II

(Akty o charakterze nieustawodawczym)

DECYZJE

DECYZJA WYKONAWCZA KOMISJI (UE) 2022/254

z dnia 17 grudnia 2021 r.

na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 stwierdzająca odpowiedni stopień ochrony danych osobowych przez Republikę Korei na mocy ustawy o ochronie danych osobowych

(notyfikowana jako dokument nr C(2021) 9316)

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) ([1]), w szczególności jego art. 45 ust. 3,

a także mając na uwadze, co następuje:

1. WPROWADZENIE

(1) W rozporządzeniu (UE) 2016/679 określono zasady dotyczące przekazywania danych osobowych przez administratorów lub podmioty przetwarzające w Unii do państw trzecich i organizacji międzynarodowych w zakresie, w jakim takie przekazywanie wchodzi w zakres stosowania rozporządzenia. Zasady dotyczące międzynarodowego przekazywania danych określono w rozdziale V (art. 44–50) tego rozporządzenia. Chociaż przepływ danych osobowych do państw spoza Unii Europejskiej oraz z takich państw jest niezbędnym warunkiem rozwoju handlu transgranicznego i współpracy międzynarodowej, przekazywanie danych osobowych do państw trzecich nie może obniżać stopnia ochrony zapewnianego tym danym w Unii ([2]).

(2) Zgodnie z art. 45 ust. 3 rozporządzenia (UE) 2016/679 Komisja może w drodze aktu wykonawczego przyjąć decyzję stwierdzającą, że państwo trzecie, terytorium lub określony sektor lub określone sektory w tym państwie trzecim lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony. Przy spełnieniu tego warunku przekazywanie danych osobowych do państwa trzeciego może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia, jak przewidziano w art. 45 ust. 1 i motywie 103 rozporządzenia (UE) 2016/679.

(3) Jak określono w art. 45 ust. 2 rozporządzenia (UE) 2016/679, przy przyjmowaniu decyzji stwierdzającej odpowiedni stopień ochrony należy opierać się na wszechstronnej analizie porządku prawnego państwa trzeciego, obejmującej zarówno jego przepisy dotyczące podmiotów odbierających dane, jak i ograniczenia oraz zabezpieczenia w zakresie dostępu organów publicznych do danych osobowych. W swojej ocenie Komisja musi ustalić, czy dane państwo trzecie daje gwarancje zapewniające stopień ochrony „zasadniczo odpowiadający" stopniowi ochrony zapewnianemu w Unii Europejskiej (motyw 104 rozporządzenia (UE) 2016/679). To, czy tak jest w istocie, należy oceniać w świetle przepisów Unii, w szczególności rozporządzenia (UE) 2016/679, a także orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej ([3]).

([1]) Dz.U. L 119 z 4.5.2016, s. 1.
([2]) Zob. motyw 101 rozporządzenia (UE) 2016/679.
([3]) Zob. niedawna sprawa C-311/18 Facebook Ireland i Schrems (Schrems II), ECLI:EU:C:2020:559.

(4) Jak wyjaśnił w swoim orzecznictwie Trybunał Sprawiedliwości Unii Europejskiej, nie oznacza to konieczności stwierdzenia identycznego stopnia ochrony ([4]). W szczególności środki, z których korzysta dane państwo trzecie do zapewnienia ochrony danych osobowych, mogą różnić się od środków stosowanych w Unii, o ile w praktyce skutecznie zapewniają odpowiedni stopień ochrony ([5]). Odpowiedni standard ochrony nie wymaga zatem dokładnego powielenia przepisów unijnych. Przy określaniu odpowiedniości chodzi raczej o stwierdzenie, czy biorąc pod uwagę istotę prawa do prywatności oraz jego skuteczne wprowadzenie w życie, egzekwowanie i nadzór nad jego przestrzeganiem, dany zagraniczny system zapewnia jako całość wymagany stopień ochrony ([6]). Wytyczne w tym zakresie zawiera również dokument Europejskiej Rady Ochrony Danych „Odpowiedni stopień ochrony przekazywanych danych osobowych", który ma na celu dalsze wyjaśnienie tego standardu ([7]).

(5) Komisja uważnie przeanalizowała koreańskie prawo i praktyki. Na podstawie ustaleń przedstawionych w motywach (8) – (208) Komisja stwierdza, że Republika Korei zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych przez administratora lub podmiot przetwarzający w Unii ([8]) podmiotom (np. osobom fizycznym lub prawnym, organizacjom, instytucjom publicznym) w Korei objętym zakresem stosowania ustawy o ochronie danych osobowych (ustawa nr. 10465 z dnia 29 marca 2011 r., ostatnio zmieniona ustawą nr. 16930 z dnia 4 lutego 2020 r.). Obejmuje to zarówno administratorów, jak i podmioty przetwarzające (zwane „dostawcami usług outsourcingowych ([9])) w rozumieniu rozporządzenia (UE) 2016/679. Stwierdzenie odpowiedniego stopnia ochrony nie obejmuje przetwarzania danych osobowych na potrzeby działalności misyjnej prowadzonej przez organizacje religijne oraz na potrzeby zgłaszania kandydatów przez partie polityczne ani przetwarzania informacji dotyczących kredytów osobistych na podstawie ustawy o informacjach kredytowych przez administratorów podlegających nadzorowi Komisji Usług Finansowych.

(6) W niniejszej decyzji uwzględniono dodatkowe zabezpieczenia określone w zawiadomieniu nr 2021-5 (załącznik I) oraz oficjalne oświadczenia, zapewnienia i zobowiązania rządu Korei wobec Komisji (załącznik II).

(7) Niniejsza decyzja skutkuje tym, że przekazywanie danych osobowych administratorom i podmiotom przetwarzającym w Republice Korei może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia. Nie ma ona wpływu na bezpośrednie stosowanie rozporządzenia (UE) 2016/679 w odniesieniu do takich podmiotów, jeżeli spełnione są warunki dotyczące terytorialnego zakresu stosowania tego rozporządzenia, określone w jego art. 3.

2. PRZEPISY MAJĄCE ZASTOSOWANIE DO PRZETWARZANIA DANYCH OSOBOWYCH

2.1 Ramy ochrony danych w Republice Korei

(8) System prawny regulujący kwestie prywatności i ochrony danych w Korei ma swoje źródło w konstytucji koreańskiej, ogłoszonej w dniu 17 lipca 1948 r. Chociaż prawo do ochrony danych osobowych nie jest wyraźnie określone w konstytucji, jest ono uznawane za prawo podstawowe, wywodzące się z konstytucyjnych praw do godności ludzkiej i dążenia do szczęścia (art. 10), życia prywatnego (art. 17) i poufności komunikacji (art. 18). Zostało to potwierdzone zarówno przez Sąd Najwyższy ([10]), jak i Trybunał Konstytucyjny ([11]). Ograniczenie podstawowych praw i wolności (w tym prawa do prywatności) można nałożyć wyłącznie przepisami prawa, gdy jest to konieczne ze względów bezpieczeństwa narodowego lub utrzymania porządku publicznego leżącego w interesie publicznym, i nie może ono naruszać istoty takiego prawa lub takiej wolności (art. 37 ust. 2).

([4]) Sprawa C-362/14 Maximilian Schrems/Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650, pkt 73.
([5]) Schrems, pkt 74.
([6]) Zob. komunikat Komisji do Parlamentu Europejskiego i Rady „Wymiana i ochrona danych osobowych w zglobalizowanym świecie" z dnia 10 stycznia 2017 r., COM(2017) 7, pkt 3.1, s. 6–7.
([7]) Europejska Rada Ochrony Danych, Odpowiedni stopień ochrony przekazywanych danych osobowych, WP 254 rev.01, dokument dostępny pod adresem: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
([8]) Niniejsza decyzja ma znaczenie dla EOG. W Porozumieniu o Europejskim Obszarze Gospodarczym (Porozumienie EOG) przewidziano rozszerzenie rynku wewnętrznego Unii Europejskiej na trzy państwa EOG – Islandię, Liechtenstein i Norwegię. Decyzja Wspólnego Komitetu włączająca rozporządzenie (UE) 2016/679 do załącznika XI do Porozumienia EOG została przyjęta przez Wspólny Komitet EOG w dniu 6 lipca 2018 r. i weszła w życie w dniu 20 lipca 2018 r. Rozporządzenie jest zatem objęte tym porozumieniem. Do celów niniejszej decyzji odniesienia do UE i państw członkowskich UE należy zatem rozumieć jako obejmujące również państwa EOG.
([9]) Zob. pkt 2.2.3 niniejszej decyzji.
([10]) Zob. np. orzeczenie Sądu Najwyższego nr 2014Da77970 z dnia 15 października 2015 r. (angielskie streszczenie oraz cytowane tam orzecznictwo, w tym orzeczenie 2012Da49933 z dnia 24 lipca 2014 r., dostępne pod linkiem „Lawmaker's disclosure of teachers' trade union members case" na stronie: https://www.privacy.go.kr/eng/enforcement_01.do).
([11]) Zob. w szczególności orzeczenie Trybunału Konstytucyjnego nr 99Hun-ma513 z dnia 26 maja 2005 r. (streszczenie w języku angielskim dostępne na stronie http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) oraz orzeczenie 2014JHunma449 2013 Hun-Ba68 (wersja skonsolidowana) z dnia 23 grudnia 2015 r. (angielskie streszczenie dostępne pod linkiem „Change of resident registration number case" na stronie https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Mimo że konstytucja w różnych miejscach odnosi się do praw koreańskich obywateli, Trybunał Konstytucyjny orzekł, że prawa podstawowe przysługują również cudzoziemcom ([12]). W szczególności Trybunał stwierdził, że ochrona godności i wartości osoby jako istoty ludzkiej, jak również prawo do dążenia do szczęścia są prawami każdej istoty ludzkiej, a nie tylko obywateli ([13]). Ponadto, zgodnie z oficjalnymi oświadczeniami rządu Korei ([14]), powszechnie uznaje się, że art. 12–22 konstytucji (które obejmują prawo do prywatności) zapewniają podstawowe prawa człowieka ([15]). Chociaż jak dotąd nie zapadło orzeczenie dotyczące konkretnie prawa do prywatności w odniesieniu do cudzoziemców, zakorzenienie tego prawa w ochronie godności ludzkiej i dążeniu do szczęścia potwierdza ten wniosek ([16]).

(10) Ponadto Korea uchwaliła szereg ustaw w dziedzinie ochrony danych, które zapewniają gwarancje wszystkim osobom fizycznym, niezależnie od ich narodowości ([17]). Do celów niniejszej decyzji właściwymi ustawami są:

— ustawa o ochronie danych osobowych (PIPA),

— ustawa o wykorzystywaniu i ochronie informacji kredytowych ([18]),

— ustawa o ochronie prywatności komunikacji.

(11) PIPA zapewnia ogólne ramy prawne ochrony danych w Republice Korei. 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 do PIPA), który podobnie jak PIPA jest prawnie wiążący i możliwy do wyegzekwowania na drodze prawnej.

(12) Ponadto regulacyjne „zawiadomienia" przyjęte przez Komisję Ochrony Danych Osobowych (PIPC) zawierają dalsze przepisy dotyczące wykładni i stosowania PIPA. Na podstawie art. 5 (Obowiązki państwa) i art. 14 (Współpraca międzynarodowa) PIPA PIPC przyjęła zawiadomienie nr 2021-5 z dnia 1 września 2020 r. (zmienione zawiadomieniem nr 2021-1 z dnia 21 stycznia 2021 r. i zawiadomieniem nr 2021-5 z dnia 16 listopada 2021 r., zwane zawiadomieniem nr 2021-5) w sprawie wykładni, stosowania i egzekwowania niektórych przepisów PIPA. Zawiadomienie to zawiera wyjaśnienia, które mają zastosowanie do każdego przypadku przetwarzania danych osobowych zgodnie z PIPA, jak również dodatkowe zabezpieczenia danych osobowych przekazywanych do Korei na podstawie niniejszej decyzji. Zawiadomienie jest prawnie wiążące dla administratorów danych osobowych i może być egzekwowane zarówno przez PIPC, jak i sądy ([19]). Naruszenie przepisów określonych w zawiadomieniu pociąga za sobą naruszenie odpowiednich przepisów PIPA, których są one uzupełnieniem. Treść dodatkowych zabezpieczeń przeanalizowano zatem w ramach oceny odpowiednich artykułów PIPA. Ponadto dalsze wskazówki dotyczące PIPA i dekretu wykonawczego do tej ustawy, które zawierają informacje o stosowaniu i egzekwowaniu przepisów o ochronie danych przez PIPC, znajdują się w podręczniku i wytycznych dotyczących PIPA przyjętych przez PIPC ([20]).

([12]) Orzeczenie Trybunału Konstytucyjnego nr 93 Hun-MA120 z dnia 29 grudnia 1994 r.
([13]) Orzeczenie Trybunału Konstytucyjnego nr 99HeonMa494 z dnia 29 listopada 2001 r.
([14]) Zob. załącznik II pkt 1.1.
([15]) Zob. również art. 1 ustawy o ochronie danych osobowych, który wyraźnie odnosi się do „wolności i praw osób fizycznych". Konkretnie artykuł ten stanowi, że celem ustawy jest „zapewnienie przetwarzania i ochrony danych osobowych w celu ochrony wolności i praw osób fizycznych oraz dalszego urzeczywistniania idei godności i wartości osób fizycznych". Podobnie w art. 5 ust. 1 ustawy o ochronie danych osobowych ustanawia się odpowiedzialność państwa za „opracowanie polityki mającej na celu zapobieganie szkodliwym skutkom zbierania danych osobowych do celów innych niż określone, nadużywania i niewłaściwego wykorzystywania danych osobowych, jawnego nadzoru i śledzenia itp. oraz promowanie godności człowieka i prywatności osób fizycznych".
([16]) Ponadto art. 6 ust. 2 konstytucji stanowi, że status cudzoziemców jest gwarantowany zgodnie z przepisami prawa międzynarodowego i postanowieniami traktatów. Korea jest stroną kilku umów międzynarodowych gwarantujących prawo do prywatności, takich jak Międzynarodowy pakt praw obywatelskich i politycznych (art. 17), Konwencja o prawach osób niepełnosprawnych (art. 22) oraz Konwencja o prawach dziecka (art. 16).
([17]) Obejmuje to przepisy, które są istotne dla ochrony danych osobowych, ale nie mają zastosowania w sytuacji, gdy dane osobowe są zbierane w Unii i przekazywane do Korei zgodnie z rozporządzeniem (UE) 2016/679, na przykład zawarte w ustawie o ochronie, wykorzystywaniu itp. informacji dotyczących lokalizacji.
([18]) Celem tej ustawy jest wspieranie rzetelnej działalności w zakresie informacji kredytowych, promowanie efektywnego wykorzystania informacji kredytowych i systematycznego zarządzania nimi oraz ochrona prywatności przed niewłaściwym wykorzystaniem i nadużywaniem informacji kredytowych (art. 1 ustawy).
([19]) Koreańskie sądy orzekały na przykład w wielu sprawach dotyczących przestrzegania takich zawiadomień, przy czym w niektórych sprawach koreańscy administratorzy danych osobowych zostali uznani za odpowiedzialnych za naruszenie przepisów zawiadomienia (zob. np. orzeczenie Sądu Najwyższego 2018Da219406 z dnia 25 października 2018 r., w którym Sąd Najwyższy nakazał administratorowi wypłatę odszkodowania osobom fizycznym za szkody poniesione w związku z naruszeniem przepisów „Zawiadomienia o standardzie dotyczącym środków zapewniających bezpieczeństwo danych osobowych"; zob. również orzeczenie Sądu Najwyższego nr 2018Da219352 z dnia 25 października 2018 r.; orzeczenie Sądu Najwyższego nr 2011Da24555 z dnia 16 maja 2016 r.; orzeczenie Centralnego Sądu Okręgowego w Seulu nr 2014Gahap511956 z 13 października 2016 r.; orzeczenie Centralnego Sądu Okręgowego w Seulu nr 2009Gahap43176 z 26 stycznia 2010 r.).
([20]) Art. 12 ust. 1 PIPA.

(13) Ponadto w ustawie o wykorzystywaniu i ochronie informacji kredytowych (CIA) określono przepisy szczegółowe, które mają zastosowanie zarówno do „zwykłych" podmiotów handlowych, jak i podmiotów wyspecjalizowanych w sektorze finansowym, gdy przetwarzają one osobowe informacje kredytowe, tj. informacje, które są niezbędne do określenia zdolności kredytowej stron transakcji finansowych lub handlowych. Dotyczy to w szczególności imienia i nazwiska/nazwy, danych kontaktowych, transakcji finansowych, ratingu kredytowego, statusu ubezpieczenia lub salda kredytowego, jeżeli informacje te są wykorzystywane do określenia zdolności kredytowej osoby fizycznej ([21]). Natomiast w przypadku gdy takie informacje są wykorzystywane do innych celów (takich jak cele kadrowe), PIPA ma zastosowanie w całości. Jeżeli chodzi o szczegółowe przepisy CIA dotyczące ochrony danych, przestrzeganie przepisów jest nadzorowane częściowo przez PIPC (w przypadku organizacji komercyjnych, zob. art. 45-3 CIA), a częściowo przez Komisję Usług Finansowych ([22]) (w odniesieniu do sektora finansowego, w tym agencji ratingowych, banków, zakładów ubezpieczeń, banków oszczędności wzajemnych, przedsiębiorstw finansowych wyspecjalizowanych w udzielaniu kredytów, przedsiębiorstw świadczących finansowe usługi inwestycyjne, przedsiębiorstw finansowych zajmujących się obrotem papierami wartościowymi, unii kredytowych itp., zob. art. 45 ust. 1 CIA w związku z art. 36-2 rozporządzenia wykonawczego do CIA oraz art. 38 ustawy o Komisji Usług Finansowych). W związku z tym zakres niniejszej decyzji jest ograniczony do podmiotów handlowych, które podlegają nadzorowi PIPC ([23]). Przepisy szczegółowe CIA, które mają zastosowanie w tym kontekście (w przypadku braku przepisów szczegółowych zastosowanie mają przepisy ogólne PIPA), opisano w pkt 2.3.11.

2.2 **Zakres przedmiotowy i podmiotowy PIPA**

(14) O ile przepisy innych ustaw nie stanowią wyraźnie inaczej, ochrona danych osobowych podlega przepisom PIPA (art. 6). Zakres przedmiotowy i podmiotowy jej stosowania został określony zdefiniowanymi w niej pojęciami „danych osobowych", „przetwarzania" i „administratora danych osobowych".

2.2.1 *Definicja danych osobowych*

(15) W art. 2 ust. 1 PIPA zdefiniowano dane osobowe jako informacje dotyczące pozostającej przy życiu osoby fizycznej, pozwalające zidentyfikować tę osobę bezpośrednio, na przykład na podstawie jej imienia i nazwiska, numeru rejestracyjnego mieszkańca lub wizerunku, albo pośrednio, tj. w przypadku, gdy informacje, które same w sobie nie pozwalają na zidentyfikowanie konkretnej osoby fizycznej, można łatwo połączyć z innymi informacjami. To, czy informacje można „łatwo" połączyć, zależy od tego, czy takie połączenie jest racjonalnie prawdopodobne, biorąc pod uwagę możliwość uzyskania innych informacji, jak również czas, koszty i technologię wymagane do zidentyfikowania osoby fizycznej.

(16) Ponadto informacje spseudonimizowane – tj. informacje, za pomocą których nie można zidentyfikować konkretnej osoby fizycznej bez wykorzystania dodatkowych informacji lub połączenia ich z dodatkowymi informacjami w celu przywrócenia ich do stanu pierwotnego – są uznawane za dane osobowe w rozumieniu PIPA (art. 2 ust. 1 lit. c) PIPA). Z kolei informacje, które są całkowicie „zanonimizowane", są wyłączone z zakresu stosowania PIPA (art. 58-2 PIPA). Dotyczy to informacji, za pomocą których nie można identyfikować konkretnej osoby fizycznej, nawet w połączeniu z innymi informacjami, biorąc pod uwagę czas, koszty i technologię rozsądnie wymagane na potrzeby identyfikacji.

(17) Odpowiada to zakresowi przedmiotowemu stosowania rozporządzenia (UE) 2016/679 i używanym w nim pojęciom „danych osobowych", „pseudonimizacji" ([24]) i „informacji zanonimizowanych" ([25]).

([21]) Art. 2 ust. 1 CIA.

([22]) Komisja Usług Finansowych jest organem nadzorczym sektora finansowego w Korei i w zakresie swojej właściwości egzekwuje również przepisy CIA.

([23]) Jeżeli w przyszłości sytuacja ta uległaby zmianie, np. w związku z rozszerzeniem zakresu właściwości PIPC na wszelkie przetwarzanie informacji dotyczących kredytów osobistych na podstawie CIA, można by rozważyć zmianę decyzji stwierdzającej odpowiedni stopień ochrony, aby objąć nią również podmioty, które obecnie podlegają nadzorowi Komisji Usług Finansowych.

([24]) W PIPA za „przetwarzanie pseudonimizujące" uważa się przetwarzanie za pomocą takich metod jak częściowe usunięcie danych osobowych lub częściowe lub całkowite zastąpienie danych osobowych w taki sposób, że bez dodatkowych informacji nie można rozpoznać konkretnej osoby fizycznej (art. 2 ust. 1–2 PIPA). Odpowiada to definicji pseudonimizacji zawartej w art. 4 ust. 5 rozporządzenia (UE) 2016/679, zgodnie z którą jest to „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej".

([25]) W szczególności w motywie 26 rozporządzenia (UE) 2016/679 wyjaśniono, że rozporządzenie nie ma zastosowania do informacji zanonimizowanych, tj. informacji, które nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. To z kolei zależy od wszelkich sposobów, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora albo inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.

2.2.2 *Definicja przetwarzania*

(18) Pojęcie „przetwarzania" jest zdefiniowane w PIPA szeroko, jako obejmujące „zbieranie, generowanie, łączenie, utrwalanie, przechowywanie, zatrzymywanie, przetwarzanie o wartości dodanej, edytowanie, odzyskiwanie, uzyskiwanie, poprawianie, pobieranie, wykorzystywanie, przekazywanie, ujawnianie i niszczenie danych osobowych oraz tworzenie między nimi powiązań, a także inne podobne działania" ([26]). Chociaż niektóre przepisy PIPA odnoszą się jedynie do określonych rodzajów przetwarzania, takich jak „wykorzystywanie", „przekazywanie" lub „zbieranie" ([27]), pojęcie „wykorzystywania" interpretuje się jako obejmujące każdy rodzaj przetwarzania inny niż „zbieranie" lub „przekazywanie" (stronie trzeciej). Ta wykładnia rozszerzająca „wykorzystania" gwarantuje tym samym brak luk w ochronie w odniesieniu do określonych czynności przetwarzania. Pojęcie przetwarzania odpowiada zatem temu samemu pojęciu w rozumieniu rozporządzenia (UE) 2016/679.

2.2.3 *Administrator danych osobowych oraz dostawca usług outsourcingowych*

(19) PIPA ma zastosowanie do „administratorów danych osobowych" (administratorów). Podobnie jak w przypadku rozporządzenia (UE) 2016/679 pojęcie to obejmuje każdą instytucję publiczną, osobę prawną, organizację lub osobę fizyczną, która przetwarza dane osobowe bezpośrednio lub pośrednio w celu prowadzenia zbiorów danych osobowych w ramach swojej działalności ([28]). W tym kontekście „zbiór danych osobowych" oznacza „zestaw lub zestawy danych osobowych uporządkowanych lub zorganizowanych w sposób systematyczny, oparte na określonej zasadzie celem zapewnienia łatwego dostępu do danych osobowych" (art. 2 ust. 4 PIPA) ([29]). W wymiarze wewnętrznym administrator jest zobowiązany do przeszkolenia osób zaangażowanych w przetwarzanie pod jego kierownictwem, takich jak członkowie kadry kierowniczej lub pracownicy spółki, oraz do sprawowania odpowiedniej kontroli i nadzoru (art. 28 ust. 1 PIPA).

(20) Szczególne obowiązki mają zastosowanie, gdy administrator („podmiot zlecający usługi outsourcingowe") zleca przetwarzanie danych osobowych stronie trzeciej w ramach outsourcingu („dostawca usług outsourcingowych"). W szczególności outsourcing musi być regulowany prawnie wiążącymi ustaleniami (zazwyczaj umową) ([30]), które określają zakres prac zleconych w ramach outsourcingu, cel przetwarzania, zabezpieczenia techniczne i zarządcze, które należy zastosować, nadzór administratora, odpowiedzialność (np. odszkodowanie za szkody spowodowane naruszeniem zobowiązań umownych), jak również ograniczenia w zakresie podwykonawstwa przetwarzania ([31]) (art. 26 ust. 1 i 2 PIPA w związku z art. 28 ust. 1 dekretu wykonawczego) ([32]).

(21) Ponadto administrator zobowiązany jest opublikować i stale aktualizować szczegółowe informacje na temat prac zleconych w ramach outsourcingu i tożsamości dostawcy usług outsourcingowych lub – w zakresie, w jakim przetwarzanie będące przedmiotem outsourcingu dotyczy działań z zakresu marketingu bezpośredniego – bezpośrednio przekazać osobom fizycznym stosowne informacje (art. 26 ust. 2 i 3 PIPA w związku z art. 28 ust. 2–5 dekretu wykonawczego) ([33]).

(22) Ponadto, zgodnie z art. 26 ust. 4 PIPA w związku z art. 28 ust. 6 dekretu wykonawczego, administrator ma obowiązek przeszkolić dostawcę usług outsourcingowych w zakresie niezbędnych środków bezpieczeństwa i nadzorować, w tym w drodze kontroli, czy podmiot ten wypełnia wszystkie obowiązki administratora wynikające z PIPA ([34]) oraz umowy outsourcingu. W przypadku wyrządzenia przez dostawcę usług outsourcingowych szkody na skutek naruszenia PIPA jego działanie lub zaniechanie zostanie przypisane administratorowi do celów przypisania odpowiedzialności, tak jak w przypadku pracownika (art. 26 ust. 6 PIPA).

([26]) Art. 2 ust. 2 PIPA.
([27]) Na przykład art. 15–19 PIPA odnoszą się jedynie do zbierania, wykorzystywania i przekazywania danych osobowych.
([28]) Art. 2 ust. 5 PIPA. Instytucje publiczne w rozumieniu PIPA obejmują wszystkie wydziały lub agencje administracji centralnej oraz ich organy powiązane, samorządy terytorialne, szkoły i podmioty prawa publicznego będące własnością samorządu terytorialnego, organy administracyjne Zgromadzenia Narodowego oraz sądy (w tym Trybunał Konstytucyjny) (art. 2 ust. 6 PIPA w związku z art. 2 dekretu wykonawczego do PIPA).
([29]) Odpowiada to zakresowi przedmiotowemu stosowania rozporządzenia (UE) 2016/679. Zgodnie z art. 2 ust. 1 rozporządzenia (UE) 2016/679 rozporządzenie ma zastosowanie do „przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych". W art. 4 pkt 6 rozporządzenia (UE) 2016/679 zdefiniowano „zbiór danych" jako „uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów". Zgodnie z tym w motywie 15 wyjaśniono, że ochrona osób fizycznych powinna mieć zastosowanie do „zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów nie powinny być objęte zakresem niniejszego rozporządzenia".
([30]) Zob. podręcznik dotyczący PIPA, rozdział III sekcja 2 poświęcona art. 26 (s. 203–212), w którym wyjaśniono, że art. 26 ust. 1 PIPA odnosi się do wiążących ustaleń, takich jak umowy lub podobne porozumienia.
([31]) Zgodnie z art. 26 ust. 5 PIPA podmiotowi przetwarzającemu nie wolno wykorzystywać danych osobowych poza zakresem prac zleconych w ramach outsourcingu ani przekazywać danych osobowych stronie trzeciej. Nieprzestrzeganie tego wymogu może prowadzić do nałożenia sankcji karnej zgodnie z art. 71 pkt 2 PIPA.
([32]) Niespełnienie tego wymogu może prowadzić do nałożenia kary pieniężnej, zob. art. 75 ust. 4 pkt 4 PIPA.
([33]) Niespełnienie tego wymogu może prowadzić do nałożenia kary pieniężnej, zob. art. 75 ust. 2 pkt 1 ust. 4 pkt 5 PIPA.
([34]) Zob. również art. 26 ust. 7 PIPA, zgodnie z którym art. 15–25, 27–31, 33–38 i 50 stosuje się odpowiednio do podmiotu przetwarzającego.

(23) Mimo iż w PIPA nie używa się różnych pojęć na określenie „administratorów" i „podmiotów przetwarzających", przepisy dotyczące outsourcingu zapewniają obowiązki i zabezpieczenia zasadniczo odpowiadające obowiązkom i zabezpieczeniom regulującym stosunki między administratorami a podmiotami przetwarzającymi na mocy rozporządzenia (UE) 2016/679.

2.2.4 *Przepisy szczególne dotyczące dostawców usług informacyjnych i komunikacyjnych*

(24) Chociaż PIPA ma zastosowanie do przetwarzania danych osobowych przez każdego administratora danych, niektóre przepisy zawierają szczegółowe przepisy (jako *lex specialis*) dotyczące przetwarzania danych osobowych „użytkowników" przez „dostawców usług informacyjnych i komunikacyjnych" ([35]). Pojęcie „użytkowników" obejmuje osoby fizyczne, które korzystają z usług informacyjnych i komunikacyjnych (art. 2 ust. 1 pkt 4 ustawy o wspieraniu wykorzystania sieci informacyjno-komunikacyjnej i ochronie danych, zwanej ustawą o sieci). Warunkiem jest, aby osoba fizyczna albo bezpośrednio korzystała z usług telekomunikacyjnych świadczonych przez koreańskiego operatora telekomunikacyjnego, albo korzystała z usług informacyjnych ([36]) świadczonych komercyjnie (tj. w celach zarobkowych) przez podmiot, który z kolei korzysta z usług operatora telekomunikacyjnego licencjonowanego/zarejestrowanego w Korei ([37]). W obu przypadkach podmiotem związanym szczegółowymi przepisami PIPA jest podmiot, który oferuje usługę online bezpośrednio osobie fizycznej (tj. użytkownikowi).

(25) Natomiast ustalenie adekwatności dotyczy wyłącznie stopnia ochrony zapewnionej danym osobowym przekazanym przez administratora/podmiot przetwarzający w Unii podmiotowi w państwie trzecim (w tym przypadku: w Republice Korei). W tym ostatnim scenariuszu osoby fizyczne w Unii będą zazwyczaj miały bezpośredni związek jedynie z „podmiotem przekazującym dane" w Unii, a nie z koreańskim dostawcą usług informacyjnych i komunikacyjnych ([38]). Dlatego też przepisy szczegółowe PIPA dotyczące danych osobowych użytkowników usług informacyjnych i komunikacyjnych będą miały zastosowanie co najwyżej w ograniczonych sytuacjach wyłącznie do danych osobowych przekazywanych na podstawie niniejszej decyzji.

2.2.5 *Wyłączenie stosowania niektórych przepisów PIPA*

(26) W art. 58 ust. 1 PIPA wyłączono stosowanie części przepisów PIPA (tj. art. 15–57) w odniesieniu do czterech kategorii przetwarzania danych ([39]). W szczególności nie mają zastosowania części PIPA dotyczące szczególnych podstaw przetwarzania, niektórych obowiązków w zakresie ochrony danych, szczegółowych zasad wykonywania praw indywidualnych, jak również zasad rozstrzygania sporów przez Komisję ds. Mediacji w Sporach Dotyczących Danych Osobowych (ang. Personal Information Dispute Mediation Committee). Inne przepisy podstawowe PIPA nadal mają zastosowanie, w szczególności przepisy ogólne dotyczące zasad ochrony danych (art. 3 PIPA) – w tym np. zasady zgodności z prawem, określania celu i ograniczenia celu, minimalizacji danych, prawidłowości i bezpieczeństwa danych – oraz praw indywidualnych (prawa dostępu, prawa do sprostowania, usunięcia i zawieszenia przetwarzania, zob. art. 4 PIPA). Ponadto w art. 58 ust. 4 PIPA nakłada się szczególne obowiązki w związku z takimi czynnościami przetwarzania, mianowicie w odniesieniu do minimalizacji danych, ograniczonego zatrzymywania danych, środków bezpieczeństwa i rozpatrywania skarg ([40]). W związku z tym osoby fizyczne mogą nadal wnieść skargę do PIPC, jeżeli te zasady i obowiązki nie będą przestrzegane, a PIPC jest uprawniona do podejmowania działań w celu ich wyegzekwowania.

([35]) Zob. w szczególności art. 18 ust. 2 oraz rozdział VI PIPA.

([36]) Usługi informacyjne obejmują zarówno dostarczanie informacji, jak i usługi pośrednictwa w dostarczaniu informacji.

([37]) Zob. art. 2 ust. 1 pkt 3 (w związku z art. 2 ust. 1 pkt 2 i 4) ustawy o sieci oraz art. 2 ust. 6 i 8 ustawy o działalności telekomunikacyjnej.

([38]) W zakresie, w jakim koreańscy dostawcy usług informacyjnych i komunikacyjnych pozostawaliby w bezpośrednich stosunkach z osobami fizycznymi w UE (poprzez oferowanie usług online), mogłoby to prowadzić do bezpośredniego stosowania rozporządzenia (UE) 2016/679 zgodnie z jego art. 3 ust. 2 lit. a).

([39]) Art. 58 ust. 2 PIPA stanowi ponadto, że art. 15, art. 22, art. 27 ust. 1–2, art. 34 i art. 37 nie mają zastosowania do danych osobowych przetwarzanych za pomocą urządzeń do przetwarzania danych wizualnych, zainstalowanych i obsługiwanych w miejscach publicznie dostępnych. Jako że przepis ten dotyczy stosowania monitoringu wizyjnego na terytorium Korei, tj. bezpośredniego zbierania danych osobowych od osób fizycznych w Korei, nie jest on istotny do celów niniejszej decyzji, która obejmuje przekazywanie danych osobowych przez administratorów/podmioty przetwarzające w UE podmiotom w Korei. Ponadto, zgodnie z art. 58 ust. 3 PIPA, art. 15 (zbieranie i wykorzystywanie danych osobowych), art. 30 (obowiązek wprowadzenia publicznej polityki prywatności) i art. 31 (obowiązek wyznaczenia urzędnika ds. ochrony prywatności) nie mają zastosowania do danych osobowych, które są przetwarzane w celu prowadzenia grup lub stowarzyszeń w celach towarzyskich (np. klubów hobbystycznych). Ze względu na to, że takie grupy są uważane za grupy o charakterze osobistym, niemające związku z działalnością zawodową czy handlową, nie jest wymagana żadna szczególna podstawa prawna (taka jak zgoda zainteresowanych osób fizycznych) do zbierania i wykorzystywania ich danych w tym kontekście. Jednakże wszystkie inne przepisy PIPA (np. minimalizacja danych, ograniczenie celu, zgodność przetwarzania z prawem, bezpieczeństwo i prawa indywidualne) nadal mają zastosowanie. Ponadto wszelkie przetwarzanie danych osobowych wykraczające poza cel utworzenia grupy społecznej nie byłoby objęte tym wyjątkiem.

([40]) W szczególności w art. 58 ust. 4 PIPA przewidziano obowiązek przetwarzania danych osobowych w minimalnym zakresie niezbędnym do osiągnięcia zamierzonego celu, przetwarzania ich przez minimalny okres oraz dokonania niezbędnych ustaleń w celu bezpiecznego zarządzania takimi danymi osobowymi i ich odpowiedniego przetwarzania. Ten ostatni element obejmuje zabezpieczenia techniczne, zarządcze i fizyczne, jak również środki zapewniające właściwe rozpatrywanie skarg indywidualnych.

(27) Po pierwsze, wyłączenie częściowe obejmuje dane osobowe zbierane zgodnie z ustawą o danych statystycznych w celu ich przetwarzania przez instytucje publiczne. Zgodnie z wyjaśnieniami otrzymanymi od rządu Korei dane osobowe przetwarzane w tym kontekście zwykle dotyczą obywateli koreańskich i tylko wyjątkowo mogą obejmować informacje o cudzoziemcach, mianowicie w przypadku statystyk dotyczących wjazdu na terytorium kraju i wyjazdu z niego lub inwestycji zagranicznych. Jednak nawet w takich sytuacjach dane takie nie są zazwyczaj przekazywane przez administratorów/podmioty przetwarzające w Unii, lecz są raczej bezpośrednio zbierane przez organy publiczne w Korei ([41]). Ponadto, podobnie jak określono w motywie 162 rozporządzenia (UE) 2016/679, przetwarzanie danych na podstawie ustawy o danych statystycznych podlega szeregowi warunków i zabezpieczeń. W szczególności ustawa o danych statystycznych nakłada szczególne obowiązki, takie jak zapewnienie prawidłowości, spójności i bezstronności; gwarancja poufności danych osób fizycznych; ochrona informacji o respondentach ankiet statystycznych, w tym w celu zapobiegania wykorzystywaniu takich informacji do celów innych niż opracowywanie danych statystycznych, oraz objęcia pracowników wymogami zachowania poufności ([42]). Organy publiczne przetwarzające dane statystyczne muszą również przestrzegać m.in. zasad minimalizacji danych, ograniczenia celu i bezpieczeństwa (art. 3 i art. 58 ust. 4 PIPA) oraz umożliwiać osobom fizycznym korzystanie z przysługujących im praw (prawa dostępu, prawa do korekty, usuwania i zawieszenia, zob. art. 4 PIPA). Ponadto dane muszą być przetwarzane w formie zanonimizowanej lub spseudonimizowanej, jeżeli pozwala to na spełnienie celu przetwarzania (art. 3 ust. 7 PIPA).

(28) Po drugie, art. 58 ust. 1 PIPA odnosi się do danych osobowych zbieranych lub żądanych do celów przeprowadzenia analizy informacji związanych z bezpieczeństwem narodowym. Zakres i skutki tego wyłączenia częściowego opisano bardziej szczegółowo w motywie (149).

(29) Po trzecie, wyłączenie częściowe ma zastosowanie do tymczasowego przetwarzania danych osobowych, w przypadku gdy jest to pilnie potrzebne ze względów bezpieczeństwa publicznego i ochrony, w tym zdrowia publicznego. Kategoria ta jest interpretowana przez PIPC wąsko i zgodnie z otrzymanymi informacjami nigdy nie została zastosowana. Ma ona zastosowanie wyłącznie w nagłych przypadkach wymagających pilnych działań, np. w celu wykrycia czynników zakaźnych lub ratowania ofiar klęsk żywiołowych i udzielenia im pomocy ([43]). Nawet w takich sytuacjach wyłączenie częściowe obejmuje przetwarzanie danych osobowych jedynie przez ograniczony okres, w celu przeprowadzenia takich działań. Sytuacje, w których mogłoby to mieć zastosowanie do przekazywania danych objętych niniejszą decyzją, są jeszcze bardziej ograniczone, biorąc pod uwagę niskie prawdopodobieństwo, że dane osobowe przekazywane z Unii operatorom koreańskim byłyby danymi tego rodzaju, że ich dalsze przetwarzanie byłoby „pilnie potrzebne" w takich nagłych przypadkach.

(30) Wreszcie wyłączenie częściowe ma zastosowanie do danych osobowych zbieranych lub wykorzystywanych przez prasę, do działalności misyjnej prowadzonej przez organizacje religijne lub do celów zgłaszania kandydatów przez partie polityczne. Wyłączenie to ma zastosowanie wyłącznie w przypadku przetwarzania danych osobowych przez prasę, organizacje religijne lub partie polityczne do tych szczególnych celów (tj. działalności dziennikarskiej, pracy misyjnej i zgłaszania kandydatów na stanowiska polityczne). Jeżeli podmioty te przetwarzają dane osobowe do innych celów, takich jak zarządzanie zasobami ludzkimi lub administracja wewnętrzna, PIPA ma zastosowanie w pełnym zakresie.

(31) W przypadku przetwarzania danych osobowych przez prasę do celów działalności dziennikarskiej równowagę między wolnością wypowiedzi a innymi prawami (w tym prawem do prywatności) zapewnia ustawa o arbitrażu i innych środkach ochrony prawnej w przypadku szkód wyrządzonych wskutek publikacji prasowych (ustawa prasowa) ([44]). W szczególności art. 5 ustawy prasowej stanowi, że prasa (tj. każda organizacja medialna, gazeta,

([41]) W tym zakresie w art. 33 ustawy o danych statystycznych nałożono na instytucje publiczne obowiązek ochrony informacji o respondentach ankiet statystycznych, w tym do zapobiegania wykorzystywaniu takich informacji do celów innych niż opracowywanie statystyk.

([42]) Art. 2 ust. 2–3, art. 30 ust. 2, art. 33 i art. 34 ustawy o danych statystycznych.

([43]) Podręcznik dotyczący PIPA, sekcja poświęcona art. 58.

([44]) Na przykład art. 4 ustawy prasowej stanowi, że publikacje prasowe muszą być bezstronne i obiektywne, muszą leżeć w interesie publicznym, nie mogą podważać godności i wartości człowieka, zniesławiać innych osób ani naruszać ich praw, moralności publicznej czy etyki społecznej.

czasopismo lub gazeta internetowa), żaden internetowy serwis informacyjny ani internetowa organizacja multimedialna nie może naruszać prywatności osób fizycznych. Jeżeli jednak dojdzie do naruszenia prywatności, należy je niezwłocznie usunąć zgodnie ze szczególnymi procedurami określonymi w ustawie. W tym zakresie w ustawie przyznano osobom, które poniosły szkodę wskutek materiału prasowego, szereg uprawnień, takich jak żądanie opublikowania sprostowania nieprawdziwej informacji, materiału o sprzecznej treści lub kolejnego materiału prasowego (w przypadku gdy publikacja prasowa dotyczy zarzutów popełnienia przestępstwa, z których dana osoba fizyczna została później oczyszczona) ([45]). Skargi osób fizycznych mogą być rozstrzygane przez redakcje prasowe bezpośrednio (za pośrednictwem rzecznika) ([46]), w drodze postępowania pojednawczego lub polubownego (przed wyspecjalizowaną komisją arbitrażową ds. prasy) ([47]) lub przed sądem. Osoby fizyczne mogą również uzyskać odszkodowanie, gdy doznają szkody majątkowej, naruszenia dóbr osobistych lub innego rodzaju cierpienia emocjonalnego z powodu bezprawnego działania prasy (z winy umyślnej lub przez niedbalstwo) ([48]). Prasa jest zwolniona z odpowiedzialności na mocy ustawy w zakresie, w jakim publikacja prasowa, która narusza prawa jednostki, nie jest sprzeczna z wartościami społecznymi i ukazała się za zgodą zainteresowanej osoby lub w interesie publicznym (i istnieją wystarczające podstawy, aby uznać, że doniesienie odpowiada prawdzie) ([49]).

(32) O ile zatem przetwarzanie danych osobowych przez prasę na potrzeby działalności dziennikarskiej podlega szczególnym zabezpieczeniom, które wynikają z ustawy prasowej, o tyle brak jest takich dodatkowych zabezpieczeń obramowujących korzystanie z wyjątków dotyczących czynności przetwarzania przez organizacje religijne i partie polityczne w sposób porównywalny do art. 85, 89 i 91 rozporządzenia (UE) 2016/679. Komisja uważa zatem za właściwe wyłączenie z zakresu stosowania niniejszej decyzji organizacji religijnych w zakresie, w jakim przetwarzają one dane osobowe na potrzeby swojej działalności misyjnej, oraz partii politycznych w zakresie, w jakim przetwarzają one dane osobowe w kontekście zgłaszania kandydatów.

2.3 **Zabezpieczenia, prawa i obowiązki**

2.3.1 *Zgodność z prawem i rzetelność przetwarzania*

(33) Dane osobowe powinno się przetwarzać zgodnie z prawem i rzetelnie.

(34) Zasada ta została ustanowiona w art. 3 ust. 1 i 2 PIPA i wzmocniona w art. 59 PIPA, w którym zabrania się przetwarzania danych osobowych „w wyniku oszustwa, w sposób niewłaściwy lub nieuczciwy", „bez podstawy prawnej" lub „poza zakresem należytego upoważnienia" ([50]). Te ogólne zasady zgodnego z prawem przetwarzania danych rozwinięto w art. 15–19 PIPA, w których określono poszczególne podstawy prawne przetwarzania danych (zbieranie, wykorzystywanie i przekazywanie stronom trzecim), w tym okoliczności, w których może się z nim wiązać zmiana celu (art. 18 PIPA).

([45]) Art. 15–17 ustawy prasowej.

([46]) Każda redakcja prasowa i medialna musi mieć swojego rzecznika, którego zadaniem jest zapobieganie wszelkim potencjalnym szkodom wyrządzonym przez publikacje i ich naprawianie (np. poprzez zalecanie sprostowania doniesień prasowych, które są fałszywe lub szkodzą dobremu imieniu innych), art. 6 ustawy prasowej.

