechwycone materiały nie są ujęte w ustawie RIPA. Brytyjsko-amerykańska umowa w sprawie wywiadu telekomunikacyjnego z dnia 5 marca 1946 r. wyraźnie zezwala na wymianę materiałów między Stanami Zjednoczonymi a Zjednoczonym Królestwem”*[132]* i uznał, że „istnieje podstawa prawna regulująca zwracanie się o dane wywiadowcze do zagranicznych agencji wywiadowczych, oraz że prawo to jest dostatecznie dostępne”[133]. Europejski Trybunał Praw Człowieka podsumował, że nie nastąpiło naruszenie art. 8[134] EKPC w odniesieniu do systemu udostępniania danych wywiadowczych, EROD zauważa jednak, że wyrok ten został obecnie przekazany do wielkiej izby i wciąż oczekuje się na jej decyzję w tej sprawie. EROD odnotowuje również, że sędzia Koskelo, do którego dołączyła sędzia Turković[135], wyrażając zdanie częściowo zgodne, a częściowo odrębne dotyczące tego wyroku, podsumowała, że nastąpiło naruszenie art. 8 EKPC w związku z systemem udostępniania danych wywiadowczych, stwierdzając, że „łatwo jest zgodzić się z zasadą, że nie powinno się zezwalać na to, aby jakiekolwiek porozumienie zgodnie z którym otrzymuje się dane wywiadowcze z przechwyconych komunikatów za pośrednictwem zagranicznych służb wywiadowczych, czy to na podstawie wniosków o przeprowadzenie takiego przechwytywania, czy też o przekazanie jego wyników pociągało za sobą

[130]Zob. komunikat prasowy: GCHQ i NSA świętują 75 lat partnerstwa (GCHQ and NSA Celebrate 75 Years of Partnership), 5 lutego 2021 r.,https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2494453/gchq-and-nsa-celebrate-75-years-of-partnership/.

[131] Zob. Schrems I, pkt 91.

[132] Zob. Europejski Trybunał Praw Człowieka, Big Brother Watch, pkt 425.

[133] Zob. Europejski Trybunał Praw Człowieka, Big Brother Watch, pkt 427.

[134] Zob. Europejski Trybunał Praw Człowieka, Big Brother Watch, pkt 448.

[135] Zob. Europejski Trybunał Praw Człowieka, Big Brother Watch, opinia częściowo zgodna, częściowo odrębna sędzi Koskelo, do której dołączyła sędzia Turković.

omijanie zabezpieczeń, które muszą być wprowadzone, aby organy krajowe prowadziły jakikolwiek nadzór (zob. pkt 216, 423 i 447). Wszelkie inne podejście byłoby w istocie nieprzekonywające".

195. Jak podkreślono w kilku doniesieniach mediów i organizacji pozarządowych[136][137], ostatnia wersja umowy w sprawie wywiadu telekomunikacyjnego między Zjednoczonym Królestwem a USA, która została upubliczniona, pochodzi z 1956 r., a od tego czasu technologia komunikacyjna i charakter rozpoznania radioelektronicznego uległy znacznym zmianom. Sprawozdania mediów ujawniły na przykład, że dane przesyłane kablami podmorskimi, które trafiają do Zjednoczonego Królestwa, są przechwytywane przez GCHQ i udostępniane NSA[138].

196. Dla EROD kluczowym pytaniem w odniesieniu do dzielenia się danymi wywiadowczymi jest to, czy sekcja 109 ustawy o ochronie danych z 2018 r. i przepisy ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r. nadal mają zastosowanie, gdy służby wywiadowcze Zjednoczonego Królestwa działają zgodnie z umową w sprawie wywiadu telekomunikacyjnego między Zjednoczonym Królestwem a Stanami Zjednoczonymi. Innym kluczowym elementem podlegającym ocenie jest to, czy przepisy lub skuteczne stosowanie tej umowy wpływają na stopień ochrony danych osobowych w czasie tranzytu z EOG do Zjednoczonego Królestwa lub umożliwiają bezpośredni dostęp i pozyskiwanie danych osobowych przez służby wywiadowcze innych państw trzecich.

