Opinia 32/2021 na podstawie rozporządzenia (UE) 2016/679 dotycząca projektu decyzji wykonawczej Komisji Europejskiej w sprawie odpowiedniej ochrony danych osobowych w Republice Korei

Wersja 1.0

Przyjęta 24 września 2021 r.

SPIS TREŚCI

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 („**RODO**"),

uwzględniając Porozumienie o Europejskim Obszarze Gospodarczym („**EOG**"), a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

PRZYJMUJE NINIEJSZĄ OPINIĘ:

1. STRESZCZENIE

1. W dniu 16 czerwca 2021 r. Komisja Europejska rozpoczęła – na podstawie RODO – formalny proces zmierzający do przyjęcia projektu decyzji wykonawczej Komisji („**projekt decyzji**") w sprawie odpowiedniej ochrony danych osobowych w Republice Korei na podstawie ustawy o ochronie danych osobowych[2].

2. W tym samym dniu Komisja Europejska zwróciła się do Europejskiej Rady Ochrony Danych („**EROD**") o przedstawienie opinii[3]. EROD przeprowadziła ocenę, czy stopień ochrony zapewnianej w Republice Korei jest odpowiedni, na podstawie analizy samego projektu, a także na podstawie analizy dokumentacji udostępnionej[4] przez Komisję Europejskiej.

3. EROD skupiła się na ocenie zarówno ogólnych aspektów projektu decyzji związanych z RODO, jak również dostępu organów publicznych do danych osobowych przekazywanych z EOG do celów egzekwowania prawa i zapewnienia bezpieczeństwa narodowego, w tym środków prawnych dostępnych dla osób fizycznych w EOG. EROD oceniła również, czy wprowadzono zabezpieczenia przewidziane w koreańskich ramach prawnych i czy są one skuteczne.

4. Głównym punktem odniesienia dla tych prac EROD były dokument roboczy dotyczący odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO[5]") przyjęty w lutym 2018 r. oraz zalecenia EROD 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru[6].

[1] Odniesienia do „**państw członkowskich**" w niniejszej opinii należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Zob. komunikat prasowy https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ibid.
[4] EROD oparła swoją analizę na oficjalnych tłumaczeniach sporządzonych przez rząd Korei.
[5] WP 254, dokument roboczy dotyczący odpowiedniego stopnia przekazywanych danych osobowych, 6 lutego 2018 r., (zatwierdzony przez EROD, zob. https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] 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_en.

1.1. Obszary zbieżności

5. Głównym celem EROD było przedstawienie Komisji Europejskiej opinii na temat tego, czy stopień ochrony zapewnianej osobom fizycznym, których dane osobowe są przekazywane do Republiki Korei, jest odpowiedni. Należy uznać, że EROD nie oczekuje, aby koreańskie ramy ochrony danych były powieleniem europejskiego prawa w zakresie ochrony danych osobowych.

6. EROD przypomina jednak, że zgodnie z art. 45 RODO oraz orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej („**TSUE**"), aby można było uznać, że zapewniany jest odpowiedni stopień ochrony, ustawodawstwo państwa trzeciego musi być spójne z istotą podstawowych zasad zawartych w RODO. W tym kontekście koreańskie ramy ochrony danych wykazują wiele podobieństw do europejskich ram ochrony danych, przy czym jeden główny dokument prawny obejmuje zarówno sektor publiczny, jak i sektor prywatny, a uzupełniają go sektorowe akty prawodawcze.

7. Jeśli chodzi o treść, EROD zwraca uwagę na najważniejsze obszary zbieżności między ramami wyznaczonymi przez RODO a koreańskimi ramami ochrony danych pod względem niektórych głównych przepisów, takich jak pojęcia (np. „dane osobowe", „przetwarzanie", „osoba, której dane dotyczą"); podstawy zgodnego z prawem i rzetelnego przetwarzania danych do prawnie uzasadnionych celów; ograniczenie celu; jakość i proporcjonalność danych; zatrzymywanie danych, ich bezpieczeństwo i poufność; przejrzystość; oraz szczególne kategorie danych.

8. Dodatkowo EROD z zadowoleniem przyjmuje dążenie Komisji Europejskiej i władz koreańskich do dopilnowania, aby Republika Korei zapewniała stopień ochrony odpowiadający temu przewidzianemu w RODO poprzez przyjmowanie przez koreański organ nadzorczy obwieszczeń (które mają zastosowanie nie tylko do danych osobowych przekazywanych z EOG do Korei) w celu usunięcia luk między RODO a koreańskimi ramami ochrony danych. W tym kontekście EROD podkreśla znaczenie tych obwieszczeń dla oceny, czy Republika Korei zapewnia odpowiedni stopień ochrony, i zwraca uwagę, że zawierają one na przykład odpowiednie objaśnienia dotyczące niektórych ważnych zabezpieczeń, między innymi w odniesieniu do zakresu stosowania odstępstw od ustawy o ochronie danych osobowych (PIPA) odnoszących się do przetwarzania spseudonimizowanych danych osobowych do celów naukowych, badawczych i statystycznych, dalszego przekazywania danych oraz zasad mających zastosowanie w kontekście dostępu organów publicznych do danych.

1.2. Wyzwania

9. Choć EROD ustaliła, że wiele aspektów koreańskich ram ochrony danych jest merytorycznie równoważnych z europejskimi ramami ochrony danych, stwierdziła również, że istnieją pewne aspekty, które mogą wymagać bliższej analizy i wyjaśnienia. W szczególności EROD uważa, że aby zapewnić merytorycznie równoważny stopień ochrony, należy poddać dalszej ocenie poniższe kwestie, a Komisja Europejska powinna je ściśle monitorować.

1.2.1. Wyzwania ogólne

10. EROD zwraca uwagę, że obwieszczenie nr 2021-1 „ma status przepisu administracyjnego z mocą prawnie wiążącą administratorów danych osobowych w tym sensie, że wszelkie naruszenie tego obwieszczenia można uznać za naruszenie odpowiednich przepisów PIPA[7]. Biorąc jednak pod uwagę, że obwieszczenie nie zawiera dodatkowych przepisów jako takich, lecz objaśnienia, jak należy rozumieć i stosować ustawowy tekst PIPA, a także w świetle jego ogólnego znaczenia zwłaszcza w odniesieniu do przepisów dotyczących pseudonimizacji ujętych w PIPA, które są według wiedzy EROD przedmiotem toczących się postępowań sądowych, EROD zwraca się do Komisji Europejskiej o przedstawienie dalszych informacji na temat wiążącego charakteru, wykonalności i ważności obwieszczenia nr 2021-1 oraz zaleca uważne monitorowanie jego przestrzegania w praktyce,

[7] Zob. sekcja I załącznika I do projektu decyzji.

szczególnie w odniesieniu do jego stosowania nie tylko przez koreański organ nadzorczy, ale również przez sądy, zwłaszcza w przypadku gdy równoważny stopień ochrony zapewniany przez koreańskie ramy prawne opiera się na objaśnieniach ujętych w tym obwieszczeniu.

1.2.2. Ogólne kwestie dotyczące ochrony danych

11. W odniesieniu do zakresu stosowania decyzji stwierdzającej odpowiedni stopień ochrony EROD zauważa, że ta decyzja będzie dotyczyć przekazywania danych objętych przepisami prawnymi EOG zarówno publicznym, jak i prywatnym „administratorom danych osobowych" podlegającym PIPA. EROD rozumie, że ten termin uwzględnia podmioty działające jako podmioty przetwarzające w rozumieniu RODO, jednak zwraca się do Komisji Europejskiej, aby w celu uniknięcia nieporozumień jasno określiła, że decyzja stwierdzająca odpowiedni stopień ochrony obejmie także przekazywanie danych „podmiotom przetwarzającym" w Korei.

12. Ważny aspekt, na który EROD zwraca uwagę, dotyczy pojęcia danych spseudonimizowanych ujętego w koreańskich ramach ochrony danych. Zgodnie z prawem koreańskim do przetwarzania spseudonimizowanych danych osobowych mają zastosowanie odstępstwa od niektórych stosownych przepisów, w tym przepisów w zakresie indywidualnych praw osób, których dane dotyczą, oraz w zakresie zatrzymywania danych. Według Komisji Europejskiej ma to miejsce jedynie, w przypadku gdy spseudonimizowane dane osobowe są przetwarzane na potrzeby statystyk, badań naukowych lub archiwizacji w interesie publicznym. Jednak stwierdzenie to znajduje potwierdzenie głównie w obwieszczeniu nr 2021-1, co sprawia, że w tym kontekście szczególnego znaczenia nabiera wspomniana już konieczność przekazania dodatkowych informacji na temat wiążącego charakteru, wykonalności i ważności tego obwieszczenia oraz monitorowania tych aspektów. Dodatkowo EROD zwraca się do Komisji Europejskiej o dalszą ocenę skutków pseudonimizacji na mocy prawa koreańskiego oraz, co najważniejsze, sposobu, w jaki może ona wpłynąć na podstawowe prawa i wolności osób, których dane dotyczą i których dane osobowe są przekazywane do Republiki Korei na podstawie decyzji stwierdzającej odpowiedni stopień ochrony. W szczególności EROD wzywa Komisję Europejską do przeprowadzenia dalszej oceny wyjątków ujętych w art. 28 ust. 7 PIPA oraz art. 40 ust. 3 ustawy o informacjach kredytowych (CIA) oraz do uważnego monitorowania stosowania tych wyjątków oraz odpowiedniego orzecznictwa w celu dopilnowania, aby prawa osób, których dane dotyczą, nie były bezpodstawnie ograniczane podczas przetwarzania do tych celów danych osobowych przekazywanych na podstawie decyzji stwierdzającej odpowiedni stopień ochrony.

13. Ponadto EROD zauważa, że zgodnie z koreańskimi przepisami prawo do wycofania zgody istnieje jedynie w szczególnych okolicznościach, i w związku z tym zwraca się do Komisji Europejskiej o dalszą ocenę skutków braku ogólnego prawa do wycofania zgody oraz do przedstawienia dalszych zapewnień, tak aby ustalić, że zawsze jest zagwarantowany odpowiedni stopień ochrony, również, w razie konieczności, poprzez objaśnienie roli prawa do zawieszenia na podstawie PIPA wobec braku ogólnego prawa do wycofania zgody.

14. Jeśli chodzi o dalsze przekazywanie danych, EROD przyznaje, że świadoma zgoda osoby, której dane dotyczą, będzie zasadniczo stosowana jako podstawa przekazania danych przez koreańskiego administratora danych osobowych do odbiorcy z państwa trzeciego oraz że obwieszczenie nr 2021-1 przewiduje obowiązek informowania osób fizycznych, do którego państwa trzeciego będą przekazane ich dane. EROD zwraca się jednak do Komisji Europejskiej o dopilnowanie, aby informacje do przekazania osobie, której dane dotyczą, obejmowały również informacje na temat możliwych zagrożeń związanych z przekazywaniem danych wynikających z braku odpowiedniej ochrony w państwie trzecim oraz braku odpowiednich zabezpieczeń. Ponadto EROD z zadowoleniem przyjęłaby, gdyby w decyzji stwierdzającej odpowiedni stopień ochrony znalazły się zapewnienia, że koreańscy administratorzy danych osobowych nie będą przekazywać danych osobowych do państw trzecich w sytuacjach, w których na podstawie RODO nie można byłoby udzielić ważnej zgody, np. ze względu na nierównowagę sił.

15. Jeśli chodzi o mianowanie członków koreańskiego organu nadzorczego, to mimo że formalna procedura w tym zakresie powinna być spójna z RODO i w związku z tym spełniać warunki badania równoważności z ramami prawnymi EOG, EROD z zadowoleniem przyjęłaby, gdyby Komisja Europejska monitorowała wszelkie zmiany mogące mieć wpływ na niezależność członków południowokoreańskiego organu nadzorczego.

16. W odniesieniu do budżetu, znów na podstawie informacji przekazanych przez Komisję Europejską, nie podano żadnych informacji o charakterystyce pracowników przydzielonych do Komisji ds. Ochrony Danych Osobowych (PIPC) ani o udostępnionych jej środkach finansowych. Dlatego EROD oczekuje, że projekt decyzji będzie zawierał dodatkowe informacje dotyczące tych dwóch istotnych kwestii.

1.2.3. Dostęp organów publicznych do danych przekazywanych do Republiki Korei

17. EROD przeanalizowała także koreańskie ramy prawne w odniesieniu do dostępu organów rządowych do danych osobowych – do celów egzekwowania prawa i bezpieczeństwa narodowego – przekazywanych z EOG do Korei. Choć EROD przyjęła oświadczenia i zapewnienia przedstawione przez rząd Korei, określone w załączniku II do projektu decyzji, wskazała na pewne aspekty, które wymagają wyjaśnienia lub wzbudzają obawy.

18. EROD zauważa, że przepisy PIPA mają zastosowanie bez ograniczeń w obszarze egzekwowania prawa. Zwraca też uwagę, że przetwarzanie danych w obszarze bezpieczeństwa narodowego podlega bardziej zawężonemu zbiorowi przepisów zawartych w PIPA.

19. W odniesieniu do dobrowolnego ujawniania danych osobowych przez dostawców usług telekomunikacyjnych organom ds. bezpieczeństwa narodowego EROD wyraża obawy, że nie jest jasny związek pomiędzy sekcją 3 załącznika I do projektu decyzji, zgodnie z którą dostawcy muszą co do zasady powiadomić daną osobę fizyczną, gdy dobrowolnie realizują wniosek, a art. 58 ust. 1 lit. 2 PIPA, dotyczącym mianowicie częściowego odstępstwa ze względu na bezpieczeństwo narodowe. To może spowodować, że wymogi informacyjne staną się nieskuteczne, co znacznie utrudni osobom, których dane dotyczą, dowodzenie swoich praw w zakresie ochrony danych, zwłaszcza w odniesieniu do sądowych środków dochodzenia roszczeń.

20. Choć w projekcie decyzji nie jest to wyraźnie stwierdzone, EROD przyjmuje na podstawie wyjaśnień przekazanych przez Komisję Europejską, że koreańskie ramy prawne nie pozwalają na masowe przechwytywanie danych telekomunikacyjnych. Dlatego najnowsze orzecznictwo Europejskiego Trybunału Praw Człowieka („**ETPC**") dotyczące systemów masowego przechwytywania danych nie będzie mieć bezpośredniego znaczenia dla oceny stopnia ochrony danych w Korei.

21. Projekt decyzji nie zawiera informacji na temat ram prawnych dotyczących dalszego przekazywania danych w dziedzinie w bezpieczeństwa narodowego. Choć EROD zrozumiała, że zdaniem Komisji Europejskiej dalsze przekazywanie danych do celów bezpieczeństwa narodowego jest dostatecznie uregulowane poprzez ogólne zabezpieczenia oraz zasady wynikające z ram konstytucyjnych i PIPA, EROD zastanawia się, czy można uznać, że spełnione są wymogi dokładności i jasności prawa oraz zapewnione skuteczne zabezpieczenia możliwe do wyegzekwowania. Zabezpieczenia, o których mówi Komisja Europejska, mają bardzo ogólny charakter i nie odnoszą się – w podstawie prawnej – do szczególnych okoliczności i warunków, po spełnieniu których jest możliwe dalsze przekazywanie danych na potrzeby bezpieczeństwa narodowego. W tym kontekście EROD zauważa również, że Komisja Europejska nie wzięła pod uwagę istnienia międzynarodowych umów pomiędzy Republiką Korei a państwami trzecimi bądź organizacjami międzynarodowymi, które mogą zawierać szczegółowe postanowienia dotyczące międzynarodowego przekazywania danych osobowych przez organy ścigania lub służby wywiadowcze do państw trzecich. EROD uważa, że zawarcie dwustronnych lub wielostronnych umów z państwami trzecimi w celu współpracy w zakresie egzekwowania prawa lub działań wywiadowczych może mieć wpływ na ocenę koreańskich ram prawnych ochrony danych.

22. EROD zauważa, że kontrola nad organami ścigania przestępstw karnych i organami ds. bezpieczeństwa narodowego jest sprawowana łącznie przez różne wewnętrzne i zewnętrzne organy, zwłaszcza przez PIPC, która dysponuje dostatecznymi uprawnieniami wykonawczymi.

23. Skuteczne środki prawne i środki dochodzenia roszczeń oznaczają konieczność, aby osoby, których dane dotyczą, mogły zwrócić się do właściwego organu, który spełnia wymogi określone w art. 47 Karty praw podstawowych Unii Europejskiej („**Karta**"), tj. ma kompetencje do ustalenia, że zachodzi przetwarzanie danych, i do sprawdzenia zgodności tego przetwarzania z prawem, oraz który ma możliwe do wyegzekwowania uprawnienia zaradcze na wypadek, gdy przetwarzanie danych jest niezgodne z prawem. W tym kontekście EROD zwraca się do Komisji Europejskiej o wyjaśnienie, czy skarga do PIPC lub sprawa sądowa podlegają wymogom merytorycznym lub proceduralnym, takim jak ciężar dowodu, oraz czy osoby fizyczne z EOG będą w stanie spełnić dany warunek wstępny.

1.3. Wnioski

24. Według EROD przedmiotowa decyzja stwierdzająca odpowiedni stopień ochrony ma zasadnicze znaczenie również ze względu na to, że – z wyjątkami określonymi w opinii – obejmie przekazywanie danych zarówno w sektorze publicznym, jak i w sektorze prywatnym.

25. EROD z zadowoleniem przyjmuje dążenie Komisji Europejskiej i władz Korei, aby ujednolicić koreańskie ramy prawne z ramami europejskimi. Korekty przewidziane w obwieszczeniu nr 2021-1, polegające na zniwelowaniu niektórych różnic między tymi dwoma systemami, są niezmiernie istotne i zostały dobrze przyjęte. EROD zauważa jednak, że nadal istnieją pewne obawy, m.in. w odniesieniu do obwieszczenia nr 2021-1, a także konieczność dalszych wyjaśnień dotyczących innych kwestii; oraz zaleca, aby Komisja Europejska odniosła się do tych obaw i wniosków o objaśnienia zgłoszonych przez EROD oraz aby przekazała dalsze informacje i wyjaśnienia w odniesieniu do kwestii poruszonych w niniejszej opinii.

2. WPROWADZENIE

2.1. Koreańskie ramy ochrony danych

26. Głównym aktem prawnym regulującym ochronę danych w Republice Korei jest ustawa o ochronie danych osobowych (ustawa nr 10465 z dnia 29 marca 2011 r., ostatnio zmieniona ustawą nr 16930 z dnia 4 lutego 2020 r., „**PIPA**"). Uzupełnia ją dekret wykonawczy (dekret prezydenta nr 23169 z dnia 29 września 2011 r., ostatnio zmieniony dekretem prezydenta nr 30892 z dnia 4 sierpnia 2020 r., "dekret wykonawczy w sprawie PIPA"), który jest prawnie wiążący i wykonalny.

27. Oprócz PIPA koreańskie ramy ochrony danych obejmują „obwieszczenia" wydane przez koreański organ nadzorczy – Komisję ds. Ochrony Danych Osobowych („**PIPC**") – zawierające dodatkowe zasady w zakresie interpretacji i stosowania PIPA. Niedawno PIPC przyjęła obwieszczenie nr 2021-1 z dnia 21 stycznia 2021 r. (zmieniające wcześniejsze obwieszczenie nr 2020-10 z dnia 1 września 2020 r., zwane dalej „**obwieszczeniem nr 2021-1**") w sprawie interpretacji, stosowania i egzekwowania niektórych przepisów PIPA. To obwieszczenie było w szczególności rezultatem rozmów na temat odpowiedniego stopnia ochrony prowadzonych między władzami koreańskimi a Komisją Europejską. Zawiera objaśnienia w zakresie stosowania szczegółowych przepisów PIPA, w tym dotyczące przetwarzania danych osobowych przekazywanych do Korei na podstawie przewidywanej decyzji stwierdzającej odpowiedni stopień ochrony[8]; „ma status przepisu administracyjnego z mocą prawnie wiążącą administratorów danych osobowych w tym sensie, że wszelkie naruszenie tego obwieszczenia można uznać za naruszenie odpowiednich przepisów PIPA"[9]. W tym kontekście EROD zauważa, że

[8] Zob. sekcja I załącznika I projektu decyzji.
[9] Ibid.

choć w projekcie decyzji obwieszczenie jest zaliczane do „przepisów uzupełniających", nie zawiera ono dodatkowych przepisów jako takich, lecz wyjaśnienia mające na celu jasne przedstawienie, jak należy rozumieć i stosować ustawowy tekst PIPA, zwłaszcza w odniesieniu do danych przekazywanych z EOG. Wobec powyższego EROD zaleca uważne monitorowanie przestrzegania obwieszczenia nr 2021-1 w praktyce, zwłaszcza jego stosowania nie tylko przez PIPC, ale także przez sądy, szczególnie w przypadku gdy równoważny stopień ochrony zapewniany przez koreańskie ramy prawne opiera się na wyjaśnieniach zawartych w obwieszczeniu nr 2021-1.