([47]) W skład komisji wchodzi 40–90 komisarzy arbitrażowych, powoływanych przez Ministra Kultury, Sportu i Turystyki spośród osób posiadających kwalifikacje sędziowskie, adwokackie, osób zajmujących się przez co najmniej 10 lat gromadzeniem lub rozpowszechnianiem informacji lub innych osób posiadających wiedzę fachową związaną z prasą. Komisarze arbitrażowi nie mogą być jednocześnie urzędnikami publicznymi, członkami partii politycznych ani dziennikarzami. Zgodnie z art. 8 ustawy prasowej komisarze arbitrażowi muszą wykonywać swoje obowiązki w sposób niezależny i nie mogą otrzymywać żadnych poleceń ani instrukcji w związku z wykonywaniem tych obowiązków. Ponadto istnieją przepisy szczególne mające na celu zapobieganie konfliktom interesów, np. poprzez wykluczenie poszczególnych komisarzy z prowadzenia indywidualnych spraw, w których stroną jest ich małżonek lub krewni (art. 10 ustawy prasowej). Komisja może rozpatrywać spory w drodze postępowania pojednawczego lub polubownego, ale może również wydawać zalecenia w celu usunięcia naruszeń (art. 5 ustawy prasowej).

([48]) Art. 30 ustawy prasowej.

([49]) Art. 5 ustawy prasowej.

([50]) W art. 59 PIPA zabrania się każdej osobie, „która przetwarza lub kiedykolwiek przetwarzała dane osobowe", „pozyskiwania danych osobowych lub uzyskiwania zgody na przetwarzanie danych osobowych w wyniku oszustwa, w sposób niewłaściwy lub nieuczciwy", „ujawniania danych osobowych uzyskanych w trakcie prowadzenia działalności gospodarczej lub udostępniania ich stronie trzeciej do wykorzystania bez upoważnienia" lub „uszkadzania, niszczenia, zmieniania, fałszowania lub ujawniania danych osobowych innych osób bez podstawy prawnej lub poza zakresem należytego upoważnienia". Naruszenie tego zakazu może prowadzić do nałożenia sankcji karnych, zob. art. 71 pkt 5 i 6 oraz art. 72 pkt 2 PIPA. W art. 70 pkt 2 PIPA przewidziano ponadto możliwość nałożenia sankcji karnej za uzyskanie danych osobowych przetwarzanych przez strony trzecie w drodze oszustwa lub za pomocą innych nieuczciwych środków lub metod lub za przekazanie ich stronie trzeciej w celach zarobkowych lub nieuczciwych, jak również za podżeganie do takich działań lub ich organizowanie.

(35) Zgodnie z art. 15 ust. 1 PIPA administrator może zbierać dane osobowe (w zakresie celu zbierania) jedynie w oparciu o ograniczoną liczbę podstaw prawnych. Są to: 1) zgoda osoby, której dane dotyczą ([51]) (pkt 1); 2) niezbędność tych danych do wykonania umowy zawartej z osobą, której dane dotyczą (pkt 4); 3) specjalne upoważnienie ustawowe lub konieczność wypełnienia obowiązku prawnego (pkt 2); niezbędność tych danych ([52]) do wykonywania przez instytucję publiczną zadań wchodzących w zakres jej właściwości zgodnie z przepisami prawa; 4) sytuacja, gdy dane te są w sposób oczywisty niezbędne do ochrony życia, integralności cielesnej lub interesów majątkowych osoby, której dane dotyczą, lub strony trzeciej przed bezpośrednim niebezpieczeństwem (wyłącznie jeśli osoba, której dane dotyczą, nie jest w stanie wyrazić swojej woli lub nie można uzyskać jej uprzedniej zgody) (pkt 5); 5) niezbędność tych danych do realizacji „uzasadnionego interesu" administratora, jeżeli jest on „w oczywisty sposób nadrzędny" wobec interesów osoby, której dane dotyczą (i wyłącznie jeśli przetwarzanie ma „istotny związek" z prawnie uzasadnionym interesem i nie wykracza poza to, co jest uzasadnione) (pkt 6) ([53]). Te podstawy przetwarzania zasadniczo odpowiadają podstawom określonym w art. 6 rozporządzenia (UE) 2016/679, w tym przesłance „uzasadnionego interesu", która jest równoważna z przesłanką „prawnie uzasadnionego interesu" określoną w art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679.

(36) Zebrane dane osobowe mogą być wykorzystywane w zakresie objętym celem zbierania (art. 15 ust. 1 PIPA) lub „w zakresie racjonalnie powiązanym" z celem zbierania, biorąc pod uwagę ewentualne niedogodności dla osoby, której dane dotyczą, oraz pod warunkiem wprowadzenia niezbędnych środków bezpieczeństwa (np. szyfrowania) (art. 15 ust. 3 PIPA). Aby ustalić, czy cel wykorzystania jest „racjonalnie powiązany" z pierwotnym celem zbierania, w dekrecie wykonawczym określono szczegółowe kryteria, które są podobne do kryteriów przewidzianych w art. 6 ust. 4 rozporządzenia (UE) 2016/679. W szczególności zbieranie danych musi mieć istotne znaczenie dla pierwotnego celu; dodatkowe wykorzystanie musi być przewidywalne (na przykład w świetle okoliczności, w których zebrano informacje) oraz, o ile to możliwe, dane muszą zostać spseudonimizowane ([54]). Konkretne kryteria stosowane przez administratora w ramach tej oceny muszą zostać wcześniej ujawnione w polityce prywatności ([55]). Ponadto urzędnik ds. ochrony prywatności (zob. motyw (94)) jest szczególnie zobowiązany do sprawdzenia, czy dalsze wykorzystanie odbywa się w ramach tych parametrów.

([51]) Zgoda musi być dobrowolna, świadoma, konkretna i wyrażona w jeden z kilku sposobów określonych w przepisach prawa. W żadnym wypadku zgoda nie może być uzyskana w wyniku oszustwa ani z zastosowaniem niewłaściwych lub z innych względów niesłusznych środków (art. 59 ust. 1 PIPA). Po pierwsze, zgodnie z art. 4 pkt 2 PIPA osoby, których dane dotyczą, mają prawo „wyrazić zgodę lub nie" i „wybrać zakres zgody" oraz powinny zostać o tym poinformowane (art. 15 ust. 2, art. 16 ust. 2 i 3, art. 17 ust. 2 i art. 18 ust. 3 PIPA). W art. 22 ust. 5 PIPA przewidziano dalsze zabezpieczenie w postaci zakazu odmowy przez administratora dostarczenia towarów lub świadczenia usług, jeżeli mogłoby to podważyć wolny wybór osoby fizycznej w zakresie wyrażenia zgody. Obejmuje to sytuacje, w których tylko niektóre rodzaje przetwarzania wymagają zgody (podczas gdy inne opierają się na umowie), jak również dalsze przetwarzanie danych osobowych zebranych w kontekście dostarczania towarów lub świadczenia usług. Po drugie, zgodnie z art. 15 ust. 2, art. 17 ust. 2 i 3 oraz art. 18 ust. 3 PIPA, zwracając się o zgodę, administrator musi poinformować osobę, której dane dotyczą, o „szczegółach" przedmiotowych danych osobowych (np. że chodzi o dane wrażliwe, zob. art. 17 ust. 2 pkt 2 lit. a) dekretu wykonawczego do PIPA), celu przetwarzania, okresie zatrzymywania danych oraz wszelkich odbiorcach tych danych. Każda taka prośba o zgodę musi być wyrażona „w wyraźnie rozpoznawalny sposób", odróżniający sprawy wymagające zgody od innych spraw (art. 22 ust. 1–4 PIPA). Po trzecie, art. 17 ust. 1 pkt 1–6 dekretu wykonawczego do PIPA przewiduje konkretne sposoby uzyskania zgody przez administratora, takie jak pisemna zgoda z podpisem osoby, której dane dotyczą, lub zgoda w formie (zwrotnej) wiadomości e-mail. Mimo że PIPA nie zapewnia konkretnie osobom fizycznym ogólnego prawa do wycofania zgody, zamiast tego osoby fizyczne mają prawo uzyskać zawieszenie przetwarzania danych ich dotyczących, a skorzystanie z takiego prawa doprowadzi do zakończenia przetwarzania i usunięcia danych (zob. motyw 78 na temat prawa do zawieszenia).

([52]) Zgodnie z informacjami otrzymanymi od PIPC instytucje publiczne mogą powoływać się na tę podstawę wyłącznie wówczas, gdy przetwarzanie danych osobowych jest niemożliwe do uniknięcia, tj. wykonywanie przez instytucję jej funkcji bez przetwarzania danych musi być niemożliwe lub nadmiernie utrudnione.

([53]) W art. 39-3 PIPA nakłada się na dostawców usług informacyjnych i komunikacyjnych szczególne (bardziej restrykcyjne) obowiązki w zakresie zbierania i wykorzystywania danych osobowych ich użytkowników. W szczególności wymaga się w nim, aby dostawca uzyskał zgodę użytkownika po podaniu informacji o celu zbierania/wykorzystania, kategoriach danych osobowych, które mają być zbierane, oraz okresie, przez jaki dane będą przetwarzane (art. 39-3 ust. 1 PIPA). To samo dotyczy zmiany któregokolwiek z tych aspektów. Nieuzyskanie zgody na zbieranie informacji jest zagrożone sankcjami karnymi (art. 71 ust. 4–5 PIPA). Wyjątkowo dane osobowe użytkowników mogą być zbierane lub wykorzystywane przez dostawców usług informacyjnych i komunikacyjnych bez uzyskania uprzedniej zgody. Dzieje się tak w przypadku 1) gdy ze względów ekonomicznych i technologicznych wyraźnie trudno jest uzyskać zwykłą zgodę w odniesieniu do danych osobowych wymaganych do realizacji umowy regulującej świadczenie usług informacyjnych i komunikacyjnych (np. gdy w procesie wykonania umowy nieuchronnie powstają dane osobowe, takie jak informacje rozliczeniowe, dzienniki dostępu i rejestr płatności); 2) gdy jest to niezbędne do rozliczenia opłat za świadczenie usług informacyjnych i komunikacyjnych lub 3) jeżeli zezwalają na to inne przepisy prawa (np. art. 21 ust. 1 pkt 6 ustawy o ochronie konsumentów w handlu elektronicznym stanowi, że przedsiębiorcy mogą zbierać dane osobowe opiekunów prawnych małoletniego w celu potwierdzenia, czy uzyskano zgodę w jego imieniu) (art. 39-3 ust. 2 PIPA). We wszystkich przypadkach dostawcy usług informacyjnych i komunikacyjnych nie mogą odmówić świadczenia usług tylko dlatego, że użytkownik nie dostarcza więcej danych osobowych niż minimum wymaganych informacji (tj. informacji, które są niezbędne do wykonania podstawowych elementów danej usługi), zob. art. 39-3 ust. 3 PIPA.

([54]) Zob. art. 14-2 dekretu wykonawczego do PIPA.

([55]) Zob. art. 14-2 ust. 2 dekretu wykonawczego do PIPA.

(37) Podobne (ale nieco bardziej rygorystyczne) zasady obowiązują w przypadku przekazywania danych stronie trzeciej. Zgodnie z art. 17 ust. 1 PIPA przekazanie danych osobowych stronie trzeciej jest dozwolone na podstawie zgody ([56]) lub, w zakresie objętym celem zbierania, jeżeli informacje zebrano w oparciu o jedną z podstaw prawnych określonych w art. 15 ust. 1 pkt 2, 3 i 5 PIPA. Wyklucza to w szczególności wszelkie ujawnienia oparte na „uzasadnionym interesie" administratora. Poza tym w art. 17 ust. 4 PIPA zezwala się na przekazywanie danych stronom trzecim „w zakresie racjonalnie powiązanym" z celem zbierania, ponownie z uwzględnieniem ewentualnych niedogodności dla osoby, której dane dotyczą, oraz pod warunkiem przyjęcia niezbędnych środków bezpieczeństwa (takich jak szyfrowanie). Przy ocenie, czy przekazywanie mieści się w zakresie racjonalnie powiązanym z celem zbierania, muszą być brane pod uwagę te same czynniki, co opisane w motywie (36), i mają zastosowanie te same zabezpieczenia (tj. w odniesieniu do przejrzystości na podstawie polityki prywatności i w drodze zaangażowania urzędnika ds. ochrony prywatności).

(38) Otrzymanie danych osobowych z Unii przez koreańskiego administratora danych osobowych jest uważane za „zbieranie" w rozumieniu art. 15 PIPA. W zawiadomieniu nr 2021-5 (sekcja I załącznika I do niniejszej decyzji) wyjaśniono, że cel, w którym dane zostały przekazane przez dany podmiot UE, stanowi dla koreańskiego administratora danych osobowych cel zbierania danych. W konsekwencji koreańscy administratorzy danych osobowych otrzymujący dane osobowe z Unii są co do zasady zobowiązani do przetwarzania takich danych w zakresie celu przekazania, zgodnie z art. 17 PIPA.

(39) W przypadku gdy administrator zamierza wykorzystać dane osobowe lub udostępnić je stronie trzeciej w innym celu niż cel zbierania, zastosowanie mają szczególne ograniczenia ([57]). Zgodnie z art. 18 ust. 2 PIPA administrator prywatny może wyjątkowo ([58]) wykorzystać dane osobowe lub przekazać je stronie trzeciej w innym celu: 1) na podstawie dodatkowej (tzn. odrębnej) zgody osoby, której dane dotyczą; 2) jeżeli jest to przewidziane w szczególnych przepisach ustawowych lub 3) jeżeli jest to w sposób oczywisty konieczne do ochrony życia, integralności cielesnej lub interesów majątkowych osoby, której dane dotyczą, lub strony trzeciej przed bezpośrednim niebezpieczeństwem (wyłącznie jeśli osoba, której dane dotyczą, nie jest w stanie wyrazić swojej woli i nie jest możliwe uzyskanie uprzedniej zgody) ([59]).

(40) Instytucje publiczne mogą także w określonych sytuacjach wykorzystać dane osobowe lub udostępnić je stronie trzeciej w innym celu. Obejmuje to przypadki, w których w przeciwnym razie instytucje publiczne nie mogłyby wykonywać swoich ustawowych obowiązków zgodnie z prawem, z zastrzeżeniem zezwolenia PIPC. Ponadto instytucje publiczne mogą udostępnić dane osobowe innemu organowi lub sądowi, gdy jest to niezbędne do prowadzenia postępowania przygotowawczego i ścigania przestępstw; do wykonywania przez sąd funkcji związanych z toczącym się postępowaniem sądowym lub do egzekwowania sankcji karnej lub nakazu opieki, lub władzy rodzicielskiej ([60]). Mogą one również udostępnić dane osobowe obcemu rządowi lub organizacji międzynarodowej w celu wypełnienia zobowiązania prawnego wynikającego z traktatu lub konwencji międzynarodowej, w którym to przypadku muszą również przestrzegać wymogów dotyczących przekazywania danych na poziomie transgranicznym (zob. motyw (90)).

(41) Zasady zgodności z prawem i rzetelności przetwarzania są zatem wdrożone w koreańskich ramach prawnych w sposób zasadniczo odpowiadający przepisom rozporządzenia (UE) 2016/679, zezwalając na przetwarzanie wyłącznie w oparciu o uzasadnione i jasno określone podstawy. Ponadto we wszystkich wymienionych przypadkach przetwarzanie jest dozwolone wyłącznie wówczas, gdy nie jest prawdopodobne, że „naruszy w sposób nieuzasadniony" interesy osoby, której dane dotyczą, lub strony trzeciej, co wymaga wyważenia interesów. Ponadto art. 18 ust. 5 PIPA przewiduje dodatkowe zabezpieczenia, w przypadku gdy administrator udostępnia dane osobowe stronie trzeciej, co może obejmować żądanie ograniczenia celu i sposobu wykorzystania lub wprowadzenia określonych środków bezpieczeństwa. Z kolei strona trzecia jest zobowiązana do wdrożenia żądanych środków.

([56]) Naruszenia art. 17 ust. 1 pkt 1 PIPA mogą prowadzić do nałożenia sankcji karnych (art. 71 ust. 1 PIPA).

([57]) „Zamierzony cel" to cel, w którym zebrano informacje. Na przykład gdy informacje są zbierane na podstawie zgody osoby fizycznej, której dane dotyczą, zamierzony cel to cel, o którym informuje się osobę fizyczną na podstawie art. 15 ust. 2 PIPA.

([58]) Por. art. 18 ust. 1 PIPA. Naruszenia art. 18 ust. 1 i 2 PIPA mogą prowadzić do nałożenia sankcji karnych (art. 71 ust. 2 PIPA).

([59]) Wykorzystywanie danych osobowych lub ich przekazywanie stronie trzeciej przez dostawców usług informacyjnych i komunikacyjnych w innym celu niż pierwotny może następować wyłącznie w oparciu o podstawy określone w art. 18 ust. 2 pkt 1 i 2 PIPA (tj. w przypadku uzyskania dodatkowej zgody lub gdy istnieją przepisy szczególne). Zob. art. 18 ust. 2 PIPA.

([60]) Z wyjątkiem sytuacji, gdy przetwarzanie jest niezbędne do celów prowadzenia postępowania przygotowawczego w sprawie przestępstwa, wniesienia aktu oskarżenia i ścigania, instytucje publiczne, które wykorzystują dane osobowe lub udostępniają je stronie trzeciej w innym celu niż cel zbierania (na przykład gdy jest to wyraźnie dozwolone na mocy przepisów prawa lub niezbędne do wykonania umowy), są zobowiązane do opublikowania podstaw prawnych przetwarzania, jego celu i zakresu na swojej stronie internetowej lub w Dzienniku Urzędowym oraz do prowadzenia rejestrów (art. 18 ust. 4 PIPA z art. 15 dekretu wykonawczego do PIPA).

(42) Ponadto art. 28-2 PIPA umożliwia (dalsze) przetwarzanie informacji spseudonimizowanych bez zgody zainteresowanej osoby fizycznej do celów statystycznych, do celów badań naukowych ([61]) i do celów archiwalnych w interesie publicznym, z zastrzeżeniem szczególnych zabezpieczeń. Podobnie jak w przypadku rozporządzenia (UE) 2016/679 ([62]) PIPA ułatwia zatem (dalsze) przetwarzanie danych osobowych do takich celów w ramach zapewniających odpowiednie zabezpieczenia na potrzeby ochrony praw osób fizycznych. Zamiast polegać na pseudonimizacji jako możliwym zabezpieczeniu, w PIPA przewidziany jest wymóg zastosowania pseudonimizacji jako warunku wstępnego przeprowadzenia określonych czynności przetwarzania do celów statystycznych, do celów badań naukowych i do celów archiwalnych w interesie publicznym (dotyczy to na przykład możliwości przetwarzania danych bez zgody lub łączenia różnych zbiorów danych).

(43) Ponadto PIPA nakłada szereg szczególnych zabezpieczeń, w szczególności w zakresie wymaganych środków technicznych i organizacyjnych, prowadzenia rejestrów, ograniczeń udostępniania danych oraz przeciwdziałania ewentualnemu ryzyku ponownej identyfikacji. Połączenie poszczególnych zabezpieczeń opisanych w motywach (44)–(48) gwarantuje, że przetwarzanie danych osobowych w tym kontekście podlega zabezpieczeniom zasadniczo odpowiadającym tym, które byłyby wymagane zgodnie z rozporządzeniem (UE) 2016/679.

(44) Po pierwsze, co najważniejsze, art. 28-5 ust. 1 PIPA zakazuje przetwarzania informacji spseudonimizowanych w celu identyfikacji określonej osoby fizycznej. Jeżeli jednak podczas przetwarzania informacji spseudonimizowanych zostałyby wygenerowane informacje, które umożliwiałyby zidentyfikowanie danej osoby fizycznej, administrator musi niezwłocznie zawiesić przetwarzanie i zniszczyć takie informacje (art. 28-5 ust. 2 PIPA). Nieprzestrzeganie tych przepisów podlega administracyjnym karom pieniężnym i stanowi przestępstwo ([63]). Oznacza to, że nawet w sytuacjach, w których ponowna identyfikacja osoby fizycznej byłaby możliwa *w praktyce*, taka ponowna identyfikacja jest *prawnie* zabroniona.

(45) Po drugie, przy (dalszym) przetwarzaniu informacji spseudonimizowanych w takich celach, administrator jest zobowiązany do wprowadzenia określonych środków technologicznych, zarządczych i fizycznych w celu zapewnienia bezpieczeństwa informacji (w tym oddzielnego przechowywania informacji niezbędnych do przywrócenia informacji spseudonimizowanych do ich pierwotnego stanu oraz zarządzania nimi) ([64]). Ponadto obowiązuje wymóg prowadzenia rejestru przetwarzanych informacji spseudonimizowanych, celu przetwarzania, historii wykorzystania oraz wszelkich odbiorców będących stronami trzecimi (art. 29-5 ust. 2 dekretu wykonawczego do PIPA).

(46) Po trzecie i ostatnie, PIPA przewiduje szczególne zabezpieczenia zapobiegające identyfikacji osób fizycznych przez strony trzecie, w przypadku gdy informacje są udostępniane. W szczególności przy przekazywaniu informacji spseudonimizowanych stronie trzeciej do celów statystycznych, do celów badań naukowych lub do celów archiwalnych w interesie publicznym administratorzy nie mogą podawać informacji, które mogłyby posłużyć do identyfikacji konkretnej osoby fizycznej (art. 28-2 ust. 2 PIPA) ([65]).

(47) Ściślej mówiąc, chociaż w PIPA zezwolono na łączenie informacji spseudonimizowanych (przetwarzanych przez różnych administratorów) do celów statystycznych, do celów badań naukowych lub do celów archiwalnych w interesie publicznym, zastrzeżono to uprawnienie dla wyspecjalizowanych instytucji wyposażonych w określone środki ochrony (art. 28-3 ust. 1) PIPA) ([66]). Ubiegając się o połączenie danych spseudonimizowanych, administrator musi przedstawić dokumentację dotyczącą m.in. danych, które mają zostać połączone, celu

([61]) Badania naukowe są zdefiniowane w art. 2 ust. 8 PIPA jako „badania, w których wykorzystuje się metody naukowe, takie jak rozwój i demonstracja technologii, badania podstawowe, badania stosowane i badania finansowane ze środków prywatnych". Kategorie te odpowiadają kategoriom określonym w motywie 159 rozporządzenia (UE) 2016/679.

([62]) Zob. art. 5 ust. 1 lit. b) i art. 89 ust. 1–2 oraz motywy 50 i 157 rozporządzenia (UE) 2016/679.

([63]) Zob. art. 28-6 ust. 1, art. 71 pkt 4-3 i art. 75 ust. 2 pkt 4-4 PIPA.

([64]) Zob. art. 28-4 i 29-5 dekretu wykonawczego do PIPA. Niedopełnienie tego obowiązku jest zagrożone sankcjami administracyjnymi i karnymi, zob. art. 73 ust. 1 i art. 75 ust. 2 pkt 6 PIPA.

([65]) Naruszenia tych wymogów mogą prowadzić do nałożenia sankcji karnych (art. 71 ust. 2 PIPA). PIPC od razu przystąpiła do egzekwowania tych nowych przepisów, np. w decyzji z dnia 28 kwietnia 2021 r., którą nałożyła karę pieniężną i wymóg wdrożenia działań naprawczych na przedsiębiorstwo, które oprócz innych naruszeń PIPA nie przestrzegało wymogu art. 28-2 ust. 2 PIPA, zob. https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

([66]) Aby zostać wyznaczonym jako taka wyspecjalizowana instytucja („agencja ekspercka ds. łączenia danych"), należy złożyć wniosek do PIPC wraz z dokumentami potwierdzającymi wyszczególniającymi między innymi obiekty i sprzęt stosowane w celu bezpiecznego łączenia danych spseudonimizowanych i potwierdzającymi, że wnioskodawca zatrudnia co najmniej trzech pełnoetatowych pracowników posiadających kwalifikacje lub doświadczenie w zakresie ochrony danych osobowych (art. 29-2 ust. 1–2 dekretu wykonawczego do PIPA). Szczegółowe wymogi np. w zakresie kwalifikacji personelu, dostępnych obiektów, środków bezpieczeństwa, wewnętrznych polityk i procedur, a także wymogi finansowe określono w zawiadomieniu 2020-9 PIPC w sprawie łączenia i ujawniania informacji spseudonimizowanych (załącznik I). Wyznaczenie agencji eksperckiej ds. łączenia danych może zostać cofnięte przez PIPC (po wysłuchaniu stron) z pewnych powodów, np. jeśli agencja nie spełnia już norm bezpieczeństwa wymaganych do wyznaczenia lub jeśli doszło do naruszenia ochrony danych w kontekście łączenia danych (art. 29-2 ust. 5–6 dekretu wykonawczego do PIPA). PIPC musi poinformować w formie publikacji o każdym przypadku wyznaczenia (lub cofnięcia wyznaczenia) agencji eksperckiej ds. łączenia danych (art. 29-2 ust. 7 dekretu wykonawczego do PIPA).

połączenia, a także proponowanych środków bezpieczeństwa przetwarzania połączonych danych ([67]). Aby umożliwić połączenie, administrator musi przesłać dane, które mają zostać połączone, do wyspecjalizowanej instytucji i przekazać „klucz połączenia" (tj. informacje, które zostały użyte do pseudonimizacji) Koreańskiej Agencji ds. Internetu i Bezpieczeństwa (ang. Korea Internet and Security Agency) ([68]). Ta ostatnia generuje „dane powiązane klucza połączenia" (co pozwala na powiązanie kluczy połączenia różnych wnioskodawców w celu uzyskania połączenia zbiorów danych) i dostarcza je wyspecjalizowanej instytucji ([69]).

(48) Administrator wnioskujący o połączenie może dokonać analizy połączonych informacji w siedzibie wyspecjalizowanej instytucji, w miejscu, w którym stosowane są określone techniczne, fizyczne i administracyjne środki bezpieczeństwa (art. 29-3 dekretu wykonawczego do PIPA). Administratorzy, którzy dostarczają zbiór danych do takiego połączenia, mogą przenieść połączone dane poza wyspecjalizowaną instytucję wyłącznie po dalszej pseudonimizacji lub anonimizacji połączonych danych i za zgodą tej instytucji (art. 28-3 ust. 2 PIPA) ([70]). Ustalając, czy udzielić takiej zgody, instytucja oceni związek między połączonymi danymi a celem przetwarzania oraz czy sporządzono specjalny plan bezpieczeństwa na potrzeby wykorzystania takich danych ([71]). Przenoszenie połączonych informacji poza instytucję nie będzie dozwolone, jeśli informacje zawierają dane umożliwiające identyfikację osoby fizycznej ([72]). Ponadto łączenie i udostępnianie danych spseudonimizowanych przez wyspecjalizowaną instytucję jest nadzorowane przez PIPC (art. 29-4 ust. 3 dekretu wykonawczego do PIPA).

2.3.2 *Przetwarzanie szczególnych kategorii danych osobowych*

(49) Jeżeli przetwarzane są „szczególne kategorie" danych, powinny istnieć szczególne zabezpieczenia.

(50) PIPA zawiera przepisy szczegółowe dotyczące przetwarzania danych wrażliwych ([73]), czyli danych osobowych ujawniających informacje dotyczące światopoglądu, przekonań, przyjęcia do związku zawodowego lub partii politycznej lub wystąpienia z nich, poglądów politycznych, zdrowia oraz życia seksualnego osoby fizycznej, a także innych danych osobowych, które mogą „wyraźnie" zagrozić prywatności osoby, której dane dotyczą, i zostały określone jako informacje szczególnie chronione na mocy dekretu prezydenckiego ([74]). Zgodnie z wyjaśnieniami otrzymanymi od PIPC życie seksualne jest interpretowane jako obejmujące również orientację lub preferencje seksualne danej osoby fizycznej ([75]). Ponadto w art. 18 dekretu wykonawczego dodano kolejne kategorie do zakresu danych wrażliwych, w szczególności informacje na temat DNA uzyskane z badań genetycznych oraz informacje z rejestru karnego. Niedawną zmianą dekretu wykonawczego do PIPA rozszerzono dodatkowo pojęcie danych wrażliwych, uwzględniając również dane osobowe ujawniające pochodzenie rasowe lub etniczne oraz informacje biometryczne ([76]). W następstwie tej zmiany pojęcie danych wrażliwych w rozumieniu PIPA zasadniczo odpowiada temu pojęciu w rozumieniu art. 9 rozporządzenia (UE) 2016/679.

(51) Zgodnie z art. 23 ust. 1 PIPA i podobnie jak w art. 9 ust. 1 rozporządzenia (UE) 2016/679 przetwarzanie danych wrażliwych jest co do zasady zabronione, chyba że ma zastosowanie jeden z konkretnie wyliczonych wyjątków ([77]). Wyjątki te dotyczą przypadków, w których administrator informuje osobę, której dane dotyczą,

([67]) Art. 8 ust. 1–2 zawiadomienia 2020-9 w sprawie łączenia i udostępniania informacji spseudonimizowanych.
([68]) Art. 2 ust. 3, 6 i art. 9 ust. 1 zawiadomienia 2020-9 w sprawie łączenia i udostępniania informacji spseudonimizowanych.
([69]) Art. 2 ust. 4 i art. 9 ust. 2–3 zawiadomienia 2020-9 w sprawie łączenia i udostępniania informacji spseudonimizowanych. Wyspecjalizowana instytucja musi niezwłocznie po połączeniu zniszczyć dane powiązane klucza połączenia (art. 9 ust. 4 zawiadomienia).
([70]) Naruszenia wymogów dotyczących łączenia zbiorów danych mogą prowadzić do nałożenia sankcji karnych (art. 71 ust. 4-2 PIPA). Zob. również art. 29-2 ust. 4 dekretu wykonawczego do PIPA.
([71]) Procedura zatwierdzania udostępniania połączonych danych została określona w art. 11 zawiadomienia 2020-9 w sprawie łączenia i udostępniania informacji spseudonimizowanych. W szczególności wyspecjalizowana instytucja musi powołać „komitet ds. przeglądu udostępniania danych", składający się z członków posiadających znaczną wiedzę i doświadczenie w zakresie ochrony danych.
([72]) Art. 29-2 ust. 4 dekretu wykonawczego do PIPA i zawiadomienie 2020-9, art. 11.
([73]) Konieczność zapewnienia szczególnej ochrony przetwarzania danych wrażliwych, takich jak dane dotyczące zdrowia lub zachowań seksualnych, została również uznana przez koreański Trybunał Konstytucyjny, zob. orzeczenie Trybunału Konstytucyjnego nr HunMa 1139 z dnia 31 maja 2007 r.
([74]) Art. 23 ust. 1 PIPA.
([75]) Zob. także podręcznik dotyczący PIPA, rozdział III sekcja 2 poświęcona art. 23 (s. 157–164)
([76]) Tzn. dane osobowe, które wynikają z określonego przetwarzania technicznego danych dotyczących cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej w celu jednoznacznej identyfikacji tej osoby fizycznej.
([77]) Niezastosowanie się do tych wymogów może prowadzić do sankcji zgodnie z art. 71 pkt 3 PIPA.

zgodnie z art. 15 i 17 PIPA, i uzyskuje odrębną zgodę (tj. odrębną od zgody na przetwarzanie innych danych osobowych) lub gdy przetwarzanie jest wymagane lub dozwolone przez ustawę. Organy publiczne mogą również przetwarzać dane biometryczne, informacje na temat DNA uzyskane z badań genetycznych, dane osobowe ujawniające pochodzenie rasowe lub etniczne oraz informacje z rejestru karnego na podstawach, które są dostępne wyłącznie dla nich (na przykład, w stosownych przypadkach, do celów postępowania przygotowawczego w sprawach o przestępstwa lub, w stosownych przypadkach, aby sąd mógł przystąpić do rozpoznawania sprawy) ([78]). W związku z tym dostępne podstawy prawne przetwarzania danych wrażliwych są bardziej ograniczone niż w przypadku innych rodzajów danych osobowych, a nawet bardziej restrykcyjne w prawie koreańskim niż na podstawie art. 9 ust. 2 rozporządzenia (UE) 2016/679.

(52) Ponadto w art. 23 ust. 2 PIPA – do którego niezastosowanie się może skutkować nałożeniem sankcji ([79]) – podkreśla się szczególne znaczenie zapewnienia odpowiedniego bezpieczeństwa podczas przetwarzania danych wrażliwych, aby „nie mogły zostać zgubione, skradzione, ujawnione, sfałszowane, zmienione lub uszkodzone". Chociaż jest to ogólny wymóg na mocy art. 29 PIPA, w art. 3 ust. 4 wyjaśniono, że poziom bezpieczeństwa musi być dostosowany do rodzaju przetwarzanych danych osobowych, co oznacza, że musi być brane pod uwagę szczególne ryzyko związane z przetwarzaniem danych wrażliwych. Ponadto przetwarzanie danych powinno zawsze odbywać się „w sposób minimalizujący możliwość naruszenia" prywatności osoby, której dane dotyczą, oraz w miarę możliwości „anonimowo" (art. 3 ust. 6 i 7 PIPA). Wymogi te są szczególnie istotne, gdy przetwarzanie dotyczy danych wrażliwych.

2.3.3 *Ograniczenie celu*

(53) Dane osobowe powinny być zbierane w określonym celu i w sposób, który nie jest niezgodny z celem przetwarzania.

(54) Tę zasadę zapewnia art. 3 ust. 1 i 2 PIPA, zgodnie z którym administrator „określa i precyzuje" cel przetwarzania, przetwarza dane osobowe w odpowiedni sposób niezbędny do osiągnięcia tego celu i nie wykorzystuje ich w sposób wykraczający poza ten cel. Ogólna zasada ograniczenia celu znajduje również potwierdzenie w art. 15 ust. 1, art. 18 ust. 1, art. 19 oraz – w przypadku podmiotów przetwarzających (tzw. dostawców usług outsourcingowych) – w art. 26 ust. 1 pkt 1, 5 i 7 PIPA. W szczególności dane osobowe mogą co do zasady być wykorzystywane i udostępniane stronom trzecim wyłącznie w zakresie celu, w którym zostały zebrane (art. 15 ust. 1 i art. 17 ust. 1 pkt 2). Przetwarzanie w zgodnym celu, tj. „w zakresie racjonalnie powiązanym z pierwotnym celem zbierania", może mieć miejsce wyłącznie wówczas, gdy nie ma to negatywnego wpływu na osoby, których dane dotyczą, i jeśli zostaną wdrożone niezbędne środki bezpieczeństwa (takie jak szyfrowanie) (art. 15 ust. 3 i 17 ust. 4 PIPA). Aby ustalić, czy dalsze przetwarzanie odbywa się w zgodnym celu, w dekrecie wykonawczym do PIPA wymieniono szczegółowe kryteria, podobne do kryteriów przewidzianych w art. 6 ust. 4 rozporządzenia (UE) 2016/679, zob. motyw (36).

(55) Jak wyjaśniono w motywie (38), celem zbierania danych w przypadku koreańskich administratorów otrzymujących dane osobowe z Unii jest cel, w którym dane te są przekazywane. Zmiana celu przez administratora jest dozwolona wyłącznie wyjątkowo, w określonych (konkretnie wyliczonych) przypadkach (art. 18 ust. 2 pkt 1–3 PIPA, zob. również motyw (39)). W zakresie, w jakim zmiana celu jest dozwolona przepisami prawa, takie przepisy z kolei muszą respektować podstawowe prawo do prywatności i ochrony danych, jak również zasady konieczności i proporcjonalności określone w koreańskiej konstytucji. Ponadto w art. 18 ust. 2 i 5 PIPA przewiduje się dodatkowe zabezpieczenia, w szczególności wymóg, aby taka zmiana celu nie „naruszyła w sposób nieuzasadniony interesu osoby, której dane dotyczą", co zawsze wymaga wyważenia interesów. Zapewnia to stopień ochrony zasadniczo odpowiadający stopniowi ochrony, o którym mowa w art. 5 ust. 1 lit. b) oraz art. 6 w związku z motywem 50 rozporządzenia (UE) 2016/679.

2.3.4 *Prawidłowość i minimalizacja danych*

(56) Dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane. Powinny być one również adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

([78]) Art. 18 dekretu wykonawczego do PIPA stanowi, że wymienione tam kategorie danych są wyłączone z zakresu stosowania przepisu art. 23 ust. 1 ustawy, gdy są przetwarzane przez instytucję publiczną na podstawie art. 18 ust. 2 pkt 5–9 PIPA.

([79]) Zob. art. 73 pkt 1 i 75 ust. 2 pkt 6 PIPA.

(57) Zasada prawidłowości jest podobnie uznana w art. 3 ust. 3 PIPA, który wymaga, aby dane osobowe były „prawidłowe, kompletne i aktualne w zakresie niezbędnym do celów", w których dane są przetwarzane. Minimalizacja danych jest wymagana na podstawie art. 3 ust. 1 i 6 i art. 16 ust. 1 PIPA, które stanowią, że administrator powinien zbierać dane osobowe (wyłącznie) „w minimalnym zakresie, jaki jest niezbędny" do osiągnięcia zamierzonego celu, i że to na nim spoczywa ciężar dowodu w tym zakresie. Jeżeli możliwe jest osiągnięcie celu zbierania w drodze przetwarzania informacji w formie zanonimizowanej, administratorzy powinni podjąć starania, aby to zrobić (art. 3 ust. 7 PIPA).

2.3.5 *Ograniczenie przechowywania*

(58) Co do zasady dane osobowe nie powinny być przechowywane przez okres dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane.

(59) Zasada ograniczenia przechowywania jest podobnie określona w art. 21 ust. 1 PIPA ([80]), który nakłada na administratora obowiązek „zniszczenia" ([81]) danych osobowych niezwłocznie po osiągnięciu celu przetwarzania lub po upływie okresu zatrzymywania (w zależności od tego, co nastąpi wcześniej), chyba że zatrzymywanie jest wymagane ustawą ([82]). W tym ostatnim przypadku odnośne dane osobowe „są przechowywane i zarządzane oddzielnie od innych danych osobowych" (art. 21 ust. 3 PIPA).

(60) Art. 21 ust. 1 PIPA nie ma zastosowania, gdy do celów statystycznych, do celów badań naukowych lub do celów archiwalnych w interesie publicznym przetwarzane są dane spseudonimizowane ([83]). Aby zapewnić przestrzeganie zasady ograniczonego zatrzymywania danych również w tym przypadku, w zawiadomieniu nr 2021-5 wymaga się od administratorów przeprowadzenia anonimizacji zgodnie z art. 58-2 PIPA, jeżeli dane nie zostały zniszczone po osiągnięciu określonego celu przetwarzania ([84]).

2.3.6 *Bezpieczeństwo danych*

(61) Dane osobowe powinny być przetwarzane w sposób zapewniający im bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. W tym celu podmioty gospodarcze powinny wdrożyć odpowiednie środki techniczne lub organizacyjne, aby chronić dane osobowe przed ewentualnymi zagrożeniami. Środki te należy ocenić, biorąc pod uwagę stan wiedzy technicznej, koszty ich wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a także zagrożenia dla praw osób fizycznych.

(62) Podobną zasadę bezpieczeństwa określono w art. 3 ust. 4 PIPA, który wymaga od administratorów „bezpiecznego zarządzania danymi osobowymi zgodnie z metodami przetwarzania, rodzajami itp. danych osobowych, z uwzględnieniem możliwości naruszenia praw osób, których dane dotyczą, oraz wagi odnośnych zagrożeń". Ponadto administrator „przetwarza dane osobowe w sposób służący ograniczeniu do minimum możliwości naruszenia prywatności osoby, której dane dotyczą", i w tym kontekście dokłada wszelkich starań, aby przetwarzać dane osobowe w sposób anonimowy lub w miarę możliwości w formie spseudonimizowanej (art. 3 ust. 6 i 7 PIPA).

(63) Te ogólne wymogi omówiono dokładniej w art. 29 PIPA, zgodnie z którym każdy administrator „podejmuje środki techniczne, zarządcze i fizyczne, takie jak ustanowienie planu zarządzania wewnętrznego oraz przechowywanie rejestrów logowania itp., niezbędne do zapewnienia bezpieczeństwa określonego w dekrecie prezydenta,

([80]) Art. 8 (w związku z art. 8-2 dekretu wykonawczego), art. 11 (w związku z art. 12 ust. 2 dekretu wykonawczego).

([81]) Informacje na temat metod niszczenia danych osobowych znajdują się w art. 16 dekretu wykonawczego do PIPA. W art. 21 ust. 2 PIPA wyjaśniono, że obejmuje to „niezbędne środki w celu zablokowania odzyskania i ponownego wykorzystania".

([82]) Nieprzestrzeganie tych wymogów może skutkować sankcjami karnymi (art. 73 ust. 1-2 PIPA). W art. 39-6 PIPA nakłada się na dostawców usług informacyjnych i komunikacyjnych dodatkowy wymóg usunięcia danych osobowych użytkowników, którzy nie korzystali z oferowanych usług informacyjnych i komunikacyjnych przez co najmniej rok (chyba że dalsze zatrzymywanie jest wymagane na mocy przepisów prawa lub na żądanie odnośnej osoby fizycznej). Osoby fizyczne muszą zostać poinformowane o zamierzonym usunięciu ich danych 30 dni przed upływem terminu jednego roku (art. 39-6 ust. 2 PIPA i art. 48-5 ust. 3 dekretu wykonawczego do PIPA). Jeżeli dalsze zatrzymywanie jest wymagane przepisami prawa, dane muszą być przechowywane oddzielnie od innych danych użytkowników i mogą być wykorzystywane lub ujawniane wyłącznie zgodnie z tymi przepisami (art. 48-5 ust. 1-2 dekretu wykonawczego do PIPA).

([83]) Art. 28-7 PIPA.

([84]) Zawiadomienie nr 2021-5 (załącznik I) sekcja 4.

aby dane osobowe nie zostały utracone, skradzione, ujawnione, podrobione, zmienione lub uszkodzone". W art. 30 ust. 1 dekretu wykonawczego do PIPA określono te środki poprzez odniesienie do 1) sformułowania i wdrożenia planu zarządzania wewnętrznego dotyczącego bezpiecznego przetwarzania danych osobowych, 2) kontroli i ograniczeń dostępu, 3) przyjęcia technologii szyfrowania w celu bezpiecznego przechowywania i przekazywania danych osobowych, 4) rejestrów logowania, 5) programów bezpieczeństwa oraz 6) środków fizycznych, takich jak system bezpiecznego przechowywania lub blokowania ([85]).

(64) Ponadto w przypadku naruszenia ochrony danych zastosowanie mają szczególne zobowiązania (art. 34 PIPA w związku z art. 39 i 40 dekretu wykonawczego do PIPA) ([86]). W szczególności administrator jest zobowiązany do niezwłocznego powiadomienia poszkodowanych osób, których dane dotyczą, o szczegółach takiego naruszenia ([87]), w tym przekazania im informacji o (obowiązkowych) środkach zaradczych zastosowanych przez administratora oraz o tym, co mogą zrobić osoby, których dane dotyczą, by zminimalizować ryzyko wystąpienia szkody (art. 34 ust. 1 i 2 PIPA) ([88]). Jeżeli naruszenie ochrony danych dotyczy co najmniej 1 000 osób, których dane dotyczą, administrator niezwłocznie zgłasza takie naruszenie ochrony danych i zastosowane środki zaradcze do PIPC oraz Koreańskiej Agencji ds. Internetu i Bezpieczeństwa, które mogą udzielić pomocy technicznej (art. 34 ust. 3 PIPA w związku z art. 39 dekretu wykonawczego do PIPA). Administratorzy ponoszą odpowiedzialność za szkody wynikające z naruszenia ochrony danych, zgodnie z przepisami kodeksu cywilnego dotyczącymi odpowiedzialności deliktowej (zob. również pkt 2.5 dotyczący dochodzenia roszczeń) ([89]).

(65) W wypełnianiu zobowiązań w zakresie bezpieczeństwa administratora musi wspierać urzędnik ds. ochrony prywatności, którego zadaniem jest m.in. budowa systemu kontroli wewnętrznej „w celu zapobiegania ujawnianiu i wykorzystywaniu danych osobowych niezgodnie z przeznaczeniem" (art. 31 ust. 2 pkt 4 PIPA). Ponadto administrator ma obowiązek prowadzenia „odpowiedniej kontroli i odpowiedniego nadzoru" nad pracownikami przetwarzającymi dane osobowe, w tym w zakresie bezpiecznego zarządzania nimi; obejmuje to niezbędne szkolenia (instruktaż) pracowników (art. 28 ust. 1 i 2 PIPA). Wreszcie, w przypadku podwykonawstwa przetwarzania, administrator musi nałożyć na „dostawcę usług outsourcingowych" wymogi dotyczące między innymi bezpiecznego zarządzania danymi osobowymi („zabezpieczenia techniczne i zarządcze") oraz musi nadzorować ich wdrażanie, przeprowadzając kontrole (art. 26 ust. 1 i 4 PIPA w związku z art. 28 ust. 1 pkt 3 i 4 oraz art. 28 ust. 6 dekretu wykonawczego do PIPA).