197. W efekcie, poza zastrzeżeniami wobec „ujawniania informacji za granicą" na podstawie części 4 ustawy o ochronie danych z 2018 r. i powiązanego z nią wyłączenia dotyczącego bezpieczeństwa narodowego, a także wniosków w ramach ustawy o uprawnieniach dochodzeniowo-śledczych z 2016 r., **EROD wyraża zaniepokojenie innymi formami wymiany i ujawniania informacji na podstawie innych instrumentów, w szczególności poszczególnych umów międzynarodowych zawartych przez Zjednoczone Królestwo z innymi państwami trzecimi, zwłaszcza w przypadkach gdy instrumenty te pozostają niedostępne publicznie, takich jak umowa w sprawie wywiadu telekomunikacyjnego (ang. Communication Intelligence Agreement) między Zjednoczonym Królestwem a Stanami Zjednoczonymi. Skutkiem takiej umowy mogłoby być obejście zabezpieczeń określonych w odniesieniu do dostępu do danych osobowych i wykorzystywanie ich do celów bezpieczeństwa narodowego.**

198. EROD podziela opinię specjalnego sprawozdawcy ONZ, Joego Cannatacciego, że „[u]dostępnianie danych wywiadowczych nie może otwierać furtki do pozyskania danych lub łatwiejszego dostępu do nich bez zastosowania krajowych zabezpieczeń ani powodować luki prawnej, dzięki której rządy państw o niższych standardach ochrony prywatności (lub innych praw człowieka) mogłyby pozyskać dane na podstawie danych wywiadowczych Zjednoczonego Królestwa, co mogłoby skutkować naruszeniem praw człowieka"[139].

---

[136] Zob. BBC, Dziennik ujawnia narodziny tajnego brytyjsko-amerykańskiego paktu szpiegowskiego, który przerodził się w Sojusz Pięciorga Oczu, 5 marca 2021 r. https://www.bbc.com/news/uk-56284453.

[137] Zob. Privacy International, dokument informacyjny - Uzgodnienia Zjednoczonego Królestwa w sprawie wymiany informacji wywiadowczych, kwiecień 2018 r. https://privacyinternational.org/sites/default/files/2018-04/Privacy%20International%20Briefing%20-%20Intelligence%20Sharing%20%28UK%29%20FINAL.pdf.

[138] Zob. The Guardian, GCHQ wykorzystuje kable światłowodowe, aby uzyskać tajny dostęp do światowej komunikacji, 21 czerwca 2013 r. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[139] Zob. deklaracja zakończenia misji specjalnego sprawozdawcy ds. prawa do prywatności w części dotyczącej podsumowania jego misji do Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej, Londyn, 29 czerwca 2018 r.

199. Co więcej **EROD uważa, że zawarcie dwustronnych lub wielostronnych umów z państwami trzecimi w celu współpracy wywiadowczej, stanowiących podstawę prawną dla bezpośredniego przechwytywania i pozyskiwania danych osobowych lub przekazywania danych osobowych do tych państw, może również znacząco wpłynąć na warunki dalszego wykorzystania zebranych informacji, ponieważ, zgodnie z oceną, takie umowy prawdopodobnie wpłyną na ramy prawne ochrony danych w Zjednoczonym Królestwie.**

4.3.3 Nadzór

200. EROD podkreśla znaczenie kompleksowego nadzoru ze strony niezależnych organów nadzorczych w celu zapewnienia odpowiedniego stopnia ochrony danych. Gwarancja niezależności organów nadzorczych w rozumieniu art. 8 ust. 3 Karty praw podstawowych Unii Europejskiej ma na celu zapewnienie efektywnego i rzetelnego monitorowana zgodności z przepisami dotyczącymi ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych.

201. W sytuacji, gdy dane osobowe są wykorzystywane do celów bezpieczeństwa narodowego, funkcję nadzorczą sprawuje głównie Komisarz ds. uprawnień dochodzeniowo-śledczych oraz komisarze sądowi (zwani dalej „komisarzami sądowymi").

202. **EROD ogólnie uznaje wprowadzenie „komisarzy sądowych" w IPA 2016 za znaczną poprawę.** Zgodnie z powyższym wnioskiem, wzywa się Komisję Europejską do **bardziej szczegółowej oceny niezależności komisarzy sądowych, a w szczególności stopnia, w jakim niezależność Komisarza ds. uprawnień dochodzeniowo-śledczych oraz biura Komisarza ds. uprawnień dochodzeniowo-śledczych jest prawnie zabezpieczona, ponieważ nie jest jako taka określona w IPA 2016.** Jest to tym ważniejsze, że Komisarz ds. uprawnień dochodzeniowo-śledczych orzeka w sprawie odwołań przez rząd w przypadku gdy wniosek o **środek** nadzoru został odrzucony **przez** komisarza sądowego.