28. Inne stosowne ustawy o ochronie danych w koreańskich ramach prawnych zawierają przepisy dotyczące przetwarzania danych osobowych w konkretnych sektorach; są to na przykład:

    - ustawa o wykorzystaniu i ochronie informacji kredytowych („**CIA**"), wraz z odpowiednim dekretem wykonawczym („**dekret wykonawczy w sprawie CIA**"), które określają szczegółowe przepisy mające zastosowanie do podmiotów komercyjnych i wyspecjalizowanych jednostek (takich jak agencje ratingowe, instytucje finansowe), gdy te przetwarzają osobowe informacje kredytowe niezbędne do ustalenia zdolności kredytowej stron transakcji finansowych lub handlowych;

    - ustawa o promowaniu korzystania z sieci informacyjnych i komunikacyjnych oraz ochronie danych („**ustawa o sieciach**");

    - ustawa o ochronie prywatności w sektorze łączności („**CPPA**").

29. W dziedzinie dostępu organów rządowych do danych EROD wzięła pod uwagę – oprócz stosowanych przepisów zawartych w PIPA i CPPA – niektóre inne akty prawne, mianowicie ustawę w sprawie postępowania karnego („**CPA**"), ustawę o działalności telekomunikacyjnej („**TBA**"), ustawę o przekazywaniu i wykorzystaniu określonych informacji o transakcjach finansowych („**ARUSFTI**") oraz ustawę o krajowej służbie wywiadowczej („**NISA**").

2.2. Zakres oceny EROD

30. Projekt decyzji Komisji Europejskiej jest rezultatem oceny dotyczącej koreańskich ram ochrony danych, a także wynikających z tej oceny rozmów z władzami Korei. Zgodnie z art. 70 ust. 1 lit. s) RODO oczekuje się, że EROD przedstawi niezależną opinię na temat ustaleń Komisji Europejskiej, określi braki w ramach prawnych zapewniających odpowiedni stopień ochrony, jeżeli takie braki występują, oraz postara się przedstawić propozycje, aby im zaradzić.

31. Aby uniknąć powtórzeń i pomóc w ocenie koreańskich ram prawnych, EROD postanowiła skupić się na pewnych konkretnych kwestiach przedstawionych w projekcie decyzji oraz przeprowadzić analizę i wydać opinię na ich temat; EROD nie powtarzała większości ustalonych faktów i ocen, w przypadku gdy nie ma podstaw, aby przypuszczać, że prawo Republiki Korei nie jest merytorycznie równoważne z prawem EOG. Dodatkowo, zgodnie z orzecznictwem TSUE bardzo ważna część analizy dotyczy prawnego systemu dostępu do danych osobowych przekazywanych do Republiki Korei w kontekście bezpieczeństwa narodowego oraz praktyk aparatu zajmującego się bezpieczeństwem narodowym w tym państwie.

32. W swojej ocenie EROD uwzględniła obowiązujące europejskie ramy ochrony danych, w tym art. 7, 8 i 47 Karty – odnoszące się odpowiednio do prawa do poszanowania życia prywatnego i rodzinnego, prawa do ochrony danych osobowych i prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu – oraz art. 8 EKPC dotyczący prawa do poszanowania życia prywatnego i rodzinnego. Ponadto EROD wzięła pod uwagę wymogi RODO oraz istotne orzecznictwo.

33. Celem tych działań jest przedstawienie Komisji Europejskiej opinii na temat oceny, czy stopień ochrony zapewnianej w Republice Korei jest odpowiedni. Pojęcie „odpowiedniego stopnia ochrony", które zastosowano już w dyrektywie 95/46, zostało dalej rozwinięte przez TSUE. Należy przypomnieć

standard ochrony określony przez TSUE w sprawie Schrems I, mianowicie, że – chociaż „stopień ochrony" w państwie trzecim musi być „merytorycznie równoważny" ze stopniem ochrony gwarantowanym w UE – *„środki, z jakich to państwo trzecie korzysta w tym względzie dla zapewnienia takiego stopnia ochrony, mogą różnić się od środków wprowadzonych w Unii"*[10]. W związku z tym celem nie jest odzwierciedlenie punkt po punkcie europejskich przepisów, lecz ustanowienie istotnych i podstawowych wymogów badanych przepisów. Odpowiedni stopień ochrony można osiągnąć dzięki połączeniu przyznania praw osobom, których dane dotyczą, nałożenia obowiązków na podmioty przetwarzające dane osobowe lub podmioty, które sprawują kontrolę nad takim przetwarzaniem, oraz nadzoru prowadzonego przez niezależne organy. Przepisy w zakresie ochrony danych osobowych są jednak skuteczne wyłącznie wtedy, gdy są możliwe do wyegzekwowania na drodze prawnej i stosuje się je w praktyce. Konieczne jest zatem nie tylko wzięcie pod uwagę treści przepisów mających zastosowanie do przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, lecz również obowiązującego systemu zapewniającego skuteczność tych przepisów. Efektywne mechanizmy egzekwowania mają zasadnicze znaczenie w odniesieniu do skuteczności przepisów w zakresie ochrony danych osobowych[11].

2.3. Ogólne uwagi i obawy

2.3.1. Międzynarodowe zobowiązania podjęte przez Republikę Korei

34. Zgodnie z art. 45 ust. 2 lit. c) RODO i dokumentem roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO[12], przy ocenie, czy stopień ochrony zapewnianej przez państwo trzecie jest odpowiedni, Komisja Europejska uwzględnia między innymi międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub inne obowiązki wynikające z udziału tego państwa trzeciego w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych, a także wdrażanie takich zobowiązań.

35. Korea jest stroną kilku umów międzynarodowych gwarantujących prawo do prywatności, na przykład Międzynarodowego paktu praw obywatelskich i politycznych (art. 17), Konwencji o prawach osób niepełnosprawnych (art. 22) oraz Konwencji o prawach dziecka (art. 16). Ponadto Korea, jako członek OECD, przestrzega zasad OECD w zakresie ochrony prywatności, zwłaszcza wytycznych dotyczących ochrony prywatności i transgranicznego przekazywania danych osobowych.

36. EROD dostrzega także, że Korea bierze udział w charakterze państwa obserwatora w pracach Komitetu Konsultacyjnego ds. Konwencji 108+ Rady Europy, mimo że nie podjęła jeszcze decyzji o przystąpieniu.

2.3.2. Zakres decyzji stwierdzającej odpowiedni stopień ochrony

37. Zgodnie z motywem 5 projektu decyzji Komisja Europejska stwierdza, że Republika Korei zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych od administratorów lub podmiotów przetwarzających w Unii do administratorów danych osobowych (np. osób fizycznych lub prawnych, organizacji, instytucji publicznych) objętych zakresem stosowania PIPA, z wyłączeniem przetwarzania danych osobowych na potrzeby działalności misyjnej organizacji religijnych i na potrzeby nominacji kandydatów przez partie polityczne[13] bądź przetwarzania osobowych informacji kredytowych na podstawie CIA przez administratorów, nad którymi kontrolę sprawuje Komisja ds. Usług Finansowych.

38. EROD zauważa, że decyzja stwierdzająca odpowiedni stopień ochrony będzie obejmować przekazywanie danych spod ram prawnych EOG publicznym i prywatnym „administratorom danych

[10] C-362/14, Maximilian Schrems/Data Protection Commissioner, wyrok z dnia 6 października 2015 r., ECLI:EU:C:2015:650, pkt 73–74.
[11] WP 254, s.2.
[12] WP 254, s.2.
[13] Więcej ogólnych informacji znajduje się w sekcji 3.1.2 niniejszej opinii.

osobowych" objętym zakresem PIPA. EROD rozumie, że podmioty działające jako podmioty przetwarzające w rozumieniu RODO są też objęte terminem „administrator danych osobowych", biorąc pod uwagę, że PIPA będzie mieć w równym stopniu zastosowanie do nich oraz że stosuje się szczególne obowiązki, w przypadku gdy administrator danych osobowych („zlecający") angażuje osobę trzecią do przetwarzania danych osobowych („podmiot zewnętrzny"); aby jednak uniknąć nieporozumień, EROD wzywa Komisję Europejską do jasnego określenia, że decyzja stwierdzająca odpowiedni stopień ochrony będzie także obejmować przekazywanie danych do „podmiotów przetwarzających" w Korei i że stopień ochrony danych osobowych przekazywanych z EOG nie będzie obniżony również w takich przypadkach.

39. Oprócz tego, biorąc pod uwagę, że decyzja stwierdzająca odpowiedni stopień ochrony obejmuje także przekazywanie danych osobowych między organami publicznymi, EROD przyjmuje, że będzie ona dotyczyć również przekazywania danych między organami nadzorczymi ds. ochrony danych, i dla zapewnienia przejrzystości zwraca się do Komisji Europejskiej, aby szczegółowo zająć się tą kwestią.

40. Ponadto jeśli chodzi o podmioty wyłączone z zakresu stosowania decyzji stwierdzającej odpowiedni stopień ochrony, EROD podkreśla, że dla tej decyzji byłoby korzystne, gdyby jaśniej określono „organizacje komercyjne" podlegające kontroli sprawowanej przez PIPC (art. 45 ust. 3 CIA), tak aby administratorzy i podmioty przetwarzające z EOG mogli łatwo ocenić, czy dany podmiot odbierający dane jest również objęty zakresem stosowania decyzji stwierdzającej odpowiedni stopień ochrony, przed przekazaniem danych podmiotom objętym zakresem stosowania CIA lub aby przynajmniej uzyskali informację o konieczności oceny tego aspektu.

41. W odniesieniu do zakresu decyzji stwierdzającej odpowiedni stopień ochrony EROD rozumie z dodatkowych wyjaśnień Komisji Europejskiej, że koreańska jednostka analityki finansowej („**KOFIU**"), ustanowiona w ramach Komisji ds. Usług Finansowych i nadzorująca zapobieganie praniu pieniędzy i finansowaniu terroryzmu na podstawie ARUSFTI[14], jest również wyłączona z zakresu decyzji, ponieważ jej jurysdykcja obejmuje tylko instytucje finansowe, które same nie podlegają decyzji stwierdzającej odpowiedni stopień ochrony. Natomiast w art. 1 ust. 2 lit. c) projektu decyzji z jej zakresu wyłącza się tylko tych administratorów danych osobowych, którzy podlegają kontroli sprawowanej przez Komisję ds. Usług Finansowych i przetwarzają osobowe informacje kredytowe na podstawie CIA. Wobec powyższego EROD zwraca się do Komisji Europejskiej o wyjaśnienie, czy KOFIU i działania KOFIU związane z przetwarzaniem danych wchodzą w zakres projektu decyzji.

3. OGÓLNE ASPEKTY OCHRONY DANYCH

3.1. Zasady dotyczące treści

42. Rozdział 3 dokumentu roboczego dotyczącego odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO jest poświęcony „zasadom dotyczącym treści". System państwa trzeciego musi je zawierać, aby można było uznać zapewniany stopień ochrony jako merytorycznie równoważny temu gwarantowanemu w przepisach UE.

43. Mimo że prawo do ochrony danych osobowych nie jest wyraźnie zapisane w samej konstytucji Korei, jest uznawane za prawo podstawowe, wynikające z konstytucyjnych praw do godności ludzkiej i dążenia do szczęścia (art. 10), do życia prywatnego (art. 17) oraz do ochrony prywatności komunikacji (art. 18). Zostało to potwierdzone zarówno przez Sąd Najwyższy, jak i Trybunał Konstytucyjny, co wskazano w projekcie decyzji Komisji Europejskiej[15]. EROD dostrzega to, ponieważ na tej podstawie stwierdza, że ochrona danych jako prawo podstawowe, zgodnie z art. 37 konstytucji Korei, *„może być*

[14] Zob. sekcja 2.2.3.1 załącznika II.

[15] Zob. motyw 8 projektu decyzji oraz stosowne orzecznictwo, o którym mowa w przypisie 10 projektu decyzji; dostępne są tylko streszczenia w języku angielskim.

ograniczona jedynie na mocy prawa i gdy jest to konieczne ze względu na bezpieczeństwo narodowe, utrzymanie porządku publicznego lub dobro publiczne" oraz że „*nawet w przypadku nałożenia takich ograniczeń nie mogą one naruszać istoty danej wolności lub danego prawa*".

44. Według Komisji Europejskiej[16] Trybunał Konstytucyjny orzekł, że prawa podstawowe przysługują również cudzoziemcom. Zgodnie z oświadczeniami rządu Korei[17], choć w orzecznictwie dotychczas nie zajmowano się konkretnie prawem do prywatności obywateli innych państw niż Korea, powszechnie przyjmuje się wśród naukowców, że art. 12–22 konstytucji określają „prawa człowieka". Ponadto Republika Korei uchwaliła zbiór ustaw w obszarze ochrony danych – np. PIPA – które przewidują zabezpieczenia dla wszystkich osób fizycznych, bez względu na ich obywatelstwo. W tym względzie EROD uwzględnia art. 6 ust. 2 konstytucji, który przewiduje, że status cudzoziemca jest zagwarantowany na podstawie prawa międzynarodowego i traktatów międzynarodowych, a także orzecznictwo wymienione w projekcie decyzji, zgodnie z którym „cudzoziemiec" może mieć „prawa podstawowe". Biorąc pod uwagę istotne znaczenie uznania prawa „obcokrajowców" do ochrony danych, EROD zwraca uwagę Komisji Europejskiej na konieczność dalszego monitorowania orzecznictwa dotyczącego ochrony danych jako prawa podstawowego uznanego nie tylko w odniesieniu do obywateli Korei, ale także w odniesieniu do wszystkich osób, których dane dotyczą, tak aby stopień ochrony osób fizycznych gwarantowany na mocy RODO nie był obniżony w przypadku przekazania danych osobowych do Korei na podstawie decyzji stwierdzającej odpowiedni stopień ochrony.

3.1.1. Pojęcia

45. Zgodnie z dokumentem roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO w ramach prawnych państwa trzeciego powinny istnieć podstawowe pojęcia lub zasady dotyczące ochrony danych osobowych. Chociaż nie muszą one powielać terminologii RODO, powinny odzwierciedlać pojęcia zawarte w europejskim prawie z obszaru ochrony danych i być z nimi spójne. Przykładowo RODO zawiera następujące istotne pojęcia: „dane osobowe", „przetwarzanie danych osobowych", „administrator danych", „podmiot przetwarzający", „odbiorca" i „dane wrażliwe"[18].

46. PIPA zawiera szereg definicji, między innymi definicje „danych osobowych", „przetwarzania" oraz „osoby, której dane dotyczą", które są bardzo podobne do odpowiadających im terminów określonych w RODO.

3.1.1.1. Pojęcie danych spseudonimizowanych

47. Wśród definicji zawartych w PIPA, w art. 2 ust. 1 PIPA zdefiniowano w szczególności dane osobowe jako wszelkie poniższe informacje dotyczące żyjącej osoby fizycznej: a) informacje umożliwiające zidentyfikowanie danej osoby poprzez jej imię i nazwisko, numer rejestracji pobytu, wizerunek itp. oraz b) informacje, które choć same nie umożliwiają zidentyfikowania danej osoby mogą być łatwo połączone z innymi informacjami w celu zidentyfikowania danej osoby. W sytuacjach opisanych w lit. b) zaistnienie łatwości połączenia danych stwierdza się poprzez odpowiednie uwzględnienie czasu, kosztów, technologii itp. przeznaczonych na zidentyfikowanie danej osoby, w tym prawdopodobieństwa pozyskania wspomnianych innych informacji.

48. Ponadto zgodnie z art. 2 ust. 1 lit. c) w PIPA za dane osobowe uznaje się także „dane spseudonimizowane". Dane spseudonimizowane definiuje się jako informacje określone w lit. a) lub b) powyżej, które zostały spseudonimizowane na podstawie akapitu 1–2 i wskutek tego uniemożliwiają zidentyfikowanie danej osoby bez wykorzystania lub połączenia informacji w celu

[16] Zob. motyw 9 projektu decyzji.
[17] Sekcja 1.1. załącznika II do projektu decyzji.
[18] WP 254, s. 4.

przywrócenia ich do stanu pierwotnego. Dane w pełni zanonimizowane są wyłączone z zakresu stosowania PIPA. Zgodnie z art. 58 ust. 2 PIPA ten akt nie ma zastosowania do danych, które już nie pozwalają na zidentyfikowanie danej osoby w połączeniu z innymi informacjami, po odpowiednim uwzględnieniu czasu, kosztów, technologii itp.

49. W motywie 17 projektu decyzji Komisja Europejska stwierdza, że to odpowiada przedmiotowemu zakresowi stosowania RODO oraz ujętym w nim pojęciom „danych osobowych", „pseudonimizacji" oraz „danych zanonimizowanych".

50. Jednak zgodnie z art. 28 ust. 7 PIPA, art. 20, 21, 27, art. 34 ust. 1, art. 35–37, art. 39 ust. 3, art. 39 ust. 4, art. 39 ust. 6–8 nie mają zastosowania do spseudonimizowanych danych osobowych.

51. Komisja Europejska stwierdza w projekcie decyzji, że art. 28 ust. 7 PIPA ma zastosowanie jedynie do spseudonimizowanych danych osobowych, gdy są one przetwarzane do celów statystyk, badań naukowych lub archiwizacji w interesie publicznym[19]. Nie wynika to jednak bezpośrednio z litery prawa, ale z wyjaśnień zawartych w obwieszczeniu nr 2021-1[20]. Choć EROD potwierdza, że można wysunąć argument oparty na strukturze i uzasadnieniu PIPA, że art. 28 ust. 2 PIPA należy rozumieć i logicznie interpretować jako mający zastosowanie również do art. 28 ust. 7 PIPA, to w świetle znaczenia, jakie Komisja Europejska przywiązuje do obwieszczenia nr 2021-1 w swojej ocenie odpowiedniości stopnia ochrony danych osobowych w Republice Korei, oraz w celu uniknięcia jakichkolwiek wątpliwości EROD zwraca się do Komisji Europejskiej o przekazanie dalszych informacji na temat wiążącego charakteru, wykonalności i ważności obwieszczenia nr 2021-1 oraz o monitorowanie jego stosowania w tym konkretnym kontekście.

52. W tym kontekście EROD przypomina, że w RODO pseudonimizacja jest rozumiana jako zalecany środek bezpieczeństwa. Innymi słowy, zgodnie z RODO dane spseudonimizowane pozostają danymi osobowymi, do których RODO w pełni się stosuje. Wobec powyższego EROD obawia się, że zapewniany przez RODO stopień ochrony spseudonimizowanych danych osobowych może być osłabiony w przypadku przekazania danych osobowych do Korei. Dlatego EROD zwraca się do Komisji Europejskiej o dalszą ocenę skutków pseudonimizacji na mocy PIPA oraz, co najważniejsze, sposobu, w jakimi może ona wpłynąć na podstawowe prawa i wolności osób, których dane dotyczą i których dane osobowe będą przekazywane do Republiki Korei na podstawie decyzji stwierdzającej odpowiedni stopień ochrony. W związku z tym EROD wzywa Komisję Europejską do przedstawienia zapewnień, że stopień ochrony danych osobowych osób, których dane dotyczą, w EOG nie zostanie obniżony po przekazaniu danych do Republiki Korei nawet w przypadku pseudonimizacji przekazywanych danych osobowych.