2.3.7 *Przejrzystość*

(66) Osoby, których dane dotyczą, powinny być informowane o głównych cechach przetwarzania ich danych osobowych.

([85]) W odniesieniu do przetwarzania danych osobowych przez dostawców usług informacyjnych i komunikacyjnych art. 39-5 PIPA wyraźnie stanowi, że liczbę osób, które przetwarzają dane osobowe użytkowników, ogranicza się do minimum. Ponadto dostawcy usług informacyjnych i komunikacyjnych zapewniają, by dane osobowe użytkowników nie były ujawniane publicznie za pośrednictwem sieci informacyjno-komunikacyjnej (art. 39-10 ust. 1 PIPA). Na wniosek PIPC ujawnione informacje muszą zostać usunięte lub zablokowane (art. 39-10 ust. 2 PIPA). Mówiąc bardziej ogólnie, dostawcy usług informacyjnych i komunikacyjnych (oraz strony trzecie, które otrzymują dane osobowe użytkowników) podlegają dodatkowym zobowiązaniom w zakresie bezpieczeństwa, określonym w art. 48-2 dekretu wykonawczego do PIPA, np. dotyczącym opracowania i wdrożenia planu zarządzania wewnętrznego w odniesieniu do środków bezpieczeństwa, środków zapewniających kontrolę dostępu, szyfrowania, stosowania oprogramowania komputerowego do wykrywania złośliwego oprogramowania itp.

([86]) Ponadto istnieje ogólny zakaz uszkadzania, niszczenia, zmieniania, podrabiania lub ujawniania danych osobowych bez podstawy prawnej, zob. art. 59 pkt 3 PIPA.

([87]) Wymóg powiadomienia osoby fizycznej nie ma zastosowania w zakresie, w jakim naruszenie ochrony danych dotyczy spseudonimizowanych informacji przetwarzanych do celów statystycznych, do celów badań naukowych lub do celów archiwalnych w interesie publicznym (art. 28-7 PIPA, który przewiduje odstępstwo od art. 34 ust. 1 i art. 39-4 PIPA). Zapewnienie powiadamiania konkretnych osób fizycznych wymagałoby od danego administratora zidentyfikowania takich osób na podstawie zbioru danych spseudonimizowanych, co jest wyraźnie zabronione w art. 28-5 PIPA. Nadal jednak obowiązuje ogólny wymóg w zakresie powiadamiania (PIPC) o naruszeniu ochrony danych.

([88]) Wymogi w zakresie powiadamiania, w tym jego termin oraz możliwość powiadamiania „etapami", doprecyzowano w art. 40 dekretu wykonawczego do PIPA. Bardziej rygorystyczne przepisy mają zastosowanie do dostawców usług informacyjnych i komunikacyjnych, którzy są zobowiązani do powiadomienia osoby, której dane dotyczą, oraz PIPC w ciągu 24 godzin od powzięcia wiadomości o fakcie utraty, kradzieży lub wycieku danych osobowych (art. 39-4 ust. 1 PIPA). Powiadomienie to musi zawierać szczegółowe informacje na temat danych osobowych, które wyciekły, momentu, w którym to nastąpiło, środków, jakie może zastosować użytkownik, środków wdrożonych przez dostawcę w odpowiedzi na taki wyciek danych oraz danych kontaktowych działu, do którego użytkownik może kierować zapytania (art. 39-4 ust. 1 pkt 1–5 PIPA). Jeżeli istnieje uzasadniony powód, np. brak danych kontaktowych użytkownika, można zastosować inne sposoby powiadomienia, np. poprzez publiczne udostępnienie informacji na stronie internetowej (art. 39-4 ust. 1 PIPA w związku z art. 48-4 ust. 4 i nast. dekretu wykonawczego do PIPA). W takim przypadku PIPC należy poinformować o tych powodach (art. 34-4 ust. 3 PIPA).

([89]) Zob. np. orzeczenia Sądu Najwyższego nr 2011Da59834, 2011Da59858 i 2011Da59841 z dnia 26 grudnia 2012 r. Streszczenie w języku angielskim jest dostępne na stronie internetowej: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm

(67) W systemie koreańskim zapewnia się to na różne sposoby. Oprócz prawa do informacji określonego w art. 4 pkt 1 (ogólnie) i art. 20 ust. 1 PIPA (w odniesieniu do danych osobowych zebranych od stron trzecich) oraz prawa dostępu określonego w art. 35 PIPA zawiera ogólny wymóg w zakresie przejrzystości w odniesieniu do celu przetwarzania (art. 3 ust. 1 PIPA) oraz szczególne wymogi przejrzystości, w przypadku gdy przetwarzanie odbywa się na podstawie zgody (art. 15 ust. 2, art. 17 ust. 2 i art. 18 ust. 3 PIPA) ([90]). Ponadto w art. 20 ust. 2 PIPA na niektórych administratorów – w przypadku których przetwarzanie przekracza określone progi ([91]) – nakłada się obowiązek powiadomienia osoby, której dane osobowe otrzymali od strony trzeciej, o źródle informacji, celu przetwarzania oraz prawie tej osoby do żądania zawieszenia przetwarzania, chyba że takie powiadomienie okaże się niemożliwe ze względu na brak jakichkolwiek danych kontaktowych. Wyjątki mają zastosowanie do niektórych zbiorów danych osobowych znajdujących się w posiadaniu organów publicznych, w szczególności zbiorów zawierających dane przetwarzane ze względów bezpieczeństwa narodowego, innych szczególnie ważnych („nadrzędnych") interesów narodowych lub do celów ścigania przestępstw, lub gdy istnieje prawdopodobieństwo, że powiadomienie może spowodować szkodę dla życia lub integralności cielesnej innej osoby lub nieuzasadnione naruszenie interesów majątkowych lub innych interesów innej osoby, jednak wyłącznie w przypadku, gdy istniejące interesy publiczne lub prywatne są „w oczywisty sposób nadrzędne" wobec praw zainteresowanych osób, których dane dotyczą (art. 20 ust. 4 PIPA). Wymaga to wyważenia interesów.

(68) Ponadto w art. 3 ust. 5 PIPA na administratorów nakłada się obowiązek podawania do publicznej wiadomości stosowanej polityki prywatności (i innych kwestii związanych z przetwarzaniem danych osobowych). Wymóg ten doprecyzowano w art. 30 PIPA w związku z art. 31 dekretu wykonawczego do PIPA. Zgodnie z tymi przepisami publiczna polityka prywatności musi zawierać m.in. informacje na temat 1) rodzajów przetwarzanych danych osobowych, 2) celu przetwarzania, 3) okresu zatrzymywania, 4) tego, czy dane osobowe są przekazywane stronie trzeciej ([92]), 5) wszelkich przypadków podwykonawstwa przetwarzania, 6) informacji o prawach osoby, której dane dotyczą, i sposobach ich wykonywania oraz 7) informacji kontaktowych (w tym imienia i nazwiska urzędnika ds. ochrony prywatności lub nazwy wewnętrznego działu odpowiedzialnego za zapewnienie zgodności z przepisami o ochronie danych i rozpatrywanie skarg). Polityka prywatności musi być publicznie dostępna w taki sposób, aby osoby, których dane dotyczą, „mogły ją z łatwością zidentyfikować" (art. 30 ust. 2 PIPA) ([93]), i musi być stale aktualizowana (art. 31 ust. 2 dekretu wykonawczego do PIPA).

(69) Instytucje publiczne podlegają dodatkowemu obowiązkowi rejestracji w PIPC w szczególności następujących informacji: 1) nazwy instytucji publicznej, 2) podstaw i celów przetwarzania zbiorów danych osobowych, 3) danych dotyczących rejestrowanych danych osobowych, 4) metody przetwarzania, 5) okresu zatrzymywania, 6) liczby osób, których dane osobowe są zatrzymywane, 7) działu, który rozpatruje wnioski osób, których dane dotyczą, oraz 8) odbiorców danych osobowych, jeżeli dane są przekazywane w sposób rutynowy lub powtarzalny (art. 32 ust. 1 PIPA) ([94]). Zarejestrowane zbiory danych osobowych są publicznie udostępniane przez PIPC i muszą być również przywoływane przez instytucje publiczne w ich polityce prywatności (art. 30 ust. 1 i art. 32 ust. 4 PIPA).

(70) Aby zwiększyć przejrzystość w stosunku do osób w Unii, których dane osobowe przekazywane są do Korei na podstawie niniejszej decyzji, w sekcji 3 pkt (i) i (ii) zawiadomienia nr 2021-5 (załącznik I) nakłada się dodatkowe wymogi w zakresie przejrzystości. Po pierwsze, otrzymując dane osobowe z Unii na podstawie niniejszej decyzji, koreańscy administratorzy muszą bez zbędnej zwłoki (a w każdym razie nie później niż w ciągu miesiąca od przekazania) powiadomić zainteresowane osoby, których dane dotyczą, o nazwie i danych kontaktowych

([90]) W szczególności gdy dane osobowe są przetwarzane za zgodą osoby fizycznej, administrator musi poinformować tę osobę o celu przetwarzania, szczegółach dotyczących informacji, które mają być przetwarzane, odbiorcy informacji, okresie zatrzymywania i wykorzystywania danych osobowych, a także o tym, że osoba ta ma prawo odmówić wyrażenia zgody (oraz o wszelkich niedogodnościach, które mogą z tego wynikać).

([91]) Zgodnie z art. 15-2 ust. 1 dekretu wykonawczego do PIPA dotyczy to administratorów przetwarzających dane szczególnie chronione dotyczące co najmniej 50 000 osób lub „zwykłe" dane osobowe dotyczące co najmniej 1 miliona osób. W art. 15-2 ust. 2 dekretu wykonawczego do PIPA określono metody i terminy powiadamiania, a w art. 15-2 ust. 3 określono wymóg prowadzenia określonych rejestrów takich powiadomień. Ponadto przepisy szczególne mają zastosowanie do niektórych kategorii dostawców usług informacyjnych i komunikacyjnych (tych, którzy osiągnęli przychody ze sprzedaży w wysokości co najmniej 10 mld wonów w poprzednim roku, lub tych, którzy przechowują dane osobowe co najmniej miliona użytkowników dziennie średnio w ciągu trzech miesięcy poprzedzających koniec poprzedniego roku lub zarządzają takimi danymi), którzy są zobowiązani do regularnego powiadamiania użytkowników o historii wykorzystania ich danych osobowych, chyba że okaże się to niemożliwe ze względu na brak jakichkolwiek danych kontaktowych (art. 39-8 PIPA i art. 48-6 dekretu wykonawczego do PIPA).

([92]) Zgodnie z informacjami otrzymanymi od rządu Korei wiąże się to z obowiązkiem wskazania poszczególnych odbiorców w publicznej polityce prywatności.

([93]) Dalsze warunki określono w art. 31 ust. 3 dekretu wykonawczego do PIPA.

([94]) Wymóg rejestracji nie ma zastosowania do niektórych rodzajów zbiorów danych osobowych, na przykład tych, które dotyczą spraw związanych z bezpieczeństwem narodowym, tajemnicą dyplomatyczną, postępowaniami przygotowawczymi, ściganiem karnym, wymierzaniem kar, dochodzeniami w sprawie przestępstw związanych z opodatkowaniem, lub zbiorów, które dotyczą wyłącznie efektywności pracy na szczeblu wewnętrznym (art. 32 ust. 2 PIPA).

podmiotów przekazujących i odbierających informacje, przekazanych danych osobowych (lub kategoriach danych osobowych), celu zbierania przez koreańskiego administratora, okresie zatrzymywania oraz prawach przysługujących tym osobom na mocy PIPA. Po drugie, przekazując stronom trzecim dane osobowe otrzymane z Unii na podstawie niniejszej decyzji, należy poinformować osoby, których dane dotyczą, między innymi o odbiorcy, danych osobowych lub kategoriach danych osobowych, które mają zostać przekazane, państwie, do którego dane są przekazywane (w stosownych przypadkach), a także o prawach przysługujących na mocy PIPA ([95]). W ten sposób zawiadomienie gwarantuje, że osoby fizyczne w UE nadal będą informowane o określonych administratorach przetwarzających ich dane i będą mogły wykonywać swoje prawa wobec odpowiednich podmiotów.

(71) W sekcji 3 pkt (iii) zawiadomienia (załącznik I) dopuszcza się pewne ograniczone wyjątki i wyjątki z zastrzeżeniami od tych dodatkowych obowiązków zapewnienia przejrzystości, które zasadniczo odpowiadają wyjątkom przewidzianym w rozporządzeniu (UE) 2016/679. W szczególności nie ma konieczności powiadamiania osób, których dane dotyczą, w Unii 1) w przypadku gdy i dopóki konieczne jest ograniczenie powiadamiania z określonych względów interesu publicznego (na przykład gdy informacje przetwarzane są do celów bezpieczeństwa narodowego lub trwającego postępowania przygotowawczego), w zakresie, w jakim te cele interesu publicznego są w oczywisty sposób nadrzędne wobec praw osoby, której dane dotyczą; 2) w przypadku gdy osoba, której dane dotyczą, dysponuje już tymi informacjami; 3) w przypadku gdy i dopóki istnieje prawdopodobieństwo, że powiadomienie może spowodować szkodę dla życia lub integralności cielesnej osoby fizycznej lub innej osoby lub nieuzasadnione naruszenie interesów majątkowych innej osoby, o ile te prawa lub interesy są w oczywisty sposób nadrzędne wobec praw osoby, której dane dotyczą; lub 4) w przypadku gdy brak jest danych kontaktowych osób, których dane dotyczą, lub powiadomienie ich wymagałoby niewspółmiernie dużego wysiłku. Określając, czy możliwe jest skontaktowanie się z osobą, której dane dotyczą, lub czy wymaga to nadmiernego wysiłku, bierze się pod uwagę możliwość współpracy z podmiotem przekazującym dane w Unii.

(72) Przepisy zawarte w motywach (67)–(71) zapewniają zatem stopień ochrony w zakresie przejrzystości zasadniczo odpowiadający temu, który przewidziano w rozporządzeniu (UE) 2016/679.

2.3.8 *Prawa indywidualne*

(73) Osobom, których dane dotyczą, powinny przysługiwać określone prawa, które można egzekwować wobec administratora lub podmiotu przetwarzającego, w szczególności prawo dostępu do danych, prawo do sprostowania danych, prawo do sprzeciwu wobec przetwarzania danych oraz prawo do usunięcia danych. Jednocześnie prawa te mogą podlegać ograniczeniom w zakresie, w jakim ograniczenia te są niezbędne i proporcjonalne do ochrony ważnych celów leżących w ogólnym interesie publicznym.

(74) Zgodnie z art. 3 ust. 5 PIPA administrator gwarantuje prawa osoby, której dane dotyczą, wymienione w art. 4 PIPA i doprecyzowane w art. 35–37, 39 i 39-2 PIPA.

(75) Po pierwsze, osoby fizyczne mają prawo do informacji i dostępu. Jeżeli administrator zebrał dane osobowe od strony trzeciej – co zawsze będzie miało miejsce w przypadku przekazywania danych z Unii – osoby, których dane dotyczą, zasadniczo mają prawo do otrzymania informacji na temat 1) „źródła" zebranych danych osobowych (tj. podmiotu przekazującego), 2) celu przetwarzania oraz 3) faktu, że osobie, której dane dotyczą, przysługuje prawo do żądania zawieszenia przetwarzania (art. 20 ust. 1 PIPA). Zastosowanie mają ograniczone wyjątki, mianowicie gdy takie powiadomienie może spowodować szkodę dla życia lub integralności cielesnej innej osoby lub „nieuzasadnione naruszenie interesów majątkowych i innych interesów" innej osoby, jednak wyłącznie w przypadku, gdy te interesy stron trzecich są „w oczywisty sposób nadrzędne" wobec praw osoby, której dane dotyczą (art. 20 ust. 4 pkt 2 PIPA).

(76) Ponadto art. 35 ust. 1 i 3 PIPA w związku z art. 41 ust. 4 dekretu wykonawczego do PIPA gwarantuje osobom, których dane dotyczą, prawo dostępu do ich danych osobowych ([96]). Prawo dostępu obejmuje potwierdzenie przetwarzania, informacje na temat rodzaju przetwarzanych danych, celu przetwarzania, okresu zatrzymywania, jak również jakiegokolwiek ujawnienia danych stronie trzeciej oraz przekazania kopii przetwarzanych danych

([95]) Zawiadomienie nr 2021-5 sekcja 3 pkt (ii) (załącznik I).

([96]) Zgodnie z art. 35 ust. 3 PIPA w związku z art. 42 ust. 2 dekretu wykonawczego do PIPA administrator może odroczyć udzielenie dostępu z „uzasadnionego powodu" (tj. z uzasadnionych przyczyn, np. jeżeli potrzeba więcej czasu na ocenę tego, czy można udzielić dostępu), lecz musi powiadomić osobę, której dane dotyczą, o takim uzasadnieniu w ciągu 10 dni i udzielić jej informacji o sposobie odwołania się od tej decyzji; jak tylko podstawa odroczenia przestanie istnieć, dostęp musi zostać udzielony.

osobowych (art. 4 pkt 3 PIPA w związku z art. 41 ust. 1 dekretu wykonawczego do PIPA) ([97]). Dostęp może być ograniczony (dostęp częściowy) ([98]) lub można go odmówić tylko wtedy, gdy przewidziano to w przepisach prawa ([99]), jeżeli mogłoby to spowodować szkodę dla życia lub integralności cielesnej strony trzeciej lub nieuzasadnione naruszenie interesów majątkowych i innych interesów innej osoby (art. 35 ust. 4 PIPA) ([100]). To ostatnie oznacza, że należy dokonać wyważenia pomiędzy chronionymi konstytucyjnie prawami i wolnościami osoby fizycznej a prawami i wolnościami innych osób. W przypadku ograniczenia lub odmowy dostępu administrator musi powiadomić osobę, której dane dotyczą, o powodach takiej decyzji oraz o sposobie odwołania się od niej (art. 41 ust. 5 oraz art. 42 ust. 2 dekretu wykonawczego do PIPA).

(77) Po drugie, osoby, których dane dotyczą, mają prawo do sprostowania lub usunięcia ([101]) swoich danych osobowych, „chyba że inne ustawy wyraźnie stanowią inaczej" (art. 36 ust. 1 i 2 PIPA) ([102]). Po otrzymaniu wniosku administrator danych musi niezwłocznie zbadać sprawę, zastosować niezbędne środki ([103]) i powiadomić o tym w ciągu 10 dni osobę, której dane dotyczą; jeżeli wniosek nie może zostać uwzględniony, ten wymóg powiadomienia obejmuje przyczyny odmowy i sposób odwołania (zob. art. 36 ust. 4 PIPA w związku z art. 43 ust. 3 dekretu wykonawczego do PIPA) ([104]).

(78) Ponadto osoby, których dane dotyczą, mają prawo do żądania niezwłocznego zawieszenia przetwarzania ich danych osobowych ([105]), chyba że zastosowanie ma jeden z konkretnie wyliczonych wyjątków (art. 37 ust. 1 i 2 PIPA) ([106]). Administrator może odrzucić wniosek 1) jeżeli jest to wyraźnie dozwolone na mocy przepisów prawa lub konieczne („niezbędne") do wypełnienia zobowiązań prawnych, 2) jeżeli takie zawieszenie mogłoby spowodować szkodę dla życia lub integralności cielesnej strony trzeciej lub nieuzasadnione naruszenie interesów majątkowych i innych interesów innej osoby, 3) jeżeli instytucja publiczna nie mogłaby wykonywać swojej funkcji przewidzianej na mocy przepisów prawa bez przetwarzania informacji lub 4) jeżeli osoba, której dane dotyczą, nie rozwiąże wyraźnie umowy z administratorem, mimo że wykonanie umowy bez takiego przetwarzania danych nie byłoby możliwe. W takim przypadku administrator musi niezwłocznie powiadomić osobę, której dane dotyczą, o przyczynach odmowy i sposobie odwołania (art. 37 ust. 2 PIPA w związku z art. 44 ust. 2 dekretu wykonawczego do PIPA). Zgodnie z art. 37 ust. 4 PIPA w odpowiedzi na wniosek o zawieszenie przetwarzania danych administrator musi niezwłocznie „zastosować niezbędne środki, w tym zniszczyć odpowiednie dane osobowe" ([107]).

(79) Prawo do żądania zawieszenia ma również zastosowanie w przypadku, gdy dane osobowe są wykorzystywane do celów marketingu bezpośredniego, tj. w celu promowania towarów lub usług lub nakłaniania do ich zakupu. Ponadto takie dalsze przetwarzanie wymaga na ogół szczegółowej (dodatkowej) zgody osoby, której dane dotyczą (zob. art. 15 ust. 1 pkt 1 oraz art. 17 ust. 2 pkt 1 PIPA) ([108]). Zwracając się o taką zgodę, administrator musi

([97]) Dostęp do danych osobowych przetwarzanych przez instytucję publiczną można uzyskać bezpośrednio od tej instytucji lub pośrednio poprzez złożenie wniosku do PIPC, która niezwłocznie przekazuje taki wniosek (art. 35 ust. 2 PIPA i art. 41 ust. 3 dekretu wykonawczego do PIPA).

([98]) Zgodnie z art. 42 ust. 1 dekretu wykonawczego do PIPA administrator jest zobowiązany do udzielenia częściowego dostępu, jeżeli przynajmniej co do części informacji nie istnieją podstawy odmowy.

([99]) Przepisy takie z kolei muszą respektować podstawowe prawo do prywatności i ochrony danych, jak również zasady konieczności i proporcjonalności określone w koreańskiej konstytucji.

([100]) Ponadto instytucje publiczne mogą odmówić udzielenia dostępu, jeżeli spowodowałoby to poważne trudności w wykonywaniu niektórych funkcji, w tym w prowadzeniu bieżących audytów lub nakładaniu, pobieraniu lub zwrocie podatków (art. 35 ust. 4 PIPA).

([101]) W takim przypadku administrator musi zastosować środki zapobiegające odzyskaniu danych osobowych, zob. art. 36 ust. 3 PIPA.

([102]) Takie ustawy muszą spełniać określone w konstytucji wymogi, zgodnie z którymi prawo podstawowe może zostać ograniczone wyłącznie wówczas, gdy jest to konieczne ze względów bezpieczeństwa narodowego lub utrzymania porządku publicznego leżącego w interesie publicznym, i nie może naruszać istoty wolności lub prawa (art. 37 ust. 2 konstytucji).

([103]) W art. 43 ust. 2 dekretu wykonawczego do PIPA przewidziano specjalną procedurę stosowaną w przypadku, gdy administrator przetwarza zbiory danych osobowych przekazane przez innego administratora.

([104]) Niezastosowanie niezbędnych środków w celu sprostowania lub usunięcia danych osobowych oraz dalsze wykorzystywanie lub przekazywanie tych informacji stronie trzeciej może skutkować sankcjami karnymi (art. 73 ust. 2 PIPA).

([105]) Zgodnie z art. 44 ust. 2 dekretu wykonawczego do PIPA administrator informuje osobę, której dane dotyczą, o tym, że należycie zawiesił przetwarzanie w ciągu 10 dni od otrzymania wniosku.

([106]) W przypadku instytucji publicznych prawo do zawieszenia przetwarzania można wykonywać w odniesieniu do informacji zawartych w zbiorach zarejestrowanych danych osobowych (art. 37 w związku z art. 32 PIPA). Taka rejestracja nie jest wymagana w ograniczonej liczbie sytuacji, np. gdy zbiory danych osobowych dotyczą bezpieczeństwa narodowego, postępowań przygotowawczych, stosunków dyplomatycznych itp. (art. 32 ust. 2 PIPA).

([107]) Niezawieszenie przetwarzania może skutkować sankcjami karnymi (art. 73 ust. 3 PIPA).

([108]) Komisja ds. Mediacji w Sporach (zob. motyw 133) zajmowała się szeregiem spraw, w których osoby fizyczne złożyły skargę na wykorzystanie ich danych osobowych do celów marketingu bezpośredniego bez ich zgody, które to sprawy zakończyły się na przykład wypłaceniem odszkodowania i usunięciem danych osobowych przez danego administratora (zob. np. Komisja ds. Mediacji w Sporach 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1)).

poinformować osobę, której dane dotyczą, w szczególności o zamierzonym wykorzystaniu danych do celów marketingu bezpośredniego – tj. o możliwości skontaktowania się z nią w celu promowania towarów lub usług lub nakłaniania do ich zakupu – w „wyraźnie rozpoznawalny sposób" (art. 22 ust. 2 i 4 PIPA w związku z art. 17 ust. 2 pkt 1 dekretu wykonawczego do PIPA).

(80) Aby ułatwić wykonywanie praw indywidualnych, administrator musi ustanowić specjalne procedury i podać je do wiadomości publicznej (art. 38 ust. 4 PIPA) ([109]). Obejmuje to procedury wnoszenia sprzeciwu wobec odrzucenia wniosku (art. 38 ust. 5 PIPA). Administrator musi dopilnować, by procedura wykonywania praw była „przyjazna dla osoby, której dane dotyczą", i nie była trudniejsza niż procedura zbierania danych osobowych; obejmuje to również obowiązek umieszczenia informacji na temat tej procedury na stronie internetowej administratora (art. 41 ust. 2, art. 43 ust. 1 i art. 44 ust. 1 dekretu wykonawczego do PIPA) ([110]). Osoby fizyczne mogą upoważnić przedstawiciela do złożenia takiego wniosku (art. 38 ust. 1 PIPA w związku z art. 45 dekretu wykonawczego do PIPA). Administrator ma prawo nałożyć opłatę (a w przypadku wniosku o przesłanie kopii danych osobowych pocztą – opłatę pocztową), jednak jej wysokość musi być określona „w granicach faktycznych wydatków niezbędnych do rozpatrzenia [wniosku]"; opłaty (ani opłaty pocztowej) nie można nałożyć, jeżeli działania administratora doprowadziły do złożenia wniosku (art. 38 ust. 3 PIPA w związku z art. 47 dekretu wykonawczego do PIPA).

(81) PIPA i dekret wykonawczy do niej nie zawierają przepisów ogólnych odnoszących się do kwestii decyzji wpływających na osobę, której dane dotyczą, i opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych. Jeżeli jednak chodzi o dane osobowe zebrane w Unii, wszelkie decyzje opierające się na zautomatyzowanym przetwarzaniu podejmowane są zazwyczaj przez administratora w Unii (który ma bezpośrednie powiązanie z zainteresowaną osobą, której dane dotyczą) i podlegają tym samym przepisom rozporządzenia (UE) 2016/679 ([111]). Obejmuje to scenariusze przekazywania, w których za przetwarzanie odpowiada zagraniczny (np. koreański) podmiot gospodarczy działający w charakterze przedstawiciela (podmiotu przetwarzającego) w imieniu administratora w Unii (lub działający w charakterze podwykonawcy przetwarzania w imieniu unijnego podmiotu przetwarzającego po otrzymaniu danych od unijnego administratora, który je zebrał), który na tej podstawie podejmuje następnie decyzję. Mało prawdopodobne jest zatem, aby fakt, iż PIPA nie zawiera szczegółowych przepisów dotyczących zautomatyzowanego podejmowania decyzji, miał wpływ na stopień ochrony danych osobowych przekazywanych na podstawie niniejszej decyzji.

(82) W drodze wyjątku przepisy dotyczące przejrzystości na żądanie (art. 20) i praw indywidualnych (art. 35–37), jak również wymóg indywidualnego powiadamiania obowiązujący dostawców usług informacyjnych i komunikacyjnych (art. 39-8 PIPA) nie mają zastosowania w odniesieniu do informacji spseudonimizowanych, jeżeli są one przetwarzane do celów statystycznych, do celów badań naukowych lub do celów archiwalnych w interesie publicznym (art. 28-7 PIPA) ([112]). Zgodnie z podejściem określonym w art. 11 ust. 2 (w związku z motywem 57) rozporządzenia (UE) 2016/679 jest to uzasadnione faktem, że w celu zapewnienia przejrzystości lub przyznania praw indywidualnych administrator musiałby sprawdzić, czy którekolwiek z danych (a jeśli tak, to które) mają związek z osobą składającą wniosek, co jest wyraźnie zakazane na podstawie PIPA (art. 28-5 ust. 1 PIPA). Ponadto, w przypadku gdy taka ponowna identyfikacja obejmowałaby odwrócenie pseudonimizacji całego (spseudonimizowanego) zbioru danych, doprowadziłoby to do narażenia danych osobowych wszystkich innych osób, których takie dane dotyczą, na zwiększone ryzyko. Podczas gdy rozporządzenie (UE) 2016/679 dotyczy sytuacji, w których ponowna identyfikacja jest praktycznie niemożliwa, w PIPA przyjmuje się bardziej rygorystyczne podejście, polegające na wyraźnym zakazie ponownej identyfikacji we wszystkich sytuacjach, w których przetwarzane są informacje spseudonimizowane.

(83) System koreański, opisany w motywach (74)–(82), zawiera zatem przepisy dotyczące praw osób, których dane dotyczą, zapewniające stopień ochrony zasadniczo odpowiadający stopniowi ochrony zagwarantowanemu w rozporządzeniu (UE) 2016/679.

([109]) Zob. również art. 30 ust. 1 pkt 5 PIPA dotyczący polityki prywatności, która m.in. zawiera informacje o prawach przysługujących osobie fizycznej i sposobie ich wykonywania.

([110]) Zob. również art. 39-7 ust. 2 PIPA w odniesieniu do dostawców usług informacyjnych i komunikacyjnych.

([111]) Natomiast w wyjątkowych przypadkach, w których koreański podmiot gospodarczy ma bezpośrednie powiązanie z osobą z UE, której dane dotyczą, wynika to zazwyczaj z faktu, że podmiot ten oferuje towary i usługi danej osobie z Unii Europejskiej lub że monitoruje on jej zachowanie. W tym scenariuszu sam koreański podmiot gospodarczy objęty jest zakresem stosowania rozporządzenia (UE) 2016/679 (art. 3 ust. 2) i ma tym samym obowiązek bezpośrednio przestrzegać unijnych przepisów o ochronie danych.

([112]) Zob. również zawiadomienie nr 2021-5, w którym potwierdzono, że sekcja III PIPA (w tym art. 28-7) ma zastosowanie wyłącznie w przypadku, gdy informacje spseudonimizowane są przetwarzane do celów badań naukowych, do celów statystycznych lub do celów archiwalnych w interesie publicznym, zob. sekcja 4 załącznika I do niniejszej decyzji.

2.3.9 *Dalsze przekazywanie danych*

(84) Stopień ochrony zapewnianej danym osobowym przekazywanym z Unii administratorom w Republice Korei nie może zostać obniżony wskutek dalszego przekazywania takich danych odbiorcom z państw trzecich.

(85) Takie „dalsze przekazywanie danych" stanowi międzynarodowe przekazywanie danych z Republiki Korei z punktu widzenia koreańskiego administratora. W tym zakresie w PIPA rozróżnia się zlecanie usług przetwarzania w ramach outsourcingu dostawcy usług outsourcingowych (tj. podmiotowi przetwarzającemu) i przekazywanie danych osobowych stronom trzecim ([113]).

(86) Po pierwsze, jeżeli przetwarzanie danych osobowych zlecane jest w ramach outsourcingu podmiotowi z siedzibą w państwie trzecim, koreański administrator musi zapewnić zgodność z przepisami PIPA dotyczącymi outsourcingu (art. 26 PIPA). Obejmuje to wprowadzenie prawnie wiążącego instrumentu, który m.in. przyczynia się do ograniczenia przetwarzania przez dostawcę usług outsourcingowych do celu tych prac zleconych w ramach outsourcingu, nałożenia zabezpieczeń technicznych i zarządczych oraz ograniczenia podwykonawstwa przetwarzania (zob. art. 26 ust. 1 PIPA); oraz rozpowszechnianie informacji na temat prac zleconych w ramach outsourcingu. Ponadto administrator ma obowiązek przeszkolić dostawcę usług outsourcingowych w zakresie niezbędnych środków bezpieczeństwa i nadzorować, w tym w drodze inspekcji, przestrzeganie wszystkich zobowiązań administratora wynikających z PIPA ([114]) oraz umowy outsourcingu.

(87) Jeżeli dostawca usług outsourcingowych wyrządzi szkodę, przetwarzając dane osobowe z naruszeniem przepisów PIPA, zostanie ona przypisana administratorowi do celów przypisania odpowiedzialności, tak jak w przypadku pracowników administratora (art. 26 ust. 6 PIPA). Koreański administrator pozostaje zatem odpowiedzialny za dane osobowe, których przetwarzanie zostało zlecone w ramach outsourcingu, i musi dopilnować, aby zagraniczny podmiot przetwarzający przetwarzał te informacje zgodnie z PIPA. Jeżeli dostawca usług outsourcingowych przetwarza informacje z naruszeniem przepisów PIPA, koreański administrator może zostać pociągnięty do odpowiedzialności za niedopełnienie obowiązku zapewnienia zgodności z PIPA, np. poprzez nadzór nad dostawcą usług outsourcingowych. Zabezpieczenia zawarte w umowie outsourcingu oraz odpowiedzialność koreańskiego administratora za działania dostawcy usług outsourcingowych zapewniają ciągłość ochrony w przypadku zlecenia przetwarzania danych osobowych w ramach outsourcingu podmiotowi spoza Korei.

(88) Po drugie, koreańscy administratorzy mogą przekazywać dane osobowe stronie trzeciej z siedzibą lub miejscem zamieszkania poza Koreą. Chociaż PIPA zawiera szereg podstaw prawnych umożliwiających ogólne przekazywanie danych stronom trzecim, jeżeli strona trzecia ma siedzibę lub miejsce zamieszkania poza Koreą, administrator zasadniczo ([115]) musi uzyskać zgodę osoby, której dane dotyczą ([116]), po przekazaniu jej informacji na temat 1) rodzaju danych osobowych, 2) odbiorcy danych osobowych, 3) celu przekazania danych w rozumieniu celu przetwarzania realizowanego przez odbiorcę, 4) okresu zatrzymywania na potrzeby przetwarzania danych przez odbiorcę, jak również 5) faktu, że osoba, której dane dotyczą, może odmówić wyrażenia zgody (art. 17 ust. 2 i 3 PIPA). W sekcji zawiadomienia nr 2021-5 poświęconej przejrzystości (zob. motyw (70)) wymaga się, aby osoby fizyczne były informowane o państwie trzecim, do którego zostaną przekazane ich dane. Gwarantuje to, że osoby, których dane dotyczą, w Unii mogą podjąć w pełni świadomą decyzję o ewentualnym wyrażeniu zgody na przekazanie danych za granicę. Ponadto administrator nie może zawrzeć umowy ze stroną trzecią będącą odbiorcą z naruszeniem przepisów PIPA, co oznacza, że umowa nie może zawierać zobowiązań, które byłyby sprzeczne z wymogami nałożonymi na administratora w PIPA ([117]).

([113]) Do dostawców usług informacyjnych i komunikacyjnych mają zastosowanie przepisy szczególne. Zgodnie z art. 39-12 PIPA dostawcy usług informacyjnych i komunikacyjnych muszą zasadniczo uzyskać zgodę użytkownika na każde przekazanie danych osobowych za granicę. W przypadku przekazywania danych osobowych w ramach outsourcingu operacji przetwarzania, w tym w celu przechowywania, zgoda nie jest wymagana, jeżeli zainteresowane osoby fizyczne zostały z wyprzedzeniem poinformowane, bezpośrednio lub w drodze publicznego ogłoszenia w sposób umożliwiający łatwy dostęp, o 1) szczegółach informacji, które mają zostać przekazane, 2) państwie, do którego informacje zostaną przekazane (a także o terminie i sposobie przekazania), 3) nazwie odbiorcy oraz 4) celu wykorzystania i zatrzymania danych przez odbiorcę (art. 39-12 ust. 3 PIPA). Ponadto w takim przypadku zastosowanie będą miały ogólne wymogi dotyczące outsourcingu. W przypadku każdego przekazania danych należy wprowadzić szczególne zabezpieczenia w odniesieniu do bezpieczeństwa, rozpatrywania skarg i sporów, jak również innych środków niezbędnych do ochrony informacji użytkowników (art. 48-10 dekretu wykonawczego do PIPA).

([114]) Zob. również art. 26 ust. 7 PIPA, zgodnie z którym art. 15–25, 27–31, 33–38 i 50 stosuje się odpowiednio do podmiotu przetwarzającego.

([115]) W przypadku przekazywania stronom trzecim danych osobowych użytkowników przez dostawców usług informacyjnych i komunikacyjnych zawsze wymaga się uzyskania zgody użytkownika (art. 39-12 ust. 2 PIPA).

([116]) Jak wyjaśniono szczegółowo w przypisie 51, aby taka zgoda była ważna, musi być dobrowolna, świadoma i konkretna.

([117]) Zob. również art. 39-12 ust. 1 PIPA w odniesieniu do dostawców usług informacyjnych i komunikacyjnych.

(89) Bez zgody osoby fizycznej dane osobowe można przekazać stronie trzeciej (za granicę), jeżeli cel ujawnienia pozostaje „w zakresie racjonalnie powiązanym" z pierwotnym celem zbierania danych (art. 17 ust. 4 PIPA, zob. motyw (36)). Jednakże przy podejmowaniu decyzji o ewentualnym ujawnieniu danych osobowych w „powiązanym" celu, administrator musi wziąć pod uwagę, czy ujawnienie danych powoduje niedogodności dla osoby fizycznej i czy zastosowano niezbędne środki bezpieczeństwa (np. szyfrowanie). Biorąc pod uwagę fakt, że państwo trzecie, do którego przekazywane są dane osobowe, może nie oferować stopnia ochrony podobnego do tego, jaki przewidziano w PIPA, w sekcji 2 zawiadomienia nr 2021-5 uznano, że takie niedogodności mogą wystąpić i można ich uniknąć tylko wtedy, gdy koreański administrator i odbiorca zagraniczny, w drodze prawnie wiążącego instrumentu (takiego jak umowa), zapewnią stopień ochrony równoważny ze stopniem przewidzianym w PIPA, w tym w odniesieniu do praw osób, których dane dotyczą.

(90) Przepisy szczególne mają zastosowanie do ujawniania danych „w innym celu", tj. przekazywania danych stronie trzeciej w nowym (niepowiązanym) celu, co może mieć miejsce wyłącznie w oparciu o jedną z podstaw określonych w art. 18 ust. 2 PIPA, opisanych w motywie (39). Jednak nawet w tych warunkach wyklucza się możliwość przekazania danych stronie trzeciej, jeżeli może to „w sposób nieuzasadniony naruszyć" interesy osoby, której dane dotyczą, lub strony trzeciej, co wymaga wyważenia interesów. Ponadto zgodnie z art. 18 ust. 5 PIPA administrator musi stosować dodatkowe zabezpieczenia, które mogą obejmować żądanie od strony trzeciej ograniczenia celu i metody przetwarzania lub wprowadzenia szczególnych środków bezpieczeństwa. Biorąc również pod uwagę fakt, że państwo trzecie, do którego przekazywane są dane osobowe, może nie oferować stopnia ochrony podobnego do tego, jaki przewidziano w PIPA, w sekcji 2 zawiadomienia nr 2021-5 uznano, że może dojść do takiego „nieuzasadnionego naruszenia" interesów osoby fizycznej lub strony trzeciej i można go uniknąć tylko wtedy, gdy koreański administrator i odbiorca zagraniczny, w drodze prawnie wiążącego instrumentu (takiego jak umowa), zapewnią stopień ochrony równoważny ze stopniem przewidzianym w PIPA, w tym w odniesieniu do praw osób, których dane dotyczą.

(91) Przepisy zawarte w motywach (86)–(90) zapewniają zatem ciągłość ochrony w przypadku dalszego przekazywania danych osobowych (dostawcy usług outsourcingowych lub stronie trzeciej) z Republiki Korei w sposób zasadniczo odpowiadający temu, który przewidziano w rozporządzeniu (UE) 2016/679.

2.3.10 *Rozliczalność*

(92) Zgodnie z zasadą rozliczalności podmioty przetwarzające dane są zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby skutecznie przestrzegać swoich obowiązków w zakresie ochrony danych oraz być w stanie wykazać taką zgodność, zwłaszcza wobec właściwego organu nadzorczego.

(93) Zgodnie z art. 3 ust. 6 i 8 PIPA administrator musi przetwarzać dane osobowe „w sposób minimalizujący możliwość naruszenia" prywatności osoby, której dane dotyczą, oraz stara się zyskać zaufanie osoby, której dane dotyczą, wykonując zadania i wypełniając obowiązki przewidziane w PIPA i innych powiązanych ustawach. Obejmuje to ustanowienie planu zarządzania wewnętrznego (art. 29 PIPA), jak również odpowiednie szkolenia i nadzór nad pracownikami (art. 28 PIPA).

(94) Aby zagwarantować rozliczalność, w art. 31 PIPA w związku z art. 32 dekretu wykonawczego do PIPA nałożono na administratorów obowiązek wyznaczenia urzędnika ds. ochrony prywatności, który „w sposób kompleksowy odpowiada za przetwarzanie danych osobowych". Taki urzędnik ds. ochrony prywatności wykonuje w szczególności następujące zadania: 1) ustanawia i wdraża plan ochrony danych osobowych oraz opracowuje politykę prywatności, 2) przeprowadza regularne badania dotyczące stanu i praktyk przetwarzania danych osobowych w celu usunięcia ewentualnych niedociągnięć, 3) rozpatruje skargi i zajmuje się odszkodowaniami, 4) ustanawia system kontroli wewnętrznej w celu zapobiegania ujawnianiu i wykorzystywaniu danych osobowych niezgodnie z przeznaczeniem, 5) przygotowuje i wdraża program szkolenia, 6) chroni i kontroluje zbiory danych osobowych oraz zarządza nimi oraz 7) niszczy dane osobowe po osiągnięciu celu przetwarzania lub po upływie okresu zatrzymywania. Wykonując te zadania, urzędnik ds. ochrony prywatności może kontrolować stan przetwarzania danych osobowych i powiązanych systemów oraz może żądać informacji na ten temat (art. 31 ust. 3 PIPA). Jeżeli urzędnik ds. ochrony prywatności dowie się o jakimkolwiek naruszeniu PIPA lub innych odpowiednich ustaw o ochronie danych, niezwłocznie podejmuje działania naprawcze i w razie potrzeby zgłasza takie działania kierownictwu („kierownikowi") administratora (art. 31 ust. 4 PIPA). Zgodnie z art. 31 ust. 5 PIPA urzędnik ds. ochrony prywatności nie może być narażony na nieuzasadnione niedogodności wynikające z wykonywania tych zadań.

(95) Ponadto administratorzy muszą aktywnie dążyć do przeprowadzenia oceny wpływu na prywatność, w przypadku gdy obsługa zbiorów danych osobowych wiąże się z ryzykiem naruszenia prywatności (art. 33 ust. 8 PIPA). Zgodnie z art. 33 ust. 1 i 2 PIPA w związku z art. 35, 36 i 38 dekretu wykonawczego do PIPA czynniki takie jak rodzaj i charakter przetwarzanych danych (w szczególności to, czy stanowią one informacje szczególnie chronione), ich ilość, okres zatrzymywania oraz prawdopodobieństwo naruszenia ochrony danych będą istotne dla oceny stopnia ryzyka naruszenia praw osób, których dane dotyczą. Celem oceny wpływu na prywatność jest zapewnienie analizy czynników ryzyka naruszenia prywatności, jak również wszelkich środków bezpieczeństwa lub innych środków zaradczych, oraz wskazanie kwestii wymagających poprawy (zob. art. 33 ust. 1 PIPA w związku z art. 38 dekretu wykonawczego do PIPA).

(96) Instytucje publiczne są zobowiązane do przeprowadzenia oceny skutków w przypadku przetwarzania niektórych zbiorów danych osobowych, które mogą stwarzać większe ryzyko naruszenia prywatności (art. 33 ust. 1 PIPA). Zgodnie z art. 35 dekretu wykonawczego do PIPA dotyczy to m.in. zbiorów, które zawierają informacje szczególnie chronione na temat co najmniej 50 000 osób, których dane dotyczą, zbiorów, które będą łączone z innymi zbiorami, w wyniku czego będą zawierać informacje na temat co najmniej 500 000 takich osób, lub zbiorów, które zawierają informacje na temat co najmniej miliona takich osób. Wynik oceny skutków przeprowadzonej przez instytucję publiczną musi zostać zakomunikowany PIPC (zgodnie z art. 33 ust. 1 PIPA), która może wydać opinię (zgodnie z art. 33 ust. 3 PIPA).