203. Komisarz ds. uprawnień dochodzeniowo-śledczych pełni funkcje nadzoru *ex ante*, jak również *ex post*. W odniesieniu do nadzoru *ex ante* EROD rozumie, że funkcją komisarzy sądowych jest zatwierdzanie, w poszczególnych przypadkach, różnych środków nadzoru, w tym ukierunkowanego przechwytywania i masowego uzyskiwania danych komunikacyjnych. EROD zauważa ponadto, że uprzednie zatwierdzenie środków nadzoru nie może wynikać z orzecznictwa TSUE jako absolutnego wymogu w odniesieniu do proporcjonalności środków nadzoru[140].

204. Aby ocenić efektywność tego poziomu nadzoru, EROD dostrzega jednak potrzebę dokładniejszego wyjaśnienia scenariuszy, w których możliwe jest zgodne z prawem przechwytywanie danych bez uprzedniego zatwierdzenia przez komisarzy sądowych.

205. W projekcie decyzji, Komisja Europejska wspomina w przypisach 201 i 266 o „ściśle określonych ograniczonych przypadkach" w IPA 2016 w sekcjach od 44 do 52 w odniesieniu do ukierunkowanych przechwytywań. EROD zauważa, że sekcje 45 - 51 IPA 2016 są wyłączeniem, które uważa się za nie używane regularnie przez służby wywiadu. Ponadto **EROD rozumie**, że w **przypadkach, w których mają zastosowanie wyłączenia** (np. operatorów telekomunikacyjnych i pocztowych), uprzednie zatwierdzenie dokonywane przez komisarzy sądowych ma być przeprowadzone w przypadku, gdy

https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E#:~:text=Intelligence%20sharing%20must%20not%20result,UK%20intelligence%20that%20could%20give.

[140] Jednak zauważa również, że TSUE, unieważniając Tarczę Prywatności w sprawie *Schrems II*, zwrócił uwagę na fakt, że zgodnie z prawem Stanów Zjednoczonych, tak zwany Sąd FISA „nie jest uprawniony do zatwierdzania poszczególnych środków nadzoru; może jednak zatwierdzać programy nadzoru (takie jak PRISM, UPSTREAM) w oparciu o roczne certyfikacje". (pkt 179).

organy ścigania lub służby wywiadu **żądają** dostępu do tych danych, **i zwraca się do Komisji Europejskiej o potwierdzenie w decyzji, że jest to właściwe**.

206. EROD uznaje, że w art. 44 ust. 2 IPA 2016 zezwala się na przechwytywanie komunikatów, jeżeli jedna ze stron (nadawca lub odbiorca) wyraziła na to zgodę oraz udzielono upoważnienia na mocy ustawy RIPA 2000 (ustawy regulującej uprawnienia dochodzeniowo-śledcze z 2000 r.) (Szkocja) (11 ustawa Parlamentu Szkockiego z 2000 r.), tj. dotychczasowego stanu prawnego przed powołaniem komisarzy sądowych. EROD **zachęca** Komisję Europejską do sprecyzowania, czy oznacza to, że w przypadkach, gdy istnieje jednostronna zgoda, procedura wcześniejszego zatwierdzenia nie miałaby żadnego zastosowania.

207. Jeżeli chodzi o nadzór *ex post*, należy również sprawdzić, czy zapewniono niezakłócony skuteczny i niezależny nadzór, w szczególności, gdy nie zostało to przewidziane *ex ante*.

208. EROD zauważa, że komisarze sądowi dokonują przeglądu *ex post* art. 48–52 IPA 2016 oraz **zachęca Komisję Europejską, aby doprecyzowała na podstawie jakich wymogów oraz z czyjej inicjatywy taki przegląd *ex post* ma zostać przeprowadzony**.