3.1.1.2. Pojęcie administratora danych osobowych

53. Zgodnie z definicją zawartą w art. 2 ust. 5 PIPA „administrator danych osobowych" to instytucja publiczna, osoba prawna, organizacja, osoba fizyczna itp., która bezpośrednio lub pośrednio przetwarza dane osobowe w celu prowadzenia akt danych osobowych *„w ramach swojej działalności*". Jednak w ramach dodatkowych zabezpieczeń określonych w obwieszczeniu nr 2021-1 termin „administrator danych osobowych" definiuje się jako instytucję publiczną, osobę prawną, organizację, osobę fizyczną itp., która bezpośrednio lub pośrednio przetwarza dane osobowe w celu prowadzenia akt danych osobowych *„do celów działalności*". Natomiast w przypisie 272 projektu decyzji na temat pojęcia „administrator danych osobowych" podano następujące stwierdzenie: *„Zgodnie z definicją zawartą w art. 2 PIPA, tj. instytucja publiczna, osoba prawna, organizacja, osoba fizyczna itp., która*

[19] Zob. m.in. motyw 82 projektu decyzji.
[20] Sekcja 4 załącznika I do projektu decyzji.

bezpośrednio lub pośrednio przetwarza dane osobowe w celu prowadzenia akt danych osobowych »do celów urzędowych lub do celów działalności".

54. EROD przyznaje, że te niespójności mogą wynikać z tłumaczeń oryginalnego tekstu przekazanych przez władze koreańskie i zwraca się do Komisji Europejskiej o regularne sprawdzanie jakości i pewności tłumaczeń. EROD podkreśla jednak fakt, że aby móc ocenić zasadniczą równoważność stopnia ochrony danych w koreańskich ramach prawnych, konieczne jest jasne zrozumienie celów przetwarzania objętych zakresem przedmiotowym PIPA. Ponadto, w tym kontekście, EROD zauważa, że w PIPA nie stosuje się tej samej terminologii co w RODO w odniesieniu do pojęć „administrator" i „podmiot przetwarzający", oraz zwraca się do Komisji Europejskiej o objaśnienie poprawnej definicji i zakresu pojęcia „administrator danych osobowych" i odniesienie się w szczególności do kwestii, czy ten termin obejmuje także podmioty przetwarzające w rozumieniu RODO, ponieważ to bezpośrednio wpływa na zakres decyzji stwierdzającej odpowiedni stopień ochrony[21].

3.1.2. Częściowe odstępstwa przewidziane w PIPA

55. W art. 58 ust. 1 PIPA wyłącza się stosowanie części PIPA (tj. art. 15–57) w odniesieniu do czterech opisanych poniżej kategorii przetwarzania danych osobowych. W szczególności odstępstwa odnoszą się do przepisów PIPA dotyczących konkretnych podstaw przetwarzania, określonych obowiązków w zakresie ochrony danych, szczegółowych zasad dotyczących wykonywania praw indywidualnych, a także zasad regulujących rozstrzyganie sporów. EROD zauważa jednak, że nadal mają zastosowanie niektóre ogólne przepisy PIPA, na przykład przepisy dotyczące zasad ochrony danych (art. 3 PIPA) i praw indywidualnych (art. 4 PIPA). Dodatkowo art. 58 ust. 4 PIPA określa szczegółowe obowiązki dla tych czterech kategorii przetwarzania danych.

56. Po pierwsze częściowe odstępstwo obejmuje dane osobowe zbierane na podstawie ustawy o statystyce na potrzeby przetwarzania danych przez instytucje publiczne. W motywie 27 projektu decyzji Komisja Europejska stwierdza, że zgodnie z wyjaśnieniami otrzymanymi od rządu koreańskiego dane osobowe przetwarzane w tym kontekście zazwyczaj dotyczą obywateli Korei i tylko w wyjątkowych sytuacjach obejmują informacje o cudzoziemcach, mianowicie w przypadku statystyk dotyczących wjazdu na to terytorium i wyjazdu z tego terytorium bądź dotyczących inwestycji zagranicznych. Jednak zgodnie z projektem decyzji nawet w takich sytuacjach te dane nie są zazwyczaj przekazywane od administratorów/podmiotów przetwarzających w EOG, a raczej bezpośrednio gromadzone przez organy publiczne w Korei.

57. EROD przyjmuje uzasadnienie Komisji Europejskiej dotyczące wyjątkowości stosowania ustawy o statystyce w odniesieniu do przetwarzania danych osobowych przekazywanych na podstawie decyzji stwierdzającej odpowiedni stopień ochrony; z zadowoleniem przyjęłaby jednak dalsze informacje i zapewnienia na temat konkretnych zabezpieczeń, które można stosować, w przypadku gdy dane osobowe przekazywane z EOG są dalej zbierane na podstawie ustawy o statystyce na potrzeby przetwarzania danych przez instytucje publiczne, zwłaszcza w odniesieniu do wykonywania praw indywidualnych przez osoby, których dane dotyczą, zgodnie z art. 89 ust. 2 RODO, o ile nie istnieje prawdopodobieństwo, że takie prawa uniemożliwią lub poważnie utrudnią osiągnięcie określonych celów, a te wyjątki nie są konieczne do wypełnienia tych celów.

58. W tym kontekście wydaje się, że stosowanie art. 4 PIPA również do tego rodzaju przetwarzania danych daje odpowiednie zapewnienia, jednak EROD z zadowoleniem przyjęłaby dodatkowe informacje i objaśnienia w decyzji stwierdzającej odpowiedni stopień ochrony dotyczące szczególnych obowiązków nałożonych, na podstawie art. 58 ust. 4 PIPA, na takie przetwarzanie danych, mianowicie w odniesieniu do minimalizacji danych, ograniczonego zatrzymywania danych, środków bezpieczeństwa i rozpatrywania skarg.

[21] Zob. także pkt 38 powyżej.

59. Po drugie częściowe odstępstwo obejmuje dane osobowe zbierane lub żądane na potrzeby analizy informacji w związku z bezpieczeństwem narodowym. EROD ma świadomość, że w sprawach bezpieczeństwa narodowego państwa mają szeroki margines swobody uznany przez ETPC. EROD dostrzega także, że zgodnie z art. 37 ust. 2 konstytucji Korei jakiekolwiek ograniczenie wolności i praw, na przykład gdy jest to konieczne dla ochrony bezpieczeństwa narodowego, nie może naruszać istoty danej wolności lub danego prawa. Ponadto EROD dostrzega zabezpieczenia określone w sekcji 6 obwieszczenia nr 2021-1 dotyczące przetwarzania danych osobowych do celów bezpieczeństwa narodowego, w tym egzekwowania przepisów i ścigania naruszeń przepisów. W tym kontekście jednak EROD wzywa Komisję Europejską do dokładniejszego objaśnienia zakresu odstępstw, ponieważ zastanawia się, czy wszystkie odstępstwa przewidziane w art. 58 ust. 1 lit. 2 PIPA (rozdziały III–VII) mają znaczenie dla pracy służb wywiadowczych i czy zapewniają równoważność z zasadami konieczności (niezbędności) i proporcjonalności. W szczególności EROD wzywa Komisję Europejską do przedstawienie dodatkowych objaśnień dotyczących tego, w jakich okolicznościach służba wywiadowcza może korzystać z tych odstępstw. EROD uważa, że koniecznie trzeba monitorować wpływ tych ograniczeń w praktyce, szczególnie na skuteczne wykonywanie i egzekwowanie praw osób, których dane dotyczą.

60. Po trzecie, częściowe odstępstwo ma zastosowanie do „*danych osobowych przetwarzanych tymczasowo, gdy jest to pilnie konieczne dla zapewnienia bezpieczeństwa publicznego i ochrony, zdrowia publicznego itp.*". Zgodnie z motywem 29 projektu decyzji Komisji Europejskiej ta kategoria jest rygorystycznie interpretowana przez PIPC i stosuje się ją wyłącznie w sytuacjach nadzwyczajnych wymagających pilnego działania, na przykład aby wykryć czynnik zakaźny lub aby ratować ofiary klęsk żywiołowych i im pomagać.

61. EROD również podkreśla, że wyjątki dotyczące stopnia ochrony danych osobowych należy interpretować rygorystycznie. Jednocześnie EROD zauważa, że ten przepis nie jest ściśle określony i nie zawiera wyczerpującej listy przykładowych sytuacji, w których przetwarzanie danych osobowych może być uznane za „*pilnie konieczne*". Na przykład EROD zastanawia się, czy międzynarodowe przekazywanie danych dotyczących zdrowia w czasie trwającej pandemii COVID-19 również wchodziłoby w zakres tego odstępstwa. Wobec powyższego EROD wzywa Komisję Europejską do przedstawienia dalszych wyjaśnień dotyczących zakresu tego odstępstwa oraz do pełnego monitorowania jego stosowania i zakresu, tak aby nie prowadził do obniżenia stopnia ochrony danych osobowych z EOG po ich przekazaniu do Korei na podstawie decyzji stwierdzającej odpowiedni stopień ochrony.

62. Wreszcie częściowe odstępstwo ma zastosowanie do danych osobowych zbieranych lub wykorzystywanych na potrzeby działalności informacyjnej prasy, działalności misyjnej organizacji religijnych i nominacji kandydatów partii politycznych[22]. W odniesieniu do przetwarzania danych osobowych przez prasę na potrzeby działalności dziennikarskiej Komisja Europejska stwierdza w motywie 31 projektu decyzji, że znajdowanie równowagi między wolnością wypowiedzi a innymi prawami, w tym prawem do prywatności, jest przedmiotem ustawy o postępowaniu polubownym, środkach prawnych itp. w zakresie szkód spowodowanych relacjami prasowymi (zwanej dalej „**ustawą prasową**"), i przedstawia konkretne zabezpieczenia wynikające z ustawy prasowej. EROD wzywa jednak Komisję Europejską do pełnego monitorowania tego odstępstwa i odpowiedniego orzecznictwa w celu dopilnowania, aby równoważny stopień ochrony danych był zapewniony również w praktyce w koreańskich ramach prawnych.

[22] W związku z tym przetwarzanie danych osobowych przez organizacje religijne na potrzeby działalności misyjnej oraz przetwarzanie danych osobowych przez partie polityczne w kontekście nominowania kandydatów są również wyłączone z zakresu decyzji stwierdzającej odpowiedni stopień ochrony. Zob. również pkt 37 powyżej w sekcji 2.3.2.

3.1.3. Podstawy zgodnego z prawem i rzetelnego przetwarzania danych do prawnie uzasadnionych celów

63. Zgodnie z dokumentem roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO oraz zgodnie z RODO dane muszą być przetwarzane w sposób zgodny z prawem, rzetelny i prawnie uzasadniony. Należy odpowiednio jasno określić podstawę prawną, w ramach której można zgodnie z prawem, rzetelnie i w sposób prawnie uzasadniony przetwarzać dane osobowe. W przepisach unijnych przewidziano kilka takich uzasadnionych prawnie podstaw, w tym np. przepisy prawa krajowego, zgodę osoby, której dane dotyczą, wykonanie umowy lub prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią, które nie są nadrzędne wobec interesów osoby fizycznej.

64. PIPA – zachowując podobną strukturę co RODO – na początku (art. 3 ust. 1 i 2 PIPA) wprowadza zasadę zgodności z prawem, rzetelności i przejrzystości, a w dalszej części (art. 15–19 PIPA) określa przepisy szczegółowe dotyczące jej stosowania. W szczególności w art. 15 PIPA zawarto wykaz podstaw prawnych, które administratorzy danych osobowych mogą zastosować do zbierania danych osobowych i wykorzystywania ich w zakresie zbierania do określonego celu. Do tych podstaw prawnych należą: (1) świadoma zgoda osoby, której dane dotyczą; (2) ustawowe upoważnienie lub konieczność przestrzegania zobowiązania prawnego; (3) konieczność wykonania obowiązków instytucji publicznej; (4) konieczność egzekwowania lub wykonania umowy z osobą, której dane dotyczą; (5) konieczność ochrony życia, zdrowia lub interesów majątkowych osoby, której dane dotyczą, lub strony trzeciej przed nadchodzącym niebezpieczeństwem (a uprzedniej zgody nie da się uzyskać); (6) konieczność uzyskania uzasadnionego interesu administratora danych osobowych, który jest nadrzędny wobec interesu osoby, której dane dotyczą.

65. Ponadto art. 17 PIPA zawiera wykaz podstaw prawnych mających zastosowanie do przekazywania danych osobowych stronom trzecim; w wykazie tym są: (1) świadoma zgoda osoby, której dane dotyczą; (2) ustawowe upoważnienie lub konieczność przestrzegania zobowiązania prawnego; (3) konieczność wykonania obowiązków instytucji publicznej; oraz (4) konieczność ochrony życia, zdrowia lub interesów majątkowych osoby, której dane dotyczą, lub strony trzeciej przed nadchodzącym niebezpieczeństwem (a uprzedniej zgody nie da się uzyskać). Nawet w przypadku braku zgody osoby, której dane dotyczą, przekazanie danych osobowych jest dozwolone, jeśli odbywa się w zakresie racjonalnie związanym z celami, dla których dane osobowe zostały pierwotnie zebrane (art. 17 ust. 4 PIPA).

66. W art. 18 PIPA określono szczegółowe zasady wykorzystania i przekazywania danych osobowych, w przypadku gdy odbywa się to poza zakresem pierwotnego powodu zbierania lub przekazania danych. Również w tym przypadku jedną z zasad dopuszczających jest m.in. zgoda.

67. Choć EROD uznaje zasadnicze podobieństwo między prawem koreańskim a RODO pod względem zasady zgodności z prawem i istnienia ogólnego prawa do zawieszenia (art. 37 PIPA), na które można się powołać również w przypadku przetwarzania danych osobowych na podstawie zgody, EROD zwraca uwagę na brak ogólnego prawa do wycofania zgody na podstawie PIPA[23]. W świetle znaczenia zgody jako podstawy prawnej we wszystkich wyżej opisanych scenariuszach oraz biorąc pod uwagę

[23] Nawet mimo że osoby, których dane dotyczą, mogą odmówić zgody w określonych okolicznościach, zob. np. art. 18 ust. 3 pkt 5 PIPA. Natomiast prawo do wycofania zgody istnieje tylko w określonych przypadkach; na podstawie art. 27 ust. 1 pkt 2 PIPA osoby, których dane dotyczą, mają prawo do wycofania zgody, w przypadku gdy nie chcą, aby ich dane osobowe były przekazywane stronom trzecim w wyniku przeniesienia części lub całości działalności administratora danych osobowych, połączenia itp.; na podstawie art. 39 ust. 7 PIPA użytkownicy mogą wycofać zgodę na zbieranie, wykorzystanie i przekazywanie danych osobowych wobec podmiotu świadczącego usługi informacyjne i komunikacyjne itp.; na podstawie art. 37 CIA osoba fizyczna, której dotyczą informacje kredytowe, może wycofać zgodę udzieloną uprzednio podmiotowi przekazującemu/wykorzystującemu informacje kredytowe.

rolę praw indywidualnych w prawnym systemie ochrony danych na potrzeby zabezpieczenia podstawowych praw i wolności osób, których dane dotyczą, EROD zwraca się do Komisji Europejskiej o dalszą ocenę skutków braku ogólnego prawa do wycofania zgody na podstawie prawa koreańskiego oraz o przedstawienie dalszych zapewnień, że w każdym przypadku gwarantowany jest zasadniczy stopień ochrony danych odpowiadający stopniowi ochrony zapewnianemu na mocy RODO, również, jeśli to konieczne, poprzez wyjaśnienie roli prawa do zawieszenia w tym konkretnym kontekście.

3.1.4. Zasada ograniczenia celu

68. Dokument roboczy dotyczący odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO, zgodnie z RODO, stanowi, że dane osobowe należy przetwarzać w określonym celu, a następnie wykorzystywać tylko w takim zakresie, w jakim nie jest to niezgodne z celem przetwarzania.

69. Zgodnie z art. 3 ust. 1 i 2 PIPA administratorzy danych osobowych wyraźnie określają cele przetwarzania danych oraz zapewniają zgodność przetwarzania z tymi celami. Chociaż ta zasada została potwierdzona w innych przepisach (tj. art. 15 ust. 1, art. 18 ust. 1 i art. 19 ust. 1 PIPA), w pewnych okolicznościach dozwolone jest przetwarzanie do celów „racjonalnie powiązanych" (zob. art. 17 ust. 4 PIPA)[24], jak również wykorzystywanie i udostępnianie danych osobowych poza zakresem pierwotnego powodu ich zbierania (zob. art. 18 i 19 PIPA)[25].

70. EROD rozumie, że w przypadku przekazywania danych osobowych z EOG do Republiki Korei na podstawie decyzji stwierdzającej odpowiedni stopień ochrony cel gromadzenia danych przez administratorów z EOG jest celem przekazywania danych mającym zastosowanie do przetwarzania danych przez otrzymującego je administratora danych osobowych z siedzibą w Korei. Zmiana celu przez administratora danych z Korei jest dopuszczalna jedynie na podstawie art. 18 ust. 2 lit. 1–3 PIPA, *„chyba że takie działanie mogłoby niesłusznie naruszyć interes osoby, której dane dotyczą, lub osoby trzeciej"*[26]. W tym kontekście EROD przyjmuje do wiadomości oświadczenie Komisji Europejskiej w motywie 55 projektu decyzji, że w przypadku gdy zmiany celu są dozwolone przez prawo, przepisy takie muszą respektować podstawowe prawo do prywatności i ochrony danych. EROD zauważa jednak, że nie przedstawiono żadnych konkretnych informacji na poparcie tego oświadczenia, np. nie odniesiono się do art. 37 (koreańskiej) konstytucji. Dlatego też EROD wzywa Komisję Europejską do przedstawienia dalszych zapewnień i gwarancji w projekcie decyzji, aby zagwarantować, że wszelkie przepisy zezwalające na zmianę celu przetwarzania danych będą uwzględniały podstawowe prawa i wolności osób, których dane dotyczą, w zakresie prywatności i ochrony danych.

3.1.5. Jakość danych i zasada proporcjonalności

71. W dokumencie roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO stwierdza się, że dane powinny być prawidłowe oraz, w razie konieczności, uaktualniane. Dane powinny być adekwatne, stosowne i nienadmierne w stosunku do celów ich przetwarzania.

72. Zgodnie z PIPA administratorzy danych osobowych muszą zapewnić, aby dane osobowe były prawidłowe, kompletne i aktualne w zakresie niezbędnym do realizacji celów ich przetwarzania (art. 3 ust. 3 PIPA). Administratorzy danych osobowych są zobowiązani do gromadzenia jedynie takiej ilości danych osobowych, która jest niezbędna do osiągnięcia danego celu. Na nich spoczywa ciężar dowodu w tym zakresie (art. 16 ust. 1 PIPA).

[24] W takim przypadku zgodność z celem musi zostać stwierdzona wcześniej na podstawie kryteriów określonych w art. 14-2 dekretu wykonawczego w sprawie PIPA.
[25] Zob. także powyżej pkt 66.
[26] Art. 18 ust. 2 PIPA.

73. W tym kontekście EROD podziela ocenę Komisji Europejskiej dotyczącą merytorycznej równoważności stopnia ochrony w ramach PIPA w stosunku do RODO w tym zakresie.

3.1.6. Zasada zatrzymywania danych

74. Zgodnie z dokumentem roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO dane co do zasady nie powinny być przechowywane przez okres dłuższy, niż jest to niezbędne do celów przetwarzania tych danych. Zgodnie z art. 21 ust. 1 PIPA ta zasada istnieje również w prawie koreańskim. Zgodnie z PIPA administratorzy danych osobowych są zobowiązani do niezwłocznego zniszczenia danych osobowych, gdy stają się one zbędne po upływie okresu zatrzymywania lub po osiągnięciu zamierzonego celu przetwarzania, chyba że zastosowanie mają ustawowe okresy zatrzymywania danych.

75. EROD ma jednak obawy dotyczące faktu, że art. 21 ust. 1 PIPA nie ma zastosowania do spseudonimizowanych danych osobowych. EROD zwraca uwagę, że zgodnie z sekcją 4 ppkt (iii) obwieszczenia nr 2021-1 „*w przypadku gdy administrator danych osobowych przetwarza spseudonimizowane dane w celu zbierania danych statystycznych, prowadzenia badań naukowych, przechowywania rejestrów publicznych itp. i jeśli spseudonimizowane dane nie zostały* [sic]*zniszczone po wypełnieniu konkretnego celu przetwarzania zgodnie z art. 37 konstytucji i art. 3 (Zasady ochrony danych osobowych) ustawy, powinien on dokonać anonimizacji tych danych w celu zapewnienia, aby nie umożliwiały one identyfikacji konkretnej osoby, samodzielnie lub w połączeniu z innymi danymi, należycie uwzględniając czas, koszty, technologię itp., zgodnie z art. 58 ust. 2 PIPA*". Biorąc pod uwagę, również w tym przypadku, znaczenie obwieszczenia nr 2021-1, oraz w celu uzyskania pewności prawnej co do równoważności stopnia ochrony danych osobowych przekazywanych do Republiki Korei na mocy decyzji stwierdzającej odpowiedni stopień ochrony EROD ponownie wzywa Komisję Europejską do przedstawienia dalszych informacji dotyczących w szczególności sposobu nadania obwieszczeniu nr 2021-1 wiążącego charakteru oraz zapewnienia jego wykonalności i ważności[27].