(97) Ponadto art. 13 PIPA stanowi, że PIPC ustanawia polityki niezbędne do promowania i wspierania „samoregulacyjnych działań w zakresie ochrony danych" administratorów, m.in. za sprawą edukacji w zakresie ochrony danych, promowania i wspierania organizacji zajmujących się ochroną danych oraz pomocy administratorom w ustanawianiu i wdrażaniu zasad samoregulacji. Co więcej, ma ona wprowadzić system ePRIVACY i ułatwiać jego działanie. W tym zakresie art. 32-2 PIPA w związku z art. 34-2–34-8 dekretu wykonawczego do PIPA przewiduje możliwość certyfikacji, że system(y) przetwarzania i ochrony danych osobowych administratora spełniają wymogi ustanowione w PIPA. Zgodnie z tymi zasadami certyfikacja ([118]) może zostać przyznana (na okres 3 lat), jeśli administrator spełnia kryteria certyfikacji ustalone przez PIPC, obejmujące ustanowienie zabezpieczeń zarządczych, technicznych i fizycznych w celu ochrony danych osobowych ([119]). Co najmniej raz w roku PIPC musi zbadać systemy administratora istotne dla certyfikacji, aby zapewnić utrzymanie ich skuteczności, co może prowadzić do cofnięcia certyfikacji (art. 32 ust. 4 PIPA w związku z art. 34-5 dekretu wykonawczego do PIPA; tzw. „zarządzanie następcze").

(98) W koreańskim systemie wdrożono zatem zasadę rozliczalności w sposób gwarantujący stopień ochrony zasadniczo odpowiadający stopniowi ochrony zapewnionemu w rozporządzeniu (UE) 2016/679, dzięki przewidzeniu różnych mechanizmów zapewniających i wykazujących zgodność z PIPA.

2.3.11 *Przepisy szczególne odnoszące się do przetwarzania informacji dotyczących kredytów osobistych*

(99) Jak opisano w motywie (13), w CIA określono szczegółowe przepisy odnoszące się do przetwarzania informacji dotyczących kredytów osobistych przez podmioty handlowe. Przetwarzając informacje dotyczące kredytów osobistych, podmioty handlowe muszą zatem spełniać ogólne wymogi przewidziane w PIPA, chyba że CIA zawiera bardziej szczegółowe przepisy. Będzie to miało na przykład miejsce w przypadku przetwarzania przez nie informacji związanych z kartą kredytową lub rachunkiem bankowym w kontekście transakcji handlowej z osobą fizyczną. Jako prawodawstwo sektorowe dotyczące przetwarzania danych kredytowych (zarówno osobowych, jak i nieosobowych) CIA nie tylko nakazuje określone zabezpieczenia służące ochronie danych (na przykład w odniesieniu do przejrzystości i bezpieczeństwa), ale również bardziej ogólnie reguluje konkretne okoliczności, w których informacje dotyczące kredytów osobistych mogą być przetwarzane. Znajduje to w szczególności odzwierciedlenie w szczegółowych wymogach dotyczących wykorzystywania, przekazywania stronie trzeciej oraz zatrzymywania takich danych.

(100) Podobnie jak w PIPA w CIA odzwierciedlono zasadę zgodności z prawem i proporcjonalności. Po pierwsze, jako wymóg ogólny, art. 15 ust. 1 CIA zezwala na zbieranie informacji dotyczących kredytów osobistych wyłącznie przy użyciu zasadnych i uczciwych środków oraz w najmniejszym zakresie niezbędnym do osiągnięcia określonego celu, zgodnie z art. 3 ust. 1–2 PIPA. Po drugie, w CIA uregulowano w sposób wyraźny zgodność z prawem przetwarzania informacji dotyczących kredytów osobistych, ograniczając zbieranie, wykorzystywanie i przekazywanie takich informacji stronie trzeciej oraz ogólnie wprowadzając wymóg uzyskania zgody osoby zainteresowanej przed przeprowadzeniem takich czynności przetwarzania.

([118]) Ponadto jeżeli administrator zamierza powoływać się na certyfikację lub ją promować w swojej działalności gospodarczej, może użyć oznaczenia dotyczącego ochrony danych osobowych ustanowionego przez PIPC. Zob. art. 34-7 dekretu wykonawczego do PIPA.

([119]) Od listopada 2018 r. rozwijano „system danych osobowych i zarządzania bezpieczeństwem informacji (ISMS-P)", który służy poświadczeniu, że administratorzy stosują kompleksowy system zarządzania.

(101) Informacje dotyczące kredytów osobistych mogą być zbierane w oparciu o jedną z podstaw przewidzianych w PIPA lub o szczególne podstawy określone w CIA. Biorąc pod uwagę, że art. 45 rozporządzenia (UE) 2016/679 zakłada przekazanie danych osobowych przez administratora lub podmiot przetwarzający w Unii, ale nie obejmuje bezpośredniego zbierania (np. od osoby fizycznej lub ze strony internetowej) przez administratora w Korei, w kontekście niniejszej decyzji istotne są wyłącznie zgoda i podstawy dostępne na mocy PIPA. Podstawy te obejmują w szczególności sytuacje, w których przekazanie danych jest konieczne do wykonania umowy z osobą fizyczną lub do celów wynikających z prawnie uzasadnionych interesów koreańskiego administratora (art. 15 ust. 1 pkt 4 i 6 PIPA) ([120]).

(102) Zebrane informacje dotyczące kredytów osobistych mogą być wykorzystywane 1) do pierwotnego celu, w którym zostały (bezpośrednio) przekazane przez osobę fizyczną ([121]); 2) do celu, który jest zgodny z pierwotnym celem zbierania danych ([122]); 3) do ustalenia, czy należy ustanowić lub utrzymać stosunek handlowy, o który wnosi osoba fizyczna ([123]); 4) do celów statystycznych, do celów badań naukowych i do celów archiwalnych w interesie publicznym ([124]), jeżeli informacje te zostały spseudonimizowane ([125]); 5) jeżeli uzyskano dalszą zgodę lub 6) zgodnie z przepisami prawa.

(103) Jeśli podmiot handlowy zamierza ujawnić stronie trzeciej informacje dotyczące kredytów osobistych, musi uzyskać zgodę zainteresowanej osoby fizycznej ([126]) po poinformowaniu jej o odbiorcy informacji, celu ich przetwarzania przez odbiorcę, szczegółach informacji, które mają zostać przekazane, okresie ich przechowywania przez odbiorcę oraz prawie do odmowy wyrażenia zgody (art. 32 ust. 1 CIA i art. 28 ust. 2 dekretu wykonawczego do CIA) ([127]). Ten wymóg uzyskania zgody nie ma zastosowania w szczególnych sytuacjach, mianowicie gdy informacje dotyczące kredytów osobistych są ujawniane ([128]): 1) dostawcy usług outsourcingowych w celach outsourcingu ([129]); 2) stronie trzeciej w przypadku przeniesienia własności przedsiębiorstwa, podziału lub fuzji; 3) do celów statystycznych, do celów badań naukowych i do celów archiwalnych w interesie publicznym, jeżeli informacje zostały spseudonimizowane; 4) w celu, który jest zgodny z pierwotnym celem zbierania; 5) stronie trzeciej, która wykorzystuje informacje do odzyskania należnego długu od osoby fizycznej ([130]); 6) w celu zastosowania się do orzeczenia sądowego; 7) prokuratorowi lub urzędnikowi policji sądowej w nagłych przypadkach,

([120]) CIA zawiera również inne podstawy prawne zbierania danych, tj. gdy jest to wymagane na mocy przepisów prawa, gdy informacje zostały upublicznione przez instytucję publiczną zgodnie z przepisami o swobodnym dostępie do informacji lub gdy informacje są dostępne w sieci społecznościowej. Aby podmiot handlowy mógł powołać się na tę ostatnią podstawę, musi być w stanie wykazać, że zbieranie danych mieści się w zakresie zgody osoby, której dane dotyczą, w oparciu o rozsądną („obiektywną") interpretację i przy uwzględnieniu charakteru danych, zamiaru i celu udostępnienia ich w sieci społecznościowej, tego, czy cel zbierania danych „ma duże znaczenie" z punktu widzenia tego celu itp. (art. 13 dekretu wykonawczego do CIA). Jak wyjaśniono w motywie (101), podstawy te jednak zasadniczo nie będą adekwatne w przypadku scenariusza przekazywania danych.

([121]) Na przykład gdy informacje dotyczące kredytów są generowane/dostarczane w kontekście transakcji handlowej z osobą fizyczną. Nie można powoływać się jednak na tę podstawę w celu wykorzystania informacji dotyczących kredytów osobistych na potrzeby marketingu bezpośredniego (zob. art. 33 ust. 1 pkt 3 CIA).

([122]) Aby ustalić, czy cel wykorzystania jest zgodny z pierwotnym celem zbierania, należy wziąć pod uwagę następujące czynniki: 1) związek („zbieżność") tych dwóch celów; 2) sposób, w jaki informacje były zbierane; 3) wpływ wykorzystania na osobę fizyczną oraz 4) czy wdrożono odpowiednie środki bezpieczeństwa, takie jak pseudonimizacja (por. art. 32 ust. 6 pkt 9-4 CIA).

([123]) Administrator może na przykład uwzględnić informacje dotyczące kredytów osobistych otrzymane od osoby fizycznej, aby podjąć decyzję, czy wydłużyć okres spłaty kredytu tej osoby.

([124]) Art. 33 CIA w związku z art. 32 ust. 6 pkt 9-2, 9-4 i 10 CIA.

([125]) Pseudonimizacja jest zdefiniowana w art. 2 ust. 15 CIA jako przetwarzanie informacji dotyczących kredytów osobistych w taki sposób, aby osoby fizyczne nie mogły być już zidentyfikowane na podstawie tych informacji, chyba że w połączeniu z dodatkowymi informacjami. Chociaż CIA przewiduje szczególne zabezpieczenia dotyczące przetwarzania informacji spseudonimizowanych do celów statystycznych, do celów badań naukowych i do celów archiwalnych w interesie publicznym (art. 40-2 CIA), przepisy te nie mają zastosowania do podmiotów gospodarczych. Te ostatnie podlegają natomiast szczególnym wymogom określonym w sekcji III PIPA, opisanym w motywach (42)–(48). Ponadto w przypadku przetwarzania do celów statystycznych, do celów badań naukowych lub do celów archiwalnych w interesie publicznym art. 40-3 CIA zwalnia przetwarzanie spseudonimizowanych informacji dotyczących kredytów z wymogów dotyczących przejrzystości i praw indywidualnych, podobnie jak w przypadku wyjątku przewidzianego w art. 28-7 PIPA i z zastrzeżeniem zabezpieczeń przewidzianych w sekcji III PIPA, opisanych szczegółowo w motywach (42)–(48).

([126]) Nie dotyczy to sytuacji, w której informacje są przekazywane stronie trzeciej w celu zachowania prawidłowości i aktualności informacji dotyczących kredytów osobistych, o ile przekazanie takich informacji pozostaje w ramach pierwotnego celu przetwarzania (art. 32 ust. 1 CIA). Może to mieć miejsce na przykład wtedy, gdy aktualne informacje są udostępniane agencji ratingowej w celu zapewnienia prawidłowości jej rejestrów.

([127]) Jeżeli udostępnienie wyżej wymienionych informacji jest niepraktyczne, wystarczające może być odesłanie danej osoby fizycznej do odbiorcy będącego stroną trzecią w celu udostępnienia wymaganych informacji.

([128]) Ponieważ CIA nie reguluje w sposób szczególny ujawniania informacji dotyczących kredytów osobistych za granicą, takie ujawnienia muszą być zgodne z zabezpieczeniami dotyczącymi dalszego przekazywania informacji nałożonymi w sekcji 2 zawiadomienia nr 2021-5.

([129]) Outsourcing przetwarzania informacji dotyczących kredytów osobistych może mieć miejsce tylko na podstawie pisemnej umowy i zgodnie z wymogami art. 26 ust. 1–3, 5 PIPA, opisanymi w motywie (20) (art. 17 CIA i art. 14 dekretu wykonawczego do CIA). Dostawca usług outsourcingowych nie może wykorzystywać informacji poza zakresem zleconych obowiązków, a przedsiębiorstwo zlecające usługi outsourcingowe musi wprowadzić określone wymogi bezpieczeństwa (np. szyfrowanie) i przeszkolić podmiot przyjmujący zlecenie w zakresie sposobów zapobiegania utracie, kradzieży, ujawnieniu, zmianie lub modyfikacji informacji dotyczących kredytów.

([130]) Zob. również art. 28 ust. 10 pkt 1, 2 i 6 dekretu wykonawczego do CIA.

gdy życie osoby fizycznej jest zagrożone lub gdy spodziewane jest naruszenie jej integralności cielesnej, a nie ma czasu na wydanie nakazu sądowego ([131]); 8) właściwym organom podatkowym, w celu zastosowania się do przepisów podatkowych lub 9) zgodnie z innymi przepisami prawa. W przypadku ujawnienia danych na jednej z tych podstaw osoba, której dane dotyczą, musi zostać o tym uprzednio poinformowana (art. 32 ust. 7 CIA).

(104) W CIA uregulowano również w sposób wyraźny okres przetwarzania informacji dotyczących kredytów osobistych w oparciu o jedną z tych podstaw w celu wykorzystania lub przekazania stronie trzeciej po zakończeniu stosunku handlowego z osobą fizyczną ([132]). Zatrzymywane mogą być jedynie informacje, które były niezbędne do nawiązania lub utrzymania tego stosunku, z zastrzeżeniem dodatkowych zabezpieczeń (muszą być przechowywane oddzielnie od informacji dotyczących kredytów osobistych, które dotyczą osób fizycznych, z którymi nadal utrzymywane są stosunki handlowe, i muszą być chronione specjalnymi środkami bezpieczeństwa oraz dostępne wyłącznie dla osób upoważnionych) ([133]). Wszystkie pozostałe dane muszą zostać usunięte (art. 17-2 ust. 1 pkt 2 dekretu wykonawczego do CIA). Aby określić, które dane były niezbędne do nawiązania stosunków handlowych, należy wziąć pod uwagę różne czynniki, w tym to, czy możliwe byłoby nawiązanie stosunków bez tych danych oraz czy odnoszą się one bezpośrednio do towarów dostarczanych lub usług świadczonych na rzecz osoby fizycznej (art. 17-2 ust. 2 dekretu wykonawczego do CIA).

(105) Nawet w przypadkach gdy informacje dotyczące kredytów osobistych mogą z zasady być przechowywane po zakończeniu stosunków handlowych, muszą one zostać usunięte w ciągu trzech miesięcy po osiągnięciu dalszego celu przetwarzania ([134]) lub po pięciu latach w każdym innym przypadku (art. 20-2 CIA). W ograniczonej liczbie przypadków informacje dotyczące kredytów osobistych mogą być przechowywanie przez okres dłuższy niż pięć lat, w szczególności, w stosownych przypadkach, na potrzeby wypełnienia zobowiązania prawnego; w stosownych przypadkach do celów ochrony żywotnych interesów związanych z życiem, integralnością cielesną lub majątkiem osoby fizycznej; do archiwizacji informacji spseudonimizowanych (które były wykorzystywane do celów badań naukowych, do celów statystycznych lub do celów archiwalnych w interesie publicznym) lub do celów ubezpieczeniowych (szczególnie wypłat z tytułu ubezpieczeń lub aby zapobiec nadużyciom finansowym w dziedzinie ubezpieczeń) ([135]). W tych wyjątkowych przypadkach mają zastosowanie szczególne zabezpieczenia (takie jak powiadomienie osoby fizycznej o dalszym wykorzystaniu, oddzielenie zatrzymanych informacji od informacji odnoszących się do osób fizycznych, z którymi nadal utrzymuje się stosunki handlowe, ograniczenie praw dostępu, zob. art. 17-2 ust. 1–2 dekretu wykonawczego do CIA).

(106) W CIA doprecyzowano również zasady prawidłowości i jakości danych, zawierając w niej wymóg, aby informacje dotyczące kredytów osobistych były „rejestrowane, modyfikowane i zarządzane" w celu zachowania ich prawidłowości i aktualności (art. 18 ust. 1 CIA i art. 15 ust. 3 dekretu wykonawczego do CIA) ([136]). Udostępniając informacje dotyczące kredytów niektórym innym podmiotom (takim jak agencje ratingowe), podmioty handlowe są również zobowiązane w szczególności do sprawdzania prawidłowości informacji, aby zapewnić rejestrowanie przez odbiorcę wyłącznie prawidłowych informacji i zarządzanie wyłącznie prawidłowymi informacjami (art. 15 ust. 1 dekretu wykonawczego do CIA w związku z art. 18 ust. 1 CIA). Ogólnie rzecz ujmując, w CIA wymaga się prowadzenia rejestrów dotyczących zbierania, wykorzystywania, ujawniania stronie trzeciej i niszczenia informacji dotyczących kredytów osobistych (art. 20 ust. 2 CIA) ([137]).

(107) Ponadto przetwarzanie informacji dotyczących kredytów osobistych podlega szczegółowym wymogom w zakresie bezpieczeństwa danych. W szczególności CIA wymaga wdrożenia środków technologicznych, fizycznych i organizacyjnych, aby zapobiec bezprawnemu dostępowi do systemów komputerowych, jak również zmianom, zniszczeniu lub dowolnemu innemu zagrożeniu dla przetwarzanych danych (na przykład poprzez kontrole dostępu, zob. art. 19 CIA i art. 16 dekretu wykonawczego do CIA). Ponadto przy wymianie informacji dotyczących kredytów osobistych ze stroną trzecią konieczne jest zawarcie umowy określającej szczególne środki bezpieczeństwa (art. 19 ust. 2 CIA). W przypadku wystąpienia naruszenia informacji dotyczących kredytów osobistych, należy niezwłocznie poinformować osoby fizyczne, których to dotyczy, a także wdrożyć środki minimalizujące szkody (art. 39-4 ust. 1–2 CIA). Ponadto o powiadomieniu osób fizycznych oraz o środkach, które zostały wdrożone, należy poinformować PIPC (art. 39-4 ust. 4 CIA).

([131]) W takim przypadku wydanie nakazu musi nastąpić niezwłocznie. Jeśli nakaz nie zostanie wydany w ciągu 36 godzin, otrzymane dane muszą zostać niezwłocznie usunięte (art. 32 ust. 6 pkt 6 CIA).

([132]) Na przykład ze względu na to, że ponieważ zobowiązania umowne zostały wypełnione, jedna ze stron skorzystała z prawa do rozwiązania umowy itp., zob. art. 17-2 ust. 5 dekretu wykonawczego do CIA.

([133]) Art. 20-2 ust. 1 CIA i art. 17-2 ust. 1 pkt 1 dekretu wykonawczego do CIA.

([134]) Okres ten uwzględnia fakt, że usunięcie danych często nie jest możliwe natychmiast, ale zazwyczaj wymaga pewnych kroków (np. oddzielenia danych, które mają być usunięte, od innych danych i przeprowadzenia usunięcia bez wpływu na stabilność systemów informacyjnych), których wykonanie wymaga określonego czasu.

([135]) Art. 20-2 ust. 2 CIA.

([136]) W art. 18 ust. 2 CIA i art. 15 ust. 4 dekretu wykonawczego do CIA ustanowiono bardziej szczegółowe przepisy w odniesieniu do wymogu prowadzenia rejestrów, np. w przypadku rejestrów dotyczących informacji, które mogą być niekorzystne dla osoby fizycznej, takie jak informacje na temat przestępczości i upadłości.

([137]) Jeżeli chodzi o inne mechanizmy rozliczalności, CIA wymaga od niektórych organizacji (np. spółdzielni i podmiotów prawa publicznego, zob. art. 21 ust. 2 dekretu wykonawczego do CIA) wyznaczenia „administratora/opiekuna informacji dotyczących kredytów", który jest odpowiedzialny za monitorowanie zgodności z CIA i wykonuje zadania „urzędnika ds. ochrony prywatności" na mocy PIPA (art. 20 ust. 3 i 4 CIA).

(108) W CIA nałożono również szczególne obowiązki w zakresie przejrzystości przy uzyskiwaniu zgody na wykorzystanie lub przekazanie informacji dotyczących kredytów osobistych (art. 32 ust. 4 i art. 34-2 CIA oraz art. 30-3 dekretu wykonawczego do CIA) oraz, bardziej ogólnie, przed przekazaniem informacji stronie trzeciej (art. 32 ust. 7 CIA) ([138]). Ponadto na wniosek osoby fizyczne mają prawo do uzyskania informacji na temat wykorzystania i przekazania ich informacji dotyczących kredytów stronom trzecim w okresie obejmującym trzy lata poprzedzające wniosek (w tym cel i daty takiego wykorzystania lub przekazania) ([139]).

(109) W ramach CIA osoby fizyczne mają również prawo dostępu do swoich informacji dotyczących kredytów osobistych (art. 38 ust. 1 CIA) i do uzyskania korekty nieprawidłowych danych (art. 38 ust. 2–3 CIA) ([140]). Ponadto, oprócz ogólnego prawa do usunięcia danych na mocy PIPA (zob. motyw (77)), CIA przewiduje szczególne prawo do usunięcia informacji dotyczących kredytów osobistych, które to informacje są zatrzymywane po upływie okresów zatrzymania wymienionych w motywie (104), tj. pięciu lat (w przypadku informacji dotyczących kredytów osobistych, które były niezbędne do nawiązania lub utrzymania stosunków handlowych) lub trzech miesięcy (w przypadku innych rodzajów informacji dotyczących kredytów osobistych) ([141]). Wniosek o usunięcie danych może zostać wyjątkowo odrzucony, gdy dalsze zatrzymywanie jest niezbędne – w okolicznościach opisanych w motywie (105). W przypadku gdy osoba fizyczna wnioskuje o usunięcie danych, ale zastosowanie ma jeden z wyjątków, w odniesieniu do informacji dotyczących kredytów osobistych należy zastosować szczególne zabezpieczenia (art. 38-3 ust. 3 CIA i art. 33-3 dekretu wykonawczego do CIA). Na przykład informacje te muszą być przechowywane oddzielnie od innych informacji, dostęp do nich może mieć tylko upoważniona osoba oraz muszą podlegać szczególnym środkom bezpieczeństwa.

(110) Oprócz praw wspomnianych w motywie (109) CIA gwarantuje osobom fizycznym prawo do wystąpienia do administratora o zaprzestanie kontaktów w celu marketingu bezpośredniego (art. 37 ust. 2 ustawy) oraz prawo do przenoszenia danych. Jeśli chodzi o to ostatnie, CIA umożliwia osobom fizycznym wystąpienie z wnioskiem o przekazanie informacji dotyczących ich kredytów osobistych im lub pewnym stronom trzecim (takim jak instytucje finansowe i agencje ratingowe). Informacje dotyczące kredytów osobistych muszą być przetwarzane i przekazane stronie trzeciej w formacie umożliwiającym przetwarzanie przez urządzenie przetwarzające informacje (takie jak komputer).

(111) W zakresie, w jakim CIA zawiera przepisy szczególne w porównaniu z PIPA, Komisja uważa, że również te przepisy zapewniają stopień ochrony zasadniczo odpowiadający stopniowi ochrony zagwarantowanemu w rozporządzeniu (UE) 2016/679.

2.4 **Nadzór i egzekwowanie przepisów prawa**

(112) W celu zapewnienia odpowiedniego stopnia ochrony danych w praktyce, należy ustanowić niezależny organ nadzorczy, któremu powierzone zostaną uprawnienia do monitorowania i egzekwowania zgodności z przepisami o ochronie danych. Wykonując swoje obowiązki i uprawnienia, organ ten działa całkowicie niezależnie i bezstronnie.

2.4.1 *Niezależny nadzór*

(113) W Republice Korei niezależnym organem odpowiedzialnym za monitoring i egzekwowanie przepisów PIPA jest Komisja Ochrony Danych Osobowych („PIPC"). PIPC składa się z przewodniczącego, wiceprzewodniczącego i siedmiu komisarzy. Przewodniczący i wiceprzewodniczący są powoływani przez prezydenta, na wniosek premiera. Dwóch spośród Komisarzy prezydent powołuje na wniosek przewodniczącego, a pięciu na wniosek Zgromadzenia Narodowego (z czego dwóch na wniosek partii politycznej, do której należy prezydent, a trzech na

([138]) Obejmuje to ogólny wymóg zgłoszenia (art. 32 ust. 7 CIA) oraz szczególny obowiązek przejrzystości w przypadku, gdy informacje, na podstawie których można określić zdolność kredytową osoby fizycznej, są przekazywane niektórym podmiotom, takim jak agencje ratingowe i agencje zbierające informacje dotyczące kredytów (art. 35-3 CIA i art. 30-3 dekretu wykonawczego do CIA), lub w przypadku odmowy lub rozwiązania transakcji handlowej na podstawie informacji dotyczących kredytów osobistych, otrzymanych od strony trzeciej (art. 36 CIA i art. 31 dekretu wykonawczego do CIA).

([139]) Art. 35 CIA. Niektóre podmioty gospodarcze, np. spółdzielnie i podmioty prawa publicznego (art. 21 ust. 2 dekretu wykonawczego do CIA) podlegają dodatkowym wymogom w zakresie przejrzystości, np. wymogowi publicznego udostępniania pewnych informacji (art. 31 CIA) oraz informowania osób fizycznych o możliwym niekorzystnym wpływie na ich rating kredytowy w przypadku zawierania transakcji finansowych wiążących się z ryzykiem kredytowym (art. 35-2 CIA).

([140]) Jeśli chodzi o warunki i wyjątki dotyczące praw dostępu i do korekty, zastosowanie mają zasady przewidziane w PIPA (opisane w motywach (76)–(77)). Ponadto w art. 38 ust. 4–8 CIA i art. 33 dekretu wykonawczego do CIA określono dalsze warunki. W szczególności podmiot handlowy, który skorygował lub usunął nieprawidłowe informacje dotyczące kredytów, musi powiadomić o tym zainteresowaną osobę fizyczną. Ponadto każda strona trzecia, której informacje te zostały ujawnione w okresie ostatnich sześciu miesięcy, oraz zainteresowana osoba fizyczna muszą zostać o tym poinformowane. Jeśli osoba fizyczna nie jest usatysfakcjonowana sposobem, w jaki rozpatrzono wniosek o skorygowanie danych, może złożyć wniosek do PIPC, która weryfikuje działania administratora i może nakazać podjęcie działań naprawczych.

([141]) Art. 38-3 CIA.

wniosek pozostałych partii politycznych (art. 7-2 ust. 2 PIPA), co pomaga przeciwdziałać stronniczości w procesie powoływania) ([142]). Procedura ta jest zgodna z wymogami mającymi zastosowanie do powoływania członków organów ochrony danych w Unii (art. 53 ust. 1 rozporządzenia (UE) 2016/679). Ponadto wszyscy komisarze muszą zaniechać prowadzenia działalności gospodarczej nastawionej na zysk i działalności politycznej oraz powstrzymać się od zajmowania stanowisk w administracji publicznej lub Zgromadzeniu Narodowym (art. 7-6 i art. 7-7 ust. 1 pkt 3 PIPA) ([143]). Wszyscy komisarze podlegają przepisom szczególnym uniemożliwiającym im udział w obradach w przypadku ewentualnego konfliktu interesów (art. 7-11 PIPA). Komisję wspomaga sekretariat (art. 7-13) i może ona powoływać podkomisje (składające się z trzech komisarzy) do rozpatrywania drobnych naruszeń i powtarzających się spraw (art. 7-12 PIPA).

(114) Każdy z członków PIPC jest mianowany na okres trzech lat i może być raz powołany na kolejną kadencję (art. 7-4 ust. 1 PIPA). Komisarze mogą zostać odwołani tylko w szczególnych okolicznościach, a mianowicie jeśli nie są w stanie dłużej wykonywać swoich obowiązków z powodu długotrwałej niepełnosprawności intelektualnej lub fizycznej, działają z naruszeniem prawa lub spełniają jedną z podstaw do pozbawienia urzędu ([144]) (art. 7-5 PIPA). To zapewnia im ochronę instytucjonalną w wykonywaniu ich funkcji.

(115) Ogólniej rzecz ujmując, art. 7 ust. 1 PIPA wyraźnie gwarantuje niezależność PIPC, natomiast art. 7-5 ust. 2 PIPA wymaga od komisarzy wykonywania obowiązków w sposób niezależny, zgodny z prawem oraz sumieniem ([145]). Opisane zabezpieczenia instytucjonalne i proceduralne, w tym w odniesieniu do powoływania i odwoływania członków PIPC, zapewniają, że działa ona w pełni niezależnie od zewnętrznych wpływów lub instrukcji. Ponadto PIPC, jako centralna agencja administracyjna, co roku przedkłada wniosek w sprawie własnego budżetu (którego przeglądu dokonuje Ministerstwo Finansów w ramach ogólnego budżetu krajowego przed jego przyjęciem przez Zgromadzenie Narodowe) i samodzielnie odpowiada za zarządzanie własnym personelem. PIPC dysponuje obecnie budżetem w wysokości około 35 mln euro i personelem w liczbie 154 osób (w tym 40 pracownikami specjalizującymi się w technologii informacyjno-komunikacyjnej, 32 pracownikami zajmującymi się prowadzeniem dochodzeń i 40 prawnikami).

(116) Zadania i uprawnienia PIPC są określone głównie w art. 7-8 oraz 7-9, a także w art. 61–66 PIPA ([146]). Do zadań PIPC należy w szczególności doradzanie w kwestii przepisów ustawowych i wykonawczych związanych z ochroną danych, opracowywanie polityk i wytycznych w zakresie ochrony danych, prowadzenie postępowań wyjaśniających w sprawach naruszeń praw indywidualnych, rozpatrywanie skarg i mediacja w sporach, egzekwowanie przestrzegania PIPA, zapewnienie edukacji i promocji w zakresie ochrony danych oraz wymiana informacji i współpraca z organami ochrony danych państw trzecich ([147]).

(117) Na podstawie art. 68 PIPA w związku z art. 62 dekretu wykonawczego do PIPA niektóre zadania PIPC zostały przekazane Koreańskiej Agencji ds. Internetu i Bezpieczeństwa, a mianowicie: 1) edukacja i public relations, 2) szkolenie specjalistów i opracowywanie kryteriów oceny wpływu na prywatność, 3) rozpatrywanie wniosków o wyznaczenie tzw. instytucji ds. oceny wpływu na prywatność, 4) rozpatrywanie wniosków pośredniego dostępu do danych osobowych znajdujących się w posiadaniu organów publicznych (art. 35 ust. 2 PIPA) oraz 5) zadanie

([142]) Na stanowisko komisarza PIPC mogą być mianowane wyłącznie osoby fizyczne spełniające następujące kryteria: urzędnicy służby cywilnej wyższego szczebla odpowiedzialni za sprawy związane z danymi osobowymi; byli sędziowie, prokuratorzy lub prawnicy, którzy wykonywali zawód przez co najmniej 10 lat; byli kierownicy z doświadczeniem w ochronie danych, którzy pracowali w instytucji lub organizacji publicznej przez okres dłuższy niż trzy lata lub którzy zostali zarekomendowani przez taką instytucję lub organizację oraz byli profesorowie nadzwyczajni posiadający wiedzę zawodową w dziedzinie ochrony danych, którzy przez co najmniej pięć lat pracowali w instytucji akademickiej (art. 7-2 PIPA).

([143]) Zob. również art. 4-2 dekretu wykonawczego do PIPA.

([144]) Zob. art. 7-7 PIPA, zgodnie z którym osoby niebędące obywatelami Korei oraz członkowie partii politycznych nie mogą zostać członkami PIPC. To samo dotyczy osób fizycznych, na które nałożono sankcje karne określonych rodzajów, zostały dyscyplinarnie usunięte z urzędu w okresie ostatnich pięciu lat itp. (art. 7-7 PIPA w związku z art. 33 ustawy o urzędnikach publicznych).

([145]) Podczas gdy art. 7 ust. 2 PIPA odnosi się do uprawnienia ogólnego premiera do zawieszenia lub uchylenia, za zgodą prezydenta, każdej niezgodnej z prawem lub bezpodstawnej decyzji centralnej agencji administracyjnej, określonego w art. 18 ustawy o organizacji rządu, takie uprawnienie nie zostało przyznane w odniesieniu do uprawnień dochodzeniowych ani wykonawczych PIPC (zob. art. 7 ust. 2 pkt 1 i 2 PIPA). Zgodnie z wyjaśnieniami otrzymanymi od rządu Korei art. 18 ustawy o organizacji rządu ma na celu zapewnienie premierowi możliwości działania w nadzwyczajnych okolicznościach, np. w celu mediacji w sporze między różnymi agencjami rządowymi. Premier jednak nigdy nie skorzystał z tego uprawnienia od czasu przyjęcia tego przepisu w 1963 r.

([146]) Jeżeli jest to konieczne do wykonania zadań zgodnie z art. 7-9 ust. 1 PIPA, PIPC może zasięgnąć opinii właściwych urzędników publicznych, ekspertów ds. ochrony danych, organizacji obywatelskich lub właściwych podmiotów gospodarczych. Ponadto PIPC może zwrócić się o istotne materiały, może wydawać zalecenia w sprawie ulepszeń oraz kontrolować, czy są one wdrażane (art. 7-9 ust. 2–5 PIPA).

([147]) Zob. również art. 9 PIPA (trzyletni centralny plan ochrony danych osobowych), art. 12 PIPA (standardowe wytyczne dotyczące ochrony danych osobowych), art. 13 PIPA (polityki promocji i wsparcia samoregulacji).

zwracania się o materiały i przeprowadzania kontroli w odniesieniu do skarg otrzymywanych za pośrednictwem centrum telefonicznego ds. prywatności. W kontekście rozpatrywania skarg za pośrednictwem centrum telefonicznego ds. prywatności Koreańska Agencja ds. Internetu i Bezpieczeństwa przekazuje sprawę do PIPC lub do prokuratury, jeśli stwierdzi, że doszło do naruszenia prawa. Możliwość wniesienia skargi do centrum telefonicznego ds. prywatności nie wyklucza możliwości wniesienia skargi przez osobę fizyczną bezpośrednio do PIPC lub zwrócenia się do PIPC w przypadku uznania, że skarga nie została odpowiednio rozpatrzona przez Koreańską Agencje ds. Internetu i Bezpieczeństwa.

2.4.2 *Egzekwowanie prawa, w tym sankcje*

(118) W celu zapewnienia zgodności z PIPA prawodawca przyznał PIPC zarówno uprawnienia dochodzeniowe, jak i wykonawcze, od zaleceń do administracyjnych kar pieniężnych. Uprawnienia te są uzupełnione systemem sankcji karnych.

(119) Jeśli chodzi o uprawnienia dochodzeniowe, w przypadku podejrzenia lub zgłoszenia naruszenia PIPA lub, w stosownych przypadkach, na potrzeby ochrony praw osób, których dane dotyczą, przed naruszeniami, PIPC może przeprowadzać kontrole na miejscu i zażądać od administratorów danych osobowych wszelkich istotnych materiałów (takich jak statuty i dokumenty) (art. 63 PIPA w związku z art. 60 dekretu wykonawczego do PIPA) ([148]).

(120) W zakresie egzekwowania prawa zgodnie z art. 61 ust. 2 PIPA PIPC może wydawać zalecenia dla administratorów danych osobowych dotyczące sposobu poprawienia stopnia ochrony danych osobowych w ramach określonych czynności przetwarzania. Administratorzy danych osobowych muszą w dobrej wierze dokładać wszelkich starań zmierzających do zastosowania się do tych zaleceń i są zobowiązani do informowania PIPC o rezultacie tych starań. Ponadto, jeżeli istnieją uzasadnione podstawy do uznania, że doszło do naruszenia PIPA, a niepodjęcie działań może spowodować trudną do naprawienia szkodę, PIPC może nakazać podjęcie działań naprawczych (art. 64 ust. 1 PIPA) ([149]). W sekcji 5 zawiadomienia nr 2021-5 (załącznik I) wyjaśniono ze skutkiem wiążącym, że warunki te są spełnione w odniesieniu do naruszenia każdego przepisu PIPA, który chroni prawo do prywatności osób fizycznych w zakresie danych osobowych ([150]). Środki, do wprowadzenia których uprawniona jest PIPC, obejmują nakazanie zaprzestania działań powodujących naruszenie, tymczasowe zawieszenie przetwarzania danych lub wszelkie inne niezbędne środki. Niepodjęcie działania naprawczego może skutkować nałożeniem sankcji w postaci kary pieniężnej w wysokości do 50 mln wonów (art. 75 ust. 2 pkt 13 PIPA).

(121) W odniesieniu do niektórych organów publicznych (takich jak Zgromadzenie Narodowe, agencje administracji centralnej, organy samorządu terytorialnego i sądy) art. 64 ust. 4 PIPA stanowi, że PIPC może „zalecić" dowolne działanie naprawcze wspomniane w motywie (120) oraz że organy te są zobowiązane do zastosowania się do takiego zalecenia, chyba że zachodzą nadzwyczajne okoliczności. Zgodnie z sekcją 5 zawiadomienia nr 2021-5 odnosi się to do nadzwyczajnych okoliczności faktycznych lub prawnych, o których PIPC nie wiedziała w chwili wydawania zalecenia. Dany organ publiczny może powołać się na takie nadzwyczajne okoliczności wyłącznie wówczas, gdy wyraźnie wykaże, że nie doszło do naruszenia prawa, a PIPC stwierdzi, że tak rzeczywiście jest. W przeciwnym razie organ publiczny musi zastosować się do zalecenia PIPC, a więc jest zobowiązany do „podjęcia działania naprawczego, w tym do natychmiastowego zaprzestania danej czynności, a w wyjątkowym przypadku także do wypłacenia odszkodowania za szkody, jeżeli mimo wszystko doszło do popełnienia czynu niezgodnego z prawem".

(122) PIPC może również zwrócić się do innych agencji administracyjnych właściwych w konkretnych dziedzinach na podstawie ustawodawstwa sektorowego (np. zdrowie, edukacja) o przeprowadzenie dochodzenia – osobno lub wspólnie z PIPC – w sprawie (podejrzewanego) naruszenia prywatności przez administratorów prowadzących działalność w dziedzinach wchodzących w zakres kompetencji takich agencji oraz o nakazanie podjęcia działań naprawczych (art. 63 ust. 4–5 PIPA). W takim przypadku PIPC określa podstawy, przedmiot i zakres takiego dochodzenia ([151]). Z kolei właściwa agencja administracyjna musi przedłożyć PIPC plan kontroli i poinformować PIPC o jej wyniku. PIPC może zalecić podjęcie konkretnego działania naprawczego, a właściwa agencja musi podjąć starania w celu jego wdrożenia. Taki wniosek w żadnym wypadku nie ogranicza kompetencji PIPC do przeprowadzenia własnego dochodzenia lub nałożenia sankcji.

([148]) PIPC może ponadto wejść do pomieszczeń administratora, aby skontrolować stan działalności gospodarczej, zapisów, dokumentów itp. (art. 63 ust. 2 PIPA). Zob. również art. 45-3 CIA i art. 36-4 dekretu wykonawczego do CIA w odniesieniu do uprawnień PIPC wynikających z tej ustawy.

([149]) Zob. również art. 45-4 CIA w odniesieniu do uprawnień PIPC na mocy CIA.

([150]) Sekcja 5 zawiadomienia stanowi, że „istnienie istotnych przesłanek do stwierdzenia, że doszło do naruszenia w odniesieniu do danych osobowych, a niepodjęcie działań może spowodować trudną do naprawienia szkodę, w rozumieniu art. 64 ust. 1 i 2 PIPA, dotyczy naruszenia dowolnej zasady, prawa i obowiązku przewidzianych w ustawie w celu ochrony praw osób fizycznych do danych osobowych". To samo ma zastosowanie do uprawnień PIPC na mocy art. 45-4 CIA.

([151]) Art. 60 dekretu wykonawczego do PIPA.

(123) Oprócz uprawnień naprawczych PIPC może nakładać administracyjne kary pieniężne w wysokości od 10 do 50 mln wonów za naruszenie różnych wymogów PIPA (art. 75 PIPA) ([152]). Dotyczy to m.in. nieprzestrzegania wymogów w zakresie zgodnego z prawem przetwarzania informacji, niewprowadzenia niezbędnych środków bezpieczeństwa, niepowiadomienia osób, których dane dotyczą, w przypadku naruszenia ochrony danych, nieprzestrzegania wymogów dotyczących podwykonawstwa przetwarzania, braku ustanowienia i ujawnienia polityki prywatności, niewyznaczenia urzędnika ds. ochrony prywatności lub niepodjęcia działań na wniosek osoby, której dane dotyczą, w ramach wykonywania jej praw indywidualnych, a także niektórych naruszeń zasad proceduralnych (brak współpracy podczas dochodzenia). W przypadku naruszenia szeregu przepisów PIPA przez tego samego administratora kara finansowa może zostać nałożona za każde z naruszeń, a przy ustalaniu wysokości kary zostanie wzięta pod uwagę liczba osób fizycznych, na których te naruszenia mają wpływ.

(124) Ponadto, jeżeli istnieją uzasadnione podstawy, by podejrzewać naruszenie PIPA lub innych „ustaw związanych z ochroną danych", PIPC może złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa do właściwego organu ścigania (takiego jak prokurator, zob. art. 65 ust. 1 PIPA). Ponadto PIPC może zalecić administratorowi zastosowanie środków dyscyplinarnych wobec osoby odpowiedzialnej (w tym odpowiedzialnego kierownika, zob. art. 65 ust. 2 PIPA). Po otrzymaniu takiego zalecenia administrator musi się do niego ([153]) zastosować i powiadomić na piśmie PIPC o wyniku podjętych działań (art. 65 PIPA w związku z art. 58 dekretu wykonawczego do PIPA).

(125) W odniesieniu do zaleceń, o których mowa w art. 61, działań naprawczych na podstawie art. 64, zarzutów lub zalecenia w sprawie środków dyscyplinarnych na podstawie art. 65 oraz nałożenia administracyjnych kar pieniężnych na podstawie art. 75 PIPA PIPC może podać odnośne fakty do publicznej wiadomości – tj. wskazać naruszenie, podmiot, który naruszył prawo, oraz nałożony środek lub środki – w drodze opublikowania ich na stronie internetowej lub w ogólnokrajowym dzienniku (art. 66 PIPA w związku z art. 61 ust. 1 dekretu wykonawczego do PIPA) ([154]).

(126) Zgodność z wymogami ochrony danych określonymi w PIPA (jak również innych „ustawach związanych z ochroną danych") jest wspierana przez system sankcji karnych. W tym zakresie art. 70–73 PIPA zawierają przepisy dotyczące kar pieniężnych, które mogą prowadzić do nałożenia grzywny (od 20 do 100 mln wonów) lub kary pozbawienia wolności (w maksymalnym wymiarze od 2 do 10 lat). Do istotnych naruszeń zalicza się m. in. wykorzystanie danych osobowych lub przekazanie ich stronie trzeciej bez wymaganej zgody, przetwarzanie informacji szczególnie chronionych wbrew zakazowi określonemu w art. 23 ust. 1 PIPA, nieprzestrzeganie obowiązujących wymogów bezpieczeństwa skutkujące utratą, kradzieżą, ujawnieniem, podrobieniem, przerobieniem lub uszkodzeniem danych osobowych, niewprowadzenie niezbędnych środków w celu skorygowania, usunięcia lub zawieszenia danych osobowych lub bezprawne przekazanie danych osobowych do państwa trzeciego ([155]). Zgodnie z art. 74 PIPA w każdym z tych przypadków odpowiedzialność ponosi pracownik, agent lub przedstawiciel administratora, jak również sam administrator ([156]).

(127) Poza sankcjami karnymi przewidzianymi w PIPA, zgodnie z kodeksem karnym wykorzystanie danych osobowych niezgodnie z przeznaczeniem może również stanowić przestępstwo. Ma to miejsce w szczególności w przypadku naruszenia tajemnicy pism, dokumentów lub dokumentacji elektronicznej (art. 316), ujawnienia informacji objętych tajemnicą zawodową (art. 317), oszustwa z wykorzystaniem komputera (art. 347-2), a także sprzeniewierzenia i naruszenia obowiązków powiernika (art. 355).

(128) Koreański system łączy zatem różne rodzaje sankcji, od działań naprawczych i administracyjnych kar pieniężnych po sankcje karne, które prawdopodobnie będą miały szczególnie silny efekt odstraszający dla administratorów i osób fizycznych zarządzających danymi. PIPC zaczęła korzystać ze swoich uprawnień natychmiast po jej

([152]) Ponadto, jeżeli systemy przetwarzania i ochrony danych osobowych stosowane przez administratora uzyskały certyfikat zgodności z PIPA, ale kryteria certyfikacji zgodnie z art. 34-2 ust. 1 dekretu wykonawczego do PIPA nie zostały faktycznie spełnione, lub w przypadku poważnego naruszenia dowolnej „ustawy związanej z ochroną danych [osobowych]" PIPC może cofnąć decyzję o przyznaniu certyfikacji (art. 32-2 ust. 3, 5 PIPA). PIPC informuje administratora o takiej decyzji i przekazuje ją do wiadomości publicznej lub publikuje na stronie internetowej lub w dzienniku urzędowym (art. 34-4 dekretu wykonawczego do PIPA). Za naruszenie przepisów CIA przewidziane są również administracyjne kary pieniężne (art. 52 CIA) oraz sankcje karne (art. 50 CIA).