209. Zgodnie z art. 229 ust. 4 IPA 2016 kontrola wykonywania określonych funkcji nie należy do zadań Komisarza ds. uprawnień dochodzeniowo-śledczych. W związku z tym EROD zachęca Komisję Europejską do doprecyzowania przepisów art. 229 ust. 4 lit. d) i e) IPA 2016 dotyczących jej praktycznego wpływu na kompetencje Komisarza ds. uprawnień dochodzeniowo-śledczych w zakresie kontroli. **Z posiadanych przez EROD informacji wynika, że Urząd Rzecznika Informacji jest właściwym organem nadzoru, w przypadku gdy zastosowanie mają wyłączenia przewidziane w art. 229 ust. 4 IPA 2016, EROD zachęca również Komisję Europejską do potwierdzenia w swojej decyzji, że jest to właściwe.**

210. **Wydaje się, że podczas przeprowadzania nadzoru *ex post* rola Komisarza ds. uprawnień dochodzeniowo-śledczych ogranicza się** do wydawania zaleceń w przypadkach nieprzestrzegania przepisów i przekazania powiadomienia osobie, której dane dotyczą, jeżeli błąd jest poważny, a poinformowanie jej leży w interesie publicznym. **EROD zachęca Komisję Europejską, aby wyjaśniła, w jaki sposób Biuro Komisarza ds. uprawnień dochodzeniowo-śledczych (IPCO) może zapewnić skuteczne przestrzeganie przepisów prawa.**

211. **Ponadto EROD rozumie, że osoby fizyczne, które zostały poszkodowane wskutek nieprzestrzegania przepisów, nie mogą zwracać się bezpośrednio do IPCO, lecz muszą złożyć skargę w Urzędzie Rzecznika Informacji, który ma jednak ograniczone kompetencje w obszarze bezpieczeństwa narodowego. W związku z tym EROD zwraca się do Komisji Europejskiej o dalsze wyjaśnienie sposobu, w jaki prawnie zagwarantowano rozpatrywanie skarg przez Biuro Komisarza ds. uprawnień dochodzeniowo-śledczych w takich przypadkach.**

4.3.4. Dochodzenie roszczeń

212. W świetle wyroków TSUE w sprawach *Schrems I* i *Schrems II* nie ulega wątpliwości, że skuteczna ochrona sądowa w rozumieniu art. 47 Karty praw podstawowych Unii Europejskiej ma podstawowe znaczenie dla przyjęcia założenia adekwatności prawa państwa trzeciego. Orzeczenia pokazały również, że w tym względzie należy zwrócić szczególną uwagę na skuteczną ochronę sądową w obszarze dostępu do danych osobowych na potrzeby bezpieczeństwa narodowego.

213. **EROD uznaje, że Zjednoczone Królestwo ustanowiło Trybunał ds. Uprawnień Dochodzeniowo-Śledczych. Trybunał ds. Uprawnień Dochodzeniowo-Śledczych jest właściwy nie tylko do rozpatrywania spraw dotyczących korzystania z uprawnień dochodzeniowych przez organy**

ścigania, ale również przez służby wywiadowcze. Z posiadanych przez EROD informacji wynika, że Trybunał ds. Uprawnień Dochodzeniowo-Śledczych funkcjonuje jako właściwy sąd w rozumieniu art. 47 Karty praw podstawowych Unii Europejskiej. Jeśli chodzi o uprawnienia, wzywa się Komisję Europejską do potwierdzenia, że Trybunał ds. Uprawnień Dochodzeniowo-Śledczych posiada wszystkie uprawnienia wymienione w motywie 262 projektu decyzji, niezależnie od podstawy prawnej, na podstawie której wniesiono skargę.

214. Niejawny nadzór prowadzony przez agencje wywiadowcze będzie często oznaczał, że obiekt nadzoru, osoba, której dane dotyczą, nie jest i nie będzie świadoma nadzoru. W tym kontekście, w przypadkach, w których zachodziła potrzeba przeanalizowania prawa amerykańskiego, EROD wielokrotnie wyrażała swoje zaniepokojenie wymogiem „legitymacji procesowej", zgodnie z interpretacją prawa amerykańskiego, w sprawach dotyczących nadzoru. W tym kontekście EROD zauważa, że skarga do Trybunału ds. Uprawnień Dochodzeniowo-Śledczych wymaga jedynie przejścia testu „przekonania", w którym skarżący musi wykazać, że może być potencjalnie objęty zastosowaniem danego środka.

215. Analizując działalność Trybunału ds. Uprawnień Dochodzeniowo-Śledczych, EROD zwraca również szczególną uwagę na fakt, że funkcjonowanie Trybunału ds. Uprawnień Dochodzeniowo-Śledczych wielokrotnie uznawano za zgodne z Europejskim Trybunałem Praw Człowieka, zgodnie z wykładnią Europejskiego Trybunału Praw Człowieka.