3.1.7. Zasada bezpieczeństwa i poufności

76. Jak opisano w dokumencie roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO zasada bezpieczeństwa i poufności wymaga od podmiotów przetwarzających dane upewnienia się, że dane osobowe są przetwarzane w sposób zapewniający ich bezpieczeństwo, w tym ochronę przed nieuprawnionym lub niezgodnym z prawem przetwarzaniem danych oraz przed ich przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych. Poziom bezpieczeństwa powinien uwzględniać aktualny stan wiedzy i związane z tym koszty.

77. Komisja Europejska opisała podobną zasadę bezpieczeństwa danych w art. 3 ust. 4 PIPA, która została doprecyzowana w art. 29 PIPA. Ponadto przepisy dotyczące bezpieczeństwa danych mają zastosowanie, w przypadku gdy administrator danych osobowych angażuje „podmiot zewnętrzny". Bezpieczeństwo przetwarzania danych musi być zapewnione poprzez techniczne i zarządcze zabezpieczenia, które muszą zostać również uwzględnione w wiążącej umowie o przetwarzaniu danych (art. 26 PIPA i art. 28 dekretu wykonawczego w sprawie PIPA). Ponadto, zgodnie z PIPA, w przypadku naruszenia ochrony danych zastosowanie mają szczególne obowiązki, w tym obowiązek powiadomienia dotkniętych naruszeniem osób, których dane dotyczą, oraz organu nadzorczego, jeżeli liczba dotkniętych naruszeniem osób przekracza obowiązujący próg (art. 34 PIPA w związku z art. 39 dekretu prezydenckiego w sprawie PIPA), z wyjątkiem sytuacji, gdy dane, których dotyczy naruszenie, to spseudonimizowane dane osobowe przetwarzane do celów statystycznych, badań naukowych lub

[27] Zob. także powyżej sekcja 3.1.1.1 pkt 51 niniejszej opinii, a także pkt. 52, w którym przedstawiono ogólne obawy EROD dotyczące skutków pseudonimizacji na podstawie prawa koreańskiego.

archiwizacji w interesie publicznym (art. 28 ust. 7 PIPA). Również w tym przypadku[28] EROD jest zaniepokojona szerokim zakresem odstępstw dotyczących spseudonimizowanych danych i ponownie wzywa Komisję Europejską do dalszej oceny tego aspektu, aby zapewnić merytorycznie równoważny stopień ochrony danych w prawie koreańskim[29].

78. Mimo to, w ujęciu łącznym EROD jest zadowolona z oceny i wniosków Komisji Europejskiej dotyczących merytorycznej równoważności prawa koreańskiego w zakresie zasady bezpieczeństwa i poufności.

3.1.8. Zasada przejrzystości

79. Zgodnie z art. 5 ust. 1 lit. a) RODO przejrzystość jest podstawową zasadą unijnego systemu ochrony danych osobowych. Motyw 39 RODO określa kluczową funkcję tej zasady, wskazując, że „*dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane*. *(...) Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem*".

80. W dokumencie roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO wyraźnie wymieniono „przejrzystość" jako jedną z zasad dotyczących treści, które należy uwzględnić podczas oceny merytorycznie równoważnego stopnia ochrony zapewnianego przez państwo trzecie. Dokładnie rzecz ujmując, stanowi ona, że „*każda osoba fizyczna powinna być informowana o wszystkich głównych elementach przetwarzania jej danych osobowych w jasnej, łatwo dostępnej, zwięzłej, przejrzystej i zrozumiałej formie*. *Informacje takie powinny obejmować cel przetwarzania danych, tożsamość administratora danych, przyznane mu prawa oraz inne informacje w zakresie, w jakim jest to niezbędne do zapewnienia rzetelności. W pewnych okolicznościach możliwe są wyjątki od tego prawa do informacji, np. w celu zabezpieczenia postępowania przygotowawczego, ze względu na bezpieczeństwo narodowe, niezależność sądów i dobro postępowania sądowego lub z uwagi na inne ważne cele leżące w ogólnym interesie publicznym, jak w przypadku art. 23 RODO*".

81. Podobnie jak w przypadku RODO, w ramach PIPA obowiązuje ogólna zasada przejrzystości, zgodnie z którą administratorzy danych osobowych są zobowiązani do publicznego udostępnienia swojej polityki prywatności i innych informacji związanych z przetwarzaniem danych osobowych (art. 3 ust. 5 PIPA). Szczególne obowiązki informacyjne mają zastosowanie, gdy administratorzy danych osobowych starają się uzyskać zgodę od osób, których dane dotyczą, na gromadzenie i przetwarzanie danych osobowych (art. 15 ust. 2 PIPA), na udostępnianie danych osobowych stronie trzeciej (art. 17 ust. 2 PIPA) oraz na przetwarzanie poza zakresem pierwotnego celu (art. 18 ust. 3 PIPA). Warto zauważyć, że te obowiązki informacyjne stosuje się odpowiednio również do podmiotu zewnętrznego, któremu zlecono przetwarzanie danych (art. 26 ust. 7 PIPA).

82. EROD uznaje i z zadowoleniem przyjmuje dodatkowe zabezpieczenia określone w sekcji 3 ppkt (i) i (ii) obwieszczenia nr 2021-1[30] dotyczące informacji, jakie należy przekazać osobom, których dane dotyczą, gdy ich dane są przekazywane przez podmiot z EOG, biorąc pod uwagę, że zgodnie z art. 20 ust. 1 PIPA, gdy dane nie zostały uzyskane od osoby, której dane dotyczą, osoby, których dane dotyczą, są informowane jedynie na wniosek, natomiast ogólne prawo do bycia informowanym jest uznawane na mocy art. 20 ust. 2 PIPA jedynie w przypadku, gdy niektóre operacje przetwarzania przekraczają progi określone w dekrecie wykonawczym w sprawie PIPA (art. 15 ust. 2).

[28] Jak już określono w pkt 51–52 powyżej oraz w sekcji 3.1.1.1 niniejszej opinii.
[29] Zob. także sekcje 3.1.6 i 3.1.10 niniejszej opinii.
[30] Załącznik I do projektu decyzji.

83. Ogólnie rzecz biorąc, EROD wyraża zadowolenie z faktu, że stopień ochrony przewidziany w prawie koreańskim w odniesieniu do zasady przejrzystości jest merytorycznie równoważny ze stopniem zapewnionym na podstawie RODO.

3.1.9. Szczególne kategorie danych osobowych

84. Aby system ochrony danych państwa trzeciego mógł zostać uznany za zapewniający stopień ochrony danych osobowych merytorycznie równoważny ze stopniem określonym w RODO, musi on uwzględniać szczegółowe zabezpieczenia w przypadku szczególnych kategorii danych osobowych w rozumieniu art. 9 i 10 RODO.

85. Na mocy PIPA przepisy szczególne mają zastosowanie do przetwarzania tzw. danych wrażliwych, do których należą dane osobowe ujawniające ideologię, przekonania, przynależność do związków zawodowych lub partii politycznych albo wystąpienie z nich, poglądy polityczne, stan zdrowia, życie seksualne oraz inne dane osobowe, które mogą w znaczący sposób zagrażać prywatności jakiejkolwiek osoby, której dane dotyczą, jak również, poprzez odniesienie do dekretu wykonawczego w sprawie PIPA, informacje DNA uzyskane w wyniku badań genetycznych, dane dotyczące karalności; dane osobowe wynikające ze specjalnego technicznego przetwarzania danych dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej w celu jednoznacznego zidentyfikowania tej osoby; oraz dane osobowe ujawniające pochodzenie rasowe lub etniczne.

86. Podobnie jak RODO, koreańskie prawo ochrony danych zabrania przetwarzania danych wrażliwych, chyba że mają zastosowanie szczególne odstępstwa polegające na (1) poinformowaniu osoby, której dane dotyczą, i uzyskaniu szczegółowej zgody oraz (2) przepisach prawnych zezwalających na przetwarzanie danych (art. 23 ust. 2 PIPA).

87. Na tej podstawie EROD zasadniczo zgadza się z wnioskami Komisji Europejskiej dotyczącymi merytorycznej równoważności prawa koreańskiego w odniesieniu do przetwarzania szczególnych kategorii danych osobowych. EROD pragnie jednak zauważyć, że nie dostarczono jej podręcznika dotyczącego PIPA ani wyjaśnień PIPC dotyczących interpretacji terminu „życie seksualne" jako obejmującego również orientację seksualną lub preferencje seksualne danej osoby, które to wyjaśnienia nie zostały uwzględnione w obwieszczeniu nr 2021-1. EROD wzywa zatem Komisję Europejską do przekazania tych informacji w celu umożliwienia ich niezależnej oceny. Ponadto EROD zwraca się do Komisji Europejskiej o wskazanie konkretnych dokumentów, w których można znaleźć informacje na ten temat.

3.1.10. Prawo dostępu do danych, sprostowania ich, usunięcia ich i sprzeciwu wobec ich przetwarzania

88. W koreańskich ramach prawnych prawa osób, których dane dotyczą, zostały uwzględnione w art. 3 ust. 5 PIPA, zgodnie z którym administrator danych osobowych gwarantuje prawa osób, których dane dotyczą, wymienione w art. 4 PIPA i doprecyzowane w art. 35–37, art. 39 i art. 39 ust. 2 PIPA, a w odniesieniu do „osobowych informacji kredytowych" (tj. informacji kredytowych, czyli informacji niezbędnych do określenia zdolności kredytowej stron transakcji finansowych lub handlowych – zob. motyw 3 projektu decyzji), w art. 37, art. 38 i art. 38 ust. 3 CIA.

89. EROD zauważa, że prawo dostępu (oraz prawo do sprostowania i usunięcia danych, z którego może skorzystać „*osoba, której dane dotyczą, która uzyskała dostęp do swoich danych osobowych zgodnie z art. 35*" PIPA) może zostać ograniczone lub wyłączone, „*jeżeli dostęp jest zabroniony lub ograniczony przez ustawy*", „*gdy dostęp może spowodować zagrożenie życia lub zdrowia osoby trzeciej albo nieuzasadnione naruszenie majątku lub innych interesów jakiejkolwiek osoby*", a ponadto w przypadku instytucji publicznych, gdy udzielenie dostępu „*spowodowałoby poważne trudności*"

w pełnieniu określonych funkcji, doprecyzowanych w art. 35 ust. 4 PIPA[31]. Podobne przepisy zawiera również art. 37 PIPA dotyczący prawa do zawieszenia przetwarzania danych osobowych.

90. Art. 23 RODO przewiduje, że prawo Unii lub prawo państwa członkowskiego może ograniczyć prawa osoby fizycznej, gdy takie ograniczenie respektuje istotę podstawowych praw i wolności oraz jest niezbędnym i proporcjonalnym środkiem w demokratycznym społeczeństwie, oraz przewiduje takie ograniczenia w celu zabezpieczenia m.in. ochrony osoby, której dane dotyczą, lub praw i wolności innych osób oraz *„funkcji kontrolnych, inspekcyjnych lub regulacyjnych związanych, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a)– e) i g) tego samego artykułu*".

91. W tym kontekście EROD oczekuje ogólnych zapewnień w projekcie decyzji dotyczące konieczności spełnienia przez ustawy lub statuty ograniczające prawa osób, których dane dotyczą, wymogów konstytucji Korei, zgodnie z którymi prawa podstawowe mogą zostać ograniczone wyłącznie wtedy, gdy jest to konieczne dla zapewnienia bezpieczeństwa narodowego lub utrzymania porządku publicznego, a ograniczenie takie nie może naruszać istoty danej wolności lub prawa (art. 37 ust. 2 konstytucji Korei).

92. Ponadto, jeśli chodzi o wyjątek dotyczący *„nieuzasadnionego naruszenia majątku lub innych interesów jakiejkolwiek osoby*", EROD zaznacza, że *„oznacza to, że należy zachować równowagę pomiędzy konstytucyjnie chronionymi prawami i wolnościami jednostki, z jednej strony, a prawami i wolnościami innych osób, z drugiej strony"*[32]; wzywa jednak Komisję Europejską do pełnego monitorowania stosowania tego wyjątku i odpowiedniego orzecznictwa w celu zapewnienia, aby równoważny stopień ochrony praw osób, których dane dotyczą, był zagwarantowany również w praktyce na gruncie koreańskich ram prawnych.

93. Z tego samego względu EROD oczekuje uważnego monitorowanie stosowania wyjątku dotyczącego organów publicznych, w szczególności w odniesieniu do przypadków, w których udzielenie dostępu zostałoby uznane za powodujące *„poważne trudności*" w wykonywaniu ich obowiązków, biorąc pod uwagę, że znaczenie tego wyrażenia wydaje się być szersze niż w innych przepisach PIPA, np. w art. 18 ust. 2 lit. 5[33], i powinno być interpretowane zawężająco, aby uniknąć nieuzasadnionego ograniczenia praw osób, których dane dotyczą.

94. Ponadto EROD zastanawia się, czy wyjątki, zgodnie z którymi przepisy dotyczące przejrzystości na żądanie (art. 20 PIPA) i praw jednostki (art. 35-37 PIPA) – a także podobne przepisy dotyczące wymogów dla dostawców usług informacyjnych i komunikacyjnych (art. 39 ust. 2, art. 39 ust. 6–8 PIPA) oraz te zawarte w CIA (zob. wyjątki przewidziane w art. 40 ust. 3 CIA) – nie mają zastosowania w odniesieniu do danych spseudonimizowanych, gdy są one przetwarzane do celów statystyk, badań naukowych lub archiwizacji w interesie publicznym (art. 28 ust. 7 PIPA); czy są zgodne z zabezpieczeniami przewidzianymi w europejskich ramach prawnych.

95. Przepisy te wydają się wprowadzać ogólny wyjątek w przypadku tego rodzaju przetwarzania, podczas gdy RODO przewiduje, że w przypadku gdy dane osobowe (w tym spseudonimizowane dane osobowe) są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych, prawo Unii lub prawo państwa członkowskiego może przewidywać wyjątki w odniesieniu do praw osoby, której dane dotyczą, ale tylko *„jeżeli istniej prawdopodobieństwo, że takie prawa uniemożliwią lub*

[31] Te same warunki i odstępstwa od prawa dostępu do danych i prawa ich sprostowania przewidziane w PIPA mają zastosowanie również w odniesieniu do prawa dostępu do danych i ich sprostowania przewidzianego w CIA w odniesieniu do osobowych informacji kredytowych (przypis 135 projektu decyzji).

[32] Motyw 76 projektu decyzji.

[33] W odniesieniu do wyjątków od wykorzystywania i udostępniania danych osobowych poza zakresem pierwotnego celu ich zbierania, art. 18 ust. 2 lit. 5 PIPA odnosi się do sytuacji, w których wykonanie obowiązków przez instytucje publiczne jest *„niemożliwe*".

poważnie utrudnią osiągnięcie określonych celów, i jeżeli te wyjątki są konieczne do wypełnienia tych celów", przy czym pseudonimizacja jest tylko jednym ze środków technicznych i organizacyjnych, które należy przyjąć, aby zapewnić przestrzeganie zasady minimalizacji danych (art. 89 ust. 1 RODO).

96. Komisja Europejska uważa, że wyjątek przewidziany w art. 28 ust. 7 PIPA jest uzasadniony również w świetle art. 28 ust. 5 PIPA, na mocy którego administrator danych osobowych ma wyraźny zakaz przetwarzania danych spseudonimizowanych w celu identyfikacji konkretnej osoby fizycznej, i odwołuje się do podejścia określonego w art. 11 ust. 2 RODO (w związku z motywem 57 RODO) w odniesieniu do przetwarzania niewymagającego identyfikacji[34].

97. Zgodnie z art. 11 RODO administrator nie ma obowiązku „*zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą*," wyłącznie w celu zapewnienia zgodności z RODO, jeśli w zamierzonych celach może przetwarzać dane osobowe, które nie wymagają lub już nie wymagają identyfikacji osoby, której dane dotyczą; w takich przypadkach, gdy administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, prawa osoby, której dane dotyczą, nie mają zastosowania. Jak potwierdziła Komisja Europejska[35], RODO wymaga zatem w takich przypadkach od administratora danych „praktycznej" niemożności i zgodnie z zasadą minimalizacji danych uznaje, że żadne dodatkowe dane nie muszą być przetwarzane „ze względu na" RODO.

98. EROD uważa jednak, że sytuacja ta różni się od tej, w której administrator jest praktycznie w stanie zidentyfikować osobę, której dane dotyczą, ale nie pozwala mu na to przepis ustawowy, taki jak ten zawarty w art. 28 ust. 5 PIPA. W tym względzie EROD z zadowoleniem przyjmuje wyjaśnienia przedstawione przez PIPC w obwieszczeniu nr 2021-1[36], potwierdzające, że sekcja 3 PIPA (w tym art. 28 ust. 7) oraz wyjątek określony w art. 40 ust. 3 CIA mają zastosowanie wyłącznie w przypadku, gdy dane spseudonimizowane są przetwarzane do celów badań naukowych, statystyk lub archiwizacji w interesie publicznym. Jednak, oprócz wspomnianych już obaw związanych ze skutecznym wiążącym charakterem obwieszczenia nr 2021-1[37], EROD nadal zastanawia się, czy wyjątki przewidziane w art. 28 ust. 7 PIPA i art. 40 ust. 3 CIA można uznać za konieczne i proporcjonalne w demokratycznym społeczeństwie w zakresie, w jakim ograniczają one prawa osób, których dane dotyczą, we wszystkich przypadkach, gdy dane spseudonimizowane są przetwarzane do takich celów – tj. nawet wtedy, gdy administrator danych osobowych jest praktycznie w stanie zidentyfikować osobę, której dane dotyczą, i nie istnieje prawdopodobieństwo, że takie prawa uniemożliwią lub poważnie utrudnią osiągnięcie określonych celów.

99. W szczególności EROD obawia się, że te wyjątki nie byłyby uzasadnione i wymagałyby dalszej analizy zwłaszcza, gdyby były stosowane przez administratora danych osobowych, który dokonuje pseudonimizacji danych „*do celów statystycznych, do celów badań naukowych, do celów archiwizacji w interesie publicznym itp.*", zgodnie z art. 28 ust. 2 PIPA „*bez zgody osób, których dane dotyczą*" (i bez przekazywania informacji przewidzianych w art. 20 PIPA)[38], o ile ten administrator zachowuje

[34] Należy zauważyć, że to samo rozumowanie nie miałoby zastosowania jako takie do wyjątku przewidzianego w art. 40 ust. 3 CIA w przypadku przetwarzania spseudonimizowanych informacji kredytowych, ponieważ art. 40 ust. 2 pkt 6 przewiduje, że: „*przedsiębiorstwo informacji kredytowej itp. nie przetwarza spseudonimizowanych informacji w sposób umożliwiający identyfikację konkretnej osoby fizycznej dla jakichkolwiek celów zarobkowych lub nieuczciwych*", a zatem mogłoby zezwolić na ponowną identyfikację dla uczciwego celu, takiego jak spełnienie wniosku osoby, której dane dotyczą.

[35] Zob. motyw 82 projektu decyzji.

[36] Sekcja 4 załącznika I do projektu decyzji.

[37] Zob. sekcja 3.1.1.1 powyżej.

[38] Zob. art. 28 ust. 7 PIPA, objaśniony w obwieszczeniu nr 2021-1, zgodnie z którym niektóre zabezpieczenia ujęte w PIPA, tj. w „*art. 20, 21, 27, art. 34 ust. 1, art. 35–37, art. 39 ust. 3, art. 39 ust. 4, art. 39 ust. 6–8*", nie mają zastosowania do danych spseudonimizowanych przetwarzanych w celu opracowywania statystyk, prowadzenia badań naukowych, przechowywania rejestrów publicznych itp.

informacje umożliwiające deanonimizację. Zgodnie z RODO osoby fizyczne powinny być w stanie wykonywać swoje prawa w odniesieniu do wszelkich informacji, które umożliwiają ich identyfikację lub wskazanie, nawet jeśli informacje te są uznawane za „spseudonimizowane", chyba że zastosowanie ma wspomniany już art. 11 RODO. W tym względzie EROD zauważa, że tylko wtedy, gdy dane te są przekazywane osobom trzecim do tych samych celów statystycznych, naukowo-badawczych i archiwizacyjnych, informacje, które mogą być wykorzystane do zidentyfikowania określonej osoby fizycznej, nie powinny być włączane, a zatem tylko administrator danych osobowych, któremu przekazywane są dane spseudonimizowane zgodnie z art. 28-2 ust. 2 PIPA, prawdopodobnie „praktycznie" nie byłby w stanie zidentyfikować osoby, której dane dotyczą, bez dodatkowych informacji.