([153]) Zgodnie z art. 58 ust. 2 dekretu wykonawczego do PIPA, w przypadku gdy szczególne okoliczności sprawiają, że zastosowanie się do zalecenia jest „niewykonalne w praktyce", administrator musi przedstawić PIPC uzasadnione wyjaśnienie.

([154]) Podejmując decyzję o podaniu takich faktów do publicznej wiadomości, PIPC uwzględnia istotę i wagę naruszenia, jego długotrwałość i częstotliwość, a także jego skutki (rozmiar szkody). Zainteresowany podmiot jest zawiadamiany wcześniej i ma możliwość obrony. Zob. art. 61 ust. 2 i 3 dekretu wykonawczego do PIPA.

([155]) Zob. art. 71 pkt 2 w związku z art. 18 ust. 1 PIPA (nieprzestrzeganie warunków z art. 17 ust. 3 PIPA, do których odnosi się art. 18 ust. 1). Zob. również art. 75 ust. 2 pkt 1 w związku z art. 17 ust. 2 PIPA (niedostarczenie niezbędnych informacji osobie fizycznej zgodnie z art. 17 ust. 2 PIPA, do której odnosi się art. 17 ust. 3).

([156]) Ponadto art. 74-2 PIPA pozwala na konfiskatę wszelkich środków pieniężnych, towarów lub innych korzyści uzyskanych w wyniku naruszenia lub, jeśli konfiskata jest niemożliwa, na „odzyskanie" korzyści uzyskanych niezgodnie z prawem.

ustanowieniu w 2020 r. Z rocznego sprawozdania PIPC za 2021 r. wynika, że PIPC już wydała szereg zaleceń i nakazów podjęcia działań naprawczych oraz nałożyła szereg administracyjnych kar finansowych, zarówno wobec sektora publicznego (około 34 organów publicznych), jak i podmiotów prywatnych (około 140 przedsiębiorstw) ([157]). Istotne przykłady to nałożenie na przedsiębiorstwo kary pieniężnej w wysokości 6,7 mld wonów w grudniu 2020 r. za naruszenie różnych przepisów PIPA (w tym wymogów bezpieczeństwa, wymogów dotyczących zgody na przekazywanie danych stronie trzeciej oraz przejrzystości) ([158]) oraz kary pieniężnej w wysokości 103,3 mln wonów w kwietniu 2021 r. na przedsiębiorstwo z sektora technologii sztucznej inteligencji (za naruszenie m.in. przepisów dotyczących zgodności przetwarzania danych z prawem, w szczególności w odniesieniu do zgody, oraz przetwarzania informacji spseudonimizowanych) ([159]). W sierpniu 2021 r. PIPC zakończyła kolejne dochodzenie, dotyczące działalności trzech przedsiębiorstw, w wyniku którego nakazano działania naprawcze i nałożono kary pieniężne w wysokości do 6,47 mld wonów (między innymi za niepoinformowanie osób fizycznych o ujawnieniu danych osobowych osobom trzecim, w tym o przekazaniu danych do państw trzecich) ([160]). Ponadto już przed niedawną reformą Korea Południowa miała udokumentowaną historię skutecznego egzekwowania przepisów, a jej właściwe organy w pełni wykorzystywały środki przymusu, takie jak administracyjne kary pieniężne, nakaz podjęcia działań naprawczych oraz publiczne ujawnianie sprawców, w odniesieniu do różnych administratorów, takich jak dostawcy usług komunikacyjnych (Koreańska Komisja Telekomunikacyjna, ang. Korea Communications Commission), jak również podmiotów handlowych, instytucji finansowych, organów publicznych, uniwersytetów i szpitali (Ministerstwo Spraw Wewnętrznych i Bezpieczeństwa) ([161]). Na tej podstawie Komisja uznaje, że koreański system zapewnia skuteczne egzekwowanie przepisów o ochronie danych w praktyce, tym samym zapewniając stopień ochrony zasadniczo odpowiadający stopniowi ochrony zagwarantowanemu w rozporządzeniu (UE) 2016/679.

2.5 **Dochodzenie roszczeń**

(129) W celu zapewnienia odpowiedniej ochrony, a w szczególności egzekwowania praw indywidualnych, osoba, której dane dotyczą, powinna mieć dostęp do dochodzenia roszczeń na drodze administracyjnej i sądowej, w tym do dochodzenia odszkodowania.

(130) Koreański system zapewnia osobom fizycznym różne mechanizmy skutecznego egzekwowania ich praw i dochodzenia roszczeń (na drodze sądowej).

(131) W pierwszej kolejności osoby fizyczne, które uważają, że ich prawa lub interesy w zakresie ochrony danych zostały naruszone, mogą zwrócić się do właściwego administratora. Zgodnie z art. 30 ust. 1 pkt 5 PIPA polityka prywatności administratora musi zawierać między innymi informacje o prawach osób, których dane dotyczą, oraz sposobach wykonywania tych praw. Ponadto musi ona zawierać dane kontaktowe, takie jak nazwisko i numer telefonu, urzędnika ds. ochrony prywatności lub działu odpowiedzialnego za ochronę danych, aby umożliwić wniesienie skargi („zażalenia"). W ramach organizacji administratora urzędnik ds. ochrony prywatności jest odpowiedzialny za rozpatrywanie skarg, podejmowanie działań naprawczych w przypadku naruszenia prywatności oraz odszkodowania (art. 31 ust. 2 pkt 3 i 4 PIPA). Ta ostatnia kwestia jest istotna na przykład w przypadku naruszenia ochrony danych, ponieważ administrator musi poinformować osobę, której dane dotyczą, między innymi o punktach kontaktowych do zgłaszania wszelkich szkód (art. 34 ust. 1 pkt 5 PIPA).

(132) Ponadto PIPA oferuje osobom fizycznym kilka dróg dochodzenia roszczeń przeciwko administratorom. Po pierwsze, każda osoba fizyczna, która uważa, że jej prawa lub interesy w zakresie ochrony danych zostały naruszone przez administratora, może zgłosić takie naruszenie bezpośrednio do PIPC lub jednej z wyspecjalizowanych instytucji wyznaczonych przez PIPC do przyjmowania i rozpatrywania skarg; należy do nich Koreańska Agencja ds. Internetu i Bezpieczeństwa, która w tym celu prowadzi centrum telefoniczne do spraw danych osobowych (tzw. centrum telefoniczne ds. prywatności) (art. 62 ust. 1 pkt 2 PIPA w związku z art. 59 dekretu

([157]) Zob. sprawozdanie roczne PIPC za 2021 r., s. 50–55 (dostępne wyłącznie w języku koreańskim) na stronie internetowej https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Zob. strona internetowa (dostępna wyłącznie w języku koreańskim) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK

([159]) Zob. strona internetowa (dostępna wyłącznie w języku koreańskim) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

([160]) Zob. strona internetowa (dostępna wyłącznie w języku koreańskim): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Zob. np. sprawozdanie roczne z 2020 r. na stronie internetowej (dostępne wyłącznie w języku koreańskim) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 i przykłady w języku angielskim na stronie internetowej https://www.privacy.go.kr/eng/enforcement_02.do

wykonawczego do PIPA). Centrum telefoniczne ds. prywatności bada i stwierdza naruszenia, zapewnia poradnictwo w zakresie przetwarzania danych osobowych (art. 62 ust. 3 PIPA) i może zgłaszać naruszenia do PIPC (ale nie może samo egzekwować prawa). Centrum telefoniczne ds. prywatności otrzymuje dużo skarg/zgłoszeń (np. 177 457 w 2020 r., 159 255 w 2019 r. i 164 497 w 2018 r.) ([162]). Według informacji otrzymanych od PIPC od sierpnia 2020 r. do sierpnia 2021 r. sama PIPC otrzymała około 1 000 skarg. W odpowiedzi na skargę PIPC może wydać zalecenie dotyczące usprawnień, nakazać podjęcie działań naprawczych, wnieść „zarzuty" do właściwego organu ścigania (np. do prokuratury) lub zalecić zastosowanie środków dyscyplinarnych (zob. art. 61, 64 i 65 PIPA). Decyzje PIPC (takie jak odmowa rozpatrzenia skargi lub odrzucenie skargi co do jej istoty) można zaskarżyć na mocy ustawy o postępowaniu administracyjnym ([163]).

(133) Po drugie, zgodnie z art. 40–50 PIPA w związku z art. 48-14–57 dekretu wykonawczego do PIPA, osoby, których dane dotyczą, mogą wystąpić z roszczeniem do „Komisji ds. Mediacji w Sporach" (ang. Dispute Mediation Committee), która składa się z przedstawicieli mianowanych przez przewodniczącego PIPC spośród członków dyrekcji PICP oraz osób fizycznych mianowanych na podstawie ich doświadczenia w dziedzinie ochrony danych spośród pewnych kwalifikujących się grup (zob. art. 40 ust. 2, 3 i 7 PIPA, art. 48-14 dekretu wykonawczego do PIPA) ([164]). Możliwość skorzystania z mediacji przed Komisją ds. Mediacji w Sporach to alternatywna droga dochodzenia roszczeń, która jednak nie ogranicza prawa osoby fizycznej do zwrócenia się zamiast tego do PIPC lub sądów. W celu zbadania sprawy komisja może zwrócić się do stron sporu o przedstawienie niezbędnych materiałów lub wezwać odpowiednich świadków do stawienia się przed nią (art. 45 PIPA). Po wyjaśnieniu sprawy komisja przygotowuje projekt ugody mediacyjnej ([165]), na który musi wyrazić zgodę większość jej członków. Projekt ugody mediacyjnej może zawierać zobowiązanie do zaprzestanie naruszenia, konieczne działania naprawcze (w tym przywrócenie stanu poprzedniego lub odszkodowanie), jak również wszelkie środki konieczne do zapobieżenia powtórzeniu się tego samego lub podobnego naruszenia (art. 47 ust. 1 PIPA). W przypadku gdy obie strony zgadzają się na zawarcie ugody mediacyjnej, ma ona taki sam skutek jak ugoda sądowa (art. 47 ust. 5 PIPA). Każda ze stron może wszcząć postępowanie przed sądem w trakcie trwania mediacji, w którym to przypadku mediacja zostanie zawieszona (zob. art. 48 ust. 2 PIPA) ([166]). Roczne statystyki publikowane przez PIPC wskazują, że osoby fizyczne regularnie korzystają z procedury mediacyjnej przed Komisją ds. Mediacji w Sporach, a procedura ta często prowadzi do pozytywnych wyników. Na przykład w 2020 r. Komisja ds. Mediacji w Sporach zajmowała się 126 sprawami, z których 89 rozstrzygnięto przed nią (w 77 z nich strony osiągnęły porozumienie przed zakończeniem procesu mediacji, a w 12 z nich strony przyjęły propozycję mediatora), co dało wskaźnik mediacji na poziomie 70,6 % ([167]). Podobnie w 2019 r. Komisja zajmowała się 139 sprawami, z których 92 rozstrzygnięto, co dało wskaźnik mediacji na poziomie 62,2 %.

(134) Ponadto, jeżeli co najmniej 50 osób fizycznych poniosło szkodę lub ich prawa do ochrony danych zostały naruszone w ten sam lub podobny sposób w następstwie tego samego (rodzaju) incydentu ([168]), osoba, której dane dotyczą, lub organizacja zajmująca się ochroną danych może złożyć wniosek o mediację w sporze zbiorowym w imieniu takiej grupy osób; inne osoby, których dane dotyczą, mogą dołączyć do takiej mediacji, co zostanie ogłoszone publicznie przez Komisję ds. Mediacji w Sporach (art. 49 ust. 1–3 PIPA w związku z art. 52–54 dekretu wykonawczego do PIPA) ([169]). Komisja ds. Mediacji w Sporach może wybrać co najmniej

([162]) Zob. sprawozdanie roczne PIPC za 2021 r., s. 174. W 2020 r. takie skargi dotyczyły na przykład zbierania danych bez zgody, nieprzestrzegania obowiązków dotyczących przejrzystości, naruszenia PIPA przez podmioty przetwarzające, niewystarczających środków bezpieczeństwa, braku odpowiedzi na wnioski osób, których dane dotyczą, jak również zagadnień ogólnych.

([163]) W szczególności osoby fizyczne mogą odwołać się od wykonywania lub odmowy wykonywania władzy publicznej przez agencję administracyjną (art. 2 ust. 1 pkt 1, art. 3 pkt 1 ustawy o postępowaniu administracyjnym). Bardziej szczegółowe informacje na temat aspektów proceduralnych, w tym wymogów dopuszczalności, przedstawiono w motywie (181).

([164]) Wszyscy członkowie są powoływani na określoną kadencję i mogą zostać odwołani wyłącznie z uzasadnionych powodów (zob. art. 40 ust. 5, art. 41 PIPA). Ponadto w art. 42 PIPA określono zabezpieczenia chroniące przed konfliktem interesów.

([165]) Zob. art. 44 PIPA. Ponadto PIPC może zaproponować projekt ugody i zalecić ugodę bez przeprowadzenia mediacji (zob. art. 46 PIPA).

([166]) Co więcej, PIPC może odrzucić mediację, jeśli uzna, że mediacja jest niewłaściwa ze względu na charakter sporu, lub jeśli wniosek o mediację został złożony w nieuczciwym celu (art. 48 PIPA).

([167]) Zob. sprawozdanie roczne PIPC za 2021 r., s. 179–180. Sprawy te dotyczyły, między innymi, naruszeń wymogu uzyskania zgody na zbieranie danych, zasady ograniczenia celu oraz praw osób, których dane dotyczą.

([168]) Zob. art. 49 ust. 1 PIPA, zgodnie z którym osoby, których dane dotyczą, muszą ponieść szkodę lub doznać naruszenia swoich praw „w identyczny lub podobny sposób", oraz art. 52 pkt 2 dekretu wykonawczego do PIPA, w którym przewidziano wymóg, aby „[n]ajważniejsze kwestie związane z incydentem były wspólne pod względem faktycznym lub prawnym".

([169]) Ponadto nawet podmioty niebędące stronami mogą skorzystać z zawartej przez administratora ugody mediacyjnej w sporze zbiorowym w taki sposób, że Komisja ds. Mediacji w Sporach może doradzić administratorowi przygotowanie i przedłożenie planu odszkodowania, który obejmie (również) te podmioty (art. 49 ust. 5 PIPA).

jedną osobę, która w najbardziej odpowiedni sposób reprezentuje wspólny interes, jako stronę reprezentatywną (art. 49 ust. 4 PIPA). W przypadku gdy administrator odrzuci mediację w sporze zbiorowym lub nie zgodzi się na zawarcie ugody mediacyjnej, pewne organizacje ([170]) mogą wnieść powództwo zbiorowe, aby zaradzić naruszeniu (art. 51–57 PIPA).

(135) Po trzecie, w przypadku naruszenia prywatności powodującego „szkodę" dla osoby fizycznej, osoba, której dane dotyczą, ma prawo do odpowiednich środków dochodzenia roszczeń w ramach „szybkiej i sprawiedliwej procedury" (art. 4 pkt 5 w związku z art. 39 PIPA) ([171]). Administrator może uwolnić się od zarzutów w drodze udowodnienia braku winy („bezprawnego zamiaru" lub zaniedbania). W przypadku gdy osoba, której dane dotyczą, poniesie szkodę na skutek utraty, kradzieży, ujawnienia, fałszerstwa, zmiany lub zniszczenia jej danych osobowych, sąd może ustalić odszkodowanie w wysokości do trzykrotności wartości faktycznej szkody, uwzględniając szereg czynników (art. 39 ust. 3 i 4 PIPA). Ewentualnie osoba, której dane dotyczą, może dochodzić „rozsądnej kwoty" odszkodowania, nieprzekraczającej 3 mln wonów (art. 39-2 ust. 1 i 2 PIPA). Ponadto, zgodnie z kodeksem cywilnym, odszkodowania można dochodzić od każdej osoby, „która powoduje straty lub szkody dla innej osoby w drodze umyślnego lub nieumyślnego bezprawnego działania" ([172]) lub od osoby, „która wyrządziła szkodę osobie, wolności lub dobremu imieniu innej osoby lub spowodowała jej cierpienie psychiczne" ([173]). Taką odpowiedzialność deliktową wynikającą z naruszenia przepisów o ochronie danych potwierdził Sąd Najwyższy ([174]). Jeżeli szkoda została spowodowana bezprawnym działaniem organu publicznego, powództwo o odszkodowanie może być ponadto wniesione na podstawie ustawy o odszkodowaniach od państwa ([175]). Powództwo na podstawie ustawy o odszkodowaniach od państwa można wnieść do wyspecjalizowanej rady ds. odszkodowań lub bezpośrednio do koreańskich sądów ([176]). Odpowiedzialność państwa obejmuje również szkody niemajątkowe (takie jak cierpienie psychiczne) ([177]). Jeśli poszkodowany jest cudzoziemcem, ustawa o odszkodowaniach od państwa ma zastosowanie, o ile kraj pochodzenia ofiary również zapewnia odszkodowanie obywatelom koreańskim ([178]).

(136) Po czwarte, Sąd Najwyższy stwierdził, że osoby fizyczne mają prawo do wystąpienia o nakaz sądowy z tytułu naruszenia ich praw wynikających z konstytucji, w tym prawa do ochrony danych osobowych ([179]). W tym kontekście sąd może na przykład nakazać administratorom zawieszenie lub zaprzestanie wszelkich bezprawnych działań. Ponadto prawa do ochrony danych, w tym prawa chronione przez PIPA, mogą być egzekwowane w drodze powództwa cywilnego. To horyzontalne zastosowanie konstytucyjnej ochrony prywatności do relacji między osobami prywatnymi zostało uznane przez Sąd Najwyższy ([180]).

([170]) Mianowicie grupy konsumentów lub organizacje pozarządowe o charakterze niezarobkowym, o określonej liczbie członków, których deklarowanym celem jest ochrona danych (chociaż w przypadku tych ostatnich z dodatkowym wymogiem, że co najmniej 100 osób, których dane dotyczą i które doświadczyły takiego samego (rodzaju) naruszenia, złożyło wniosek o wniesienie powództwa zbiorowego). Zob. art. 51 PIPA.

([171]) Art. 43–43-3 CIA również przewidują odpowiedzialność za szkody wynikające z naruszeń tej ustawy.

([172]) Art. 750 kodeksu cywilnego.

([173]) Art. 751 ust. 1 kodeksu cywilnego.

([174]) Zob. na przykład orzeczenie Sądu Najwyższego 2015Da251539, 251546, 251553, 251560, 251577 z dnia 30 maja 2018 r. Ponadto Sąd Najwyższy potwierdził, że naruszenia ochrony danych mogą prowadzić do przyznania odszkodowania na podstawie kodeksu cywilnego, zob. orzeczenie Sądu Najwyższego nr 2011Da59834, 59858, 59841 z dnia 26 grudnia 2012 r. (streszczenie w języku angielskim dostępne na stronie internetowej http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). W tej sprawie Sąd Najwyższy wyjaśnił, że przy ocenie, czy osoba fizyczna doświadczyła cierpienia emocjonalnego kwalifikującego się jako szkoda podlegająca odszkodowaniu, musi zostać uwzględnionych kilka czynników, takich jak: rodzaj i charakter ujawnionych informacji, możliwość identyfikacji osoby fizycznej na skutek naruszenia, możliwość dostępu stron trzecich do informacji, zakres, w jakim dane osobowe zostały rozpowszechnione, czy doprowadziło to do dodatkowych naruszeń praw indywidualnych, jak dane osobowe były zarządzane i chronione itp.

([175]) Na podstawie ustawy o odszkodowaniach od państwa osoby fizyczne mogą ubiegać się o odszkodowanie za szkody wyrządzone przez urzędników publicznych wykonujących swoje oficjalne obowiązki z naruszeniem prawa (art. 2 ust. 1 ustawy).

([176]) Art. 9 i 12 ustawy o odszkodowaniach od państwa. W ustawie ustanawia się rady okręgowe (którym przewodniczy zastępca prokuratora odpowiedniej prokuratury), radę centralną (której przewodniczy wiceminister sprawiedliwości) i radę specjalną (której przewodniczy wiceminister obrony narodowej, odpowiedzialną za odszkodowania za szkody wyrządzone przez personel wojskowy lub cywilnych pracowników wojska). Powództwa o odszkodowanie są z zasady rozpatrywane przez rady okręgowe, które w określonych okolicznościach mogą przekazywać sprawy do rady centralnej lub specjalnej, np. jeśli dochodzone odszkodowanie przekracza określoną kwotę lub gdy osoba fizyczna wnioskuje o ponowne rozpatrzenie sprawy. Członków wszystkich rad powołuje minister sprawiedliwości (np. spośród urzędników publicznych Ministerstwa Sprawiedliwości, urzędników sądowych, prawników i osób posiadających wiedzę fachową w dziedzinie odszkodowań od państwa) i członkowie ci podlegają przepisom szczególnym dotyczącym konfliktu interesów (zob. art. 7 dekretu wykonawczego do ustawy o odszkodowaniach od państwa).

([177]) Zob. art. 8 ustawy o odszkodowaniach od państwa (który zawiera odniesienie do kodeksu cywilnego), jak również art. 751 kodeksu cywilnego.

([178]) Art. 7 ustawy o odszkodowaniach od państwa.

([179]) Orzeczenie Sądu Najwyższego 93Da40614 z dnia 12 kwietnia 1996 r. i orzeczenie Sądu Najwyższego 2008Da42430 z dnia 2 września 2011 r., (streszczenie w języku angielskim dostępne na stronie internetowej https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Zob. na przykład orzeczenie Sądu Najwyższego 2008Da42430 z dnia 2 września 2011 r. (streszczenie w języku angielskim dostępne na stronie internetowej https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Osoby fizyczne mogą złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa na podstawie ustawy o postępowaniu karnym (art. 223) do prokuratora lub funkcjonariusza policji sądowej ([181]).

(138) Koreański system oferuje zatem różne możliwości dochodzenia roszczeń – od łatwo dostępnych i tanich (na przykład w drodze kontaktu z centrum telefonicznym ds. prywatności lub mediacji (zbiorowej)) po środki administracyjne (przed PIPC) i sądowe, takie jak możliwość uzyskania odszkodowania.

3. DOSTĘP DO DANYCH OSOBOWYCH PRZEKAZANYCH Z UNII EUROPEJSKIEJ I WYKORZYSTANIE ICH PRZEZ ORGANY PUBLICZNE W REPUBLICE KOREI

(139) Komisja oceniła również ograniczenia i zabezpieczenia, w tym mechanizmy nadzoru i indywidualnych środków dochodzenia roszczeń dostępnych w prawie koreańskim, jeśli chodzi o zbieranie i późniejsze wykorzystanie przez koreańskie organy publiczne danych osobowych przekazywanych w interesie publicznym administratorom w Korei, szczególnie do celów ścigania przestępstw i bezpieczeństwa narodowego (dostęp rządowy). W tym zakresie rząd Korei przedstawił Komisji oficjalne oświadczenia, zapewnienia i zobowiązania podpisane na najwyższym szczeblu ministerialnym i na szczeblu agencji, zawarte w załączniku II do niniejszej decyzji.

(140) Oceniając, czy warunki dostępu rządu do danych przekazywanych Korei na podstawie niniejszej decyzji spełniają kryterium „zasadniczej równoważności" na podstawie art. 45 ust. 1 rozporządzenia (UE) 2016/679, zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej, w świetle Karty praw podstawowych, Komisja uwzględniła w szczególności poniższe kryteria.

(141) Po pierwsze, wszelkie ograniczenia prawa do ochrony danych osobowych muszą być przewidziane przepisami prawa, a podstawa prawna, która pozwala na ingerencję w takie prawo, musi sama określać zakres ograniczenia w wykonywaniu danego prawa ([182]).

(142) Po drugie, aby spełnić wymóg proporcjonalności, zgodnie z którym odstępstwa od ochrony danych osobowych i ograniczenia tej ochrony powinny mieć zastosowanie tylko w takim zakresie, w jakim jest to absolutnie niezbędne w społeczeństwie demokratycznym do osiągnięcia szczególnych celów interesu ogólnego, równoważnych z celami uznanymi przez Unię, ustawodawstwo danego państwa trzeciego, które zezwala na ingerencję, powinno określać jasne i precyzyjne zasady regulujące zakres i stosowanie środków oraz przewidywać wymagane zabezpieczenia, aby osoby, których dane zostały przekazane, miały wystarczające gwarancje skutecznej ochrony swoich danych osobowych przed ryzykiem nadużyć ([183]). Przepisy muszą w szczególności wskazywać, w jakich okolicznościach i na jakich warunkach można wprowadzić środek przewidujący przetwarzanie takich danych ([184]), a także poddawać spełnienie takich wymogów niezależnemu nadzorowi ([185]).

(143) Po trzecie, prawodawstwo i jego wymogi muszą być prawnie wiążące na mocy prawa krajowego. Dotyczy to przede wszystkim organów danego państwa trzeciego, ale te wymogi prawne muszą być również egzekwowalne wobec władz danego państwa trzeciego przed sądami ([186]). W szczególności osoby, których dane dotyczą, muszą mieć możliwość wytoczenia powództwa przed niezależnym i bezstronnym sądem, aby uzyskać dostęp do swoich danych osobowych lub uzyskać sprostowanie lub usunięcie takich danych ([187]).

3.1 Ogólne ramy prawne

(144) Ograniczenia i zabezpieczenia mające zastosowanie do zbierania, a następnie wykorzystywania danych osobowych przez koreańskie organy publiczne wynikają z nadrzędnych ram konstytucyjnych, ustaw szczególnych, które regulują działalność tych organów w dziedzinie ścigania przestępstw i bezpieczeństwa narodowego, jak również przepisów, które mają szczególne zastosowanie do przetwarzania danych osobowych.

([181]) Jak wyjaśniono w motywie (127), wykorzystanie danych niezgodnie z przeznaczeniem może stanowić czyn zabroniony na mocy kodeksu karnego.

([182]) Zob. Schrems II, pkt 174–175 oraz przytaczane orzecznictwo. W odniesieniu do dostępu organów publicznych państw członkowskich zob. również sprawa C-623/17 Privacy International, ECLI:EU:C:2020:790, pkt 65; i sprawy połączone C-511/18, C-512/18 i C-520/18 La Quadrature du Net i in., ECLI:EU:C:2020:791, pkt 175.

([183]) Zob. Schrems II, pkt 176 i 181, jak również przytaczane orzecznictwo. W odniesieniu do dostępu organów publicznych państw członkowskich zob. również Privacy International, pkt 68; oraz La Quadrature du Net i in., pkt 132.

([184]) Zob. Schrems II, pkt 176. W odniesieniu do dostępu organów publicznych państw członkowskich zob. również Privacy International, pkt 68; oraz La Quadrature du Net i in., pkt 132.

([185]) Zob. Schrems II, pkt 179.

([186]) Zob. Schrems II, pkt 181–182.

([187]) Zob. Schrems I, pkt 95 oraz Schrems II, pkt 194. W tym zakresie Trybunał Sprawiedliwości Unii Europejskiej podkreślił w szczególności, że zgodność z art. 47 Karty praw podstawowych, gwarantującej prawo do skutecznego środka odwoławczego przed niezależnym i bezstronnym sądem, „przyczynia się do wypracowania wymaganego w Unii stopnia ochrony, [a jego] poszanowanie Komisja musi stwierdzić, zanim wyda na podstawie art. 45 ust. 1 [rozporządzenia (UE) 2016/679] decyzję stwierdzającą odpowiedni stopień ochrony" (Schrems II, pkt 186).

(145) Po pierwsze, dostęp do danych osobowych przez koreańskie organy publiczne jest regulowany ogólnymi zasadami zgodności z prawem, konieczności i proporcjonalności, które wynikają z koreańskiej konstytucji ([188]). W szczególności podstawowe prawa i wolności (w tym prawo do prywatności i tajemnicy korespondencji) ([189]) mogą być ograniczone przepisami prawa tylko wówczas, gdy jest to konieczne do celów bezpieczeństwa narodowego lub utrzymania porządku publicznego i do celów dobra publicznego. Takie ograniczenia nie mogą naruszać istoty danego prawa lub wolności. W odniesieniu do przeszukania i zajęcia konstytucja stanowi, że mogą mieć one miejsce wyłącznie w sposób przewidziany przepisami prawa, na podstawie nakazu wydanego przez sędziego i z poszanowaniem sprawiedliwości proceduralnej ([190]). Osoby fizyczne mogą powołać się na swoje prawa i wolności przed Trybunałem Konstytucyjnym, jeżeli uważają, że zostały one naruszone przez organy publiczne w ramach wykonywania ich uprawnień ([191]). Podobnie osoby fizyczne, które poniosły szkody z powodu bezprawnego czynu popełnionego przez urzędnika publicznego w trakcie wykonywania obowiązków służbowych, mają prawo dochodzić słusznego odszkodowania ([192]).

(146) Po drugie, jak opisano szczegółowo w pkt 3.2.1 i 3.3.1, ogólne zasady wymienione w motywie (145) są również odzwierciedlone w ustawach szczególnych, które regulują uprawnienia organów ścigania i bezpieczeństwa narodowego. Na przykład w odniesieniu do postępowania przygotowawczego ustawa o postępowaniu karnym (CPA, od ang. Criminal Procedure Act) stanowi, że środki przymusu mogą zostać zastosowane wyłącznie w przypadkach wyraźnie przewidzianych w CPA i w najmniejszym zakresie niezbędnym do osiągnięcia celu dochodzenia ([193]). Podobnie w art. 3 ustawy o ochronie prywatności komunikacji (CPPA, od ang. Communications Privacy Protection Act) zabrania się dostępu do komunikacji prywatnej, z wyjątkiem sytuacji, gdy jest on oparty na przepisach prawa i podlega określonym w nich ograniczeniom i zabezpieczeniom. W dziedzinie bezpieczeństwa narodowego ustawa o Narodowej Służbie Wywiadu (ustawa o NIS, od ang. National Intelligence Service) stanowi, że każdy dostęp do informacji dotyczących komunikacji lub informacji dotyczących lokalizacji musi być zgodny z prawem, a nadużywanie władzy i naruszanie prawa jest zagrożone sankcjami karnymi ([194]).

(147) Po trzecie, zgodnie z PIPA, przetwarzanie danych osobowych przez organy publiczne, w tym do celów ścigania przestępstw i bezpieczeństwa narodowego, podlega przepisom o ochronie danych ([195]). Zgodnie z zasadą ogólną w art. 5 ust. 1 PIPA zobowiązano organy publiczne do opracowania polityki mającej na celu zapobieganie „nadużywaniu i niewłaściwemu wykorzystywaniu danych osobowych, jawnemu nadzorowi i śledzeniu itp. oraz promowanie godności człowieka i prywatności osób fizycznych". Ponadto każdy administrator musi przetwarzać dane osobowe w sposób, który minimalizuje możliwość naruszenia prywatności osoby, której dane dotyczą (art. 3 ust. 6 PIPA).

(148) Wszystkie wymogi przewidziane w PIPA, opisane szczegółowo w sekcji 2, mają zastosowanie do przetwarzania danych osobowych na potrzeby ścigania przestępstw. Obejmuje to podstawowe zasady (takie jak zgodność z prawem i rzetelność, ograniczenie celu, prawidłowość, minimalizacja danych, ograniczenie przechowywania, bezpieczeństwo i przejrzystość), zobowiązania (np. w zakresie powiadamiania o naruszeniu ochrony danych i danych wrażliwych) oraz prawa (do dostępu do informacji, do korekty, usunięcia i zawieszenia przetwarzania danych).

(149) Chociaż przetwarzanie danych osobowych do celów bezpieczeństwa narodowego podlega bardziej ograniczonemu zestawowi przepisów na mocy ustawy PIPA, zastosowanie mają podstawowe zasady, jak również przepisy dotyczące nadzoru, egzekwowania i środków dochodzenia roszczeń ([196]). W szczególności w art. 3 i 4 PIPA ustanowiono ogólne zasady ochrony danych (zgodność z prawem i rzetelność, ograniczenie celu, prawidłowość, minimalizacja danych, bezpieczeństwo i przejrzystość) oraz prawa indywidualne (prawo do informacji, prawo dostępu, prawo do korekty, usunięcia i zawieszenia przetwarzania danych) ([197]). Ponadto art. 4 ust. 5 PIPA zapewnia osobom fizycznym prawo do odpowiedniego środka dochodzenia roszczeń, w drodze szybkiej i uczciwej procedury, z tytułu wszelkich szkód wynikających z przetwarzania ich danych osobowych. Uzupełnieniem

([188]) Zob. załącznik II pkt 1.1.
([189]) Art. 37 ust. 2 konstytucji.
([190]) Art. 16 i art. 12 ust. 3 konstytucji. W art. 12 ust. 3 konstytucji określono ponadto wyjątkowe okoliczności, w których może mieć miejsce przeszukanie lub zajęcie bez nakazu (choć nadal wymagany jest nakaz *ex post*), tj. *in flagrante delicto* lub, w przypadku przestępstw zagrożonych karą pozbawienia wolności w wymiarze co najmniej trzech lat, jeżeli istnieje ryzyko, że dowody zostaną zniszczone lub podejrzany zniknie.
([191]) Art. 68 ust. 1 ustawy o Trybunale Konstytucyjnym.
([192]) Art. 29 ust. 1 konstytucji.
([193]) Art. 199 ust. 1 CPA. Co do zasady, wykonując swoje uprawnienia na mocy CPA, organy publiczne muszą przestrzegać praw podstawowych osób podejrzanych o popełnienie przestępstwa i wszystkich innych zainteresowanych osób (art. 198 ust. 2 CPA).
([194]) Art. 14 ustawy NIS.
([195]) Zob. załącznik II pkt 1.2.
([196]) Art. 58 ust. 1 pkt 2 PIPA. Zob. również sekcja 6 zawiadomienia nr 2021-5 (załącznik I). Wyłączenie stosowania niektórych przepisów PIPA ma zastosowanie wyłącznie wówczas, gdy dane osobowe są przetwarzane „do celów bezpieczeństwa narodowego". Po zakończeniu sytuacji dotyczącej bezpieczeństwa narodowego uzasadniającej przetwarzanie danych nie można się już powołać na to wyłączenie i zastosowanie mają wszystkie wymogi PIPA.
([197]) Takie prawa mogą być ograniczone wyłącznie wówczas, gdy jest to przewidziane w przepisach prawa, tak długo oraz w takim zakresie, w jakim jest to konieczne i proporcjonalne do ochrony ważnego celu leżącego w interesie publicznym lub gdy przyznanie prawa może spowodować szkodę dla życia lub integralności cielesnej strony trzeciej lub nieuzasadnione naruszenie majątku i innych interesów strony trzeciej. Zob. zawiadomienie nr 2021-5 sekcja 6.

tego przepisu są bardziej szczególne zobowiązania do przetwarzania danych osobowych wyłącznie w minimalnym zakresie niezbędnym do osiągnięcia zamierzonego celu i przez możliwie najkrótszy okres, do wprowadzenia niezbędnych środków w celu zapewnienia bezpiecznego zarządzania danymi i właściwego przetwarzania (takie jak zabezpieczenia techniczne, zarządcze i fizyczne), jak również wprowadzenia środków służących właściwemu rozpatrywaniu indywidualnych skarg (zażaleń) ([198]). Ogólne zasady zgodności z prawem, konieczności i proporcjonalności wynikające z koreańskiej konstytucji (zob. motyw (145)) mają zastosowanie również do przetwarzania danych osobowych do celów bezpieczeństwa narodowego.

(150) Na te ogólne ograniczenia i zabezpieczenia osoby fizyczne mogą powoływać się przed niezależnymi organami nadzoru (np. PIPC lub Krajową Komisją Praw Człowieka, zob. motywy (177)–(178)) oraz sądami (zob. motywy (179)–(183)), aby dochodzić swoich roszczeń.

3.2 **Dostęp koreańskich organów publicznych do danych na potrzeby ścigania przestępstw i wykorzystanie tych danych przez te organy w tym samym celu**

(151) W prawie Republiki Korei ustanowiono szereg ograniczeń w zakresie dostępu do danych osobowych i ich wykorzystywania do celów ścigania przestępstw, a także zapewniono mechanizmy nadzoru i dochodzenia roszczeń zgodne z wymogami, o których mowa w motywach (141)–(143) niniejszej decyzji. Warunki uzyskania takiego dostępu oraz zabezpieczenia mające zastosowanie do wykonywania tych uprawnień poddano szczegółowej ocenie w kolejnych sekcjach.

3.2.1 *Podstawy prawne, ograniczenia i zabezpieczenia*

(152) Dane osobowe przetwarzane przez koreańskich administratorów, które byłyby przekazywane z Unii na podstawie niniejszej decyzji ([199]), mogą być zbierane przez koreańskie władze do celów ścigania przestępstw w kontekście przeszukania lub zajęcia (na podstawie CPA) w drodze dostępu do informacji dotyczących komunikacji (na podstawie CPPA) lub w drodze pozyskiwania danych abonentów za pośrednictwem wniosków o dobrowolne ujawnienie (na podstawie ustawy o działalności telekomunikacyjnej, ang. Telecommunications Business Act, TBA) ([200]).

3.2.1.1 Przeszukanie i zajęcie

(153) CPA stanowi, że przeszukanie lub zajęcie może mieć miejsce wyłącznie wówczas, gdy osoba jest podejrzana o popełnienie przestępstwa, jest to konieczne do celów dochodzenia oraz istnieje związek między dochodzeniem a osobą, która ma zostać przeszukana, lub przedmiotem, który ma zostać poddany kontroli lub zajęty ([201]). Ponadto przeszukanie lub zajęcie (jak każdy środek przymusu) może być dozwolone lub przeprowadzone jedynie w najmniejszym niezbędnym zakresie ([202]). Jeżeli przeszukanie dotyczy dysku komputerowego lub innego nośnika danych, co do zasady zajęte zostają wyłącznie same niezbędne dane (skopiowane lub wydrukowane), a nie cały nośnik ([203]). Nośnik może zostać zajęty wyłącznie wówczas, gdy uznano, że wyodrębnione wydrukowanie lub skopiowanie wymaganych danych jest niemożliwe, lub gdy uznano, że nie można zrealizować celu przeszukania w inny sposób ([204]). W CPA ustanowiono w związku z tym jasne i precyzyjne zasady dotyczące zakresu i stosowania tych środków, aby zapewnić tym samym, że ingerencja w prawa osób fizycznych w przypadku przeszukania lub zajęcia będzie ograniczona do tego, co jest niezbędne do celów określonego postępowania przygotowawczego i proporcjonalne do zamierzonego celu.

([198]) Art. 58 ust. 4 PIPA.

([199]) Zob. załącznik II pkt 2.1. Oficjalne oświadczenie rządu Korei (załącznik II pkt 2.1) również odnosi się do możliwości zbierania informacji o transakcjach finansowych w celu zapobiegania praniu pieniędzy i finansowaniu terroryzmu na podstawie ustawy o zgłaszaniu i wykorzystaniu określonych informacji o transakcjach finansowych (ARUSFTI). Jednakże w ARUSFTI nakłada się obowiązki ujawniania informacji wyłącznie na administratorów, którzy przetwarzają informacje dotyczące kredytów osobistych zgodnie z CIA i podlegają nadzorowi Komisji Usług Finansowych (zob. motyw (13)). Z uwagi na to, że przetwarzanie informacji dotyczących kredytów osobistych przez administratorów jest wyłączone z zakresu niniejszej decyzji, ARUSFTI nie jest dla niniejszej oceny istotna.

([200]) W art. 3 CPPA jako możliwą podstawę prawną zbierania danych dotyczących komunikacji wymienia się również ustawę o sądach wojskowych. Ustawa ta reguluje jednak zbieranie informacji na temat personelu wojskowego i może mieć zastosowanie do osób cywilnych wyłącznie w ograniczonej liczbie przypadków, (np. jeżeli personel wojskowy i osoby cywilne popełniłyby wspólnie przestępstwo lub jeżeli osoba fizyczna popełniłaby przestępstwo przeciwko wojsku, postępowanie może zostać wszczęte przed sądem wojskowym, zob. art. 2 ustawy o sądach wojskowych). W każdym razie zawiera ona przepisy ogólne regulujące przeszukania i zajęcia, podobne do przepisów zawartych w CPA (zob. np. art. 146–149 i 153–156 ustawy o sądach wojskowych) oraz stanowiące na przykład, że korespondencję pocztową można zbierać wyłącznie wówczas, gdy jest to konieczne do przeprowadzenia dochodzenia i na podstawie nakazu sądu wojskowego. W zakresie, w jakim na podstawie tej ustawy byłyby zbierane dane z łączności elektronicznej, miałyby zastosowanie ograniczenia i zabezpieczenia przewidziane w CPPA. Zob. załącznik II pkt 2.2.2 i przypis 50.

([201]) Art. 215 ust. 1 i 2 CPA. Zob. również art. 106 ust. 1, art. 107 i art. 109 CPA, które stanowią, że sądy mogą dokonywać przeszukania i zajęcia, o ile podlegające im przedmioty lub osoby uważa się za związane z konkretną sprawą. Zob. załącznik II pkt 2.2.1.2.

([202]) Art. 199 ust. 1 CPA.

([203]) Art. 106 ust. 3 CPA.

([204]) Art. 106 ust. 3 CPA.

(154) Jeżeli chodzi o zabezpieczenia proceduralne, w CPA wymaga się uzyskania nakazu sądowego w celu przeprowadzenia przeszukania lub zajęcia ([205]). Przeszukanie lub zajęcie bez nakazu jest dopuszczalne wyłącznie w wyjątkowych okolicznościach, mianowicie w sprawach pilnych ([206]), na miejscu w chwili zatrzymania lub aresztowania osoby podejrzanej ([207]), lub w przypadku gdy przedmiot został porzucony lub dobrowolnie przekazany przez osobę podejrzaną lub osobę trzecią (w odniesieniu do danych osobowych – przez samą osobę zainteresowaną) ([208]). Nielegalne przeszukania i zajęcia są zagrożone sankcjami karnymi ([209]), a wszelkie dowody uzyskane z naruszeniem CPA uznaje się za niedopuszczalne ([210]). Ponadto zainteresowane osoby fizyczne muszą być zawsze bezzwłocznie powiadamiane o przeszukaniu lub zajęciu (w tym o zajęciu ich danych) ([211]), co z kolei ułatwi wykonanie przysługujących im praw podmiotowych i prawa do dochodzenia roszczeń (zob. w szczególności możliwość zaskarżenia wykonania nakazu zajęcia – motyw (180)).

3.2.1.2 Dostęp do informacji dotyczących komunikacji

(155) Na podstawie CPPA koreańskie organy ścigania mogą zastosować dwa rodzaje środków ([212]): z jednej strony, mogą zbierać „dane potwierdzające komunikację" ([213]), które obejmują datę połączenia telekomunikacyjnego, czas jego rozpoczęcia i zakończenia, liczbę połączeń wychodzących i przychodzących, jak również numer abonenta drugiego rozmówcy, częstotliwość połączeń, pliki dziennika dotyczące korzystania z usług telekomunikacyjnych oraz informacje dotyczące lokalizacji (na przykład z wież przekaźnikowych, które odbierają sygnały); oraz, z drugiej strony, mogą zastosować „środki ograniczające komunikację", które obejmują zarówno zbieranie treści pochodzących z poczty tradycyjnej, jak i bezpośrednie przechwytywanie treści przekazów telekomunikacyjnych ([214]).

(156) Dostęp do danych potwierdzających komunikację można uzyskać wyłącznie wówczas, gdy jest to konieczne do przeprowadzenia postępowania przygotowawczego lub wykonania wyroku ([215]), na podstawie nakazu wydanego przez sąd ([216]). W tym zakresie w CPPA wymaga się przedstawienia szczegółowych informacji zarówno we wniosku o wydanie nakazu (np. na temat powodów wystąpienia z wnioskiem, związku z osobą, której dotyczy wniosek/abonentem oraz niezbędnych danych), jak i w samym nakazie (np. na temat celu, osoby, której dotyczy nakaz, i zakresu środka) ([217]). Zbieranie danych bez nakazu może mieć miejsce wyłącznie wówczas, gdy ze

([205]) Art. 215 ust. 1 i 2 oraz art. 113 CPA. Składając wniosek o wydanie nakazu, zainteresowany organ musi przedłożyć materiały uzasadniające podejrzenie, że dana osoba popełniła czyn zabroniony, że przeszukanie, oględziny lub zajęcie są konieczne oraz że istnieją stosowne przedmioty, które mają zostać zajęte (art. 108 ust. 1 rozporządzenia w sprawie postępowania karnego). Sam nakaz musi zawierać między innymi imiona i nazwiska osób podejrzanych oraz określenie rodzaju przestępstwa; wskazanie miejsca, osoby lub przedmiotów, które mają zostać przeszukane, lub przedmiotów, które mają zostać zajęte; datę wystawienia oraz okres obowiązywania (art. 114 ust. 1 w związku z art. 219 CPA). Zob. załącznik II pkt 2.2.1.2.