100. W skrócie, biorąc pod uwagę, że – jak uznała Komisja Europejska – *„zamiast polegać na pseudonimizacji jako ewentualnym zabezpieczeniu, w PIPA uważa się ją za warunek wstępny do przeprowadzenia pewnych działań związanych z przetwarzaniem danych do celów statystycznych, badawczych i archiwizacyjnych w interesie publicznym (takich jak możliwość przetwarzania danych bez zgody lub łączenia różnych zbiorów danych)"*[39], ale przewiduje się w takich przypadkach istotne ograniczenia praw osób, których dane dotyczą, EROD wzywa Komisję Europejską do dalszej oceny wyjątków zawartych w art. 28 ust. 7 PIPA i art. 40 ust. 3 CIA oraz do uważnego monitorowania ich stosowania i stosownego orzecznictwa[40] w celu zapewnienia, aby prawa osób, których dane dotyczą, nie były nadmiernie ograniczane, gdy dane osobowe przekazywane na mocy decyzji stwierdzającej odpowiedni stopień ochrony są przetwarzane w tych celach, biorąc pod uwagę, że w wielu przypadkach prawa te pomagają również administratorowi w zapewnieniu jakości przetwarzanych danych.

3.1.11. Ograniczenia dotyczące dalszego przekazywania danych

101. W dokumencie roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO wyjaśniono, że stopień ochrony osób fizycznych, których dane osobowe są przekazywane na mocy decyzji stwierdzającej odpowiedni stopień ochrony, nie może zostać osłabiony przez dalsze przekazywanie danych, a zatem wszelkie dalsze przekazywanie danych *„powinno być dozwolone tylko wtedy, gdy dalszy odbiorca (tj. odbiorca dalszego przekazywania danych) również podlega przepisom (w tym przepisom umownym) zapewniającym odpowiedni stopień ochrony i przestrzega odpowiednich poleceń podczas przetwarzania danych w imieniu administratora danych*".

102. Jeśli chodzi o dalsze przekazywanie danych podmiotom zewnętrznym (tj. „podmiotom przetwarzającym") mającym siedzibę w innych państwach trzecich, EROD zaznacza, że w koreańskich ramach prawnych nie istnieją żadne specjalne przepisy obejmujące takie przypadki oraz że, jak uważa Komisja Europejska[41], koreańscy administratorzy danych osobowych muszą zapewnić zgodność z przepisami PIPA dotyczącymi zleceń zewnętrznych (art. 26 PIPA) za pomocą prawnie wiążącego instrumentu i będą odpowiedzialni za dane osobowe, które zostały przekazane w ramach zlecenia zewnętrznego (art. 26 PIPA).

103. Jeśli chodzi o dalsze przekazywanie danych osobom trzecim (tj. innym administratorom danych osobowych), zgodnie z art. 17 ust. 3 PIPA koreańscy administratorzy danych osobowych muszą informować osoby, których dane dotyczą, o transgranicznym przekazaniu danych i uzyskać ich zgodę na takie przekazanie, a także *„nie mogą zawierać umów transgranicznego przekazywania danych osobowych z naruszeniem przepisów PIPA*". EROD zauważa, że ten ostatni przepis zapewni – jak uznała Komisja Europejska[42] – aby żadna umowa transgranicznego przekazywania danych osobowych nie

[39] Motyw 42 projektu decyzji.
[40] Zob. na przykład wyzwania konstytucyjne przedstawione przez Open Net (informacje na stronie https://opennet.or.kr/19909 dostępne tylko w języku koreańskim).
[41] Motyw 87 projektu decyzji.
[42] Motyw 88 projektu decyzji.

zawierała zobowiązań sprzecznych z wymogami nałożonymi przez PIPA na administratorów danych osobowych, a zatem można go uznać za zabezpieczenie; nie nakłada on jednak żadnego obowiązku wprowadzenia zabezpieczeń gwarantujących, że odbiorca danych zapewni taki sam stopień ochrony, jaki zapewnia PIPA. W związku z tym EROD uznaje, że świadoma zgoda osoby, której dane dotyczą, będzie zasadniczo stosowana jako podstawa przekazywania danych od koreańskiego administratora danych osobowych do odbiorcy w państwie trzecim.

104. W tym względzie z zadowoleniem przyjmuje się dodatkowe wyjaśnienia przedstawione przez PIPC w obwieszczeniu nr 2021-1 dotyczące obowiązku informowania osób fizycznych o państwie trzecim, do którego zostaną przekazane ich dane[43], ponieważ – jak podkreśliła Komisja Europejska[44] – pomoże to osobom, których dane dotyczą, z EOG podjąć w pełni świadomą decyzję co do tego, czy wyrazić zgodę na transgraniczne przekazanie danych.

105. Jednak, jak również zauważono w opinii 28/2018 dotyczącej projektu decyzji wykonawczej Komisji w sprawie odpowiedniej ochrony danych osobowych w Japonii, należy podkreślić, że zgodnie z RODO osoby, których dane dotyczą, muszą być wyraźnie poinformowane przed wyrażeniem zgody o możliwym ryzyku takiego przekazania wynikającym z braku odpowiedniej ochrony w państwie trzecim i braku odpowiednich zabezpieczeń. Takie powiadomienie powinno zawierać na przykład informację, że w państwie trzecim może nie być organu nadzorczego lub zasad przetwarzania danych lub praw przysługujących osobom, których dane dotyczą[45]. EROD uważa, że przedstawienie tych informacji jest kluczowe, aby umożliwić osobie, której dane dotyczą, wyrażenie świadomej zgody przy pełnej wiedzy na temat tych szczególnych okoliczności przekazania danych[46]. W związku z tym EROD ma obawy co do ustaleń Komisji Europejskiej zawartych w projekcie decyzji stwierdzającej odpowiedni stopień ochrony danych w odniesieniu do tego konkretnego rodzaju przekazywania danych. Osoby, których dane dotyczą, zazwyczaj nie znają ram ochrony danych w państwach trzecich. Dlatego też nie można uznać, że osoba, której dane dotyczą, jest w stanie ocenić ryzyko przekazania danych, znając jedynie kraj przeznaczenia. Przed wyrażeniem zgody przez osobę, której dane dotyczą, należy raczej wyraźnie poinformować ją o konkretnym ryzyku związanym z takim przekazaniem danych osobowych do kraju poza terytorium Republiki Korei.

106. EROD wzywa zatem Komisję Europejską do zapewnienia, aby informacje, które należy przekazać osobie, której dane dotyczą, „*o okolicznościach związanych z przekazywaniem*" obejmowały informacje na temat ewentualnego ryzyka związanego z przekazaniem, wynikającego z braku odpowiedniej ochrony w państwie trzecim i stosownych zabezpieczeń. Dla EROD istotne jest, aby ocenić, czy wymogi dotyczące zgody są merytorycznie równoważne z RODO.

107. Ponadto, biorąc pod uwagę, że zgoda musi być dobrowolna, świadoma, konkretna i jednoznaczna, EROD z zadowoleniem przyjęłaby zapewnienie w decyzji stwierdzającej odpowiedni stopień ochrony, że dane osobowe nie będą przekazywane od koreańskich administratorów danych osobowych do osób trzecich w państwie trzecim w każdej sytuacji, w której zgodnie z RODO nie można byłoby udzielić ważnej zgody, np. ze względu na nierównowagę sił.

108. W odniesieniu do przypadków, w których administrator danych osobowych może przekazać dane osobowe osobie trzeciej za granicą bez zgody osoby, której dane dotyczą – tj. (1) jeżeli dane osobowe są przekazywane w zakresie racjonalnie związanym z pierwotnym celem zbierania danych zgodnie z art. 17 ust. 4 PIPA; (2) jeżeli dane osobowe można przekazać osobie trzeciej w wyjątkowych przypadkach, o których mowa w art. 18 ust. 2 PIPA – EROD odnotowuje wyjaśnienia przedstawione

[43] Ibid.
[44] Ibid.
[45] Wytyczne EROD 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, 25 maja 2018 r., s. 8.
[46] Wytyczne EROD 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679, 25 maja 2018 r., s. 7.

przez PIPC w sekcji 2 obwieszczenia nr 2021-1 (i z zadowoleniem przyjmuje obowiązek nałożony na administratora z siedzibą w Korei i zagranicznego odbiorcę danych, polegający na zapewnieniu, za pomocą prawnie wiążącego instrumentu (takiego jak umowa), stopnia ochrony równoważnego z przepisami PIPA, w tym w odniesieniu do praw osoby, której dane dotyczą).

3.1.12. Marketing bezpośredni

109. Zgodnie z art. 21 ust. 2 i 3 RODO oraz dokumentem roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO osoba, której dane dotyczą, musi zawsze mieć możliwość wniesienia bezpłatnego sprzeciwu wobec przetwarzania danych do celów profilowania i marketingu bezpośredniego.

110. W odniesieniu do prawa do zawieszenia przetwarzania danych przewidzianego w art. 37 PIPA, EROD przyjmuje do wiadomości, że Komisja Europejska uważa, iż prawo to ma również zastosowanie, gdy dane są wykorzystywane do celów marketingu bezpośredniego[47]. EROD z zadowoleniem przyjęłaby jednak dodatkowe informacje i wyjaśnienia zawarte w projekcie decyzji w odniesieniu do tej oceny, a w szczególności w odniesieniu do praktycznego zastosowania prawa do zawieszenia przetwarzania danych w kontekście marketingu bezpośredniego (np. odniesienia do odpowiedniego orzecznictwa itp.). W tym względzie EROD pragnie również podkreślić, że prawo do zwrócenia się do dostawcy/użytkownika informacji kredytowych o zaprzestanie kontaktowania się z nim w celu zaprezentowania lub zachęcenia do zakupu towarów lub usług jest wyraźnie określone w CIA (art. 37 ust. 2).

111. Ponadto, jak uznała Komisja Europejska[48], w koreańskich ramach prawnych takie przetwarzanie wymaga na ogół szczegółowej (dodatkowej) zgody osoby, której dane dotyczą (zob. art. 15 ust. 1 lit. 1, art. 17 ust. 2 lit. 1 PIPA).

112. Ponieważ nie można wykluczyć, że dane osobowe przekazane z EOG mogą być przetwarzane w Korei do takich celów, EROD z zadowoleniem przyjęłaby również wyjaśnienia w decyzji stwierdzającej odpowiedni stopień ochrony danych dotyczące istnienia prawa osoby, której dane dotyczą, do wycofania zgody[49] oraz prawa do usunięcia jej danych osobowych i zaprzestania ich przetwarzania, jeżeli przetwarzanie odbywa się na podstawie zgody (np. w przypadku przetwarzania do celów marketingowych), a osoba, której dane dotyczą, wycofała zgodę.

3.1.13. Zautomatyzowane podejmowanie decyzji i profilowanie

113. Jak przyznała Komisja Europejska w swoim projekcie decyzji[50], PIPA i dekret wykonawczy w sprawie PIPA nie zawierają ogólnych przepisów dotyczących kwestii decyzji mających wpływ na osobę, której dane dotyczą, i opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych. Koreański system prawny przewiduje jednak takie prawo w CIA, która zawiera przepisy dotyczące zautomatyzowanych decyzji (art. 36 ust. 2), nawet jeśli ich stosowanie wydaje się być poza zakresem nadzoru PIPC (i jako takie poza zakresem stosowania przedmiotowego projektu decyzji – zob. sekcja 2.3.2 powyżej dotycząca zakresu stosowania projektu decyzji).

[47] Motyw 79 projektu decyzji.
[48] Ibid.
[49] Zob. także powyżej pkt 67: choć możliwość wycofania zgody jest wyraźnie przewidziana w art. 37 ust. 1 CIA, prawo to jest wymienione w PIPA tylko dwukrotnie w kontekście szczególnych okoliczności w art. 27 ust. 1 i art. 39 ust. 7.
[50] Zob. motyw 81 projektu decyzji.

114. Jak już zostało stwierdzone przez Grupę Roboczą Art. 29[51] w opinii 1/2016 w sprawie Tarczy Prywatności oraz przez EROD w jej poprzedniej opinii dotyczącej decyzji w sprawie odpowiedniej ochrony danych osobowych w Japonii[52], rosnące znaczenie zautomatyzowanego podejmowania decyzji, profilowania i sztucznej inteligencji sugerowałoby przyjęcie bardziej ochronnego podejścia w tym względzie. W przeciwieństwie do argumentów Komisji Europejskiej[53], zgodnie z którymi brak szczegółowych przepisów dotyczących zautomatyzowanego podejmowania decyzji w PIPA prawdopodobnie nie wpłynie na stopień ochrony w odniesieniu do danych osobowych, które zostały zebrane na terenie Unii (ponieważ wszelkie decyzje oparte na zautomatyzowanym przetwarzaniu byłyby zazwyczaj podejmowane przez administratora w Unii, który pozostaje w bezpośrednim związku z daną osobą, której dane dotyczą), EROD uważa, że nie można wykluczyć, iż zautomatyzowane podejmowanie decyzji mogłoby być stosowane przez administratora danych osobowych z Korei w przypadku danych przekazywanych na mocy decyzji stwierdzającej odpowiedni stopień ochrony (na przykład w kontekście zatrudnienia, w celu oceny wyników w pracy, rzetelności, postępowania itp.).

115. Rozwój nowych technologii umożliwia przedsiębiorstwom łatwiejsze wdrażanie lub rozważanie wdrożenia systemów zautomatyzowanego podejmowania decyzji, co może prowadzić do osłabienia pozycji osób fizycznych. W przypadku gdy decyzje podejmowane wyłącznie w ramach takich zautomatyzowanych systemów mają wpływ na sytuację prawną osób fizycznych lub istotnie na nie oddziałują (np. poprzez umieszczenie na czarnej liście, a tym samym pozbawianie osób fizycznych przysługujących im praw), kluczowe znaczenie ma zapewnienie wystarczających zabezpieczeń, w tym prawa do uzyskania informacji o konkretnych powodach podjęcia danej decyzji oraz o jej logice, prawa do skorygowania nieprawidłowych lub niekompletnych informacji oraz prawa do zakwestionowania decyzji, jeżeli została ona podjęta na podstawie błędnie ustalonego stanu faktycznego[54].

116. W tym kontekście EROD wyraża zaniepokojenie brakiem przepisów prawnych dotyczących zautomatyzowanego podejmowania decyzji w ustawie PIPA i w związku z tym zwraca się do Komisji Europejskiej o zajęcie się tą kwestią oraz ciągłe monitorowanie rozwoju koreańskich ram prawnych w tym zakresie.

3.1.14. Rozliczalność

117. Koreańskie ramy prawne zawierają kilka zasad mających na celu zapewnienie, aby administratorzy danych osobowych wprowadzili odpowiednie środki techniczne i organizacyjne w celu skutecznego wypełniania swoich obowiązków w zakresie ochrony danych oraz aby byli w stanie wykazać taką zgodność, m.in. przed właściwym organem nadzorczym. W szczególności EROD z zadowoleniem przyjmuje istnienie przepisów przewidujących przyjęcie wewnętrznego planu zarządzania (art. 29 PIPA), obowiązku przeprowadzenia tzw. oceny skutków dla ochrony prywatności („**PIA**") w przypadkach, gdy przetwarzanie wiąże się z wyższym ryzykiem ewentualnego naruszenia prywatności (art. 33 ust. 1 PIPA i art. 35 dekretu wykonawczego w sprawie PIPA), przepisów dotyczących szkolenia i nadzoru personelu (art. 28 PIPA), jak również obowiązku wyznaczenia inspektora ochrony prywatności (art. 31 PIPA w związku z art. 32 dekretu wykonawczego w sprawie PIPA).

118. EROD podziela pogląd Komisji Europejskiej dotyczący merytorycznie równoważnej ochrony, jaką te przepisy zapewniają – nawet w przypadkach, w których wydają się one względnie odbiegać od przepisów przewidzianych w RODO, np. nie ma przepisu stwierdzającego konieczność niezależności

[51] Tę grupę roboczą ustanowiono na mocy art. 29 dyrektywy 95/46/WE. Była ona niezależnym europejskim organem doradczym ds. ochrony danych osobowych i prywatności. Jej zadania określono w art. 30 dyrektywy 95/46/WE i w art. 15 dyrektywy 2002/58/WE. Grupa Robocza Art. 29 przekształciła się w EROD.

[52] Opinia 28/2018 dotycząca projektu decyzji wykonawczej Komisji w sprawie odpowiedniej ochrony danych osobowych w Japonii, przyjęta w dniu 5 grudnia 2018 r.

[53] Motyw 81 projektu decyzji.

[54] WP 254, s. 7.

inspektora ochrony prywatności, jednak wyraźnie określono, że musi on podlegać kierownictwu administratora danych osobowych (art. 31 ust. 4 PIPA) oraz że nie może on doznawać nieuzasadnionych niedogodności w wyniku pełnienia tych funkcji (art. 31 ust. 5 PIPA) – i sugeruje, aby Komisja Europejska monitorowała, podczas przeglądu decyzji stwierdzającej odpowiedni stopień ochrony, faktyczne stosowanie tych przepisów w celu oceny ich skutecznego wdrożenia.

3.2. Mechanizmy proceduralne i mechanizmy egzekwowania prawa

119. Na podstawie kryteriów określonych w dokumencie roboczym dotyczącym odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO EROD przeanalizowała następujące aspekty koreańskich ram ochrony danych osobowych ujętych w projekcie decyzji: istnienie skutecznie działającego niezależnego organu nadzorczego; istnienie systemu zapewniającego odpowiedni stopień zgodności i systemu dostępu do odpowiednich mechanizmów dochodzenia roszczeń zapewniającego osobom fizycznym z UE dostęp do środków pozwalających na egzekwowanie swoich praw i dochodzenie roszczeń bez napotykania uciążliwych przeszkód w korzystaniu z administracyjnych i sądowych środków dochodzenia roszczeń.

120. Zgodnie z rozdziałem VI RODO i rozdziałem 3 dokumentu roboczego dotyczącego odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO istnieć musi co najmniej jeden niezależny organ nadzorczy, którego zadaniem jest monitorowanie, zapewnianie i egzekwowanie zgodności z przepisami dotyczącymi ochrony danych i prywatności w państwie trzecim w celu zagwarantowania stopnia ochrony równoważnego temu w EOG.

121. W tym kontekście organ nadzorczy w państwie trzecim w ramach wykonywania swoich obowiązków i uprawnień musi działać przy zachowaniu całkowitej bezstronności i niezależności, a przy tym nie może zwracać się o instrukcje ani przyjmować poleceń. Dodatkowo organ nadzorczy powinien dysponować wszystkimi koniecznymi i dostępnymi uprawnieniami i delegacjami, aby zapewnić przestrzeganie praw do ochrony danych oraz propagować wiedzę. Należy również wziąć pod uwagę personel i budżet organu nadzorczego. Organ nadzorczy musi mieć także możliwość wszczynanie postępowań z urzędu.

3.2.1. Właściwy niezależny organ nadzorczy

122. W Republice Korei niezależnym organem odpowiedzialnym za monitorowanie i egzekwowanie PIPA jest PIPC. W skład PIPC wchodzą jeden przewodniczący, jeden wiceprzewodniczący i siedmiu komisarzy. Przewodniczący i wiceprzewodniczący są mianowani przez prezydenta na podstawie rekomendacji premiera. Jeśli chodzi o komisarzy, dwóch jest mianowanych z rekomendacji przewodniczącego, dwóch – z rekomendacji przedstawicieli partii politycznej, do której należy prezydent, a pozostałych trzech – z rekomendacji przedstawicieli innych partii politycznych (art. 7 ust. 2 pkt 2 PIPA). Prace PIPC obsługuje sekretariat (art. 7 ust. 13), a komisja ta może ustanawiać podkomisje (złożone z trzech komisarzy) do zajmowania się drobnymi naruszeniami i powtarzającymi się sprawami (art. 7 ust. 12 PIPA).
123. W tym sensie EROD przyznaje, że pomimo niedawnej reorganizacji dogłębnie zmieniającej status i uprawnienia tej komisji PIPC poczyniła znaczne starania, aby stworzyć konieczną infrastrukturę do wdrażania PIPA i jej najnowszych zmian. Do tych starań zaliczyć można ustanowienie regulaminu PIPC, opracowanie wytycznych zawierających wskazówki dotyczące interpretacji PIPA oraz utworzenie infolinii przekazującej podmiotom gospodarczym i osobom fizycznym porady na temat przepisów dotyczących ochrony danych, a także usługi mediacyjnej do rozpatrywania skarg. Do zadań PIPC należą w szczególności: udzielanie porad na temat ustawowych i wykonawczych przepisów odnoszących się do ochrony danych, opracowywanie polityk i wytycznych dotyczących ochrony danych, prowadzenie dochodzeń w sprawie naruszeń praw indywidualnych, rozpatrywanie skarg i prowadzenie mediacji przy rozstrzyganiu sporów, egzekwowanie zgodności z PIPA, działania edukacyjne i promocyjne

w dziedzinie ochrony danych oraz wymiana i współpraca z organami ochrony danych z państw trzecich[55].

124. Mianowanie członków i skład PIPC są opisane w art. 7 ust. 2 PIPA. Chociaż PIPC podlega jurysdykcji premiera (a przewodniczący i wiceprzewodniczący są mianowani przez prezydenta z rekomendacji premiera), ramy prawne pozwalają komisarzom na niezależne wykonywanie swoich obowiązków, zgodnie z prawem i sumieniem. EROD uznaje instytucjonalne i proceduralne zabezpieczenia zawarte w PIPA, w szczególności w art. 7 ust. 4–7. Mimo to EROD oczekuje, aby Komisja Europejska monitorowała wszelkie zmiany mogące mieć wpływ na niezależność członków tego południowokoreańskiego organu nadzorczego.

125. Ponadto projekt decyzji nie zawiera jeszcze analizy budżetu PIPC, w tym źródeł finansowania i przejrzystości budżetowej. EROD uważa, że ten element – wymieniony zarówno w art. 56 ust. 1 RODO, jak i w zasadach i mechanizmach proceduralnych i wdrożeniowych do uwzględnienia na podstawie dokumentu roboczego dotyczącego odpowiedniego stopnia przekazywanych danych osobowych na podstawie RODO przy ocenie systemu danego państwa lub organizacji międzynarodowej – należy dokładnie wziąć pod uwagę, ponieważ jest on wskaźnikiem zasobów ekonomicznych i kadrowych, którymi dysponuje organ nadzorczy w celu niezależnego wykonywania swoich ustawowych obowiązków i zadań w zakresie ochrony danych; dlatego EROD doradza Komisji Europejskiej, aby ten element uwzględnić bardziej szczegółowo w projekcie decyzji.

3.2.2. Istnienie systemu ochrony danych zapewniającego odpowiedni stopień zgodności

126. Jeśli chodzi o obszar egzekwowania przepisów, EROD dostrzega uprawnienia i sankcje PIPC w tym zakresie przewidziane w PIPA i CIA oraz bierze pod uwagę objaśnienia zwarte w obwieszczeniu nr 2021-1, zgodnie z którymi warunki określone w art. 64 ust. 1 PIPA i art. 45 ust. 4 CIA[56] będą mieć zastosowanie w przypadku naruszenia którychkolwiek z zasad, praw i obowiązków ujętych w prawie o ochronie danych osobowych. EROD zaleca jednak, aby Komisja Europejska ściśle monitorowała stosowanie w praktyce uprawnień PIPC w zakresie nakazywania sprawcom naruszeń przyjęcia środka uznanego za odpowiedni spośród środków wymienionych w art. 64 ust. 1 bądź art. 45 ust. 4 CIA.

127. Ponadto w odniesieniu do środków naprawczych przewidzianych w art. 64 ust. 1 PIPA w sytuacji nieprzestrzegania środka naprawczego PIPC ma prawo nałożyć karę pieniężną w wysokości do 50 mln KRW (art. 75 ust. 2 lit. 13 PIPA). Ta kwota stanowi równowartość 36 564 EUR. EROD obawia się, że tak ograniczony zakres sankcji pieniężnych może nie mieć szczególnie silnego skutku odstraszającego dla sprawców naruszeń, co zamierzano osiągnąć poprzez prawo w celu zapewnienia egzekwowania przepisów o ochronie danych, ponieważ taki zakres sankcji nie wydaje się wystarczająco zniechęcać, zwłaszcza dużych organizacji lub przedsiębiorstw dysponujących znacznymi środkami finansowymi.

128. W odniesieniu do możliwości żądania przez PIPC, aby dyrektor centralnej agencji administracyjnej przeprowadził dochodzenie w sprawie administratora danych osobowych lub wspólnie przeprowadził dochodzenie w sprawie naruszeń PIPA, lub nawet nałożenia środków naprawczych wobec administratorów danych osobowych podlegających ich jurysdykcji (art. 63 ust. 4–5 PIPA), EROD zauważa, że choć w motywie 122 projektu decyzji przedstawiono pewne informacje, to charakter tych innych agencji i ich relacje prawne z PIPC są, ogólnie rzecz biorąc, dość niejasne. Dodatkowo art. 68 ust. 1 PIPA odnosi się do wielu podmiotów, którym można byłoby przekazać uprawnienia PIPC. Nawet jeśli ten przepis stosowano jedynie w odniesieniu do Koreańskiej Agencji ds. Internetu i Bezpieczeństwa[57], EROD z zadowoleniem przyjęłaby objaśnienia dotyczące charakteru możliwych

[55] Zadania i uprawnienia PIPC są określone przede wszystkim w art. 7 ust. 8 i 9, a także w art. 61–66 PIPA.

[56] Tj. „*uznaje się za prawdopodobne, że naruszenie prawa będzie stanowić naruszenie praw i wolności osób fizycznych w odniesieniu do danych osobowych, a zaniechanie działania może spowodować szkodę trudną do naprawienia*”.

[57] Zob. motyw 117 projektu decyzji i art. 62 dekretu wykonawczego.

interakcji między tymi podmiotami oraz uważne monitorowanie stosowania tego przepisu w przyszłości, tak aby zapewnić niezależność podmiotów odpowiedzialnych za stosowanie przepisów o ochronie danych.

129. Jeśli chodzi o sankcje, system koreański łączy w sobie różne rodzaje sankcji, od środków naprawczych i administracyjnych kar pieniężnych po sankcje karne, które mogą mieć silny skutek odstraszający, i władze koreańskie przedstawiły kilka przykładów kar pieniężnych nałożonych ostatnio przez PIPC, m.in. karę pieniężną w wysokości 6,7 mld KRW nałożoną w grudniu 2020 r. na pewne przedsiębiorstwo za naruszenie różnych przepisów PIPA oraz karę pieniężną w wysokości 103,3 mln KRW nałożoną w dniu 28 kwietnia 2021 r. na przedsiębiorstwo zajmujące się technologią sztucznej inteligencji za naruszenie zasad zgodności przetwarzania z prawem, zwłaszcza uzyskania zgody, oraz zasad przetwarzania danych spseudonimizowanych.

130. Choć powyższe kwoty mogą działać odstraszająco, EROD oczekuje dodatkowych informacji na temat metody stosowanej przez PIPC do obliczania wysokości administracyjnych kar pieniężnych, na przykład w przypadku kar pieniężnych nakładanych za nieprzestrzeganie środka naprawczego określonego na podstawie art. 64 ust. 1 PIPA (zob. art. 75 ust. 2 lit. 13 PIPA). Ma to szczególnie duże znaczenie w odniesieniu do sankcji karnych i stosowania koreańskiego kodeksu karnego.

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

131. Jeśli chodzi o dochodzenie roszczeń, system koreański daje różne możliwości zapewnienia odpowiedniej ochrony oraz, w szczególności, egzekwowania praw indywidualnych dzięki skutecznym administracyjnym i sądowym środkom dochodzenia roszczeń, w tym odszkodowaniom za szkody.

132. System koreański oferuje też alternatywne mechanizmy, które osoby fizyczne mogą wykorzystać w dochodzeniu roszczeń – oprócz środków administracyjnych i sądowych – jak wyjaśniono w motywach 132 i 133 projektu decyzji, odnoszących się, odpowiednio, do telefonicznego centrum ds. prywatności i do komitetu ds. mediacji w rozwiązywaniu sporów. Ponieważ są to dodatkowe ścieżki dochodzenia roszczeń, EROD z zadowoleniem przyjęłaby bardziej szczegółowe wyjaśnienia, w jaki sposób dopełniają one możliwości dochodzenia roszczeń przed PIPC i sądami dla osób, których dane dotyczą i których dane osobowe są przekazywane do Korei na mocy decyzji stwierdzającej odpowiedni stopień ochrony.

4. DOSTĘP ORGANÓW PUBLICZNYCH W KOREI POŁUDNIOWEJ DO DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UNII EUROPEJSKIEJ ORAZ ICH WYKORZYSTANIE PRZEZ TE ORGANY

133. Jeśli chodzi o ocenę stopnia ochrony danych w obszarze egzekwowania prawa i bezpieczeństwa narodowego, Komisja Europejska przedstawiła pełne informacje w projekcie decyzji i udostępnionych załącznikach. W związku z tym EROD nie powtarza w niniejszej opinii większości ustalonych faktów i ocen.

134. Komisja Europejska stwierdza, że w wyżej wskazanych obszarach istniejący stopień ochrony danych odpowiada wymogom określonym w orzecznictwie TSUE i dlatego może być uznany za merytorycznie równoważny ze stopniem ochrony danych w Unii Europejskiej.

135. Ogólnie rzecz ujmując, EROD pragnie podkreślić, że nawet w przypadku gdy wydaje się mało prawdopodobne lub gdy Komisja Europejska uważa za mało prawdopodobne, że do danych przekazywanych z UE do Korei Południowej odnosić się będą stosowne przepisy prawa koreańskiego,

nadal należy dokonać oceny odpowiedniości stopnia ochrony danych w Korei w odniesieniu do takich przypadków. O stosowności przepisów świadczy też fakt, że sama Komisja Europejska odniosła się do nich w projekcie decyzji.

4.1. Ogólne ramy ochrony danych w kontekście dostępu organów rządowych

136. Jeśli chodzi o dostęp organów publicznych do danych osobowych, aby ocenić stopień ochrony prawa do ochrony prywatności i danych, należy przeanalizować różne koreańskie przepisy ustawowe. Po pierwsze, EROD zwraca uwagę, że PIPA – kluczowa ustawa dotycząca ochrony danych – ma w zamierzeniu szeroki zakres stosowania. Jednak, choć PIPA ma w pełni zastosowanie do obszaru egzekwowania prawa, stosowanie tej ustawy do przetwarzania danych na potrzeby bezpieczeństwa narodowego jest ograniczone. Zgodnie z art. 58 ust. 1 lit. 2 PIPA rozdziały III–VII nie mają zastosowania do przetwarzania danych na potrzeby bezpieczeństwa narodowego. Natomiast rozdziały I, II, IX i X nadal stosuje się do obszaru bezpieczeństwa narodowego. W związku z tym podstawowe zasady PIPA, a także podstawowe gwarancje dotyczące praw osób, których dane dotyczą, oraz przepisy w zakresie nadzoru, egzekwowania przepisów i środków prawnych mają zastosowanie do dostępu organów ds. bezpieczeństwa narodowego do danych osobowych i ich wykorzystywania przez te organy.

137. Również w konstytucji Korei Południowej zapisano podstawowe zasady ochrony danych, mianowicie zasady legalności, konieczności i proporcjonalności. Te zasady mają też zastosowanie do dostępu organów publicznych Korei Południowej do danych osobowych w obszarach egzekwowania prawa i bezpieczeństwa narodowego[58].

138. W obszarze egzekwowania prawa policja, prokuratorzy, sądy i inne organy publiczne mogą zbierać dane osobowe na podstawie określonych przepisów, mianowicie ustawy w sprawie postępowania karnego („**CPA**"), ustawy o ochronie prywatności w sektorze łączności („**CPPA**"), ustawy o działalności telekomunikacyjnej („**TBA**") oraz ustawy o przekazywaniu i wykorzystaniu określonych informacji o transakcjach finansowych („**ARUSFTI**"), którą stosuje się do ścigania prania pieniędzy i finansowania terroryzmu oraz zapobiegania takim działaniom. W powyższych szczegółowych przepisach ustawowych określono dalsze ograniczenia, zabezpieczenia i odstępstwa.

139. W obszarze bezpieczeństwa narodowego krajowa służba wywiadowcza („**NIS**") może – na podstawie ustawy o krajowej służbie wywiadowczej („**NISA**") i dodatkowych „ustawowych przepisów dotyczących bezpieczeństwa narodowego"[59] – zbierać dane osobowe i przechwytywać komunikację. EROD przyjmuje, że NIS przy wykonywaniu swoich uprawnień musi przestrzegać powyższych przepisów prawnych oraz PIPA.

140. EROD zwraca się do Komisji o wyjaśnienie, czy oprócz NIS istnieją w Korei inne organy odpowiedzialne za bezpieczeństwo narodowe, jako że w sekcji 6 załącznika I przedstawiony przez Komisję Europejską opis sugeruje, że NIS jest przykładową agencją bezpieczeństwa narodowego.

4.2. Ochrona i zabezpieczenia danych potwierdzających łączność w kontekście dostępu organów rządowych do danych na potrzeby egzekwowania prawa

141. Na podstawie odpowiednich przepisów (CPPA) organy ścigania mogą przyjmować dwa rodzaje środków w zakresie dostępu do informacji dotyczących łączności. W CPPA rozróżnia się między środkami ograniczającymi komunikację, obejmującymi zbieranie treści zwykłych przesyłek pocztowych

[58] Zob. motyw 145 projektu decyzji.

[59] Do ustawowych przepisów dotyczących bezpieczeństwa narodowego należą na przykład ustawa o ochronie prywatności w sektorze łączności, ustawa o zwalczaniu terroryzmu w celu ochrony obywateli i bezpieczeństwa publicznego bądź ustawa o działalności telekomunikacyjnej.

i bezpośrednie przechwytywanie treści telekomunikacyjnych[60], a zbieraniem tak zwanych danych potwierdzających łączność. Ten drugi rodzaj danych obejmuje datę połączeń telekomunikacyjnych, czas ich rozpoczęcia i zakończenia, liczbę połączeń wychodzących i przychodzących oraz numer abonenta drugiej strony, częstotliwość korzystania z usług, rejestry korzystania z usług telekomunikacyjnych i informacje o lokalizacji[61].

142. EROD zauważa, że dane potwierdzające łączność nie wiążą się z takimi samymi zabezpieczeniami co dane zbierane w ramach środków ograniczających komunikację, tj. dane dotyczące treści. EROD zwraca uwagę, że w przypadku zbierania treści istnieje więcej zabezpieczeń niż w przypadku zbierania danych potwierdzających łączność na potrzeby egzekwowania prawa: po pierwsze, w przeciwieństwie do zbierania danych dotyczących treści zbieranie danych potwierdzających łączność nie jest ograniczone do ścigania niektórych poważnych przestępstw, ale może mieć miejsce, gdy zostanie to uznane za konieczne do prowadzenia „jakiegokolwiek dochodzenia lub wykonania jakiejkolwiek kary" (art. 13 ust. 1 CPPA). Po drugie, zbieranie danych potwierdzających łączność co do zasady nie stanowi środka ostatecznego i może być wykorzystane, gdy tylko jest trudno w inny sposób zapobiec popełnieniu przestępstwa, aresztować przestępców lub zebrać dowody[62]. Dane potwierdzające łączność można zbierać, gdy prokurator lub sądowy funkcjonariusz policji „uzna to za konieczne" dla ścigania przestępstwa lub wykonania kary. Istnieje jednak wyjątek w tym względzie w odniesieniu do danych monitorujących w czasie rzeczywistym i danych potwierdzających łączność dotyczących konkretnej stacji bazowej, przewidziany w art. 13 ust. 2 CPPA. Po trzecie organy ścigania zbierające treść komunikacji muszą natychmiast tego zaprzestać, gdy stały dostęp przestaje być uznawany za konieczny[63]. W odniesieniu do danych potwierdzających łączność nie jest to – przynajmniej nie wyraźnie – określone ani w CPPA, ani w dekrecie wykonawczym w sprawie CPPA.

143. EROD przyjmuje do wiadomości, że zbieranie danych potwierdzających łączność może się odbywać jedynie na podstawie nakazu wydanego przez sąd. Ponadto CPPA zawiera wymóg, aby we wniosku o wydanie nakazu oraz w samym nakazie podawać szczegółowe informacje[64]. Takie uprzednie zezwolenie organu sądowego ma na celu ograniczenie uznaniowości organów ścigania w stosowaniu prawa oraz sprawdzenie, czy w każdym przypadku istnieją wystarczające powody zbierania danych potwierdzających łączność. EROD dostrzega również, że prawo Republiki Korei nie przewiduje ogólnego i niekontrolowanego zatrzymywania danych potwierdzających łączność. W związku z tym dostęp organów rządowych do takich danych zawsze dotyczy danych, które są w każdym razie zatrzymywane na potrzeby naliczania opłat i samego świadczenia usług komunikacyjnych.

144. EROD podkreśla jednak, że TSUE zakwestionował fakt, że dane o ruchu są mniej wrażliwe niż inne dane, zwłaszcza niż dane dotyczące treści[65]. Biorąc pod uwagę, że dane potwierdzające łączność mają pod wieloma względami niższy stopień ochrony niż dane dotyczące treści, EROD zwraca się do Komisji Europejskiej o dokładne monitorowanie, czy określone w prawie koreańskim zabezpieczenia dla tej

[60] Art. 3 ust. 2, art. 2 ust. 6, art. 2 ust. 7 CPPA.
[61] Art. 2 ust. 11 CPPA.
[62] Jest tak w przypadku danych dotyczących treści, zgodnie z art. 3 ust. 2 i art. 5 ust. 1 CPPA.
[63] Art. 2 dekretu wykonawczego w sprawie CPPA.
[64] Zob. motyw 156 projektu decyzji.
[65] Zob. wyrok TSUE w sprawie C-623/17, Privacy International, z dnia 6 października 2020 r., ECLI:EU:C:2020:790, 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)*".

kategorii danych osobowych zapewniają merytorycznie równoważny stopień ochrony ze stopniem gwarantowanym w UE, zwłaszcza w odniesieniu do proporcjonalności i przewidywalności prawa.

4.3. Dostęp koreańskich organów publicznych do informacji dotyczących łączności na potrzeby bezpieczeństwa narodowego

145. Jeśli chodzi o ramy prawne dostępu organów ds. bezpieczeństwa narodowego do informacji dotyczących łączności przekazywanych z EOG do Korei, EROD wskazała dwie problematyczne kwestie i obie te kwestie odnoszą się do systemu dostępu do komunikacji między obywatelami innych państw niż Korea podlegającej określonemu zbiorowi przypadków użycia (zob. pkt 29). W takich przypadkach zarówno do danych potwierdzających łączność, jak i do danych dotyczących treści nie stosuje się niektórych zabezpieczeń, które są dostępne w pozostałych sytuacjach. Innymi słowy, w tych konkretnych przypadkach wspomniane dane nie są objęte tymi samymi zabezpieczeniami, co dane przekazywane w komunikacji z udziałem co najmniej jednego obywatela Korei.

4.3.1. Brak obowiązku powiadamiania osób fizycznych o dostępie organów rządowych do komunikacji między obcokrajowcami

146. W scenariuszu opisanym powyżej, tj. gdy żadna ze stron komunikacji nie jest obywatelem Korei, organy ds. bezpieczeństwa narodowego nie mają obowiązku powiadamiania osób fizycznych o zbieraniu i przetwarzaniu ich danych. EROD uznaje, że ta kwestia dotyczy tylko niektórych przypadków. Po pierwsze jak już wskazano, gdy w komunikacji uczestniczy co najmniej jeden obywatel Korei, wymogi dotyczące powiadamiania wynikające z CPPA mają zastosowanie do wszystkich stron komunikacji, niezależnie od ich obywatelstwa[66]. Po drugie zbieranie danych osobowych pochodzących z komunikacji wyłącznie między obcokrajowcami podlega szczególnemu zbiorowi przypadków użycia. W szczególności prawo dostępu w takich przypadkach odnosi się do komunikacji prowadzonej przez a) państwa wrogie wobec Republiki Korei, b) zagraniczne agencje, grupy lub obywateli podejrzewanych o udział w działalności antykoreańskiej[67] lub c) członków grup działających na Półwyspie Koreańskim, ale w rzeczywistości niepodlegających suwerenności Republiki Korei, i ich grup patronackich z siedzibą w innych państwach. Dane pochodzące z komunikacji między osobami fizycznymi z UE przekazywane z EOG do Korei mogą zatem być zbieranie na potrzeby bezpieczeństwa narodowego jedynie, jeśli mieszczą się w jednej z trzech powyższych kategorii[68]. Z dodatkowych wyjaśnień Komisji Europejskiej EROD wnioskuje, że kolejnym czynnikiem ograniczającym jest to, że obowiązujące ramy prawne nie przewidują przechwytywania danych przekazywanych poza obszarem Korei.