([206]) To znaczy, gdy uzyskanie nakazu jest niemożliwe ze względu na pilny charakter sprawy na miejscu popełnienia przestępstwa (art. 216 ust. 3 CPA), w którym to przypadku nakaz należy niezwłocznie uzyskać w późniejszym terminie (art. 216 ust. 3 CPA).

([207]) Art. 216 ust. 1 i 2 CPA.

([208]) Art. 218 CPA. Ponadto, jak wyjaśniono w załączniku II pkt 2.2.1.2, dobrowolnie okazane przedmioty są dopuszczane jako dowód w postępowaniu sądowym wyłącznie wówczas, gdy nie ma zasadnych wątpliwości co do dobrowolnego charakteru ujawnienia, a wykazanie tego faktu należy do prokuratora.

([209]) Art. 321 kodeksu karnego.

([210]) Art. 308-2 CPA. Ponadto osoba fizyczna (i jej pełnomocnik) może być obecna przy wykonywaniu nakazu przeszukania lub zajęcia, a zatem może również wnieść sprzeciw w czasie wykonywania nakazu (art. 121 i 219 CPA).

([211]) Art. 121 i 122 CPA (w odniesieniu do przeszukania) oraz art. 219 w związku z art. 106 ust. 4 CPA (w odniesieniu do zajęcia).

([212]) Zob. także załącznik II pkt 2.2.2.1. Środki takie mogą być stosowane z pomocą operatorów telekomunikacyjnych wezwanych do współpracy na mocy przedstawionego im pisemnego zezwolenia uzyskanego od sądu (art. 9 ust. 2 CPPA), które musi być przechowywane przez operatorów (art. 15-2 CPPA i art. 12 dekretu wykonawczego do CPPA). Dostawcy usług telekomunikacyjnych mogą odmówić współpracy, jeżeli informacje na temat osoby fizycznej, której dotyczą środki, wskazane w pisemnym zezwoleniu sądu (np. numer telefonu tej osoby) są nieprawidłowe; ponadto, bez względu na okoliczności, nie mogą ujawniać haseł używanych do celów korzystania z usług telekomunikacyjnych (art. 9 ust. 4 CPPA).

([213]) Art. 2 ust. 11 CPPA.

([214]) Zob. art. 2 ust. 6 CPPA, który odnosi się do „cenzury" (otwieranie poczty bez zgody zainteresowanej strony lub zapoznawanie się z jej treścią, rejestrowanie jej lub zatrzymywanie za pomocą innych środków), oraz art. 2 ust. 7 CPPA, który odnosi się do „podsłuchu" (pozyskiwanie lub rejestrowanie treści przekazów telekomunikacyjnych poprzez słuchanie dźwięków lub równoczesne czytanie słów i oglądanie symboli lub obrazów pochodzących z przekazów telekomunikacyjnych za pomocą urządzeń elektronicznych i mechanicznych bez zgody zainteresowanej strony lub zakłócanie ich przekazywania i odbioru).

([215]) Art. 13 ust. 1 CPPA. Zob. także załącznik II pkt 2.2.2.3. Ponadto dane dotyczące śledzenia lokalizacji w czasie rzeczywistym oraz dane potwierdzające komunikację dotyczące konkretnej stacji bazowej mogą być zbierane wyłącznie w celu prowadzenia postępowań przygotowawczych w sprawie poważnych przestępstw lub w przypadku gdy w inny sposób trudno byłoby zapobiec popełnieniu przestępstwa lub zebrać dowody (art. 13 ust. 2 CPPA). Odzwierciedla to potrzebę zapewnienia dodatkowych zabezpieczeń w przypadku środków szczególnie ingerujących w prywatność, zgodnie z zasadą proporcjonalności.

([216]) Art. 13 i 6 CPPA.

([217]) Zob. art. 13 ust. 3 i 9 w związku z art. 6 ust. 4 i 6 CPPA.

względu na pilny charakter sprawy niemożliwe jest uzyskanie zezwolenia sądu – w takim przypadku należy uzyskać nakaz i przekazać go dostawcy usług telekomunikacyjnych niezwłocznie po wystąpieniu o dane ([218]). Jeżeli sąd odmówi następnie udzielenia zezwolenia, zebrane informacje muszą zostać zniszczone ([219]).

(157) W zakresie dodatkowych zabezpieczeń w odniesieniu do zbierania danych potwierdzających komunikację w CPPA nakłada się szczególne wymogi dotyczące prowadzenia rejestrów i przejrzystości ([220]). W szczególności zarówno organy ścigania ([221]), jak i dostawcy usług telekomunikacyjnych ([222]) muszą prowadzić rejestry wniosków i dokonanych ujawnień. Ponadto organy ścigania muszą co do zasady powiadomić osoby fizyczne o fakcie, że zebrano dotyczące ich dane potwierdzające komunikację ([223]). Odroczenie takiego powiadomienia może nastąpić wyłącznie w wyjątkowych okolicznościach, na podstawie zezwolenia dyrektora właściwej prokuratury okręgowej ([224]). Zezwolenia takiego można udzielić wyłącznie w przypadku, gdy istnieje prawdopodobieństwo, że powiadomienie może 1) zagrażać bezpieczeństwu narodowemu oraz bezpieczeństwu i porządkowi publicznemu, 2) spowodować śmierć lub uszczerbek na zdrowiu, 3) utrudnić rzetelne postępowanie sądowe (na przykład prowadząc do zniszczenia dowodów lub grożenia świadkom) lub 4) zniesławić osobę podejrzaną, poszkodowanych lub inne osoby związane ze sprawą lub naruszyć ich prywatność. W takich przypadkach powiadomienie musi zostać dostarczone w terminie 30 dni od ustania przyczyn odroczenia ([225]). Po otrzymaniu powiadomienia osoby fizyczne mają prawo do uzyskania informacji o powodach zbierania ich danych ([226]).

(158) Bardziej rygorystyczne zasady mają zastosowanie w odniesieniu do środków ograniczających komunikację, które mogą być stosowane wyłącznie w przypadku istotnego powodu do podejrzeń, że planuje się, popełnia lub popełniono określone poważne przestępstwa wyraźnie wymienione w CPPA ([227]). Ponadto środki ograniczające komunikację można wykorzystywać wyłącznie jako środek ostateczny i gdy trudno jest w inny sposób zapobiec popełnieniu przestępstwa, aresztować przestępcę lub zebrać dowody ([228]). Należy natychmiast zaprzestać stosowania takich środków, gdy nie są już niezbędne, aby ograniczyć naruszenie prywatności komunikacji do niezbędnego minimum ([229]). Informacje, które zostały nielegalnie uzyskane za pomocą środków ograniczających komunikację, nie są dopuszczane jako dowód w postępowaniu sądowym lub postępowaniu dyscyplinarnym ([230]).

(159) Jeżeli chodzi o zabezpieczenia proceduralne, w CPPA wymaga się uzyskania nakazu w celu zastosowania środków ograniczających komunikację ([231]). Również w tym przypadku w CPPA wymaga się, aby wniosek o wydanie nakazu oraz sam nakaz zawierały szczegółowe informacje ([232]), w tym uzasadnienie wniosku, jak również informacje dotyczące komunikacji, które mają zostać zebrane (które muszą dotyczyć podejrzanego, przeciwko któremu wszczęto postępowanie przygotowawcze) ([233]). Środki takie można zastosować bez nakazu wyłącznie w przypadku bezpośredniego zagrożenia przestępczością zorganizowaną lub w przypadku bezpośredniego zagrożenia innym poważnym przestępstwem, które może bezpośrednio spowodować śmierć lub poważny uszczerbek

([218]) Art. 13 ust. 2 CPPA.
([219]) Art. 13 ust. 3 CPPA.
([220]) Zob. załącznik II pkt 2.2.2.3.
([221]) Art. 13 ust. 5 i 6 CPPA.
([222]) Art. 13 ust. 7 CPPA. Ponadto dostawcy usług telekomunikacyjnych muszą dwa razy w roku składać sprawozdania z ujawniania danych potwierdzających komunikację do Ministerstwa Nauki i Technologii Informacyjno-Komunikacyjnych.
([223]) Zob. art. 13-3 ust. 7 w związku z art. 9-2 CPPA. W szczególności osoby fizyczne muszą zostać powiadomione w terminie 30 dni od wydania postanowienia o wniesieniu aktu oskarżenia lub zaniechaniu ścigania karnego lub w terminie 30 dni następujących po upływie roku od wydania postanowienia o zawieszeniu postępowania karnego (chociaż powiadomienie musi w każdym przypadku zostać dostarczone w terminie 30 dni następujących po upływie roku od zebrania informacji), zob. art. 13-3 ust. 1 CPPA.
([224]) Art. 13-3 ust. 2–3 CPPA.
([225]) Art. 13-3 ust. 4 CPPA.
([226]) Art. 13-3 ust. 5 CPPA. Na wniosek osoby fizycznej prokurator lub funkcjonariusz policji sądowej musi przedstawić uzasadnienie na piśmie w terminie 30 dni od otrzymania wniosku, chyba że ma zastosowanie jeden z wyjątków odroczenia powiadomienia (art. 13-3 ust. 6 CPPA).
([227]) Na przykład rewolucja, przestępstwa związane z narkotykami, przestępstwa z użyciem materiałów wybuchowych, jak również przestępstwa związane z bezpieczeństwem narodowym, stosunkami dyplomatycznymi lub bazami i instalacjami wojskowymi, zob. art. 5 ust. 1 CPPA. Zob. także załącznik II pkt 2.2.2.2.
([228]) Art. 3 ust. 2 i art. 5 ust. 1 CPPA.
([229]) Art. 2 dekretu wykonawczego do CPPA.
([230]) Art. 4 CPPA.
([231]) Art. 6 ust. 1, 2 i 5–6 CPPA.
([232]) We wniosku o wydanie nakazu należy określić: 1) istotne przesłanki wskazujące na (zasadne) podejrzenie, że jedno z wymienionych przestępstw jest planowane, jest popełniane lub zostało popełnione, a także wszelkie materiały potwierdzające; 2) środki ograniczające komunikację, jak również ich przedmiot, zakres, cel i okres obowiązywania; oraz 3) miejsce i sposób wykonania środków (art. 6 ust. 4 CPPA art. 4 ust. 1 dekretu wykonawczego do CPPA). W samym nakazie konieczne jest określenie środków, a także ich przedmiotu, zakresu, okresu oraz miejsca i sposobu wykonania (art. 6 ust. 6 CPPA).
([233]) Środek ograniczający komunikację musi być ukierunkowany na konkretne przesyłki pocztowe lub przekazy telekomunikacyjne wysłane lub otrzymane przez osobę podejrzaną lub przesyłki pocztowe lub przekazy telekomunikacyjne wysłane lub otrzymane przez osobę podejrzaną w ustalonym okresie(art. 5 ust. 2 CPPA).

na zdrowiu, oraz w sytuacji nadzwyczajnej, która uniemożliwia zastosowanie zwykłej procedury ([234]). Jednakże w takim przypadku wniosek o wydanie nakazu należy złożyć niezwłocznie po zastosowaniu środka ([235]). Środki ograniczające komunikację mogą być stosowane wyłącznie przez okres maksymalnie dwóch miesięcy ([236]) i mogą zostać przedłużone wyłącznie za zgodą sądu, jeżeli warunki stosowania tych środków nadal będą spełnione ([237]). Okres przedłużenia nie może przekroczyć łącznie jednego roku lub trzech lat w przypadku niektórych szczególnie poważnych przestępstw (takich jak przestępstwa związane z rewolucją, agresją zagraniczną, bezpieczeństwem narodowym) ([238]).

(160) Podobnie jak w przypadku zbierania danych potwierdzających komunikację w CPPA wymaga się od dostawców usług telekomunikacyjnych ([239]) i organów ścigania ([240]) prowadzenia rejestrów wykonywania środków ograniczających komunikację oraz przewiduje się powiadamianie zainteresowanej osoby fizycznej, które wyjątkowo może zostać odroczone, w stosownych przypadkach, ze względu na ważny interes publiczny ([241]).

(161) Ponadto nieprzestrzeganie określonych ograniczeń i zabezpieczeń przewidzianych w CPPA (w tym na przykład obowiązków dotyczących uzyskania nakazu, prowadzenia rejestrów i powiadamiania osoby fizycznej), zarówno w odniesieniu do zbierania danych potwierdzających komunikację, jak i stosowania środków ograniczających komunikację, jest zagrożone sankcjami karnymi ([242]).

(162) Uprawnienia organów ścigania do zbierania danych dotyczących komunikacji na podstawie CPPA (zarówno treści komunikacji, jak i danych potwierdzających komunikację) są zatem ograniczone jasnymi i precyzyjnymi zasadami i podlegają licznym zabezpieczeniom. Zabezpieczenia te w szczególności gwarantują nadzór nad wykonywaniem takich środków – zarówno *ex ante* (poprzez uprzednią zgodę sądu), jak i *ex post* (poprzez wymogi dotyczące prowadzenia rejestrów i sprawozdawczości) – oraz ułatwiają osobom fizycznym dostęp do skutecznych środków prawnych (zapewniając, aby zostały one poinformowane o zbieraniu ich danych).

3.2.1.3 Wnioski o dobrowolne ujawnienie danych abonentów

(163) Oprócz korzystania ze środków przymusu opisanych w motywach (153)–(162) koreańskie organy ścigania mogą zwrócić się do dostawców usług telekomunikacyjnych o dobrowolne przekazanie „danych dotyczących komunikacji" w celu wsparcia procesu karnego, postępowania przygotowawczego lub wykonania wyroku (art. 83 ust. 3 TBA). Możliwość ta istnieje wyłącznie w odniesieniu do ograniczonych zbiorów danych, tj. imienia i nazwiska, numeru rejestracyjnego mieszkańca, adresu i numeru telefonu użytkowników, terminów rozpoczęcia lub zakończenia abonamentu, jak również kodów identyfikacyjnych użytkowników (czyli kodów używanych do identyfikacji prawowitego użytkownika systemów komputerowych lub sieci komunikacyjnych) ([243]). Ponieważ za „użytkowników" ([244]) uważa się wyłącznie osoby fizyczne, które bezpośrednio korzystają z usług koreańskiego dostawcy usług telekomunikacyjnych, osoby fizyczne z UE, których dane zostały przekazane do Republiki Korei, zwykle nie należą do tej kategorii ([245]).

(164) Do takich dobrowolnych ujawnień mają zastosowanie różne ograniczenia, zarówno w odniesieniu do wykonywania uprawnień przez organ ścigania, jak i reakcji operatora telekomunikacyjnego. Zgodnie z ogólnym wymogiem organy ścigania muszą działać zgodnie z konstytucyjnymi zasadami konieczności i proporcjonalności (art. 12 ust. 1 i art. 37 ust. 2 konstytucji), także wtedy, gdy zwracają się o przekazanie informacji na zasadzie dobrowolności. Ponadto muszą one przestrzegać przepisów PIPA, w szczególności zbierając wyłącznie minimalne dane osobowe, w zakresie niezbędnym do osiągnięcia zgodnego z prawem celu, w sposób minimalizujący wpływ

([234]) Art. 8 ust. 1 CPPA. Zbieranie informacji w sytuacjach nadzwyczajnych musi jednak zawsze odbywać się zgodnie z „oświadczeniem o cenzurze/podsłuchu w sytuacji nadzwyczajnej", przy czym organ prowadzący zbieranie musi prowadzić rejestr wszelkich środków nadzwyczajnych (art. 8 ust. 4 CPPA).

([235]) Zbieranie musi zostać natychmiast przerwane, jeżeli organ ścigania nie uzyska zezwolenia sądu w ciągu 36 godzin (art. 8 ust. 2 CPPA), w którym to przypadku, jak wyjaśniono w załączniku II pkt 2.2.2.2, zebrane informacje zostaną co do zasady zniszczone. Sąd należy również powiadomić wówczas, gdy środki nadzwyczajne zostały wykonane w tak krótkim czasie, że nie ma potrzeby uzyskania zezwolenia (np. jeżeli osoba podejrzana została aresztowana natychmiast po rozpoczęciu przechwytywania danych, zob. art. 8 ust. 5 CPPA). W takim przypadku konieczne jest przedstawienie sądowi informacji o celu, przedmiocie, zakresie, okresie, miejscu i sposobie zbierania, a także o przyczynach niezłożenia wniosku o udzielenie zezwolenia przez sąd (art. 8 ust. 6-7 CPPA).

([236]) Art. 6 ust. 7 CPPA. Jeżeli cel środków zostanie osiągnięty wcześniej w tym okresie, należy natychmiast zaprzestać ich wykonywania.

([237]) Art. 6 ust. 7–8 CPPA.

([238]) Art. 6 ust. 8 CPPA.

([239]) Art. 9 ust. 3 CPPA.

([240]) Art. 18 ust. 1 dekretu wykonawczego do CPPA.

([241]) W szczególności prokurator musi powiadomić osobę fizyczną w terminie 30 dni od wniesienia aktu oskarżenia lub wydania postanowienia o zaniechaniu ścigania lub aresztowania (art. 9-2 ust. 1 CPPA). Powiadomienie może zostać odroczone za zgodą prezesa prokuratury okręgowej, jeżeli mogłoby to poważnie zagrozić bezpieczeństwu narodowemu lub zakłócić bezpieczeństwo publiczne i porządek publiczny lub gdyby mogło spowodować istotną szkodę dla życia i integralności cielesnej innych osób (art. 9-2 ust. 4–6 CPPA).

([242]) Art. 16 i 17 CPPA.

([243]) Art. 83 ust. 3 TBA. Zob. także załącznik II pkt 2.2.3.

([244]) Art. 2 ust. 9 TBA.

([245]) Zob. także załącznik II pkt 2.2.3.

na prywatność osób fizycznych (uwzględniając art. 3 ust. 1 i 6 PIPA). W szczególności wnioski o uzyskanie danych dotyczących komunikacji na podstawie TBA muszą być składane na piśmie i muszą zawierać uzasadnienie wniosku oraz wskazanie związku z danym użytkownikiem i zakresu danych objętych wnioskiem ([246]).

(165) Dostawcy usług telekomunikacyjnych nie są zobowiązani do zastosowania się do takich wniosków i mogą to zrobić wyłącznie zgodnie z PIPA. Oznacza to w szczególności, że muszą oni wziąć pod uwagę poszczególne interesy wchodzące w grę i nie mogą dostarczyć danych, jeśli mogłoby to naruszyć w sposób nieuzasadniony interesy osoby fizycznej lub strony trzeciej ([247]). Byłoby tak na przykład w przypadku, gdyby było oczywiste, że organ wnoszący nadużył swoich uprawnień ([248]). Operatorzy telekomunikacyjni muszą prowadzić ewidencję ujawnień na podstawie TBA i dwa razy w roku przedkładać sprawozdanie Ministrowi Nauki i Technologii Informacyjno-Komunikacyjnych ([249]).

(166) Ponadto, zgodnie z sekcją 3 zawiadomienia nr 2021-5 (załącznik I), dostawcy usług telekomunikacyjnych co do zasady muszą powiadomić zainteresowaną osobę fizyczną, jeżeli dobrowolnie zastosują się do wniosku ([250]). To z kolei umożliwi osobie fizycznej wykonanie przysługujących jej praw oraz – w przypadku bezprawnego ujawnienia danych – dochodzenie roszczeń albo od administratora (np. za ujawnienie danych z naruszeniem PIPA lub za uwzględnienie wniosku, który był wyraźnie nieproporcjonalny), albo od organów ścigania (np. za działanie wykraczające poza granice tego, co konieczne i proporcjonalne, lub za nieprzestrzeganie wymogów proceduralnych określonych w TBA).

3.2.2 *Dalsze wykorzystywanie zebranych informacji*

(167) Przetwarzanie danych osobowych zebranych przez koreańskie organy ścigania podlega wszystkim wymogom PIPA, w tym w odniesieniu do ograniczenia celu (art. 3 ust. 1–2 PIPA), zgodności z prawem wykorzystywania i przekazywania stronom trzecim (art. 15, 17 i 18 PIPA), przekazywania międzynarodowego (art. 17 i 18 PIPA w związku z sekcją 2 zawiadomienia nr 2021-5) ([251]), proporcjonalności lub minimalizacji danych (art. 3 ust. 1 i 6 PIPA) oraz ograniczenia przechowywania (art. 21 PIPA) ([252]).

(168) W odniesieniu do treści komunikacji, uzyskanych w wyniku zastosowania środków ograniczających komunikację, CPPA wyraźnie ogranicza możliwość ich wykorzystania do celów postępowania przygotowawczego, ścigania karnego lub zapobiegania poważnym przestępstwom ([253]); postępowań dyscyplinarnych w związku z tymi samymi przestępstwami; dochodzenia roszczeń odszkodowawczych przez stronę komunikacji lub gdy jest to wyraźnie dozwolone na mocy innych przepisów ([254]). Ponadto zbierane treści przekazów telekomunikacyjnych przesyłanych przez internet mogą być zatrzymywane wyłącznie za zgodą sądu, który wydał zezwolenie na zastosowanie środków ograniczających komunikację ([255]), w celu wykorzystania ich do celów postępowania przygotowawczego, ścigania lub zapobiegania poważnym przestępstwom ([256]). Co do zasady, w CPPA zakazuje się ujawniania informacji poufnych uzyskanych w wyniku stosowania środków ograniczających komunikację oraz wykorzystywania takich informacji w celu zaszkodzenia reputacji podmiotów, które podlegały tym środkom ([257]).

3.2.3 *Nadzór*

(169) W Korei działania organów ścigania są nadzorowane przez różne organy ([258]).

([246]) Art. 83 ust. 4 TBA. Jeżeli dostarczenie pisemnego wniosku nie jest możliwe ze względu na pilny charakter sprawy, wniosek taki należy dostarczyć niezwłocznie po ustaniu przyczyny tego pilnego charakteru (art. 83 ust. 4 TBA).

([247]) Art. 18 ust. 2 PIPA.

([248]) Orzeczenie Sądu Najwyższego nr 2012Da105482 z dnia 10 marca 2016 r. Zob. także załącznik II pkt 2.2.3 w odniesieniu do tego orzeczenia Sądu Najwyższego.

([249]) Art. 83 ust. 5–6 TBA.

([250]) Wymóg ten podlega ograniczonym wyjątkom i wyjątkom z zastrzeżeniami, w szczególności w przypadku gdy i dopóki istnieje prawdopodobieństwo, że powiadomienie zagrażałoby toczącemu się postępowaniu przygotowawczemu lub że może spowodować szkodę dla życia lub integralności cielesnej innej osoby, o ile te prawa lub interesy są w oczywisty sposób nadrzędne wobec praw osoby, której dane dotyczą. Zob. zawiadomienie sekcja 3 pkt (iii) ppkt 1.

([251]) W szczególności koreańskie organy publiczne mają obowiązek zapewnić, w drodze prawnie wiążącego instrumentu, poziom ochrony równoważny z PIPA, zob. również motyw (90).

([252]) Zob. także załącznik II pkt 1.2.

([253]) Zob. motyw (158).

([254]) Art. 12 CPPA. Zob. załącznik II pkt 2.2.2.2.

([255]) Prokurator lub policjant wykonujący środki ograniczające komunikację musi w ciągu 14 dni od zakończenia stosowania środków wybrać przekazy telekomunikacyjne, które mają zostać zatrzymane, i wystąpić do sądu o zezwolenie (funkcjonariusz policji składa wniosek do prokuratora, który następnie składa wniosek do sądu), zob. art. 12-2 ust. 1 i 2 CPPA.

([256]) Wniosek o wydanie takiego zezwolenia musi zawierać informacje na temat środków ograniczających komunikację, podsumowanie wyników zastosowania tych środków, powody zatrzymania (wraz z materiałami potwierdzającymi) oraz przekazy telekomunikacyjne, które mają zostać zatrzymane (art. 12-2 ust. 3 CPPA). Jeżeli wniosek nie zostanie złożony, pozyskane dane muszą zostać usunięte w ciągu 14 dni od zakończenia stosowania środka ograniczającego komunikację (art. 12-2 ust. 5 CPPA), a jeżeli wniosek zostanie odrzucony — w ciągu siedmiu dni (art. 12-2 ust. 5 CPPA). W obu przypadkach w ciągu siedmiu dni należy złożyć w sądzie, który zezwolił na zbieranie danych, sprawozdanie z usunięcia danych.

([257]) Art. 11 ust. 2 dekretu wykonawczego do CPPA.

([258]) Zob. załącznik II pkt 2.3.

(170) Po pierwsze, policja podlega wewnętrznemu nadzorowi Inspektora Generalnego ([259]), który przeprowadza kontrolę zgodności z prawem, w tym w odniesieniu do ewentualnych naruszeń praw człowieka. Funkcję Inspektora Generalnego utworzono w celu wdrożenia ustawy o audycie w sektorze publicznym, w której zachęca się do powoływania organów kontrolujących własną działalność i określa szczegółowe wymagania dotyczące ich składu i zadań. W szczególności ustawa zawiera wymóg, aby szef organu kontrolującego własną działalność był powoływany spoza danego organu (np. spośród byłych sędziów, profesorów) na okres od dwóch do pięciu lat ([260]), aby mógł zostać odwołany wyłącznie z uzasadnionych powodów (np. gdy nie jest w stanie wykonywać swoich obowiązków ze względów zdrowotnych lub gdy podlega środkom dyscyplinarnym) ([261]) i aby miał zagwarantowaną niezależność w jak najszerszym zakresie ([262]). Utrudnianie kontrolowania własnej działalności jest zagrożone administracyjnymi karami pieniężnymi ([263]). Sprawozdania z audytu (które mogą zawierać zalecenia, wnioski o zastosowanie środków dyscyplinarnych oraz wnioski o odszkodowanie lub dokonanie korekty) są przekazywane szefowi właściwego organu publicznego i Komisji Kontroli i Audytu (BAI) ([264]) oraz, co do zasady, podawane do wiadomości publicznej ([265]). O wynikach wdrażania sprawozdania należy również powiadomić BAI ([266]) (zob. motyw (173) dotyczący roli nadzorczej i uprawnień BAI).

(171) Po drugie, PIPC nadzoruje zgodność przetwarzania danych przez organy ścigania z PIPA i innymi przepisami chroniącymi prywatność osób fizycznych, w tym przepisami regulującymi zbieranie (elektronicznego) materiału dowodowego do celów ścigania przestępstw, jak opisano w pkt 3.2.1 ([267]). W szczególności, ponieważ nadzór PIPC obejmuje zgodność z prawem i słuszność zbierania i przetwarzania danych (art. 3 ust. 1 PIPA), które zostaną naruszone, jeżeli dostęp do danych osobowych i ich wykorzystywanie odbywa się z naruszeniem tych przepisów ([268]), PIPC może również badać i egzekwować zgodność z ograniczeniami i zabezpieczeniami opisanymi w pkt 3.2.1 ([269]). Wykonując tę funkcję nadzorczą, PIPC może korzystać ze wszystkich swoich uprawnień dochodzeniowych i zaradczych, opisanych szczegółowo w pkt 2.4.2. Już przed niedawną reformą PIPA (tj. w ramach swojej poprzedniej funkcji nadzoru dla sektora publicznego) PIPC przeprowadziła kilka działań nadzorczych w zakresie przetwarzania danych osobowych przez organy ścigania, np. w kontekście przesłuchań podejrzanych (sprawa nr 2013-16, 26 sierpnia 2013 r.), w zakresie dostarczania osobom fizycznym powiadomień o nałożeniu administracyjnych kar pieniężnych (sprawa nr 2015-02-04, 26 stycznia 2015 r.), udostępniania danych innym organom (sprawa nr 2018-15-146, 9 lipca 2018 r., sprawa nr 2018-25-308, 10 grudnia 2018 r.; sprawa nr 2019-02-015, 29 stycznia 2019 r.), zbierania odcisków palców lub fotografii (sprawa nr 2019-17-273, 9 września 2019 r.), użycia bezzałogowych statków powietrznych (sprawa nr 2020-01-004, 13 stycznia 2020 r.). W tych sprawach PIPC badała zgodność z kilkoma przepisami PIPA (np. zgodność przetwarzania z prawem, zasady ograniczenia celu i minimalizacji danych), ale także z odpowiednimi przepisami innych ustaw, takich jak ustawa o postępowaniu karnym, i w razie potrzeby wydawała zalecenia w celu dostosowania przetwarzania do wymogów w zakresie ochrony danych.

(172) Po trzecie, niezależny nadzór zapewnia Krajowa Komisja Praw Człowieka (ang. National Human Rights Commission, NHRC) ([270]), która może prowadzić dochodzenia w sprawie naruszeń prawa do prywatności i prawa do prywatności korespondencji w ramach swojego ogólnego mandatu ochrony praw podstawowych zagwarantowanych w art. 10-22 konstytucji. NHRC składa się z 11 komisarzy, którzy muszą dysponować określonymi kwalifikacjami ([271]) i są powoływani przez prezydenta zgodnie z procedurami ustanowionymi na mocy przepisów prawa. W szczególności powołanie czterech komisarzy następuje na podstawie nominacji Zgromadzenia Narodowego, czterech – na podstawie nominacji prezydenta, a trzech – na podstawie nominacji prezesa Sądu Najwyższego ([272]). Przewodniczącego powołuje prezydent spośród komisarzy, a następnie wymagane jest zatwierdzenie przez Zgromadzenie Narodowe ([273]). Komisarze (w tym przewodniczący) są powoływani na odnawialną trzyletnią

([259]) Zob. załącznik II pkt 2.3.1. Zob. również https://www.police.go.kr/eng/knpa/org/org01.jsp
([260]) Podobnie audytorzy są powoływani na podstawie szczegółowych warunków określonych w ustawie, zob. art. 16 i nast. ustawy o audycie w sektorze publicznym.
([261]) Art. 8–11 ustawy o audycie w sektorze publicznym.
([262]) Art. 7 ustawy o audycie w sektorze publicznym.
([263]) Art. 41 ustawy o audycie w sektorze publicznym.
([264]) Art. 23 ust. 1 ustawy o audycie w sektorze publicznym.
([265]) Art. 26 ustawy o audycie w sektorze publicznym.
([266]) Art. 23 ust. 3 ustawy o audycie w sektorze publicznym.
([267]) Zob. art. 7-8 ust. 3 i 4 oraz art. 7-9 ust. 5 PIPA.
([268]) Zob. zawiadomienie PIPC nr 2021-5 sekcja 6 (załącznik I).
([269]) Zob. także załącznik II pkt 2.3.4.
([270]) Art. 1 ustawy o Krajowej Komisji Praw Człowieka (ustawa o NHRC).
([271]) Aby zostać powołanym, komisarz musi 1) przepracować co najmniej dziesięć lat na uniwersytecie lub w autoryzowanym instytucie badawczym na stanowisku co najmniej profesora nadzwyczajnego; 2) przez co najmniej dziesięć lat wykonywać zawód sędziego, prokuratora lub radcy prawnego; 3) przez co najmniej dziesięć lat angażować się w działalność na rzecz praw człowieka (np. w organizacji nienastawionej na zysk, organizacji pozarządowej lub organizacji międzynarodowej); lub 4) otrzymać rekomendację od grup społeczeństwa obywatelskiego (art. 5 ust. 3 ustawy o NHRC). Ponadto po powołaniu komisarze nie mogą pełnić jednocześnie funkcji w Zgromadzeniu Narodowym, radach lokalnych ani w żadnych organach administracji państwowej lub samorządowej (jako urzędnicy publiczni), zob. art. 10 ustawy o NHRC.
([272]) Art. 5 ust. 1 i 2 ustawy o NHRC.
([273]) Art. 5 ust. 5 ustawy o NHRC.

kadencję i mogą zostać odwołani wyłącznie w przypadku skazania na karę pozbawienia wolności lub gdy nie są w stanie dłużej wykonywać swoich obowiązków z powodu długotrwałej niepełnosprawności intelektualnej lub fizycznej (w takim przypadku dwie trzecie komisarzy musi wyrazić zgodę na odwołanie) ([274]). W ramach prowadzonego dochodzenia NHRC może zażądać przedłożenia odpowiednich materiałów, przeprowadzić kontrolę i wezwać osoby fizyczne do złożenia zeznań ([275]) Jeśli chodzi o uprawnienia zaradcze, NHRC może wydawać (podawane do wiadomości publicznej) zalecenia dotyczące poprawy lub skorygowania określonych polityk i praktyk, na które organy publiczne muszą odpowiedzieć, proponując plan wdrożenia ([276]). Jeżeli odnośny organ nie wykona zaleceń, musi poinformować o tym komisję ([277]), która z kolei może ujawnić takie zaniechanie Zgromadzeniu Narodowemu lub podać je do wiadomości publicznej. Zgodnie z oficjalnym oświadczeniem rządu Korei (załącznik II pkt 2.3.5) władze koreańskie co do zasady stosują się do zaleceń NHRC i mają ku temu silną motywację, ponieważ wdrożenie zaleceń jest przedmiotem oceny w ramach ogólnej, ciągłej oceny przeprowadzanej pod nadzorem kancelarii premiera. Z rocznych danych dotyczących działalności NHRC wynika, że komisja aktywnie nadzoruje działalność organów ścigania albo na podstawie wniosków indywidualnych, albo w ramach dochodzeń z urzędu ([278]).

(173) Po czwarte, ogólny nadzór nad zgodnością z prawem działań organy publiczne sprawuje BAI, która bada dochody i wydatki państwa, ale także sprawuje ogólny nadzór nad wypełnianiem obowiązków przez organy publiczne w celu poprawy funkcjonowania administracji publicznej ([279]). BAI jest formalnie ustanowiona przy prezydencie Republiki Korei, ale zachowuje niezależny status w odniesieniu do swoich obowiązków ([280]). Ponadto przyznano jej pełną niezależność w zakresie powoływania, odwoływania i organizacji własnych pracowników oraz opracowywania budżetu ([281]). W skład BAI wchodzi przewodniczący (powoływany przez prezydenta za zgodą Zgromadzenia Narodowego) ([282]) i sześciu komisarzy (powoływanych przez prezydenta na podstawie rekomendacji przewodniczącego) ([283]), którzy muszą dysponować określonymi kwalifikacjami wymienionymi w ustawie ([284]) i mogą zostać odwołani wyłącznie w przypadku impeachmentu, skazania na karę pozbawienia wolności lub niezdolności do wykonywania obowiązków z powodu długotrwałej niepełnosprawności intelektualnej lub fizycznej ([285]). BAI przeprowadza corocznie audyt ogólny, ale może również przeprowadzać audyty specjalne w sprawach będących przedmiotem szczególnego zainteresowania. Podczas przeprowadzania audytu lub kontroli BAI może zażądać przedłożenia dokumentów i wezwać osoby fizyczne do stawiennictwa ([286]). BAI może wydawać zalecenia, wnosić o zastosowanie środków dyscyplinarnych lub złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa ([287]).

(174) Ponadto Zgromadzenie Narodowe sprawuje parlamentarny nadzór nad organami publicznymi, prowadząc dochodzenia i kontrole ([288]) ich działalności ([289]). Zgromadzenie może zażądać ujawnienia dokumentów, wezwać świadków do stawiennictwa ([290]), zalecić działania naprawcze (jeśli stwierdzi, że miały miejsce bezprawne lub

([274]) Art. 7 ust. 1 i art. 8 ustawy o NHRC.
([275]) Art. 36 ustawy o NHRC. Zgodnie z art. 6 ust. 7 ustawy można odmówić przedłożenia materiałów lub przedmiotów, jeżeli naruszałoby to tajemnicę państwową, co mogłoby mieć istotny wpływ na bezpieczeństwo państwa lub stosunki dyplomatyczne albo stanowiłoby poważną przeszkodę w prowadzeniu postępowania przygotowawczego lub sądowego. W takich przypadkach Komisja może w razie konieczności zażądać od szefa właściwej agencji (który musi działać w dobrej wierze) dalszych informacji, aby umożliwić sprawdzenie, czy odmowa udzielenia informacji jest uzasadniona.
([276]) Art. 25 ust. 1 i 3 ustawy o NHRC.
([277]) Art. 25 ust. 4 ustawy o NHRC.
([278]) Na przykład w latach 2015–2019 NHRC otrzymywała rocznie od 1 380 do 1 699 skarg przeciwko organom ścigania i rozpatrywała corocznie równie wysoką liczbę skarg (np. rozpatrzyła 1 546 skarg na policję w 2018 r. i 1 249 w 2019 r.); przeprowadziła również kilka dochodzeń z urzędu, co opisano bardziej szczegółowo sprawozdaniu rocznym NHRC za 2018 r. (dostępnym pod adresem https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) i sprawozdaniu rocznym za 2019 r. (dostępnym pod adresem https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Art. 20 i 24 ustawy o Komisji Kontroli i Audytu (ustawa o BAI). Zob. załącznik II pkt 2.3.2.
([280]) Art. 2 ust. 1 ustawy o BAI.
([281]) Art. 2 ust. 2 ustawy o BAI.
([282]) Art. 4 ust. 1 ustawy o BAI.
([283]) Art. 5 ust. 1 i 6 ustawy o BAI.
([284]) Na przykład co najmniej dziesięcioletni staż pracy w charakterze sędziego, prokuratora lub radcy prawnego, co najmniej ośmioletni staż pracy w charakterze funkcjonariusza państwowego, profesora lub pracownika na wyższym stanowisku na uniwersytecie, co najmniej dziesięcioletni staż pracy w spółce notowanej na giełdzie lub instytucji z udziałem skarbu państwa (w tym co najmniej pięcioletni staż pracy na stanowisku kierowniczym), zob. art. 7 ustawy o BAI. Ponadto komisarze mają zakaz uczestniczenia w działalności politycznej oraz jednoczesnego pełnienia funkcji w Zgromadzeniu Narodowym, agencjach administracyjnych, organizacjach podlegających audytowi i kontroli BAI lub pełnienia innych urzędów lub zajmowania innych stanowisk, za które otrzymują wynagrodzenie (art. 9 ustawy o BAI).
([285]) Art. 8 ustawy o BAI.
([286]) Zob. np. art. 27 ustawy o BAI.
([287]) Art. 24 oraz 31–35 ustawy o BAI.
([288]) Art. 128 ustawy o Zgromadzeniu Narodowym oraz art. 2, 3 i 15 ustawy o kontroli i nadzorowaniu administracji państwowej. Obejmuje to coroczne kontrole działalności rządu ogółem, ale również dochodzenia w konkretnych sprawach.
([289]) Zob. załącznik pkt 2.2.3.
([290]) Art. 10 ust. 1 ustawy o kontroli i nadzorowaniu administracji państwowej. Zob. także art. 128 i 129 ustawy o Zgromadzeniu Narodowym.

niewłaściwe działania) ([291]) oraz podać wyniki swoich ustaleń do publicznej wiadomości ([292]). Jeżeli Zgromadzenie Narodowe zaleci działania naprawcze, które mogą na przykład obejmować przyznanie odszkodowania, zastosowanie środków dyscyplinarnych lub poprawę procedur wewnętrznych, odnośny organ publiczny jest zobowiązany do niezwłocznego podjęcia działań i złożenia sprawozdania z ich wyniku Zgromadzeniu Narodowemu ([293]).

3.2.4 *Dochodzenie roszczeń*

(175) W ramach systemu koreańskiego możliwe są różne (sądowe) drogi dochodzenia roszczeń, w tym uzyskania odszkodowania.

(176) Po pierwsze, PIPA zapewnia osobom fizycznym prawo dostępu oraz prawo do poprawiania, usuwania i żądania zawieszenia przetwarzania w odniesieniu do danych osobowych przetwarzanych do celów ścigania przestępstw ([294]).

(177) Po drugie, osoby fizyczne mogą skorzystać z poszczególnych mechanizmów dochodzenia roszczeń określonych w PIPA, jeżeli ich dane zostały przetworzone przez organ ścigania z naruszeniem przepisów tej ustawy lub z naruszeniem ograniczeń i zabezpieczeń regulujących zbieranie danych osobowych przewidzianych w innych ustawach (tj. CPA lub CPPA, zob. motyw (171)). W szczególności osoby fizyczne mogą wnieść skargę do PIPC (m.in. za pośrednictwem centrum telefonicznego ds. prywatności prowadzonego przez Koreańską Agencję ds. Internetu i Bezpieczeństwa ([295])) lub do Komisji ds. Mediacji w Sporach Dotyczących Danych Osobowych ([296]). Te możliwości dochodzenia roszczeń nie podlegają dalszym wymogom w zakresie dopuszczalności. Ponadto na podstawie ustawy o postępowaniu administracyjnym osoby fizyczne mogą odwołać się od decyzji PIPC lub wnieść skargę na bezczynność tego organu (zob. motyw (132)).

(178) Po trzecie, każda osoba fizyczna ([297]) może wnieść do NHRC skargę dotyczącą naruszenia prawa do prywatności i ochrony danych przez koreański organ ścigania. NHRC może zalecić poprawienie lub ulepszenie wszelkich stosownych ustaw, instytucji, polityk lub praktyk ([298]) lub wdrożenie środków zaradczych, takich jak mediacja ([299]), zaprzestanie naruszania praw człowieka, odszkodowanie i środki zapobiegające ponownemu wystąpieniu takich samych lub podobnych naruszeń ([300]). Zgodnie z oficjalnym oświadczeniem rządu Korei (załącznik II pkt 2.4.2) może to również obejmować usunięcie danych osobowych zebranych niezgodnie z prawem. Mimo iż NHRC nie ma uprawnień do wydawania wiążących decyzji, proponuje ona bardziej nieformalną, niskokosztową i łatwo dostępną drogę dochodzenia roszczeń, w szczególności dlatego, że – jak wyjaśniono w załączniku II pkt 2.4.2 – nie wymaga wykazania faktycznej szkody, aby skarga mogła zostać rozpatrzona ([301]). Pozwala to zagwarantować, że skargi osób fizycznych dotyczące zbierania ich danych będą rozpatrywane, nawet wtedy, gdy dana osoba fizyczna nie jest w stanie wykazać, że jej dane faktycznie zbierano (np. ze względu na to, że jeszcze jej o tym nie zawiadomiono). Roczne sprawozdania z działalności NHRC pokazują, że osoby fizyczne również korzystają z tej drogi w praktyce, aby zaskarżyć działania organów ścigania, w tym w odniesieniu do przetwarzania danych osobowych ([302]). Jeżeli osoba fizyczna nie jest zadowolona z wyniku postępowania przed

([291]) Art. 16 ust. 2 ustawy o kontroli i nadzorowaniu administracji państwowej.
([292]) Art. 12-2 ustawy o kontroli i nadzorowaniu administracji państwowej.
([293]) Art. 16 ust. 3 ustawy o kontroli i nadzorowaniu administracji państwowej.
([294]) Prawo to może być wykonywane bezpośrednio wobec właściwego organu lub pośrednio przez PIPC (art. 35 ust. 2 PIPA). Jak opisano szczegółowo w motywach (76)–(78), wyjątki od tych praw będą miały zastosowanie wyłącznie wówczas, gdy będzie to konieczne do ochrony ważnego (publicznego) interesu.
([295]) Art. 62 PIPA.
([296]) Art. 40–50 PIPA i od art. 48-2 do 57 dekretu wykonawczego do PIPA. Zob. także załącznik II pkt 2.4.1.
([297]) Jak wyjaśniono w załączniku II pkt 2.4.2, chociaż art. 4 ustawy o NHRC odnosi się do obywateli i cudzoziemców zamieszkałych na terytorium Republiki Korei, termin „zamieszkały" odzwierciedla raczej pojęcie jurysdykcji niż terytorium. Dlatego też, jeśli podstawowe prawa osoby fizycznej spoza Korei są naruszane przez instytucje krajowe w Korei, osoba ta może wnieść skargę do NHRC. Będzie to miało miejsce w przypadku, gdy dane osobowe cudzoziemca przekazane do Korei są bezprawnie udostępniane koreańskim organom publicznym. Zob. w szczególności wyjaśnienia przedstawione na stronie https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2
([298]) Art. 44 ustawy o NHRC.
([299]) Osoba fizyczna może również wnieść o rozwiązanie skargi w drodze mediacji, zob. art. 42 i nast. ustawy o NHRC.
([300]) Art. 42 ust. 4 ustawy o NHRC. Ponadto NHCR może pilnie przyjąć środki naprawcze w przypadku trwającego naruszenia, które może spowodować szkodę trudną do naprawienia, jeżeli żadne środki nie zostaną wprowadzone, zob. art. 48 ustawy o NHRC.
([301]) Skarga musi co do zasady zostać złożona w ciągu jednego roku od naruszenia, ale NHRC może wciąż podjąć decyzję o rozpatrzeniu skargi złożonej po tym okresie, o ile nie upłynął termin przedawnienia wynikający z przepisów prawa karnego lub cywilnego (art. 32 ust. 1 pkt 4 ustawy o NHRC).
([302]) NHRC rozpatrywała na przykład w przeszłości skargi i wydawała zalecenia w odniesieniu do bezprawnych zajęć i naruszeń wymogu informowania osób fizycznych o zajęciu (zob. s. 80 i 91 sprawozdania rocznego NHRC z 2018 r. dostępnego pod adresem https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), jak również bezprawnego przetwarzania danych osobowych przez policję, prokuraturę i sądy (zob. s. 157–158 sprawozdania rocznego NHRC z 2019 r. dostępnego pod adresem. https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, oraz s. 76 sprawozdania rocznego z 2019 r. dostępnego na stronie https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

NHRC, może zaskarżyć wydane przez tę komisję decyzje (takie jak decyzja o niekontynuowaniu rozpatrywania skargi ([303])) i zalecenia przed sądami koreańskimi na mocy ustawy o postępowaniu administracyjnym (zob. motyw (181)) ([304]). Ponadto procedura przed NHRC może dodatkowo ułatwić dostęp do sądów, ponieważ osoba fizyczna mogłaby dochodzić dalszych roszczeń wobec organu publicznego, który według ustaleń NHRC bezprawnie przetwarzał jej dane, zgodnie z procedurami opisanymi w motywach (181)–(183).