147. W związku z tym można uznać, że krytyczne znaczenie braku wymogu powiadamiania ma – w ujęciu praktycznych skutków – ograniczony zakres. EROD podkreśla jednak znaczenie (późniejszego) poinformowania o dostępie organów rządowych do danych, zwłaszcza w odniesieniu do zapewnienia skutecznych środków prawnych. Według TSUE informacja ta jest „*niezbędna, aby umożliwić tym osobom wykonywanie ich praw wynikających z art. 7 i 8 karty, domaganie się dostępu do ich danych osobowych objętych tymi środkami oraz, w razie potrzeby, ich sprostowania lub usunięcia, a także wniesienie, zgodnie z art. 47 akapit pierwszy karty, skutecznego środka prawnego przed sądem*”[69]. Dostęp organów rządowych do danych na potrzeby bezpieczeństwa narodowego często obejmuje

[66] Zob. motyw 192 projektu decyzji.
[67] Zob. przypis 244 w załączniku II: zgodnie z tym przypisem pojęcie działalności antykoreańskiej oznacza działania, które zagrażają istnieniu i bezpieczeństwu tego narodu, jego demokratycznemu porządkowi oraz życiu i wolności jego ludności.
[68] Zob. motyw 187 projektu decyzji.
[69] Wyrok TSUE w sprawach połączonych 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 190.

poufne środki nadzoru, co oznacza, że osoby obserwowane – osoby, których dane dotyczą – nie są świadome, że ich dane są przetwarzane. W związku z tym „*osoba zainteresowana ma co do zasady niewielkie możliwości odwołania się do sądu, chyba że osoba ta zostanie powiadomiona o środkach podjętych bez jej wiedzy i tym samym może zakwestionować ich zgodność z prawem wstecznie lub ewentualnie, osoba, która podejrzewa, że jej komunikaty są lub zostały przechwycone, może zwrócić się do sądów, tak że jurysdykcja sądów nie zależy od powiadomienia osoby przechwytywanej o przechwyceniu jej wiadomości*”[70]. W tym kontekście i zgodnie z powyższym EROD wielokrotnie wyraziła obawy co do skutecznych środków prawnych w przypadkach nadzoru. EROD podkreśla, że poufność środków rządowych nie może prowadzić do tego, że nie można się od nich skutecznie odwołać. Wobec powyższego w ramach ogólnej oceny należy sprawdzić, czy brak wymogu powiadamiania w przypadkach komunikacji między obcokrajowcami ma wpływ na stopień ochrony danych określony w projekcie decyzji, przy czym szczególną uwagę należy poświęcić mechanizmom kontroli i dochodzenia roszczeń przewidzianym w prawie koreańskim (zob. sekcje 4.7 i 4.8).

148. Ponadto EROD zauważa w tym kontekście, że ustawa odnosi się do dość szerokich terminów, takich jak działalność antykoreańska i antynarodowa[71], i że trudno jest przewidzieć sposób interpretacji tych terminów na gruncie prawa koreańskiego. EROD zwraca się do Komisji Europejskiej o monitorowanie, w jaki sposób te terminy są doprecyzowane w prawie koreańskim i czy ich stosowanie w praktyce spełnia wymogi proporcjonalności wynikające z prawa UE.

4.3.2. Brak uprzedniego niezależnego zezwolenia na zbieranie informacji dotyczących łączności między obcokrajowcami

149. W przypadkach, gdy dane osobowe z EOG pochodzące z komunikacji między obywatelami innych państw niż Korea (w ramach jednego z powyższych przypadków użycia) mają być przetwarzane w Korei na potrzeby bezpieczeństwa narodowego, zbieranie takich danych nie podlega uprzedniemu zatwierdzeniu przez niezależny organ (co ma miejsce w przypadku komunikacji, w której co najmniej jedna uczestnicząca osoba jest obywatelem Korei)[72].

150. Szczególnie w świetle niedawnych orzeczeń Europejskiego Trybunału Praw Człowieka („**ETPC**”) w sprawach „Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu" oraz „Centrum för Rättvisa przeciwko Szwecji” EROD uważa, że trzeba zbadać, czy to stanowi krytyczną wadę koreańskich ram ochrony danych. W tym względzie EROD przypomina, że jak podkreślono w jej zaktualizowanych zaleceniach dotyczących niezbędnych gwarancji europejskich dla środków nadzoru,[73] art. 6 ust. 3 Traktatu o Unii Europejskiej stanowi, że prawa podstawowe zapisane w EKPC są ogólnymi zasadami prawa UE, jednak, jak przypomina TSUE w swoim orzecznictwie, ta konwencja – dopóki Unia Europejska do niej nie przystąpi – nie stanowi instrumentu prawnego formalnie włączonego do prawa UE[74]. W związku z tym stopień ochrony praw podstawowych wymagany na mocy art. 45 RODO należy określić na podstawie przepisów tego rozporządzenia interpretowanych w świetle praw podstawowych zapisanych w Karcie. Wobec powyższego, zgodnie z art. 52 ust. 3 Karty prawa w niej zawarte odpowiadające prawom zagwarantowanym przez EKPC mają mieć takie samo znaczenie i taki

[70] Wyrok ETPC w sprawie Big Brother Watch i in./Zjednoczone Królestwo, z dnia 25 maja 2021 r., ECLI:CE:ECHR:2021:0525JUD005817013, pkt 337 oraz wyrok ETPC w sprawie Roman Zakharov/Rosja, z dnia 4 grudnia 2015 r., ECLI:CE:ECHR:2015:1204JUD004714306, pkt 234.

[71] Komisja Europejska wyjaśniła, zgodnie z wyjaśnieniami rządu koreańskiego, że ten termin oznacza „działania, które zagrażają istnieniu i bezpieczeństwu narodu, jego demokratycznemu porządkowi oraz życiu i wolności ludności”; zob. również przypis 319 projektu decyzji stwierdzającej odpowiedni stopień ochrony.

[72] Zob. motyw 190 projektu decyzji.

[73] Zob. Zalecenia EROD 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru, pkt 10, 11.

[74] Zob. wyrok TSUE w sprawie C-311/18, Data Protection Commissioner/Facebook Ireland Ltd. i Maximilian Schrems, z dnia 16 lipca 2020 r., ECLI:EU:C:2020:559 (zwanej dalej „Schrems II”), pkt 98.

sam zakres jak prawa określone w tej konwencji. W konsekwencji należy uwzględniać orzecznictwo ETPC dotyczące praw, które są również przewidziane w Karcie, jako minimalny próg ochrony w celu interpretacji odpowiednich praw ujętych w Karcie, tj. w zakresie, w jakim Karta – zgodnie z wykładnią TSUE – nie przewiduje wyższego stopnia ochrony[75].

151. EROD zauważa, że choć uprzednie (niezależne) zatwierdzanie środków nadzoru uznaje się za ważne zabezpieczenie przed arbitralnością, z orzecznictwa TSUE nie wynika, że takie zatwierdzenie jest bezwzględnym wymogiem dotyczącym proporcjonalności środków nadzoru. Jednak ETPC wyraźnie już ustanowił wymóg niezależnego zezwolenia ex ante na masowe przechwytywanie danych[76]. Choć w projekcie decyzji wyraźnie tego nie stwierdzono, EROD rozumie, że ramy prawne Republiki Korei nie przewidują masowego przechwytywania danych, lecz jedynie ukierunkowane przechwytywanie przekazów telekomunikacyjnych[77]. Komisja Europejska potwierdziła takie rozumienie.

152. Wobec powyższego wskazane powyżej decyzje ETPC, zgodnie z orzecznictwem TSUE[78] i wcześniejszym orzecznictwem ETPC[79], raz jeszcze pokazują znaczenie kompleksowego nadzoru sprawowanego przez niezależne organy nadzorcze. EROD podkreśla, że niezależna kontrola na wszystkich etapach procesu udostępniania danych organom rządowym na potrzeby egzekwowania prawa i bezpieczeństwa narodowego jest ważnym zabezpieczeniem przed arbitralnymi środkami nadzoru, a tym samym pod kątem oceny odpowiedniego stopnia ochrony danych. Gwarancja niezależności organów nadzorczych w rozumieniu art. 8 ust. 3 Karty ma na celu zapewnienie skutecznego i rzetelnego monitorowania zgodności z przepisami o ochronie osób fizycznych w zakresie przetwarzania danych osobowych. Ma to zastosowanie w szczególności w okolicznościach, gdy ze względu na charakter tajnego nadzoru dana osoba nie może wystąpić z odwołaniem ani bezpośrednio uczestniczyć w postępowaniu odwoławczym przed wykonaniem środka nadzoru lub w jego trakcie.

153. Brak uprzedniego niezależnego zatwierdzenia nie może sam w sobie zostać uznany za poważną wadę w prawie koreańskim w odniesieniu do oceny, czy stopień ochrony danych jest merytorycznie równoważny. Jak już wskazano, ocena odpowiedniości stopnia ochrony zależy od wszystkich okoliczności danego przypadku, zwłaszcza od skuteczności kontroli ex post i prawnych środków odwoławczych przewidzianych w koreańskich ramach prawnych (zob. sekcje 4.7 i 4.8 poniżej).

4.4. Dobrowolne ujawnianie informacji

154. Zgodnie z art. 83 ust. 3 TBA podmioty świadczące usługi telekomunikacyjne mogą dobrowolnie przekazywać tzw. „dane abonenta”[80] organom ds. bezpieczeństwa narodowego i organom ścigania na

[75] Zob. wyrok TSUE w sprawach połączonych C-511/18, C-512/18 i C-520/18, La Quadrature du Net i in., z dnia 6 października 2020 r., pkt 124.

[76] Zob. wyrok ETPC w sprawie Big Brother Watch i in./Zjednoczone Królestwo, z dnia 25 maja 2021 r., ECLI:CE:ECHR:2021:0525JUD005817013, pkt 351: „Masowe przechwytywanie danych powinno podlegać niezależnemu uprzedniemu zezwoleniu”, „na masowe przechwytywanie danych zezwolenie powinien udzielać niezależny organ; tj. organ, który jest niezależny od władzy wykonawczej”.

[77] Jedynie sekcja 3.2 załącznika II zawiera wyraźne oświadczenie dotyczące celów bezpieczeństwa narodowego, gdy stwierdza się, że ograniczenia i zabezpieczenia *„zapewniają, aby zbieranie i przetwarzanie informacji ograniczały się do tego, co jest absolutnie niezbędne do osiągnięcia prawnie uzasadnionego celu. To nie obejmuje masowego i niekontrolowanego zbierania danych osobowych na potrzeby bezpieczeństwa narodowego*”.

[78] Zob. na przykład wyrok TSUE w sprawach połączonych C-203/15 i C-698/15, Tele2 Sverige AB i in., ECLI:EU:C:2016:970.

[79] Zob. na przykład wyrok ETPC w sprawie Roman Zakharov/Rosja, z dnia 4 grudnia 2015 r., ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Te zbiory danych obejmują: nazwę / imię i nazwisko, numer rejestracji rezydenta, adres i numer telefonu użytkowników, daty rozpoczęcia i zakończenia subskrypcji przez użytkowników, a także kody identyfikacyjne użytkowników (wykorzystywane do identyfikowania prawnego użytkownika systemów komputerowych lub sieci komunikacyjnych).

ich wniosek. EROD zauważa, że choć przypadki dotyczące danych osobowych przekazanych z EOG do Korei prawdopodobnie będą rzadkie, mimo to wymagają analizy, aby ocenić stopień ochrony danych, jak już wspomniano powyżej.

155. EROD przyjmuje, że w takich przypadkach zastosowanie mają zabezpieczenia ochrony danych przewidziane w PIPA, a organy publiczne i podmioty telekomunikacyjne muszą przestrzegać tych wymogów[81], a także ponoszą odpowiedzialność za ewentualne naruszenia praw i wolności zainteresowanych osób, których dane dotyczą[82]. Ponadto EROD rozumie, że podmioty telekomunikacyjne nie muszą stosować się do takich wniosków.

156. Jednak w odniesieniu do koncepcji dostępu organów krajowych do danych abonenta na potrzeby egzekwowania prawa i, w szczególności, na potrzeby bezpieczeństwa narodowego w drodze „dobrowolnego ujawniania" przez podmioty telekomunikacyjne, istnieje obawa dotycząca zwiększonego ryzyka naruszenia praw i wolności osób, których dane dotyczą, zwłaszcza ich prawa do informacji.

157. Zgodnie z art. 58 ust. 1 lit. 2 PIPA przepisy określone w rozdziałach III–VII nie mają zastosowania do danych osobowych żądanych w związku z bezpieczeństwem narodowym. W tym względzie na przykład przepisy określone w art. 18 (Ograniczenie wykorzystywania i udostępniania danych osobowych poza zakresem pierwotnego powodu ich zbierania) i art. 20 (Informowanie o źródłach danych osobowych zbieranych od stron trzecich) PIPA nie mają zastosowania do takich wniosków. W przypadkach, gdy wniosek jest składany przez organ ds. bezpieczeństwa narodowego, z jednej strony powstaje kwestia, czy art. 58 ust. 1 lit. 2 również wyklucza stosowanie PIPA do podmiotów telekomunikacyjnych. Z drugiej strony, pojawia się pytanie, czy wyłączenie stosowania art. 20 PIPA w takich przypadkach dotyczy także odpowiedniego przepisu sekcji 3 załącznika I (Powiadamianie o danych, gdy dane osobowe nie zostały uzyskane od osoby, której dane dotyczą (art. 20 ustawy)). Gdyby to miało miejsce i gdyby art. 58 ust. 1 lit. 2 dotyczył również podmiotów telekomunikacyjnych, to zgodnie z dostępnymi informacjami pojawiłoby się ryzyko, że nie będzie żadnego prawnego obowiązku informowania osób, których dane dotyczą, o dobrowolnym ujawnieniu.

158. EROD zastanawia się zatem nad możliwością, że wymogi udzielania informacji mogą stać się nieskuteczne, a przez to znacznie trudniejsze może być dla osób, których dane dotyczą, dochodzenie swoich praw w zakresie ochrony danych, zwłaszcza sądowych środków dochodzenia roszczeń. W związku z tym EROD zwraca się do Komisji Europejskiej o wyjaśnienie zakresu odpowiednich przepisów.

4.5. Dalsze wykorzystywanie informacji

159. Zasada ograniczenia celu jest podstawowym wymogiem prawnym dotyczącym ochrony danych. Polega na tym, że dane osobowe są zbierane jedynie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie mogą być przetwarzane dalej w sposób niezgodny z tymi celami. Ponadto prawo UE pozwala organom publicznym przetwarzać dane osobowe w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych lub ścigania czynów zabronionych, nawet jeśli te dane zostały pierwotnie pozyskane w innym celu, o ile organy te mają prawną podstawę, aby przetwarzać dane na mocy odpowiednich przepisów, a dalsze przetwarzanie nie jest nieproporcjonalne[83].

160. W związku z tym EROD zwraca uwagę, że zabezpieczenia i ograniczenia ujęte w koreańskich ramach ochrony danych są podobne do zabezpieczeń i ograniczeń przewidzianych w prawie UE w odniesieniu

[81] Zob. motywy 164 i 194 projektu decyzji.
[82] Zob. motyw 166 projektu decyzji.
[83] Zob. art. 4 ust. 2 dyrektywy (UE) 2016/680.

do dalszego przetwarzania informacji zebranych do celów egzekwowania prawa i bezpieczeństwa narodowego: przykładem jest zasada ograniczenia celu określona w art. 3 ust. 1–2 PIPA.

4.6. Dalsze przekazywanie danych i wymiana danych wywiadowczych

161. Art. 44 RODO przewiduje, że przekazywanie i dalsze przekazywanie danych osobowych następuje jedynie, jeśli nie zostaje naruszony stopień ochrony zagwarantowany przez RODO. W związku z tym dalsze przekazywanie danych odbiorcom w państwie trzecim nie może naruszyć stopnia ochrony zapewnianego w przypadku danych osobowych przekazywanych z EOG do Korei, tj. dalsze przekazywanie powinno być dozwolone tylko wtedy, gdy zapewnione jest utrzymanie stopnia ochrony merytorycznie równoważnego ze stopniem ochrony przewidzianym w prawie UE. W konsekwencji przy ocenie, czy dane państwo trzecie zapewnia odpowiedni stopień ochrony danych, należy uwzględnić ramy prawne tego państwa dotyczące dalszego przekazywania danych. Jest to bezsporne i zgodne z opinią zarówno Komisji Europejskiej[84], jak i EROD.

162. W tym kontekście EROD zwraca uwagę, że ETPC – w swoich niedawnych decyzjach „Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu" oraz „Centrum för Rättvisa przeciwko Szwecji" – przedstawił wskazówki[85] dotyczące środków ostrożności w zakresie ochrony danych, które należy przestrzegać w umawiających się państwach przy przekazywaniu danych osobowych innym stronom do celów egzekwowania prawa i bezpieczeństwa narodowego w przypadkach masowego zbierania danych: „*Po pierwsze, okoliczności, w jakich takie przekazanie może nastąpić, muszą być jasno określone w prawie krajowym. Po drugie, państwo przekazujące musi zapewnić, aby państwo otrzymujące – przy przetwarzaniu danych – dysponowało zabezpieczeniami mogącymi zapobiec nadużyciom i nieproporcjonalnej ingerencji. W szczególności państwo otrzymujące musi zagwarantować bezpieczne przechowywanie przekazanych materiałów i ograniczyć ich dalsze ujawnianie. [...] Po trzecie, gdy staje się jasne, że przekazywane są materiały wymagające szczególnej poufności – np. poufne materiały dziennikarskie – konieczne będą wzmocnione zabezpieczenia*"[86].

163. Stosując te standardy ETPC ustalił w sprawie „Centrum för Rättvisa przeciwko Szwecji", że brak w systemie przechwytywania danych wyraźnego wymogu prawnego, aby oceniać konieczność i proporcjonalność wymiany danych wywiadowczych pod kątem jej ewentualnego wpływu na prawo do prywatności, stanowi naruszenie art. 8 EKPC. ETPC skrytykował to, że wskutek poziomu ogólności prawa przechwycone materiały można wysłać za granicę zasadniczo w każdym przypadku, gdy uznaje się, że leży to w interesie narodowym, niezależnie od tego, czy zagraniczny odbiorca zapewnia dopuszczalny minimalny stopień zabezpieczeń[87].

164. Przyjmując, że ramy prawne Korei Południowej nie dopuszczają masowego przechwytywania danych, a mimo to rozważając implikacje przedstawionego powyżej orzecznictwa ETPC, EROD uważa, że przy ocenie, czy prawne ramy dalszego przekazywania danych do państwa trzeciego zapewniają odpowiednie standardy ochrony danych, oprócz wymogów wynikających z prawa UE zgodnie z wykładnią TSUE należy uwzględnić argumentację ETPC.

---

[84] Zob. motyw 84 i nast. projektu decyzji.

[85] Poniższe elementy stwierdzono przy okazji spraw *Big Brother Watch* oraz *Centrum för Rättvisa*, które dotyczą systemów masowego przechwytywania danych. Wymóg zachowania środków ostrożności przy przekazywaniu materiałów innym stronom był już uwzględniony w kryteriach opracowanych przez ETPC w kontekście ukierunkowanego przechwytywania i nie został doprecyzowany przez ETPC (zob. Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu, pkt 335, 362).

[86] Wyrok ETPC w sprawie Big Brother Watch i in./Zjednoczone Królestwo, z dnia 25 maja 2021 r., ECLI:CE:ECHR:2021:0525JUD005817013, pkt 362.

[87] Zob. wyrok w sprawie Centrum för Rättvisa/Szwecja, z dnia 25 maja 2021 r., ECLI:CE:ECHR:2021:0525JUD003525208, pkt 326.

4.6.1. Obowiązujące ramy prawne dalszego przekazywania danych przez organy ścigania

165. Na podstawie wyjaśnień Komisji Europejskiej EROD przyjmuje, że w odniesieniu do dalszego przekazywania danych przez właściwe organy do celów egzekwowania prawa zastosowanie ma sekcja 2 załącznika I do projektu decyzji dotycząca ograniczenia dalszego przekazywania, m.in. w przypadku gdy dane są przekazywane na podstawie aktu prawnego innego niż PIPA. Zgodnie z tym przepisem *„jeśli dane osobowe są przekazywane osobie trzeciej za granicą, mogą one nie być objęte stopniem ochrony zagwarantowanym na mocy koreańskiej ustawy o ochronie danych osobowych z powodu różnic w systemach ochrony danych osobowych w różnych państwach. W związku z tym takie przypadki będą uznawane za „przypadki, gdy osoba, której dane dotyczą, znajduje się w niekorzystnej sytuacji" wymienione w art. 17 ust. 4 ustawy lub „przypadki nieuczciwego naruszenia interesów osoby, której dane dotyczą, lub strony trzeciej" wymienione w art. 18 ust. 2 ustawy oraz w art. 14 ust. 2 dekretu wykonawczego w sprawie tej ustawy. Dlatego aby spełnić wymogi określone w tych przepisach, administrator danych osobowych i strona trzecia muszą wyraźnie zapewnić stopień ochrony równoważny z przepisami ustawy, w tym gwarancję korzystania przez osobę, której dane dotyczą, z jej praw w prawnie wiążących dokumentach, np. umowach, nawet po przekazaniu danych osobowych za granicę"*[88].

166. EROD z zadowoleniem przyjmuje ten przepis, który – przy założeniu odpowiedniego stopnia ochrony przekazywanych w tym celu danych w Korei – zapewnia utrzymanie stopnia ochrony, który merytorycznie jest przewidziany w unijnych przepisach dotyczących dalszego przekazywania danych. Komisja potwierdziła poprawność rozumienia przyjętego przez EROD, mianowicie, że ta sekcja załącznika I ma zastosowanie do wszystkich przypadków dalszego przekazywania przez właściwe organy do celów egzekwowania prawa. EROD podkreśla jednak, że należy zapewnić, aby to uregulowanie przewidywało utrzymanie stopnia ochrony w praktyce, ponieważ może wystąpić niepewność, jakie zabezpieczenia i zobowiązania umowne lub inne podobne mechanizmy można stosować do osiągnięcia takiego stopnia ochrony w przypadku przetwarzania danych do celów egzekwowania prawa. W tym względzie należy dodatkowo stwierdzić na przykład, że dane osobowe mogą być udostępniane jedynie odpowiednim właściwym organom w państwie trzecim.

167. Z zastrzeżeniem wyjaśnień, o które się wnioskuje powyżej, co do tego, czy projekt decyzji obejmuje KOFIU, EROD zauważa, że w oficjalnym oświadczeniu dotyczącym dostępu organów rządowych do danych[89] wyjaśniono, że zgodnie z art. 8 ust. 1 ARUSFTI komisarz KOFIU może przekazać zagranicznym służbom analityki finansowej określone informacje o transakcjach finansowych, jeśli to zostanie uznane za konieczne do osiągnięcia celu ARUSFTI[90]. Art. 8 ARUSFTI sam w sobie nie przewiduje obowiązku ustalenia, czy państwo obce oferuje odpowiednie zabezpieczenia w zakresie ochrony danych, oraz zapewnienia, aby tak było. W tym względzie załącznik II nie odnosi się do nowej sekcji załącznika I. Dlatego EROD wzywa Komisję Europejską do wyjaśnienia wzajemnych powiązań między odpowiednią sekcją załącznika I dotyczącą ograniczenia dalszego przekazywania a podstawą prawną dalszego przekazywania na mocy ARUSFTI.

[88] Załącznik I projektu decyzji, s. 7.

[89] Zob. załącznik II projektu decyzji.

[90] Zob. sekcja 2.2.3.2 załącznika II projektu decyzji. Chociaż taka wymiana informacji może nastąpić jedynie pod warunkiem, że zagraniczna służba nie może wykorzystać przekazanych informacji do celów innych niż pierwotny cel ujawnienia, zwłaszcza nie do celów dochodzenia lub procesu karnego (art. 8 ust. 2 ARUSFTI), komisarz KOFIU może, na wniosek państwa obcego, udzielić zgody na wykorzystanie takich danych na potrzeby dochodzeń lub procesów karnych w sprawach przestępstw po otrzymaniu uprzedniej zgody Ministra Sprawiedliwości (art. 8 ust. 3 ARUSFTI).

4.6.2. Obowiązujące ramy prawne dalszego przekazywania danych do celów bezpieczeństwa narodowego

168. Projekt decyzji nie zawiera żadnych informacji na temat ram prawnych dalszego przekazywania danych w obszarze bezpieczeństwa narodowego. W tym względzie EROD przyjmuje, że w przeciwieństwie do celów egzekwowanie prawa, sekcja 2 załącznika I nie ma zastosowania do dalszego przekazywania danych do celów bezpieczeństwa narodowego. Art. 17 i 18 PIPA, które podlegają wspomnianej sekcji załącznika I, należą do rozdziału III PIPA, który z kolei nie ma zastosowania do przetwarzania danych osobowych do celów bezpieczeństwa narodowego (art. 58 ust. 1 PIPA).

169. EROD zakłada jednak, że Korea może mieć konieczność przekazywania danych osobowych zagranicznym służbom wywiadowczym i je faktycznie im przekazuje do celów bezpieczeństwa narodowego, np. na potrzeby współpracy w zwalczaniu transgranicznych zagrożeń dla bezpieczeństwa narodowego, ostrzegania zagranicznych rządów przed takimi zagrożeniami lub zwracania się do nich o pomoc w identyfikowaniu takich zagrożeń.

170. EROD zrozumiała, że zdaniem Komisji Europejskiej dalsze przekazywanie danych jest w wystarczającym stopniu uregulowane w prawie koreańskim poprzez gwarancje wynikające z nadrzędnych ram konstytucyjnych, zwłaszcza zasady konieczności i proporcjonalności, a także poprzez podstawowe zasady ochrony danych określone w PIPA, takie jak zgodność z prawem i rzetelność przetwarzania, ograniczenie celu, minimalizacja danych, bezpieczeństwo i ogólne obowiązki w zakresie zapobiegania nadużyciom i niewłaściwemu wykorzystywaniu danych osobowych.

171. EROD uznaje i potwierdza ogólny zakres stosowania tych kluczowych zasad (ochrony danych), ale wyraża obawy, że te zabezpieczenia mają bardzo ogólny charakter oraz nie dotyczą konkretnie ani nie uwzględniają – w podstawie prawnej – szczególnych okoliczności i warunków dalszego przekazywania danych pochodzących z EOG do celów bezpieczeństwa narodowego. Choć te ogólne i nadrzędne zasady mają szerokie zastosowanie, EROD stawia pytanie, czy można uznać, że spełnione są kryteria jasnych i precyzyjnych przepisów oraz wystarczająco zapisane są skuteczne zabezpieczenia możliwe do wyegzekwowania. Zwłaszcza w przypadku gdy dostęp organów rządowych do danych osobowych i ich przetwarzanie przez te organy są tajne, a wnioski, które można wyciągnąć z danych, są szczególnie poważne, konieczne jest dysponowanie jasnymi i szczegółowymi zasadami. Prawo powinno określać zakres uznaniowości przyznanej właściwym organom oraz wystarczająco jasny sposób jej wykonywania, aby zapewnić osobie fizycznej odpowiednią ochronę. W wyroku w sprawie *Schrems II* TSUE przypomina, że podstawa prawna umożliwiająca ingerencję w prawa podstawowe – aby spełniać wymogi dotyczące zasad konieczności i proporcjonalności – musi sama określać zakres ograniczenia wykonywania danego prawa, przewidywać jasne i precyzyjne zasady regulujące zakres i stosowanie danego środka oraz ustanawiać zabezpieczenia minimalne[91]. W związku z tym EROD obawia się, że nie wystarczy, aby takie zabezpieczenia były ogólnie zapisane w prawie wyższego rzędu bez szczegółowego wprowadzenia pojęcia np. proporcjonalności w samej stosownej podstawie prawnej.

172. Te obawy znajdują potwierdzenie w wyżej wymienionej decyzji ETPC, w której Trybunał stwierdził, że zasada ogólna bez wyraźnego wymogu, aby ocenić konieczność i proporcjonalność lub uwzględnić kwestię prywatności, nie jest zgodna z prawem do prywatności określonym w art. 8 EKPC. W tym względzie EROD zauważa, że w przepisach dotyczących rozpatrywanej sprawy (jak również w prawie Korei) istnieją nadrzędne (zagwarantowane konstytucyjnie) zasady konieczności i proporcjonalności, np. wynikające z Karty i przystąpienia do EKPC.

173. EROD zwraca się do Komisji Europejskiej o wyjaśnienie podstawy prawnej, sposobu, zakresu i szczegółowych warunków, w ramach których agencje wywiadowcze są zobowiązane uwzględnić

[91] Zob. Schrems II, pkt 175 i 180.

kwestie prywatności i zabezpieczeń ochrony danych przed ujawnieniem partnerom zagranicznym danych osobowych do celów bezpieczeństwa narodowego. W przypadku gdy taki obowiązek wynika bezpośrednio z zasad konstytucyjnych, Komisja Europejska powinna dokonać dalszej oceny wymogów dokładności i jasności odpowiednich przepisów oraz potwierdzić, że ogólne zasady konstytucyjne i zasady ochrony danych są odpowiednio stosowane i wdrażane.

4.6.3. Umowy międzynarodowe

174. EROD zwraca uwagę, że Komisja Europejska nie uwzględniła – w ramach oceny odpowiedniości stopnia ochrony – istnienia umów międzynarodowych zawartych między Koreą a państwami trzecimi lub organizacjami międzynarodowymi, które mogą zawierać szczegółowe postanowienia dotyczące międzynarodowego przekazywania danych osobowych przez organy ścigania lub służby wywiadowcze do państw trzecich. EROD uważa, że zawarcie dwustronnych lub wielostronnych umów z państwami trzecimi do celów współpracy w zakresie egzekwowania prawa lub działań wywiadowczych może mieć wpływ na ocenę koreańskich ram prawnych ochrony danych.

175. W związku z tym EROD zwraca się do Komisji Europejskiej o wyjaśnienie, czy takie umowy istnieją i pod jakimi warunkami można je zawrzeć, oraz o ocenę, czy postanowienia umów międzynarodowych mogą mieć wpływ na stopień ochrony danych osobowych przekazywanych z EOG do Korei zapewniany poprzez ramy prawne i praktyki dotyczące ujawniania informacji za granicą do celów egzekwowania prawa i bezpieczeństwa narodowego.

4.7. Kontrola

176. EROD zauważa, że kontrola nad organami ścigania przestępstw karnych i organami ds. bezpieczeństwa narodowego jest sprawowana łącznie przez różne wewnętrzne i zewnętrzne organy.

177. W tym kontekście należy zwrócić uwagę, że TSUE wielokrotnie podkreślał konieczność istnienia niezależnej kontroli jako istotnego elementu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych. Pojęcie niezależności obejmuje obszary autonomii instytucjonalnej, niepodlegania poleceniom i niezależności materialnej. Aby zapewnić spójne monitorowanie i egzekwowanie przepisów o ochronie danych, organy nadzorcze muszą mieć skuteczne uprawnienia, w tym uprawnienia naprawcze i zaradcze.

178. EROD zgadza się z konkluzją Komisji Europejskiej, że w ramach ogólnej oceny można uznać, że Korea ma niezależny i skuteczny system nadzoru, mimo że kilka organów tego systemu nadzoru indywidualnie nie spełnia powyższych wymogów. Przykładowo większość z nich – np. Krajowa Komisja Praw Człowieka czy Rada ds. Audytów i Kontroli – nie ma uprawnień wykonawczych, a ich działalność ogranicza się do zwykłych zaleceń. Ponadto większość odpowiednich organów publicznych nie jest wyłącznie instytucjami ochrony danych, ale zazwyczaj powierza się im inne zadania w obszarze ochrony praw podstawowych.

179. EROD zwraca jednak uwagę, że zgodnie z wyjaśnieniami Komisji Europejskiej, nadzór nad organami ścigania jest zagwarantowany kompleksowo i bezwyjątkowo przez PIPC. W związku z tym PIPC ma uprawnienia dochodzeniowe, zaradcze i wykonawcze na mocy PIPA i innych ustaw dotyczących ochrony danych (np. CPPA), które stosuje się do całego obszaru dostępu organów ścigania i organów ds. bezpieczeństwa narodowego do danych osobowych.

180. W tym kontekście EROD pragnie raz jeszcze podkreślić, że aby organy nadzorcze mogły wykonywać swoje zadania i uprawnienia, muszą dysponować wystarczającymi zasobami ludzkimi, technicznymi i finansowymi. W tym względzie nie ma niestety informacji odnoszących się do wyznaczonych organów nadzorczych, w szczególności PIPC. Dlatego EROD ponownie zwraca się do Komisji Europejskiej o przekazanie dalszych informacji w tej sprawie.

181. W ujęciu ogólnym EROD pragnie zauważyć, że w projekcie decyzji nie ma prawie żadnych oświadczeń, przykładów lub danych liczbowych dotyczących działań nadzorczych oraz egzekwowania przepisów o ochronie danych przez organy nadzorcze w obszarze egzekwowania prawa i bezpieczeństwa narodowego. Takie oświadczenia, przykłady i dane liczbowe byłyby użyteczne w kontekście oceny skuteczności organów nadzorczych.

4.8. Sądowe środki prawne i dochodzenie roszczeń

182. EROD przypomina, że dla zapewnienia odpowiedniego stopnia ochrony danych zasadnicze znaczenie ma, aby osoby, których dane dotyczą, dysponowały kompleksowymi środkami prawnymi i możliwościami dochodzenia roszczeń w przypadku nieuprawnionego dostępu do ich danych lub nieuprawnionego przetwarzania ich danych. Te środki prawne muszą być wystarczające, aby umożliwić osobie, której dane dotyczą, uzyskanie dostępu do przechowywanych danych dotyczących tej osoby oraz żądanie ich skorygowania lub usunięcia.

183. W świetle wyroków TSUE w sprawach *Schrems I* i *Schrems II* wyraźnie widać, że dla przyjęcia założenia adekwatności prawa w państwie trzecim podstawowe znaczenie ma, oprócz prawa do zwrócenia się do właściwych organów, skuteczna ochrona sądowa w rozumieniu art. 47 ust. 1 Karty.

184. EROD uznaje, że Korea ustanowiła różne ścieżki korzystania przez osoby fizyczne z praw do dostępu, zatrzymania, usuwania i zawieszenia na podstawie PIPA. Te prawa mogą być wykonywane przez zwrócenie się do samego administratora lub w drodze skargi złożonej do PIPC lub innych organów nadzorczych, np. Krajowej Komisji Praw Człowieka. Ponadto EROD wskazuje na możliwość zaskarżenia administratorów lub decyzji organów publicznych wydanych w odpowiedzi na ich wniosek na podstawie ustawy o postępowaniu administracyjnym.

185. Dodatkowo EROD przyjmuje z wyjaśnień przekazanych przez Komisję Europejską, że osoby fizyczne mogą zaskarżyć działania organów ścigania i organów ds. bezpieczeństwa narodowego przed właściwymi sądami na podstawie ustawy o postępowaniu administracyjnym i ustawy o sądownictwie konstytucyjnym oraz mają możliwość uzyskania odszkodowania za szkody na podstawie ustawy o odszkodowaniach państwowych[92].

186. W tym kontekście EROD zastanawia się jednak nad skutecznym dochodzeniem roszczeń przez osoby fizyczne z UE w sprawach dotyczących bezpieczeństwa narodowego, w których nie uczestniczy obywatel Korei. Jak zauważono w pkt 33 i nast., organy ds. bezpieczeństwa narodowego nie mają obowiązku powiadamiania osób, których dane dotyczą, o zbieraniu i przetwarzaniu ich danych osobowych. Ponieważ uzyskanie skutecznej ochrony prawnej w takich sprawach jest znacznie trudniejsze, EROD pragnie podkreślić, że pewne zabezpieczenia prawne są konieczne w takich przypadkach, gdy przekazywane są dane z EOG. Te zabezpieczenia muszą oznaczać, że osoby, których dane dotyczą, mogą przeciwko niezgodnemu z prawem przetwarzaniu danych podjąć skuteczne działania w sposób bezpieczny pod względem prawnym i pozbawiony przeszkód ze względu na nadmiernie zacieśnione wymogi proceduralne, np. nałożenie ciężaru dowodu, którego nie mogą spełnić bez wiedzy o przetwarzaniu. Ponadto osoby, których dane dotyczą, muszą mieć możliwość zwrócenia się do właściwego organu, który spełnia wymogi określone w art. 47 Karty praw podstawowych Unii Europejskiej, tj. ma kompetencje do ustalenia, że zachodzi przetwarzanie danych, do sprawdzenia zgodności tego przetwarzania z prawem oraz do zastosowania możliwych do wyegzekwowania uprawnień zaradczych na wypadek, gdy przetwarzanie danych jest niezgodne z prawem. W tej sytuacji samo prawo do wniesienia skargi, na przykład, do Krajowej Komisji Praw Człowieka nie jest wystarczające. W związku z tym EROD wzywa Komisję do bardziej szczegółowego wyjaśnienia, w jaki sposób te wymogi są wprowadzone w ujęciu proceduralnym i merytorycznym, np.

[92] Zob. sekcja 3.2.4 załącznika II w związku z sekcją 2.4.3 załącznika II.

czy osoby, których dane dotyczą, mogą zwrócić się do PIPC oraz do sądu bez konieczności udowodnienia faktu przetwarzania danych.

187. Dodatkowo EROD zauważa, że w projekcie decyzji przewidziano mechanizm kierowania skarg, w ramach którego osoby fizyczne z UE mogą złożyć skargę do PIPC za pośrednictwem odpowiedniego krajowego organu ochrony danych lub EROD. Następnie PIPC powiadomi daną osobę fizyczną tą samą drogą po zakończeniu dochodzenia[93]. EROD z zadowoleniem przyjmuje dążenie do ułatwienia dostępu do środków dochodzenia roszczeń przeciwko koreańskim organom ds. bezpieczeństwa narodowego. Jednocześnie EROD opowiada się za tym, aby ten mechanizm kierowania skarg działał za pośrednictwem europejskich krajowych organów ochrony danych, a nie za pośrednictwem EROD, ponieważ te organy są właściwe i ściślej zajmują się rozpatrywaniem indywidualnych skarg.

188. Ponadto EROD zwraca uwagę na możliwą sprzeczność w odniesieniu do dobrowolnego ujawniania informacji. Z jednej strony, w projekcie decyzji stwierdza się, że osoby fizyczne mogą dochodzić roszczeń, gdy ich dane zostały ujawnione niezgodnie z prawem w następstwie wniosku o dobrowolne ujawnienie, m.in. przeciwko organowi ścigania, który wystąpił z wnioskiem[94]. Z drugiej strony, w projekcie decyzji w odniesieniu do prawa osób fizycznych do zaskarżenia działań organów publicznych wskazuje się wymóg bezpośredniego wpływu i wymienia (jedynie) wnioski o obowiązkowe ujawnienie informacji jako przykład sytuacji, w której uznaje się, że działanie administracyjne ma bezpośredni wpływ na prawo do prywatności[95]. Z wyjaśnień Komisji Europejskiej EROD przyjmuje, że w rzeczywistości nie ma ograniczenia możliwości dochodzenia roszczeń w stosunku do wniosków o dobrowolne ujawnienie informacji, i w związku z tym zwraca się do Komisji Europejskiej o dalsze objaśnienie tej kwestii w decyzji, zarówno w obszarze egzekwowania prawa, jak i w obszarze bezpieczeństwa narodowego (w przeciwieństwie do sekcji dotyczącej egzekwowania prawa sekcja dotycząca dobrowolnego ujawniania informacji do celów bezpieczeństwa narodowego nie zawiera żadnego wyraźnego stwierdzenia o dochodzeniu roszczeń w tym kontekście).

[93] Zob. motyw 205 oraz załącznik I, s. 19 projektu decyzji.
[94] Zob. motyw 166 projektu decyzji.
[95] Zob. motyw 181(egzekwowanie prawa) oraz motywy 208 i 181 (bezpieczeństwo narodowe) projektu decyzji.