(179) Dodatkowo dostępne są różne środki ochrony prawnej przed sądem, umożliwiające osobom fizycznym powołanie się na ograniczenia i zabezpieczenia opisane w pkt 3.2.1 w celu dochodzenia roszczeń ([305]).

(180) W odniesieniu do zajęć (w tym danych) CPA przewiduje możliwość wniesienia sprzeciwu wobec wykonania nakazu lub zakwestionowania jego wykonania w drodze złożenia wniosku o unieważnienie lub zmianę decyzji prokuratora lub policjanta do sądu właściwego (tzw. „quasi-skarga") ([306]).

(181) Ogólnie rzecz biorąc, osoby fizyczne mogą zaskarżać działania ([307]) lub zaniechania ([308]) organów publicznych (w tym organów ścigania) zgodnie z ustawą o postępowaniu administracyjnym ([309]). Działanie administracyjne uznaje się za „decyzję zaskarżalną", jeżeli ma ono bezpośredni wpływ na prawa i obowiązki obywatelskie ([310]), co – jak potwierdził rząd Korei (załącznik II pkt 2.4.3) – ma miejsce w przypadku środków służących zbieraniu danych osobowych, czy to bezpośrednio (np. w drodze przechwytywania komunikacji), czy za pośrednictwem wiążących żądań ujawnienia (np. wobec dostawcy usług) lub wniosków o dobrowolną współpracę. Aby skarga na podstawie ustawy o postępowaniu administracyjnym była dopuszczalna, osoba fizyczna musi mieć interes prawny w dochodzeniu roszczenia ([311]). Zgodnie z orzecznictwem Sądu Najwyższego „interes prawny" jest rozumiany jako „interes prawnie chroniony", tj. bezpośredni i konkretny interes chroniony przepisami ustawowymi i wykonawczymi, na których opierają się decyzje administracyjne (niebędący ogólnym pośrednim i abstrakcyjnym interesem społeczeństwa) ([312]). Osoby fizyczne mają taki interes prawny w przypadku naruszenia ograniczeń i zabezpieczeń, które mają zastosowanie do zbierania ich danych osobowych do celów ścigania przestępstw (na mocy ustaw szczególnych lub PIPA). Na podstawie ustawy o postępowaniu administracyjnym sąd może postanowić o uchyleniu lub zmianie niezgodnej z prawem decyzji, o stwierdzeniu nieważności (tj. stwierdzeniu, że decyzja nie wywołuje skutków prawnych lub nie istnieje w porządku prawnym) lub o stwierdzeniu, że zaniechanie jest niezgodne z prawem ([313]). Wyrok kończący postępowanie w sprawie wydany na podstawie ustawy o postępowaniu administracyjnym jest wiążący dla stron ([314]).

([303]) Jeżeli na przykład NHRC wyjątkowo nie jest w stanie przeprowadzić kontroli określonych materiałów lub obiektów, ponieważ są one związane z tajemnicami państwowymi, które mogą mieć istotny wpływ na bezpieczeństwo państwa lub stosunki dyplomatyczne, lub jeżeli kontrola stanowiłaby poważną przeszkodę dla postępowania przygotowawczego lub toczącego się procesu i jeżeli uniemożliwia to Komisji przeprowadzenie dochodzenia niezbędnego do oceny zasadności otrzymanego wniosku, Komisja informuje daną osobę fizyczną o przyczynach odrzucenia skargi, zgodnie z art. 39 ustawy o NHRC. W takim przypadku osoba ta może odwołać się od decyzji NHRC na podstawie ustawy o postępowaniu administracyjnosądowym.

([304]) Zob. np. orzeczenie Sądu Apelacyjnego w Seulu nr 2007Nu27259 z dnia 18 kwietnia 2008 r., potwierdzone orzeczeniem Sądu Najwyższego nr 2008Du7854 z dnia 9 października 2008 r.; orzeczenie Sądu Apelacyjnego w Seulu nr 2017Nu69382 z 2 lutego 2018 r.

([305]) Zob. załącznik II pkt 2.4.3.

([306]) art. 417 CPA w związku z art. 414 ust. 2 CPA. Zob. również orzeczenie Sądu Najwyższego nr 97Mo66 z dnia 29 września 1997 r.

([307]) Ustawa o postępowaniu administracyjnym odnosi się do „decyzji", tj. sprawowania lub odmowy sprawowania władzy publicznej w konkretnym przypadku.

([308]) Zgodnie z ustawą o postępowaniu administracyjnym odnosi się to do długotrwałego niepodejmowania przez organ administracji określonej decyzji wbrew obowiązkowi prawnemu.

([309]) Odwołanie od decyzji administracyjnej można najpierw wnieść do administracyjnych komisji odwoławczych ustanowionych przy niektórych organach publicznych (np. NIS, NHRC) lub do Centralnej Administracyjnej Komisji Odwoławczej ustanowionej przy Komisji Antykorupcyjnej i Praw Obywatelskich (art. 6 ustawy o odwołaniach administracyjnych i art. 18 ust. 1 ustawy o postępowaniu administracyjnym), co stanowi bardziej nieformalną drogę dochodzenia roszczeń. Można jednak również wnieść pozew bezpośrednio do sądów koreańskich na podstawie ustawy o postępowaniu administracyjnym.

([310]) Orzeczenie Sądu Najwyższego nr 98Du18435 z dnia 22 października 1999 r., orzeczenie Sądu Najwyższego nr 99Du1113 z dnia 8 września 2000 r. oraz orzeczenie Sądu Najwyższego nr 2010Du3541 z dnia 27 września 2012 r.

([311]) Art. 12, 35 i 36 ustawy o postępowaniu administracyjnym. Ponadto wniosek o uchylenie/zmianę decyzji oraz wniosek o stwierdzenie niezgodności z prawem zaniechania należy złożyć w terminie 90 dni od dnia, w którym osoba fizyczna dowiedziała się o decyzji/zaniechaniu, i co do zasady nie później niż w ciągu roku od dnia wydania decyzji lub wystąpienia zaniechania, chyba że istnieją uzasadnione przyczyny zwłoki (art. 20 i 38 ust. 2 ustawy o postępowaniu administracyjnosądowym). Pojęcie „uzasadnionych przyczyn" zostało zinterpretowane szeroko przez Sąd Najwyższy i wymaga oceny, czy w świetle wszystkich okoliczności sprawy wniesienie skargi po terminie jest dopuszczalne społecznie (orzeczenie Sądu Najwyższego nr 90Nu6521 z dnia 28 czerwca 1991 r.). Jak potwierdził rząd Korei w załączniku II pkt 2.4.3, obejmuje to (między innymi) przyczyny opóźnień, za które dana strona nie może być odpowiedzialna (tj. sytuacje, które są poza kontrolą skarżącego, na przykład gdy nie został on powiadomiony o zbieraniu jego danych osobowych) lub siłę wyższą (np. klęski żywiołowe, wojny).

([312]) Orzeczenie Sądu Najwyższego nr 2006Du330 z dnia 26 marca 2006 r.

([313]) Art. 2 i 4 ustawy o postępowaniu administracyjnym.

([314]) Art. 30 ust. 1 ustawy o postępowaniu administracyjnym.

(182) Oprócz zaskarżania działań rządu w drodze postępowania administracyjnego osoby fizyczne mogą również wnieść skargę konstytucyjną do Trybunału Konstytucyjnego w związku z naruszeniem ich praw podstawowych wskutek działania lub zaniechania administracji rządowej (z wyłączeniem wyroków sądowych) ([315]). Jeśli dostępne są inne środki ochrony prawnej, należy je wyczerpać w pierwszej kolejności. Zgodnie z orzecznictwem Trybunału Konstytucyjnego cudzoziemcy mogą wnieść skargę konstytucyjną w zakresie, w jakim ich prawa podstawowe są uznawane na mocy konstytucji koreańskiej (zob. wyjaśnienia w pkt 1.1) ([316]). Trybunał Konstytucyjny może uchylić akt organu administracji rządowej, który spowodował naruszenie, lub potwierdzić, że określone zaniechanie jest niezgodne z konstytucją ([317]). W takim przypadku właściwy organ jest zobowiązany do wdrożenia środków w celu zastosowania się do orzeczenia Trybunału.

(183) Ponadto osoby fizyczne mogą uzyskać odszkodowanie przed sądami koreańskimi. Obejmuje to przede wszystkim możliwość dochodzenia odszkodowania za naruszenia PIPA popełnione przez organy ścigania, zgodnie z art. 39 (zob. również motyw (135)). Ogólnie rzecz biorąc, osoby fizyczne mogą ubiegać się o odszkodowanie za szkody wyrządzone przez urzędników publicznych podczas wykonywania obowiązków służbowych z naruszeniem prawa, na podstawie ustawy o odszkodowaniach od państwa (zob. również motyw (135)) ([318]).

(184) Mechanizmy opisane w motywach (176)–(183) zapewniają osobom, których dane dotyczą, skuteczne środki administracyjne i środki ochrony prawnej przed sądem umożliwiające im w szczególności egzekwowanie ich praw, w tym prawa do dostępu do swoich danych osobowych lub do uzyskania korekty lub usunięcia takich danych.

3.3 **Dostęp koreańskich organów publicznych do danych do celów bezpieczeństwa narodowego i wykorzystywanie przez nie tych danych w celach związanych z bezpieczeństwem narodowym**

(185) W prawie Republiki Korei ustanowiono szereg ograniczeń i zabezpieczeń w zakresie dostępu do danych osobowych i korzystania z nich do celów bezpieczeństwa narodowego, a także mechanizmy nadzoru i dochodzenia roszczeń, które są zgodne z wymogami określonymi w motywach (141)–(143) niniejszej decyzji. Warunki uzyskania takiego dostępu oraz zabezpieczenia mające zastosowanie do wykonywania tych uprawnień poddano szczegółowej ocenie w kolejnych sekcjach.

3.3.1 *Podstawy prawne, ograniczenia i zabezpieczenia*

(186) W Republice Korei dostęp do danych osobowych do celów bezpieczeństwa narodowego jest możliwy na podstawie CPPA, TBA i ustawy o zwalczaniu terroryzmu do celów ochrony obywateli i bezpieczeństwa publicznego (ustawa o zwalczaniu terroryzmu) ([319]). Głównym organem ([320]), do którego należą kompetencje w dziedzinie bezpieczeństwa narodowego, jest Narodowa Służba Wywiadu (ang. National Intelligence Service, NIS) ([321]). Zbieranie i wykorzystywanie danych osobowych przez NIS musi odbywać się w sposób zgodny z odpowiednimi

([315]) Art. 68 ust. 1 ustawy o Trybunale Konstytucyjnym. Skargę konstytucyjną należy wnieść w terminie 90 dni od chwili, w której dana osoba dowiedziała się o naruszeniu, oraz w terminie jednego roku od jego wystąpienia. Jak wyjaśniono również w załączniku II pkt 2.4.3, biorąc pod uwagę, że procedura przewidziana w ustawie o postępowaniu administracyjnosądowym jest stosowana do postępowania sądowego na mocy ustawy o Trybunale Konstytucyjnym zgodnie z art. 40 ustawy o Trybunale Konstytucyjnym, skarga będzie nadal dopuszczalna, jeśli występują „uzasadnione przyczyny" zgodnie z wykładnią dokonaną w orzecznictwie Sądu Najwyższego, o którym mowa w przypisie 312. Jeżeli w pierwszej kolejności konieczne jest wyczerpanie innych środków ochrony prawnej, skargę konstytucyjną należy wnieść w terminie 30 dni od zapadnięcia prawomocnego orzeczenia w sprawie takiego środka (art. 69 ustawy o Trybunale Konstytucyjnym).

([316]) Orzeczenie Trybunału Konstytucyjnego nr 99HeonMa194 z dnia 29 listopada 2001 r.

([317]) Art. 75 ust. 3 ustawy o Trybunale Konstytucyjnym.

([318]) Art. 2 ust. 1 ustawy o odszkodowaniach od państwa.

([319]) Zob. załącznik II pkt 3.1.

([320]) W drodze wyjątku, również policja i prokuratura mogą zbierać dane osobowe do celów bezpieczeństwa narodowego (zob. przypis 327 i załącznik II pkt 3.2.1.2). Ponadto koreańska agencja wywiadu wojskowego (Dowództwo Wsparcia Bezpieczeństwa Wojskowego, które podlega Ministerstwu Obrony) posiada uprawnienia w dziedzinie bezpieczeństwa narodowego. Jak wyjaśniono w załączniku II pkt 3.1, odpowiada ona jedynie za wywiad wojskowy i prowadzi nadzór nad ludnością cywilną, w przypadku gdy jest to konieczne do wykonywania jej zadań wojskowych. W szczególności może prowadzić dochodzenia dotyczące personelu wojskowego, cywilnych pracowników wojska, osób odbywających szkolenie wojskowe, osób odbywających służbę wojskową w rezerwie lub poborowych oraz jeńców wojennych (art. 1 ustawy o sądach wojskowych). Zbierając informacje dotyczące komunikacji do celów bezpieczeństwa narodowego, Dowództwo Wsparcia Bezpieczeństwa Wojskowego podlega ograniczeniom i zabezpieczeniom określonym w CPPA i dekrecie wykonawczym do CPPA.

([321]) Zadaniem NIS jest zbieranie, kompilowanie i rozpowszechnianie informacji o państwach obcych (tj. ogólnych informacji o tendencjach i rozwoju sytuacji w odniesieniu do państw obcych lub o działalności podmiotów państwowych); danych wywiadowczych związanych z przeciwdziałaniem szpiegostwu (w tym szpiegostwu wojskowemu i przemysłowemu), terroryzmowi i działalności międzynarodowych grup przestępczych; danych wywiadowczych dotyczących niektórych rodzajów przestępstw przeciwko bezpieczeństwu publicznemu i narodowemu (np. rewolucja wewnątrz kraju, podżeganie do agresji zewnętrznej) oraz danych wywiadowczych związanych z zadaniem polegającym na zapewnieniu cyberbezpieczeństwa oraz zapobieganiu lub przeciwdziałaniu cyberatakom i cyberzagrożeniom (art. 4 ust. 2 ustawy o NIS). Zob. także załącznik II pkt 3.1.

wymogami prawnymi (w tym PIPA i CPPA) ([322]) oraz ogólnymi wytycznymi sporządzonymi przez prezydenta i poddanymi przeglądowi przez Zgromadzenie Narodowe ([323]). Co do zasady NIS musi zachować neutralność polityczną oraz chronić wolność i prawa osób fizycznych ([324]). Ponadto personel NIS nie może nadużywać swojej władzy publicznej w celu zmuszenia jakiejkolwiek instytucji, organizacji lub osoby fizycznej do czynności, których ta nie ma obowiązku wykonać (na podstawie ustawy), ani nie może utrudniać jakiejkolwiek osobie wykonywania przysługujących jej praw ([325]).

3.3.1.1 Dostęp do informacji dotyczących komunikacji

(187) Na podstawie CPPA organy publiczne Korei ([326]) mogą zbierać dane potwierdzające komunikację (tj. datę połączenia telekomunikacyjnego, czas jego rozpoczęcia i zakończenia, liczbę połączeń wychodzących i przychodzących, jak również numer abonenta drugiego rozmówcy, częstotliwość połączeń, pliki dziennika dotyczące korzystania z usług telekomunikacyjnych oraz informacje dotyczące lokalizacji, zob. motyw (155)) oraz treść komunikacji (za pomocą środków ograniczających komunikację, zob. motyw (155)) lub do celów bezpieczeństwa narodowego (zgodnie z mandatem NIS, zob. przypis 322). Uprawnienia te obejmują dwa rodzaje informacji: 1) komunikacji, w której jedna strona lub obie strony są obywatelami Korei ([327]); oraz 2) komunikacji a) państw wrogich Republice Korei, b) zagranicznych agencji, grup lub obywateli podejrzanych o prowadzenie działalności antykoreańskiej ([328]) lub c) członków grup działających na Półwyspie Koreańskim, ale w praktyce pozostających poza jurysdykcją Republiki Korei, oraz ich grup parasolowych mających siedzibę w innych państwach ([329]) W związku z tym dane dotyczące komunikacji osób fizycznych z UE przekazywanej z Unii do Republiki Korei na podstawie niniejszej decyzji można zbierać na podstawie CPPA do celów bezpieczeństwa narodowego (z zastrzeżeniem warunków określonych w motywach (188)–(192)), jeżeli uczestniczy w niej osoba fizyczna z UE i obywatel Korei albo jeżeli odbywa się ona wyłącznie między osobami niebędącymi obywatelami Korei i należy do jednej z trzech wspomnianych kategorii – pkt 2 lit. a), b) i c).

(188) W przypadku obu scenariuszy zbieranie danych potwierdzających komunikację może odbywać się wyłącznie w celu przeciwdziałania zagrożeniom dla bezpieczeństwa narodowego ([330]), natomiast środki ograniczające komunikację można wprowadzić wyłącznie w przypadku poważnego zagrożenia dla bezpieczeństwa narodowego, gdy zbieranie danych jest konieczne, aby zapobiec temu zagrożeniu ([331]). Ponadto dostęp do treści komunikacji można uzyskać wyłącznie jako środek ostateczny i należy podjąć starania, aby zminimalizować naruszenie prywatności komunikacji ([332]), zapewniając tym samym jego proporcjonalność do celu związanego z bezpieczeństwem narodowym. Zbieranie zarówno treści komunikacji, jak i danych potwierdzających komunikację może trwać maksymalnie cztery miesiące, przy czym należy go natychmiast zaprzestać, jeżeli zamierzony cel zostanie osiągnięty wcześniej ([333]). Jeżeli odnośne warunki będą nadal spełnione, okres ten można przedłużyć, za uprzednim zezwoleniem sądu (w odniesieniu do środków opisanych w motywie (189)) lub prezydenta (w odniesieniu do środków opisanych w motywie (190)) ([334]), o maksymalnie cztery miesiące.

(189) Te same zabezpieczenia proceduralne dotyczą zbierania danych potwierdzających komunikację oraz treści komunikacji ([335]). W szczególności jeżeli przynajmniej jedna z osób uczestniczących w komunikacji jest obywatelem Korei, agencja wywiadowcza musi złożyć pisemny wniosek do prokuratury apelacyjnej, która z kolei musi

([322]) Zob. także art. 14, 22 i 23 ustawy o NIS.
([323]) Art. 4 ust. 2 ustawy o NIS.
([324]) Art. 3 ust. 1, art. 6 ust. 2, art. 11 i art. 21 ustawy o NIS. Zob. także przepisy dotyczące konfliktu interesów, w szczególności art. 10 i 12 ustawy o NIS.
([325]) Art. 13 ustawy NIS.
([326]) Obejmuje to agencje wywiadowcze (tj. Narodową Służbę Wywiadu i Dowództwo Wsparcia Bezpieczeństwa Wojskowego) oraz policję/prokuraturę.
([327]) Art. 7 ust. 1 pkt 1 CPPA.
([328]) Jak wyjaśnił rząd Korei w przypisie 244 w załączniku II, dotyczy to działań, które zagrażają istnieniu i bezpieczeństwu narodu, ładowi demokratycznemu lub przetrwaniu i wolności ludności.
([329]) Art. 7 ust. 1 pkt 2 CPPA.
([330]) Art. 13-4 CPPA.
([331]) Art. 7 ust. 1 CPPA.
([332]) Art. 3 ust. 2 CPPA. Ponadto należy natychmiast zaprzestać stosowania środków ograniczających komunikację, jeżeli przestaną być potrzebne, zapewniając w ten sposób ograniczenie do minimum wszelkich naruszeń poufności komunikacji danej osoby (art. 2 dekretu wykonawczego do CPPA).
([333]) Art. 7 ust. 2 CPPA.
([334]) Wniosek o uzyskanie zgody na przedłużenie stosowania środków nadzoru należy sporządzić na piśmie, podając uzasadnienie wniosku o przedłużenie i załączając materiały potwierdzające (art. 7 ust. 2 i art. 5 dekretu wykonawczego do CPPA).
([335]) Zob. art. 13-4 ust. 2 CPPA i art. 37 ust. 4 dekretu wykonawczego do CPPA, zgodnie z którymi procedury mające zastosowanie do zbierania treści komunikacji mają również zastosowanie do zbierania danych potwierdzających komunikację. Zob. także załącznik II pkt 3.2.1.1.1.

wystąpić z wnioskiem o wydanie nakazu do Prezesa Sądu Apelacyjnego ([336]). W CPPA wymieniono informacje, które należy zawrzeć we wniosku do prokuratury, we wniosku o wydanie nakazu oraz w samym nakazie, które obejmują w szczególności uzasadnienie wniosku i główne podstawy podejrzeń, materiały potwierdzające, jak również informacje dotyczące celu, przedmiotu (tj. osoby lub osób fizycznych, których dotyczy środek), zakresu i okresu obowiązywania proponowanego środka ([337]). Zbieranie danych bez nakazu może odbywać się wyłącznie w przypadku zmowy zagrażającej bezpieczeństwu narodowemu oraz w sytuacji nadzwyczajnej, która uniemożliwia zastosowanie wspomnianych procedur ([338]). Również w takim przypadku wniosek o wydanie nakazu należy złożyć niezwłocznie po zastosowaniu środka ([339]). W związku z tym w CPPA wyraźnie określono zakres i warunki wspomnianego rodzaju zbierania danych oraz objęto je szczególnymi zabezpieczeniami (proceduralnymi) (w tym uprzedniemu zatwierdzeniu przez sąd), co zapewnia ograniczenie stosowania takich środków do tego, co jest konieczne i proporcjonalne. Ponadto wymóg podania szczegółowych informacji zarówno we wniosku o wydanie nakazu, jak i w samym nakazie wyklucza nieograniczony dostęp.

(190) W przypadku komunikacji z osobami niebędącymi obywatelami Korei, które należą do jednej z trzech szczególnych kategorii wymienionych w motywie (187), należy złożyć wniosek do dyrektora NIS, który – po zbadaniu odpowiedniości proponowanych środków – musi wcześniej uzyskać pisemną zgodę prezydenta Republiki Korei ([340]). Wniosek sporządzony przez agencję wywiadowczą powinien zawierać takie same szczegółowe informacje jak informacje zawarte we wniosku o wydanie nakazu sądowego (zob. motyw (189)), w szczególności dotyczące uzasadnienia wniosku i głównych podstaw podejrzeń, materiałów potwierdzające oraz informacji na temat celów, osoby lub osób fizycznych, których dotyczą środki, zakresu i okresu obowiązywania proponowanych środków ([341]). W sytuacjach nadzwyczajnych ([342]) należy uzyskać uprzednią zgodę ministra, któremu podlega dana agencja wywiadowcza, przy czym agencja ta musi wystąpić o zgodę prezydenta niezwłocznie po zastosowaniu środków nadzwyczajnych ([343]). Również w odniesieniu do zbierania informacji dotyczących komunikacji między osobami niebędącymi obywatelami Korei w CPPA ograniczono stosowanie takich środków do tego, co konieczne i proporcjonalne, poprzez wyraźne określenie kategorii osób fizycznych, które mogą podlegać takim środkom, oraz poprzez ustanowienie szczegółowych kryteriów, których spełnienie agencje wywiadowcze muszą wykazać, aby uzasadnić wniosek o zbieranie informacji. Ponadto ponownie wyklucza to możliwość nieograniczonego dostępu. W przypadku braku uprzedniego niezależnego zatwierdzenia takich środków niezależny nadzór jest zapewniony *ex post* w szczególności przez PIPC i NHRC (zob. np. motywy (199)–(200)).

(191) Ponadto w CPPA ustanowiono szereg dodatkowych zabezpieczeń, które przyczyniają się do nadzoru *ex post* i ułatwiają osobom fizycznym dostęp do skutecznych środków prawnych. Po pierwsze, w odniesieniu do każdego rodzaju zbierania danych do celów bezpieczeństwa narodowego w CPPA przewidziano różne wymogi dotyczące prowadzenia rejestrów i sprawozdawczości. W szczególności wzywając operatorów prywatnych do współpracy, agencje wywiadowcze muszą przedstawić nakaz sądowy/zezwolenie prezydenta lub odpis oświadczenia o cenzurze w sytuacji nadzwyczajnej, którą podmiot wezwany do współpracy musi przechowywać w swoich rejestrach ([344]). W przypadku gdy podmioty prywatne są wzywane do współpracy, zarówno wzywający organ

([336]) Art. 6 ust. 5 i 8, art. 7 ust. 1 pkt 1 i art. 7 ust. 3 CPPA w związku z art. 7 ust. 3–4 dekretu wykonawczego do CPPA.

([337]) Zob. art. 7 ust. 3 i art. 6 ust. 4 CPPA (w przypadku wniosku złożonego przez agencję wywiadowczą), art. 4 dekretu wykonawczego do CPPA (w przypadku wniosku złożonego przez prokuratora) oraz art. 7 ust. 3 i art. 6 ust. 6 CPPA (w przypadku nakazu).

([338]) Art. 8 CPPA.

([339]) Art. 8 ust. 2 i 8 CPPA. Zbierania należy natychmiast zaprzestać, jeśli zezwolenie sądu nie zostanie uzyskane w ciągu 36 godzin od chwili podjęcia działań. W przypadku szybkiego zakończenia nadzoru, co wyklucza możliwość uzyskania zezwolenia sądu, właściwa prokuratura apelacyjna musi przesłać zawiadomienie o środkach nadzwyczajnych przygotowane przez agencję wywiadowczą do prezesa właściwego sądu, który na tej podstawie może zbadać zgodność zbierania danych z prawem (art. 8 ust. 5 i 7 CPPA). W powiadomieniu należy wskazać cel, przedmiot, zakres, okres, miejsce i sposób przeprowadzania nadzoru, jak również powód niezłożenia wniosku przed zastosowaniem środka (art. 8 ust. 6 CPPA). Zasadniczo agencje wywiadowcze mogą stosować środki nadzwyczajne wyłącznie zgodnie z „oświadczeniem o cenzurze/podsłuchu w sytuacji nadzwyczajnej" i muszą prowadzić rejestry takich środków (art. 8 ust. 4 CPPA).

([340]) Art. 8 ust. 1 i 2 dekretu wykonawczego do CPPA.

([341]) Art. 8 ust. 3 dekretu wykonawczego do CPPA w związku z art. 6 ust. 4 CPPA.

([342]) Tzn. w przypadkach, gdy środek jest skierowany przeciwko aktowi zmowy zagrażającej bezpieczeństwu narodowemu, nie ma wystarczająco dużo czasu na uzyskanie zgody prezydenta, a nieprzyjęcie środków nadzwyczajnych może naruszyć bezpieczeństwo narodowe (art. 8 ust. 8 CPPA).

([343]) Art. 8 ust. 9 CPPA. Zbierania należy natychmiast zaprzestać, jeżeli zezwolenie nie zostanie uzyskane w ciągu 36 godzin od chwili złożenia wniosku.

([344]) Art. 9 ust. 2 CPPA i art. 12 dekretu wykonawczego do CPPA. Zob. art. 13 dekretu wykonawczego do CPPA dotyczący możliwości wezwania placówek pocztowych i dostawców usług telekomunikacyjnych do współpracy. Operatorzy prywatni, których wezwano do ujawnienia informacji, mogą odmówić ich udostępnienia, jeżeli nakaz/upoważnienie lub oświadczenie o cenzurze w sytuacji nadzwyczajnej odnosi się do niewłaściwego identyfikatora (np. numeru telefonu należącego do innej osoby fizycznej niż osoba, która została zidentyfikowana). W żadnym wypadku nie wolno im ujawniać haseł używanych do celów korzystania z usług komunikacyjnych (art. 9 ust. 4 CPPA).

publiczny, jak i odpowiedni operator muszą prowadzić rejestry dotyczące celu i przedmiotu środków, jak również terminu ich wykonania ([345]). Ponadto agencje wywiadowcze muszą przedkładać dyrektorowi NIS sprawozdania na temat zebranych przez siebie informacji i wyników działań nadzorczych ([346]).

(192) Po drugie, osoby fizyczne należy powiadamiać o zbieraniu dotyczących ich danych (danych potwierdzających komunikację lub treści komunikacji) do celów bezpieczeństwa narodowego, jeżeli dotyczy to komunikacji, w której przynajmniej jedna ze stron jest obywatelem Korei ([347]). Powiadomienie to należy przekazać na piśmie w terminie 30 dni od daty zakończenia zbierania danych (uwzględniając sytuację, w której dane zostały uzyskane zgodnie z procedurą nadzwyczajną) i można je odroczyć na tak długo, jak długo stanowiłoby to zagrożenie dla bezpieczeństwa narodowego lub zagrażałoby życiu i bezpieczeństwu fizycznemu ludzi ([348]). Niezależnie od takiego powiadomienia osoby fizyczne mogą dochodzić roszczeń na różne sposoby, co wyjaśniono bardziej szczegółowo w pkt 3.3.4.

3.3.1.2 Zbieranie informacji na temat osób podejrzanych o terroryzm

(193) W ustawie o zwalczaniu terroryzmu przewidziano, że NIS może zbierać dane dotyczące osób podejrzanych o terroryzm ([349]) zgodnie z ograniczeniami i zabezpieczeniami określonymi w innych ustawach ([350]). W szczególności NIS może uzyskać dane dotyczące komunikacji (na podstawie CPPA) i pozostałe dane osobowe (w ramach wniosku o dobrowolne ujawnienie) ([351]). W odniesieniu do zbierania informacji ze środków komunikacji (tj. treści komunikacji lub danych potwierdzających komunikację) zastosowanie mają ograniczenia i zabezpieczenia opisane w pkt 3.3.1.1, w tym wymóg uzyskania nakazu zatwierdzonego przez sąd. Jeżeli chodzi o wnioski o dobrowolne ujawnienie innych rodzajów danych osobowych osób podejrzanych o terroryzm, NIS musi spełniać wymogi dotyczące konieczności i proporcjonalności określone w konstytucji i PIPA (zob. motyw (164)) ([352]). Administratorzy otrzymujący takie wnioski mogą dobrowolnie zastosować się do nich na warunkach określonych w PIPA (np. zgodnie z zasadą minimalizacji danych i poprzez ograniczenie wpływu na prywatność osoby fizycznej) ([353]). W tym przypadku muszą oni również spełnić wymóg powiadamiania danej osoby fizycznej wynikający z zawiadomienia nr 2021-5 (zob. motyw (166)).

([345]) W przypadku środków ograniczających komunikację takie rejestry należy przechowywać przez trzy lata, zob. art. 9 ust. 3 CPPA i art. 17 ust. 2 dekretu wykonawczego do CPPA. W odniesieniu do danych potwierdzających komunikację agencje wywiadowcze muszą przechowywać rejestry dotyczące faktu złożenia wniosku o takie dane, jak również samego pisemnego wniosku i instytucji, która działała na jego podstawie (art. 13 ust. 5 i art. 13-4 ust. 3 CPPA). Dostawcy usług telekomunikacyjnych muszą przechowywać rejestry przez siedem lat i dwa razy w roku przedkładać Ministrowi Nauki i Technologii Informacyjno-Komunikacyjnych sprawozdanie dotyczące częstotliwości ujawniania takich informacji (art. 9 ust. 3 CPPA w związku z art. 13 ust. 7 CPPA oraz art. 37 ust. 4 i 39 dekretu wykonawczego do CPPA).

([346]) Art. 18 ust. 3 dekretu wykonawczego do CPPA.

([347]) Art. 9-2 ust. 3 oraz art. 13-4 CPPA. Powiadomienie musi zawierać: 1) informację o zbieraniu danych, 2) nazwę agencji stosującej środki oraz 3) okres stosowania.

([348]) Art. 9-2 ust. 4 CPPA. W takim przypadku powiadomienie musi zostać dostarczone w terminie 30 dni od ustania przyczyn odroczenia, zob. art. 13-4 ust. 2 i art. 9-2 ust. 6 CPPA.

([349]) Tzn. członkowie grupy terrorystycznej (zgodnie z definicją ONZ, zob. art. 2 ust. 2 ustawy o zwalczaniu terroryzmu); osoby, które promują i rozpowszechniają idee lub praktyki grupy terrorystycznej, pozyskują lub przekazują środki na działalność terrorystyczną albo angażują się w inne działania polegające na przygotowywaniu aktów terrorystycznych, zmowie, propagandzie lub podżeganiu do terroryzmu; lub osoby, co do których istnieją uzasadnione podejrzenia, że prowadziły takie działania (art. 2 ust. 3 ustawy o zwalczaniu terroryzmu). „Terroryzm" zdefiniowano w art. 2 ust. 1 ustawy o zwalczaniu terroryzmu jako działanie prowadzone w celu utrudnienia wykonywania władzy przez państwo, organy samorządu terytorialnego lub rząd państwa obcego (w tym organizacje międzynarodowe) lub w celu zmuszenia ich do podjęcia działań, do których nie są zobowiązane, lub w celu stworzenia zagrożenia dla społeczeństwa. Takie działanie może na przykład obejmować zabójstwo, uprowadzenie lub branie zakładników; bezprawne zawładnięcie statkiem powietrznym, zniszczenie lub uszkodzenie statku lub statku powietrznego; użycie broni biochemicznej, wybuchowej lub zapalającej z zamiarem spowodowania śmierci, poważnego uszczerbku na zdrowiu lub znacznych szkód; oraz wykorzystanie materiałów jądrowych lub promieniotwórczych niezgodnie z przeznaczeniem.

([350]) Art. 9 ust. 1 i ust. 3 ustawy o zwalczaniu terroryzmu.

([351]) Chociaż ustawa o zwalczaniu terroryzmu odnosi się również do możliwości zbierania informacji na temat wjazdu do Republiki Korei i wyjazdu z niej na podstawie ustawy o imigracji i ustawy celnej, w ustawach tych nie przewidziano takiego uprawnienia (zob. załącznik II pkt 3.2.2.1). Co do zasady nie miałyby one zastosowania do danych przekazywanych na podstawie niniejszej decyzji, ponieważ zazwyczaj dotyczyłyby informacji, które byłyby zbierane bezpośrednio przez organy Korei (a nie dostępu do danych, które zostały wcześniej przekazane z Unii administratorom koreańskim). Ponadto w ustawie o zwalczaniu terroryzmu wymieniono ARUSFTI jako podstawę prawną do zbierania informacji na temat transakcji finansowych. Jak wyjaśniono w przypisie 200, rodzaje danych, które można uzyskać na podstawie wspomnianej ustawy, nie wchodzą jednak w zakres niniejszej decyzji. Ponadto w ustawie o zwalczaniu terroryzmu przewidziano również, że NIS może zbierać informacje o lokalizacji za pomocą niewiążących wniosków, a wtedy dostawcy informacji dotyczących lokalizacji mogliby dobrowolnie ujawnić takie informacje na warunkach określonych w PIPA (opisanych w motywie (193)) i ustawie o informacjach dotyczących lokalizacji. Jak wyjaśniono również w przypisie 17, informacje dotyczące lokalizacji nie byłyby przekazywane z Unii do koreańskich administratorów na podstawie niniejszej decyzji, lecz generowane w Korei.

([352]) Zob. załącznik II pkt 3.2.2.2.

([353]) Zob. art. 58 ust. 4 PIPA, w którym ustanowiono wymóg, że dane osobowe należy przetwarzać w minimalnym zakresie wymaganym do osiągnięcia zamierzonego celu, a także art. 3 ust. 6 PIPA, w którym nałożono wymóg przetwarzania danych osobowych w sposób minimalizujący możliwość naruszenia prywatności osoby fizycznej. Zob. również art. 59 pkt 2 i 3 PIPA, zgodnie z którym administratorom zakazuje się ujawniania danych osobowych stronom trzecim bez upoważnienia.

3.3.1.3 Wnioski o dobrowolne ujawnienie danych abonentów

(194) Na podstawie TBA dostawcy usług telekomunikacyjnych mogą dobrowolnie ujawniać dane abonentów (zob. motyw (163)) na wniosek agencji wywiadowczej, która zamierza zbierać takie informacje, aby zapobiec zagrożeniu dla bezpieczeństwa narodowego ([354]). W odniesieniu do takich wniosków ze strony NIS obowiązują takie same ograniczenia (wynikające z konstytucji, PIPA i TBA) jak w dziedzinie ścigania przestępstw, jak określono w motywie (164) ([355]). Dostawcy usług telekomunikacyjnych nie są zobowiązani do przestrzegania tego i mogą to czynić wyłącznie na warunkach określonych w PIPA (w szczególności zgodnie z zasadą minimalizacji danych oraz ograniczając wpływ na prywatność osoby fizycznej, zob. także motyw (193)). W odniesieniu do prowadzenia rejestru i powiadamiania danej osoby fizycznej zastosowanie mają takie same wymogi jak w dziedzinie ścigania przestępstw (zob. motywy (165) i (166)).

3.3.2 *Dalsze wykorzystywanie zebranych informacji*

(195) Przetwarzanie danych osobowych zbieranych przez organy koreańskie do celów bezpieczeństwa narodowego podlega zasadom ograniczenia celu (art. 3 ust. 1–2 PIPA), zgodności z prawem i rzetelności przetwarzania (art. 3 ust. 1 PIPA), proporcjonalności/minimalizacji danych (art. 3 ust. 1 i 6 i art. 58 PIPA), prawidłowości (art. 3 ust. 3 PIPA), przejrzystości (art. 3 ust. 5 PIPA), bezpieczeństwa (art. 58 ust. 4 PIPA) i ograniczenia przechowywania (art. 58 ust. 4 PIPA) ([356]). Ewentualne ujawnienie danych stronom trzecim (w tym państwom trzecim) może się odbywać wyłącznie zgodnie z tymi zasadami (w szczególności z zasadami ograniczenia celu i minimalizacji danych), po dokonaniu oceny zgodności z zasadami konieczności i proporcjonalności (art. 37 ust. 2 koreańskiej konstytucji) i z uwzględnieniem wpływu na prawa osób fizycznych, których dane dotyczą (art. 3 ust. 6 PIPA).

(196) W odniesieniu do treści komunikacji i danych potwierdzających komunikację w CPPA określono dalsze ograniczenia dotyczące wykorzystania takich danych do postępowań sądowych, w przypadku gdy strona uczestnicząca w komunikacji powołuje się na nie w roszczeniu o odszkodowanie; lub ograniczenia dotyczące dozwolonych sposobów wykorzystania na podstawie innych ustaw ([357]).

3.3.3 *Nadzór*

(197) Działania koreańskich organów bezpieczeństwa narodowego są nadzorowane przez różne organy ([358]).

(198) Po pierwsze, w ustawie o zwalczaniu terroryzmu przewidziano szczególne mechanizmy nadzoru nad działaniami antyterrorystycznymi, w tym nad zbieraniem danych dotyczących osób podejrzanych o terroryzm. W szczególności, na szczeblu władzy wykonawczej, działania antyterrorystyczne nadzoruje Komisja ds. Zwalczania Terroryzmu ([359]), której dyrektor NIS jest zobowiązany przedkładać sprawozdania z dochodzeń i śledzenia osób podejrzanych o terroryzm w celu zbierania informacji lub materiałów niezbędnych w ramach działań antyterrorystycznych ([360]). Ponadto urzędnik ds. ochrony praw człowieka nadzoruje w szczególności zgodność działań antyterrorystycznych z prawami podstawowymi ([361]). Urzędnika ds. ochrony praw człowieka powołuje przewodniczący Komisji ds. Zwalczania Terroryzmu spośród osób fizycznych dysponujących określonymi kwalifikacjami wymienionymi w dekrecie wykonawczym do ustawy o zwalczaniu terroryzmu ([362]) na dwuletnią (odnawialną) kadencję i może zostać odwołany ze stanowiska tylko z określonych przyczyn i ważnego powodu ([363]). Wykonując swoją funkcję nadzorczą, urzędnik ds. ochrony praw człowieka może wydawać ogólne zalecenia dotyczące poprawy

([354]) Art. 83 ust. 3 TBA.
([355]) Zob. także załącznik II pkt 3.2.3.
([356]) Zob. załącznik II pkt 1.2.
([357]) Art. 5 ust. 1–2, ust. 12 i 13-5 CPPA.
([358]) Zob. załącznik II pkt 3.3.
([359]) Art. 5 ust. 3 ustawy o zwalczaniu terroryzmu. Komisji przewodniczy premier, a w jej skład wchodzi kilku ministrów i szefów agencji rządowych, m.in. ministrowie spraw zagranicznych, sprawiedliwości, obrony narodowej, spraw wewnętrznych i bezpieczeństwa, dyrektor NIS oraz komisarz generalny Agencji Policji Krajowej (art. 3 ust. 1 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu).
([360]) Art. 9 ust. 4 ustawy o zwalczaniu terroryzmu.
([361]) Art. 7 ustawy o zwalczaniu terroryzmu.
([362]) Tzn. każdy, kto posiada uprawnienia radcy prawnego z co najmniej dziesięcioletnim doświadczeniem zawodowym lub posiada wiedzę specjalistyczną w dziedzinie praw człowieka i pracuje lub pracował (przynajmniej) jako profesor nadzwyczajny przez co najmniej dziesięć lat, lub pracował jako wyższy urzędnik publiczny w agencjach państwowych lub organach samorządu terytorialnego, lub posiada co najmniej dziesięcioletnie doświadczenie zawodowe w dziedzinie praw człowieka, np. w organizacji pozarządowej (art. 7 ust. 1 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu).
([363]) Na przykład gdy zostanie oskarżony w sprawie karnej związanej z jego obowiązkami, gdy ujawnia informacje poufne lub z powodu długotrwałej niepełnosprawności intelektualnej lub fizycznej (art. 7 ust. 3 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu).

ochrony praw człowieka ([364]) oraz szczegółowe zalecenia dotyczące działań naprawczych w przypadku stwierdzenia naruszenia praw człowieka ([365]). Organy publiczne mają obowiązek informowania urzędnika ds. ochrony praw człowieka o działaniach następczych podjętych w związku z jego zaleceniami ([366]).

(199) Po drugie, PIPC nadzoruje przestrzeganie przepisów o ochronie danych przez krajowe organy bezpieczeństwa, co obejmuje zarówno mające zastosowanie przepisy PIPA (zob. motyw (149)), jak i ograniczenia i zabezpieczenia mające zastosowanie do zbierania danych osobowych na podstawie pozostałych ustaw (CPPA, ustawy o zwalczaniu terroryzmu oraz TBA, zob. również motyw (171)) ([367]). Wykonując tę funkcję nadzorczą, PIPC może korzystać ze wszystkich swoich uprawnień dochodzeniowych i zaradczych, opisanych szczegółowo w pkt 2.4.2.

(200) Po trzecie, działalność krajowych organów bezpieczeństwa podlega niezależnemu nadzorowi NHRC, zgodnie z procedurami opisanymi w motywie (172) ([368]).

(201) Po czwarte, funkcja nadzorcza BAI rozszerza się również na krajowe organy bezpieczeństwa, chociaż NIS może, w wyjątkowych okolicznościach, odmówić dostarczenia określonych informacji lub materiałów, tj. gdy stanowią one tajemnicę państwową, a ich upublicznienie miałoby poważny wpływ na bezpieczeństwo narodowe ([369]).

(202) Ponadto nadzór parlamentarny nad działaniami NIS sprawuje Zgromadzenie Narodowe (za pośrednictwem wyspecjalizowanej Komisji ds. Wywiadu) ([370]). W CPPA ustanowiono szczególną funkcję nadzorczą dla Zgromadzenia Narodowego w kwestii stosowania środków ograniczających komunikację do celów bezpieczeństwa narodowego ([371]). W szczególności Zgromadzenie Narodowe może przeprowadzać kontrole na miejscu sprzętu podsłuchowego i może nałożyć na NIS i operatorów telekomunikacyjnych, którzy ujawnili treść komunikacji, wymóg składania sprawozdań na ten temat. Zgromadzenie Narodowe może również sprawować swoje ogólne funkcje nadzorcze (zgodnie z procedurami opisanymi w motywie (174)). W ustawie o NIS nałożono na dyrektora tego organu obowiązek bezzwłocznego udzielenia odpowiedzi na wniosek Komisji ds. Wywiadu o sporządzenie sprawozdania w określonej sprawie ([372]), z zachowaniem przepisów szczegółowych dotyczących niektórych informacji szczególnie chronionych. W szczególności dyrektor NIS może odmówić udzielenia odpowiedzi lub złożenia zeznań przed komisją wyłącznie w wyjątkowych okolicznościach, tj. jeżeli wniosek dotyczy tajemnicy państwowej dotyczącej kwestii wojskowych, dyplomatycznych lub związanych z Koreą Północną, w przypadku których publiczne ujawnienie mogłoby mieć poważny wpływ na „losy państwa" ([373]). W takim przypadku Komisja ds. Wywiadu może zażądać wyjaśnień od premiera, a jeżeli ten nie udzieli ich w ciągu siedmiu dni, nie można odmówić udzielenia odpowiedzi lub złożenia zeznań.

3.3.4 *Dochodzenie roszczeń*

(203) Również w dziedzinie bezpieczeństwa narodowego w ramach systemu koreańskiego możliwe są różne (sądowe) drogi dochodzenia roszczeń, w tym uzyskania odszkodowania. Mechanizmy te zapewniają osobom, których dane dotyczą, skuteczne dochodzenie roszczeń na drodze administracyjnej i sądowej, dzięki czemu mogą one dochodzić swoich praw, w tym prawa do uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania lub usunięcia takich danych.

(204) Po pierwsze, zgodnie z art. 3 ust. 5 i art. 4 ust. 1, 3 i 4 PIPA, osoby fizyczne mogą wykonywać swoje prawa w zakresie dostępu, korekty, usunięcia i zawieszenia wobec krajowych organów bezpieczeństwa. W sekcji 6 zawiadomienia nr 2021-5 (załącznik I do niniejszej decyzji) wyjaśniono szczegółowo, w jaki sposób prawa te

([364]) Art. 8 ust. 1 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu.
([365]) Art. 9 ust. 1 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu. Urzędnik ds. ochrony praw człowieka samodzielnie podejmuje decyzje o wydaniu zaleceń, ale ma obowiązek zgłaszać je przewodniczącemu Komisji ds. Zwalczania Terroryzmu.
([366]) Art. 9 ust. 2 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu. Zgodnie z oficjalnym oświadczeniem rządu Korei niewdrożenie zalecenia urzędnika ds. ochrony praw człowieka zostałoby zgłoszone Komisji ds. Zwalczania Terroryzmu, w tym premierowi, choć do tej pory nie odnotowano przypadków, w których zalecenia urzędnika ds. ochrony praw człowieka nie zostałyby wdrożone (zob. załącznik II pkt 3.3.1).
([367]) Zob. załącznik II pkt 3.3.4.
([368]) W szczególności w odniesieniu do NIS w przeszłości NHRC prowadziła dochodzenia z urzędu i rozpatrywała szereg skarg indywidualnych. Zob. np. sprawozdanie roczne NHRC za 2018 r., s. 128 (dostępne pod adresem https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) i sprawozdanie roczne NHRC za 2019 r., s. 70 (dostępne pod adresem https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Art. 13 ust. 1 ustawy o NIS.
([370]) Art. 36 i art. 37 ust. 1 pkt 15 ustawy o Zgromadzeniu Narodowym.
([371]) Art. 15 CPPA.
([372]) Art. 15 ust. 2 ustawy o NIS.
([373]) Art. 17 ust. 2 ustawy o NIS. „Tajemnice państwowe" oznaczają (niejawne) fakty, dobra lub wiedzę, których nie można ujawniać żadnemu innemu państwu ani organizacji, aby uniknąć poważnej szkody dla bezpieczeństwa narodowego, i do których dozwolony jest wyłącznie ograniczony dostęp. Zob. art. 13 ust. 4 ustawy o NIS.

mają zastosowanie w kontekście przetwarzania danych do celów bezpieczeństwa narodowego. W szczególności krajowy organ bezpieczeństwa może ograniczyć lub odmówić wykonania prawa tak długo, oraz w takim zakresie, w jakim jest to konieczne i proporcjonalne do ochrony ważnego celu leżącego w interesie publicznym (na przykład tak długo oraz w takim zakresie, w jakim przyznanie prawa zagroziłoby trwającemu postępowaniu przygotowawczemu lub bezpieczeństwu narodowemu), lub gdy przyznanie prawa może spowodować szkodę dla życia lub integralności cielesnej strony trzeciej. Powołanie się na takie ograniczenie wymaga wyważenia praw i interesów osoby fizycznej względem istotnego interesu publicznego i w żadnym wypadku nie może naruszać istoty tego prawa (art. 37 ust. 2 konstytucji). W przypadku odrzucenia lub ograniczenia wniosku należy bezzwłocznie powiadomić daną osobę fizyczną o przyczynach takiego odrzucenia.

(205) Po drugie, osoby fizyczne mają prawo do dochodzenia roszczeń na podstawie PIPA, jeżeli ich dane zostały przetworzone przez krajowy organ bezpieczeństwa z naruszeniem tej ustawy lub z naruszeniem ograniczeń i zabezpieczeń zawartych w innych ustawach regulujących zbieranie danych osobowych (w szczególności w CPPA, zob. motyw (171)) ([374]). Z prawa tego można skorzystać, wnosząc skargę do PIPC (w tym za pośrednictwem centrum telefonicznego ds. prywatności prowadzonego przez Koreańską Agencję ds. Internetu i Bezpieczeństwa) ([375]). Ponadto, w celu ułatwienia dostępu do środków dochodzenia roszczeń wobec koreańskich krajowych organów bezpieczeństwa, osoby fizyczne z UE mogą wnieść skargę do PIPC za pośrednictwem swojego krajowego organu ochrony danych ([376]). W takim przypadku PIPC powiadomi osobę fizyczną za pośrednictwem jej krajowego organu ochrony danych o zakończeniu dochodzenia (w tym, w stosownych przypadkach, o zastosowanych działaniach naprawczych). Ponadto na podstawie ustawy o postępowaniu administracyjnym osoby fizyczne mogą odwołać się od decyzji PIPC lub wnieść skargę na bezczynność tego organu (zob. motyw (132)).

(206) Po trzecie, osoby fizyczne mogą wnieść skargę do urzędnika ds. ochrony praw człowieka w sprawie naruszenia ich prawa do prywatności/ochrony danych w kontekście działań antyterrorystycznych (tj. zgodnie z ustawą o zwalczaniu terroryzmu) ([377]), który może zalecić działania naprawcze. Ponieważ w postępowaniu przed urzędnikiem ds. ochrony praw człowieka nie obowiązują wymogi dopuszczalności, skarga zostanie rozpatrzona nawet wtedy, gdy dana osoba fizyczna nie jest w stanie wykazać, że faktycznie poniosła szkodę (na przykład z powodu domniemanego bezprawnego zbierania jej danych przez krajowy organ bezpieczeństwa) ([378]). Właściwy organ musi poinformować urzędnika ds. ochrony praw człowieka o wszelkich środkach zastosowanych w celu wdrożenia jego zaleceń.

(207) Po czwarte, osoby fizyczne mogą wnieść skargę do NHRC dotyczącą zbierania ich danych przez krajowe organy bezpieczeństwa i dochodzić roszczeń zgodnie z procedurą opisaną w motywie (178) ([379]).

(208) Dodatkowo dostępne są różne środki ochrony prawnej przed sądem ([380]), umożliwiające osobom fizycznym powołanie się na ograniczenia i zabezpieczenia opisane w pkt 3.3.1 w celu dochodzenia roszczeń. W szczególności osoby fizyczne mogą kwestionować legalność działań organów bezpieczeństwa narodowego na podstawie ustawy o postępowaniu administracyjnym (zgodnie z procedurą opisaną w motywie (181)) lub ustawy o Trybunale Konstytucyjnym (zob. motyw (182)). Co więcej, mogą oni uzyskać odszkodowanie na podstawie ustawy o odszkodowaniach od państwa (opisanej bardziej szczegółowo w motywie (183)).

4. **PODSUMOWANIE**

(209) Komisja uważa, że Republika Korei – za pośrednictwem PIPA, przepisów szczególnych mających zastosowanie do niektórych sektorów (zgodnie z analizą przedstawioną w sekcji 2) oraz dodatkowych zabezpieczeń przewidzianych w zawiadomieniu nr 2021-5 (załącznik I) – zapewnia stopień ochrony danych osobowych przekazywanych z Unii Europejskiej zasadniczo odpowiadający stopniowi ochrony zagwarantowanemu w rozporządzeniu (UE) 2016/679.

(210) Ponadto Komisja stwierdza, że mechanizmy nadzoru i możliwości dochodzenia roszczeń przewidziane w prawie Korei – rozumiane jako całość – zapewniają możliwość identyfikowania przypadków naruszenia przepisów o ochronie danych przez administratorów i w praktyce nakładania za te naruszania kar oraz oferują osobom, których dane dotyczą, możliwość skorzystania ze środków ochrony prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych, a także – ostatecznie – sprostowania lub usunięcia takich danych.

([374]) Art. 58 ust. 4 i art. 4 ust. 5 PIPA. Zob. załącznik II pkt 3.4.2.
([375]) Art. 62 i art. 63 ust. 2 PIPA.
([376]) Zawiadomienie 2021-5 (załącznik I sekcja 6).
([377]) Art. 8 ust. 1 pkt 2 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu.
([378]) Zob. załącznik II pkt 3.4.1.
([379]) Na przykład Krajowa Komisja Praw Człowieka regularnie otrzymuje skargi dotyczące Narodowej Służby Wywiadu, zob. dane w sprawozdaniu rocznym NHRC z 2019 r. dotyczące liczby skarg otrzymanych w latach 2015–2019, s. 70 (dostępne pod adresem https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Zob. załącznik II pkt 3.4.4.

(211) Wreszcie, na podstawie dostępnych informacji na temat koreańskiego porządku prawnego, w tym oświadczeń, zapewnień i zobowiązań rządu Korei zawartych w załączniku II, Komisja uważa, że wszelkie naruszenia praw podstawowych osób fizycznych, których dane osobowe są przekazywane z Unii Europejskiej do Republiki Korei, jakich dopuszczają się koreańskie organy publiczne do celów interesu publicznego, w szczególności do celów ścigania przestępstw i bezpieczeństwa narodowego, będą ograniczać się do tego, co jest absolutnie niezbędne do osiągnięcia tego uzasadnionego celu oraz że ustanowiono skuteczną ochronę prawną przed takimi naruszeniami.

(212) W świetle ustaleń niniejszej decyzji należy zatem uznać, że Republika Korei zapewnia odpowiedni stopień ochrony w rozumieniu art. 45 rozporządzenia (UE) 2016/679, interpretowanego w świetle Karty praw podstawowych Unii Europejskiej, danych osobowych przekazywanych z Unii Europejskiej do Republiki Korei administratorom danych osobowych w Republice Korei podlegającym PIPA, z wyjątkiem organizacji religijnych w zakresie, w jakim przetwarzają one dane osobowe na potrzeby swojej działalności misyjnej; partii politycznych, w zakresie, w jakim przetwarzają one dane osobowe w kontekście zgłaszania kandydatów, oraz administratorów podlegających nadzorowi Komisji Usług Finansowych w zakresie przetwarzania informacji dotyczących kredytów osobistych zgodnie z ustawą o informacjach kredytowych, w zakresie, w jakim przetwarzają takie informacje.

5. SKUTKI NINIEJSZEJ DECYZJI I DZIAŁANIA ORGANÓW OCHRONY DANYCH

(213) Państwa członkowskie i ich organy mają obowiązek stosować środki niezbędne do zapewnienia zgodności z aktami instytucji unijnych, ponieważ domniemywa się, że akty te są zgodne z prawem, a zatem wywołują skutki prawne do chwili ich uchylenia, stwierdzenia ich nieważności w postępowaniu o stwierdzenie nieważności lub orzeczenia o ich nieważności w następstwie wniosku o wydanie orzeczenia w trybie prejudycjalnym lub zarzutu niezgodności z prawem.

(214) Decyzja stwierdzająca odpowiedni stopień ochrony danych osobowych przyjęta przez Komisję na podstawie art. 45 ust. 3 rozporządzenia (UE) 2016/679 jest zatem wiążąca dla wszystkich organów państw członkowskich, do których jest skierowana, w tym ich niezależnych organów nadzorczych. W szczególności przekazywanie danych przez administratora lub podmiot przetwarzający w Unii Europejskiej administratorom w Republice Korei może odbywać się bez konieczności uzyskania jakiegokolwiek dodatkowego zezwolenia.

(215) Należy przypomnieć, że zgodnie z art. 58 ust. 5 rozporządzenia (UE) 2016/679 i jak wyjaśnił Trybunał Sprawiedliwości w wyroku w sprawie Schrems I ([381]), jeżeli krajowy organ ochrony danych kwestionuje, w tym na podstawie skargi, zgodność wydanej przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony z przysługującymi osobie fizycznej prawami podstawowymi do prywatności i ochrony danych, należy zapewnić w prawie krajowym drogę prawną umożliwiającą tej osobie podniesienie tych zarzutów przed sądem krajowym, który może być zobowiązany do wystąpienia z odesłaniem prejudycjalnym do Trybunału Sprawiedliwości ([382]).

6. MONITOROWANIE I PRZEGLĄD NINIEJSZEJ DECYZJI

(216) Zgodnie z orzecznictwem Trybunału Sprawiedliwości ([383]), a także jak wskazano w art. 45 ust. 4 rozporządzenia (UE) 2016/679, Komisja powinna na stale monitorować istotne zmiany zachodzące w państwie trzecim po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony, aby ocenić, czy państwo trzecie nadal zapewnia stopień ochrony zasadniczo odpowiadający temu w Unii Europejskiej. Taka kontrola jest wymagana w każdym przypadku, gdy Komisja otrzyma informacje budzące uzasadnione wątpliwości w tym względzie.

(217) W związku z powyższym Komisja powinna na bieżąco monitorować sytuację w zakresie ram prawnych i rzeczywistej praktyki w Republice Korei w odniesieniu do przetwarzania danych osobowych, podlegających ocenie w niniejszej decyzji, w tym wywiązywanie się przez władze koreańskie z oświadczeń, zapewnień i zobowiązań zawartych w załączniku II. W celu ułatwienia tego procesu zachęca się władze koreańskie do niezwłocznego informowania Komisji o zmianach w prawie materialnym, które są istotne dla niniejszej decyzji w związku z przetwarzaniem danych osobowych przez podmioty gospodarcze i organy publiczne, jak również z ograniczeniami i zabezpieczeniami dotyczącymi dostępu organów publicznych do danych osobowych.

([381]) Schrems, pkt 65.

([382]) Schrems, pkt 65: „W tym względzie do krajowego ustawodawcy należy ustanowienie drogi prawnej umożliwiającej krajowemu organowi nadzorczemu podniesienie zarzutów, które uważa on za zasadne, przed sądami krajowymi, po to, aby te ostatnie, jeśli podzielają wątpliwości tego organu co do ważności decyzji Komisji, wystąpiły z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym w celu zbadania ważności tej decyzji".

([383]) Schrems, pkt 76.

(218) Ponadto, aby Komisja mogła skutecznie realizować funkcję monitorowania, państwa członkowskie powinny informować ją o wszelkich istotnych działaniach podejmowanych przez organy ochrony danych państw członkowskich, zwłaszcza w odniesieniu do zapytań lub skarg osób z UE, których dane dotyczą, dotyczących przekazywania danych osobowych z Unii Europejskiej administratorom danych osobowych w Republice Korei. Komisja powinna być również informowana o wszelkich sygnałach świadczących o tym, że działania koreańskich organów publicznych odpowiedzialnych za zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie przestępstw nie gwarantują wymaganego stopnia ochrony.

(219) W zastosowaniu art. 45 ust. 3 rozporządzenia (UE) 2016/679 ([384]) oraz w świetle tego, że stopień ochrony zapewniany w porządku prawnym Korei może ulec zmianie, Komisja po przyjęciu niniejszej decyzji powinna okresowo sprawdzać, czy ustalenia odnoszące się do adekwatności stopnia ochrony gwarantowanego przez Republikę Korei są nadal faktycznie i prawnie uzasadnione.

(220) W tym celu niniejsza decyzja powinna zostać poddana pierwszemu przeglądowi w ciągu trzech lat od jej wejścia w życie. Po przeprowadzeniu tego pierwszego przeglądu oraz w zależności od jego wyników Komisja, w ścisłym porozumieniu z komitetem powołanym na podstawie art. 93 ust. 1 rozporządzenia (UE) 2016/679, podejmie decyzję co do tego, czy trzyletni cykl powinien zostać utrzymany. W każdym przypadku kolejne przeglądy powinny mieć miejsce co najmniej raz na cztery lata ([385]). Przegląd powinien uwzględniać wszystkie aspekty funkcjonowania niniejszej decyzji, w szczególności stosowanie dodatkowych zabezpieczeń zawartych w załączniku I do niniejszej decyzji, przy czym szczególną uwagę należy poświęcić środkom ochronnym w związku z dalszym przekazywaniem danych; nowym rozstrzygnięciom w orzecznictwie w tej dziedzinie; przepisom dotyczącym przetwarzania informacji spseudonimizowanych do celów statystycznych, do celów badań naukowych i do celów archiwalnych w interesie publicznym, jak również stosowaniu wyjątków na podstawie art. 28 ust. 7 PIPA; skuteczności korzystania z praw indywidualnych, w tym przed zreformowaną w ostatnim czasie PIPC, oraz stosowaniu wyjątków do tych praw; stosowaniu częściowych wyłączeń na podstawie PIPA; jak również ograniczeniom i zabezpieczeniom w odniesieniu do dostępu rządowego (jak wskazano w załączniku II do niniejszej decyzji), w tym współpracy PIPC z unijnymi organami ochrony danych w sprawie skarg osób fizycznych. Przegląd powinien również uwzględniać skuteczność nadzoru i egzekwowania w odniesieniu do PIPA, jak i w obszarze ścigania przestępstw i bezpieczeństwa narodowego (w szczególności przez PIPC i NHRC).

(221) W celu przeprowadzenia przeglądu Komisja powinna odbyć spotkanie z PIPC, której będą towarzyszyć, w stosownych przypadkach, inne koreańskie organy odpowiedzialne za dostęp rządowy do informacji, w tym właściwe organy nadzorcze. Uczestnictwo w tym spotkaniu powinno być otwarte dla przedstawicieli członków Europejskiej Rady Ochrony Danych. W ramach przeglądu Komisja powinna wystąpić do PIPC o przedłożenie wyczerpujących informacji na temat wszystkich kwestii istotnych dla ustaleń dotyczących stwierdzenia odpowiedniego stopnia ochrony, w tym na temat ograniczeń i zabezpieczeń związanych z dostępem rządowym ([386]). Komisja powinna również zwracać się o wyjaśnienia dotyczące wszelkich otrzymanych informacji istotnych dla niniejszej decyzji, w tym o wyjaśnienia dotyczące publicznych sprawozdań przygotowanych przez koreańskie władze lub inne zainteresowane strony z Korei, informacji otrzymanych od Europejskiej Rady Ochrony Danych, poszczególnych organów ochrony danych, organizacji społeczeństwa obywatelskiego, a także doniesień medialnych i informacji pochodzących z innych dostępnych źródeł.

(222) Na podstawie przeglądu Komisja powinna przygotować ogólnodostępne sprawozdanie, które przedłoży Parlamentowi Europejskiemu i Radzie.

7. ZAWIESZENIE, UCHYLENIE LUB ZMIANA NINIEJSZEJ DECYZJI

(223) W przypadku gdy z dostępnych informacji, w szczególności informacji uzyskanych w wyniku monitorowania niniejszej decyzji lub przedstawionych przez władze Korei lub państw członkowskich, wynika, że stopień ochrony zapewniany przez Republikę Korei może nie być już odpowiedni, Komisja powinna niezwłocznie powiadomić o tym właściwe organy Korei i zwrócić się o zastosowanie właściwych środków w określonym, rozsądnym terminie.

(224) Jeśli po upływie tego określonego terminu właściwe organy Korei nie zastosują tych środków lub w inny zadowalający sposób nie wykażą, że niniejsza decyzja jest nadal oparta na odpowiednim stopniu ochrony, Komisja rozpocznie procedurę, o której mowa w art. 93 ust. 2 rozporządzenia (UE) 2016/679, w celu częściowego lub całkowitego zawieszenia lub uchylenia niniejszej decyzji.

(225) Ewentualnie Komisja rozpocznie tę procedurę w celu zmiany decyzji, zwłaszcza uzależniając przekazywanie danych od spełnienia dodatkowych warunków lub ograniczając zakres stwierdzenia odpowiedniego stopnia ochrony wyłącznie do przekazywania danych, co do których zapewniono ciągłość odpowiedniego stopnia ochrony.

([384]) Zgodnie z art. 45 ust. 3 rozporządzenia (UE) 2016/679 „[w] akcie wykonawczym przewiduje się mechanizm okresowego przeglądu […], podczas którego uwzględnia się wszelkie mające znaczenie zmiany w państwie trzecim lub organizacji międzynarodowej".

([385]) Zgodnie z art. 45 ust. 3 rozporządzenia (UE) 2016/679 okresowy przegląd musi odbywać się „przynajmniej raz na cztery lata". Zob. również Europejska Rada Ochrony Danych, Odpowiedni stopień ochrony przekazywanych danych osobowych, WP 254 rev.01.

([386]) Zob. załącznik II do niniejszej decyzji.

(226) Komisja powinna w szczególności wszcząć procedurę zawieszenia lub uchylenia w przypadku wystąpienia przesłanek wskazujących, że dodatkowe zabezpieczenia zawarte w załączniku I nie są przestrzegane przez podmioty gospodarcze otrzymujące dane osobowe na podstawie niniejszej decyzji lub nie są skutecznie egzekwowane, albo jeżeli władze koreańskie nie wywiązują się z oświadczeń, zapewnień i zobowiązań zawartych w załączniku II do niniejszej decyzji.

(227) Komisja powinna również rozważyć wszczęcie procedury prowadzącej do zmiany, zawieszenia lub uchylenia niniejszej decyzji, jeżeli, w kontekście przeglądu lub w inny sposób, właściwe koreańskie władze nie przedłożą informacji lub wyjaśnień wymaganych w związku z oceną stopnia ochrony zapewnianego w odniesieniu do danych osobowych przekazywanych z Unii Europejskiej do Republiki Korei albo w odniesieniu do oceny zgodności z niniejszą decyzją. W tej kwestii Komisja powinna uwzględnić również zakres, w jakim właściwe informacje można uzyskać z innych źródeł.

(228) W należycie uzasadnionych, szczególnie pilnych przypadkach Komisja skorzysta z możliwości przyjęcia zgodnie z procedurą, o której mowa w art. 93 ust. 3 rozporządzenia (UE) 2016/679, mających natychmiastowe zastosowanie aktów wykonawczych zawieszających, uchylających lub zmieniających decyzję.

8. **UWAGI KOŃCOWE**

(229) Europejska Rada Ochrony Danych opublikowała swoją opinię ([387]), która została uwzględniona podczas przygotowywania niniejszej decyzji.

(230) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na podstawie art. 93 ust. 1 rozporządzenia (UE) 2016/679,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. Do celów art. 45 rozporządzenia (UE) 2016/679 Republika Korei zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii Europejskiej podmiotom w Republice Korei na podstawie ustawy o ochronie danych osobowych uzupełnionej dodatkowymi zabezpieczeniami zawartymi w załączniku I, wraz z oficjalnymi oświadczeniami, zapewnieniami i zobowiązaniami zawartymi w załączniku II.

2. Niniejsza decyzja nie obejmuje danych osobowych przekazywanych odbiorcom, którzy zaliczają się do jednej z następujących kategorii oraz w przypadku których wszystkie lub niektóre cele przetwarzania danych osobowych odpowiadają jednemu z celów wymienionych w tej decyzji, odpowiednio:

a) organizacje religijne w zakresie, w jakim przetwarzają dane osobowe do celów działalności misyjnej;

b) partie polityczne w zakresie, w jakim przetwarzają dane osobowe w kontekście zgłaszania kandydatów;

c) podmioty podlegające nadzorowi Komisji Usług Finansowych w zakresie przetwarzania informacji dotyczących kredytów osobistych zgodnie z ustawą o informacjach kredytowych, w zakresie, w jakim przetwarzają takie informacje.

Artykuł 2

W każdym przypadku, gdy właściwe organy w państwach członkowskich, w celu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych, wykonują swoje uprawnienia na podstawie art. 58 rozporządzenia (UE) 2016/679 w odniesieniu do przekazywania danych wchodzącego w zakres stosowania określony w art. 1 niniejszej decyzji, dane państwo członkowskie niezwłocznie informuje o tym fakcie Komisję.

Artykuł 3

1. Komisja stale monitoruje stosowanie ram prawnych, na których opiera się niniejsza decyzja, w tym warunki, na których przeprowadza się dalsze przekazywanie danych i wykonuje się prawa indywidualne oraz warunki, na których koreańskie organy publiczne mają dostęp do danych przekazywanych na podstawie niniejszej decyzji, w celu oceny, czy Republika Korei nadal zapewnia odpowiedni stopień ochrony w rozumieniu art. 1.

([387]) Opinia 32/2021 dotycząca projektu decyzji wykonawczej Komisji Europejskiej na podstawie rozporządzenia (UE) 2016/679 w sprawie odpowiedniego stopnia ochrony danych osobowych w Korei Południowej, dostępna pod następującym linkiem: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en.

2. Państwa członkowskie oraz Komisja informują się nawzajem o przypadkach, w których Komisja Ochrony Danych Osobowych lub jakikolwiek inny właściwy organ koreański nie zapewniły zgodności z ramami prawnymi, na których opiera się niniejsza decyzja.

3. Państwa członkowskie i Komisja informują się nawzajem o wszelkich sygnałach wskazujących, że ingerencje koreańskich organów publicznych w prawo osób fizycznych do ochrony ich danych osobowych wykraczają poza to, co jest absolutnie niezbędne, lub że nie zapewniono skutecznej ochrony prawnej przed takimi ingerencjami.

4. Po trzech latach od dnia powiadomienia państw członkowskich o wydaniu niniejszej decyzji, a następnie co najmniej co cztery lata, Komisja ocenia ustalenie, o którym mowa w art. 1 ust. 1, na podstawie wszystkich dostępnych informacji, w tym informacji otrzymanych w ramach przeglądu przeprowadzanego wspólnie z właściwymi organami koreańskimi.

5. Jeżeli Komisja wejdzie w posiadanie dowodów na to, że odpowiedni stopień ochrony nie jest już zapewniony, powiadamia o tym właściwe organy koreańskie. W razie potrzeby Komisja może postanowić o zawieszeniu, zmianie albo uchyleniu niniejszej decyzji albo o ograniczeniu jej zakresu, zgodnie z art. 45 ust. 5 rozporządzenia (UE) 2016/679, zwłaszcza w przypadku, gdy istnieją przesłanki, by sądzić że:

a) koreańscy administratorzy, którzy otrzymali dane osobowe z Unii Europejskiej na podstawie niniejszej decyzji, nie przestrzegają dodatkowych zabezpieczeń zawartych w załączniku I lub nadzór i egzekwowanie przepisów w tym zakresie są niewystarczające;

b) koreańskie organy publiczne nie wywiązują się z oświadczeń, zapewnień i zobowiązań zawartych w załączniku II, w tym w zakresie warunków i ograniczeń zbierania danych osobowych przekazanych na podstawie niniejszej decyzji i uzyskiwania dostępu do nich przez koreańskie organy publiczne do celów ścigania przestępstw lub bezpieczeństwa narodowego.

Komisja może również przyjąć takie środki, jeżeli brak współpracy ze strony rządu Republiki Korei nie pozwala Komisji ustalić, czy Republika Korei nadal zapewnia odpowiedni stopień ochrony.

Artykuł 4

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 17 grudnia 2021 r.

W imieniu Komisji
Didier REYNDERS
Członek Komisji

ZAŁĄCZNIK I

PRZEPISY UZUPEŁNIAJĄCE DOTYCZĄCE WYKŁADNI I STOSOWANIA USTAWY O OCHRONIE DANYCH OSOBOWYCH W ZWIĄZKU Z PRZETWARZANIEM DANYCH OSOBOWYCH PRZEKAZYWANYCH DO REPUBLIKI KOREI

Spis treści

I. **Zarys**

Republika Korei („Korea") i Unia Europejska („UE") uczestniczyły w rozmowach dotyczących odpowiedniego stopnia ochrony, w wyniku których Komisja Europejska stwierdziła, że Korea zapewnia odpowiedni stopień ochrony danych osobowych zgodnie z art. 45 RODO.

W tym kontekście oraz opierając się na art. 5 („Obowiązki państwa" itp.) i art. 14 („Współpraca międzynarodowa") ([1]) ustawy o ochronie danych osobowych, Komisja Ochrony Danych Osobowych przyjęła niniejsze powiadomienie, aby doprecyzować wykładnię, stosowanie i egzekwowanie niektórych przepisów wspomnianej ustawy, w tym w odniesieniu do przetwarzania danych osobowych przekazywanych do Korei na podstawie decyzji UE stwierdzającej odpowiedni stopień ochrony.

Ponieważ niniejsze powiadomienie ma status zarządzenia administracyjnego ustanawianego i ogłaszanego przez właściwą agencję administracyjną w celu wyjaśnienia norm regulujących interpretację, stosowanie i egzekwowanie ustawy o ochronie danych osobowych w systemie prawnym Korei, ma ono prawnie wiążącą moc wobec administratora danych osobowych w tym sensie, że każde naruszenie niniejszego powiadomienia może być traktowane jako naruszenie odpowiednich przepisów PIPA. Ponadto w przypadku naruszenia praw lub interesów w wyniku naruszenia niniejszego powiadomienia odnośnym osobom fizycznym przysługuje prawo do dochodzenia roszczeń przed Komisją Ochrony Danych Osobowych lub sądem.

W związku z powyższym niepodjęcie działań zgodnych z niniejszym powiadomieniem przez administratora danych osobowych, który przetwarza dane osobowe przekazywane do Korei zgodnie z decyzją UE stwierdzającą odpowiedni stopień ochrony, zostanie uznane za „istnienie istotnych przesłanek do uznania, że doszło do naruszenia w odniesieniu do danych osobowych, a niepodjęcie stosownych działań może spowodować trudną do naprawienia szkodę", zgodnie z art. 64 ust. 1 i 2 ustawy. W takich przypadkach Komisja Ochrony Danych Osobowych lub powiązane centralne

([1]) Zgodnie z art. 14 ustawy o ochronie danych osobowych rząd Korei jest uprawniony do ustanowienia polityki mającej na celu zwiększenie stopnia ochrony danych osobowych w otoczeniu międzynarodowym i zapobieganie naruszaniu praw osób, których dane dotyczą, w związku z transgranicznym przekazywaniem danych osobowych.

agencje administracyjne mogą zarządzić, aby odpowiedni administrator danych osobowych podjął działania naprawcze itp., zgodnie z uprawnieniem nadanym na mocy tego przepisu, a także – w zależności od konkretnych naruszeń prawa – może zostać nałożona odpowiednia kara (grzywna, administracyjna kara pieniężna itp.).

II **Definicje pojęć**

W niniejszych przepisach zastosowano terminy o następujących definicjach:

(i) ustawa: ustawa o ochronie danych osobowych (ustawa nr 16930, zmieniona dnia 4 lutego 2020 r., weszła w życie dnia 5 sierpnia 2020 r.);

(ii) dekret prezydencki: dekret wykonawczy do ustawy o ochronie danych osobowych (dekret prezydencki nr 30509 z dnia 3 marca 2020 r., zmieniający inne ustawy);

(iii) osoba, której dane dotyczą: osoba fizyczna, którą można zidentyfikować na podstawie przetwarzanych informacji, przez co staje się ona podmiotem tych informacji;

(iv) administrator danych osobowych: instytucja publiczna, osoba prawna, organizacja, osoba fizyczna itp., która w sposób bezpośredni lub pośredni przetwarza dane osobowe w ramach swojej działalności;

(v) UE: UE (od lutego 2020 r. obejmuje 27 państw członkowskich [2]), w tym Belgię, Niemcy, Francję, Włochy, Luksemburg, Niderlandy, Danię, Irlandię, Grecję, Portugalię, Hiszpanię, Austrię, Finlandię, Szwecję, Cypr, Czechy, Estonię, Węgry, Łotwę, Litwę, Maltę, Polskę, Słowację, Słowenię, Rumunię, Bułgarię i Chorwację) oraz kraje stowarzyszone z UE w ramach Porozumienia o Europejskim Obszarze Gospodarczym (Islandia, Liechtenstein, Norwegia).

(vi) RODO: ogólne przepisy prawa UE dotyczące ochrony danych osobowych, ogólne rozporządzenie o ochronie danych (rozporządzenie (UE) 2016/679);

(vii) decyzja stwierdzająca odpowiedni stopień ochrony: zgodnie z art. 45 ust. 3 RODO Komisja Europejska przyjęła decyzję stwierdzającą, że państwo trzecie, terytorium w państwie trzecim, określony sektor lub określone sektory lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych osobowych.

III **Przepisy uzupełniające**

1. **Ograniczenie wykorzystywania i przekazywania danych osobowych do celów innych niż przewidziane (art. 3, 15 i 18 ustawy)**

<Ustawa o ochronie danych osobowych

(ustawa nr 16930, częściowo zmieniona dnia 4 lutego 2020 r.)>

Artykuł 3 (Zasady ochrony danych osobowych) 1) Administrator danych osobowych określa wyraźnie, do jakich celów przetwarzane są dane osobowe; ponadto administrator danych osobowych zbiera dane osobowe uczciwie i zgodnie z prawem, w minimalnym zakresie, jaki jest niezbędny do osiągnięcia tych celów.

2) Administrator danych osobowych przetwarza dane osobowe w odpowiedni sposób niezbędny do osiągnięcia celów, do których dane te są przetwarzane, i nie wykorzystuje ich w sposób wykraczający poza te cele.

Artykuł 15 (Zbieranie i wykorzystywanie danych osobowych) 1) Administrator danych osobowych może zbierać dane osobowe w każdej z następujących okoliczności oraz wykorzystywać te dane w zakresie zgodnym z celem zbierania:

1. w przypadku uzyskania zgody osoby, której dane dotyczą;

2. w przypadku istnienia szczególnych przepisów ustawowych lub gdy jest to niezbędne do przestrzegania zobowiązań prawnych;

3. w przypadku gdy jest to niezbędne do wykonania przez instytucję publiczną obowiązków objętych zakresem jej kompetencji określonych w ustawie;

4. w przypadku gdy jest to niezbędnie konieczne do egzekwowania i wykonania umowy zawartej z osobą, której dane dotyczą;

[2] Do końca okresu przejściowego wykaz ten obejmuje również Zjednoczone Królestwo, zgodnie z art. 126, 127 i 132 Umowy o wystąpieniu Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej z Unii Europejskiej i Europejskiej Wspólnoty Energii Atomowej (2019/C 384 I/01).

5. w przypadku gdy zostanie to uznane za wyraźnie konieczne do ochrony życia, potrzeb fizycznych lub interesów majątkowych osoby, której dane dotyczą, lub strony trzeciej, przed bezpośrednim zagrożeniem, jeżeli osoba, której dane dotyczą, lub jej przedstawiciel ustawowy nie są w stanie wyrazić zamiaru, lub nie można uzyskać wcześniejszej zgody z powodu nieznanych adresów itp.;
6. w przypadku gdy jest to konieczne do realizacji uzasadnionego interesu administratora danych osobowych, jeżeli taki interes jest w oczywisty sposób nadrzędny wobec praw osoby, której dane dotyczą. W takich przypadkach przetwarzanie jest dozwolone wyłącznie w rozsądnym zakresie, w jakim przetwarzanie jest merytorycznie związane z uzasadnionym interesem administratora danych osobowych.

Artykuł 18 (Ograniczenie wykorzystywania i przekazywania danych osobowych do celów innych niż zostało to przewidziane) 1) Administrator danych osobowych nie wykorzystuje danych osobowych w zakresie wykraczającym poza zakres określony w art. 15 ust. 1 i art. 39-3 ust. 1 i 2 ani nie przekazuje ich żadnej stronie trzeciej w zakresie wykraczającym poza zakres określony w art. 17 ust. 1 i 3.

2) Nie naruszając ust. 1, w przypadku gdy zastosowanie ma którykolwiek z poniższych punktów, administrator danych osobowych może wykorzystywać dane osobowe lub przekazywać je stronie trzeciej do innych celów, chyba że takie działanie może naruszać w sposób nieuzasadniony interes osoby, której dane dotyczą, lub strony trzeciej: pod warunkiem, że usługodawcy świadczący usługi informacyjne i komunikacyjne [określeni np. w art. 2 ust. 1 pkt 3 ustawy o promowaniu stosowania sieci informacyjno-komunikacyjnych i ochronie danych; stosuje się odpowiednio w dalszej części] przetwarzający dane osobowe użytkowników [określonych np. w art. 2 ust. 1 pkt 4 ustawy o promowaniu stosowania sieci informacyjno-komunikacyjnych i ochronie danych; stosuje się odpowiednio w dalszej części] podlegają wyłącznie pkt 1 i 2, a pkt 5–9 mają zastosowanie wyłącznie do instytucji publicznych:

1. w przypadku uzyskania dodatkowej zgody od osoby, której dane dotyczą;
2. w przypadku istnienia innych szczególnych przepisów ustawowych;
3. w przypadku gdy zostanie to uznane za wyraźnie konieczne do ochrony życia, potrzeb fizycznych lub interesów majątkowych osoby, której dane dotyczą, lub strony trzeciej, przed bezpośrednim zagrożeniem, jeżeli osoba, której dane dotyczą, lub jej przedstawiciel ustawowy nie są w stanie wyrazić intencji, lub nie można uzyskać wcześniejszej zgody z powodu nieznanych adresów;
4. uchylony; <ustawą nr 16930 z dnia 4 lutego 2020 r.>
5. w przypadku gdy administrator danych osobowych nie ma możliwości wykonywania obowiązków wchodzących w jego zakres kompetencji, określonych w dowolnej ustawie, chyba że wykorzystuje on dane osobowe do celu innego niż zamierzony lub przekazuje je stronie trzeciej, przy czym kwestie dotyczące takiego wykorzystywania lub przekazywania danych osobowych podlegają rozpatrzeniu i rozstrzygnięciu przez Komisję Ochrony Danych Osobowych;
6. w przypadku konieczności przekazania danych osobowych rządowi obcego państwa lub organizacji międzynarodowej w celu wykonania traktatu lub innej konwencji międzynarodowej;
7. jeżeli jest to konieczne w związku z postępowaniem przygotowawczym w sprawie przestępstwa, aktem oskarżenia i ściganiem karnym;
8. jeżeli jest to konieczne, aby sąd mógł przystąpić do wykonywania obowiązków związanych z procesem;
9. jeżeli jest to konieczne do celów egzekwowania kary, probacji i prawa pieczy.

Ustępy 3 i 4 pominięto.

5) W przypadku gdy administrator danych osobowych dostarcza dane osobowe stronie trzeciej do celu innego niż zamierzony w którymkolwiek z przypadków, o których mowa w ust. 2, administrator danych osobowych zwraca się do odbiorcy danych osobowych o ograniczenie celu i metody wykorzystywania danych i innych niezbędnych kwestii lub o przygotowanie niezbędnych zabezpieczeń, aby zapewnić bezpieczeństwo danych osobowych. W takich przypadkach osoba, do której zwrócił się administrator danych osobowych, wprowadza niezbędne środki, aby zapewnić bezpieczeństwo danych osobowych.

(i) Art. 3 ust. 1 i 2 ustawy przewiduje zasadę, zgodnie z którą administrator danych osobowych może zbierać wyłącznie minimalną ilość danych osobowych niezbędnych do osiągnięcia celu przetwarzania takich danych zgodnie z prawem oraz nie powinien wykorzystywać danych osobowych do celów innych niż zamierzone ([3]).

(ii) Zgodnie z tą zasadą art. 15 ust. 1 ustawy przewiduje, że w przypadku gdy administrator danych osobowych zbiera dane osobowe, dane takie można wykorzystać w ramach celu zbierania, a art. 18 ust. 1 przewiduje, że dane osobowe nie powinny być wykorzystywane w zakresie wykraczającym poza zakres celu zbierania ani przekazywane stronie trzeciej.

([3]) Ponieważ przepisy te określają ogólne zasady, które mają zastosowanie do każdego przetwarzania danych osobowych, w tym do przypadków, w których takie przetwarzanie jest szczegółowo uregulowane innymi ustawami, wyjaśnienia zawarte w niniejszym punkcie mają zastosowanie także do przypadków, w których dane osobowe są przetwarzane na podstawie innych przepisów (zob. np. art. 15 ust. 1 ustawy o informacjach kredytowych, która odnosi się szczegółowo do tych przepisów).

(iii) Ponadto, nawet jeżeli dane osobowe można wykorzystywać do celów innych niż zamierzone oraz przekazywać stronie trzeciej w wyjątkowych przypadkach ([4]), o których mowa w art. 18 ust. 2 pkt 1–9 ustawy, należy zażądać ograniczenia celu lub metody wykorzystywania danych, tak aby zapewnić możliwość bezpiecznego przetwarzania danych osobowych zgodnie z ust. 5, lub wprowadzić środki niezbędne do zapewnienia bezpieczeństwa takich danych.

(iv) Powyższe przepisy stosuje się jednakowo do przetwarzania wszystkich danych osobowych otrzymanych na obszarze objętym jurysdykcją prawną Korei od państwa trzeciego, niezależnie od narodowości osoby, której dane dotyczą.

(v) Na przykład jeżeli administrator danych osobowych w UE przekazuje dane osobowe do koreańskiego administratora danych osobowych zgodnie z decyzją Komisji Europejskiej stwierdzającą odpowiedni stopień ochrony, cel przekazania danych osobowych, jakim kieruje się administrator danych osobowych w UE, uznaje się za cel zbierania danych osobowych, jakim kieruje się koreański administrator danych osobowych, przy czym w takich przypadkach koreański administrator danych osobowych może wykorzystać dane osobowe lub przekazać je stronie trzeciej wyłącznie w ramach celu zbierania z wyjątkiem nadzwyczajnych przypadków, o których mowa w art. 18 ust. 2 pkt 1–9 ustawy.

2. **Ograniczenie dalszego przekazywania danych osobowych (art. 17 ust. 3 i 4, art. 18 ustawy)**

<Ustawa o ochronie danych osobowych

(ustawa nr 16930, częściowo zmieniona dnia 4 lutego 2020 r.)>

Artykuł 17 (Przekazywanie danych osobowych) 1) Pomija się.

2) Jeżeli administrator danych osobowych uzyska zgodę, o której mowa w ust. 1 pkt 1, informuje on osobę, której dane dotyczą, o poniższych kwestiach. Przepis ten stosuje się również w przypadku modyfikacji którychkolwiek z następujących danych:

1. odbiorcy danych osobowych;
2. celu wykorzystywania przez odbiorcę danych osobowych takich danych;
3. szczegółów danych osobowych, które mają zostać przekazane;
4. okresu, w jakim odbiorca zatrzymuje i wykorzystuje dane osobowe;
5. faktu, że osobie, której dane dotyczą, przysługuje prawo odmowy udzielenia zgody oraz niedogodności, jakie mogłyby wyniknąć z takiej odmowy.

3) Administrator danych osobowych informuje osobę, której dane dotyczą, o kwestiach, o których mowa w ust. 2, i uzyskuje zgodę od takiej osoby w celu przekazania danych osobowych stronie trzeciej za granicę; ponadto administrator danych osobowych nie może zawrzeć umowy o transgraniczne przekazywanie danych osobowych z naruszeniem przepisów ustawy.

4) Administrator danych osobowych może przekazywać dane osobowe bez zgody osoby, której dane dotyczą, w zakresie racjonalnie powiązanym z celami, w których dane te zostały pierwotnie zebrane, jak określono w dekrecie prezydenckim i z uwzględnieniem kwestii, czy powstały w związku z tym niedogodności po stronie osoby, której dane dotyczą, czy wprowadzono niezbędne środki w celu zapewnienia bezpieczeństwa, takie jak np. szyfrowanie

※ Więcej informacji dotyczących art. 18 można znaleźć na stronach 3, 4 i 5.

< **Dekret wykonawczy dotyczący ustawy o ochronie danych osobowych**

([Data wejścia w życie: 5 lutego 2021 r.] [dekret prezydencki nr 30892 z dnia 4 sierpnia 2020 r., zmieniający inne ustawy])>

Artykuł 14-2 (Inne normy dotyczące dodatkowego wykorzystywania/przekazywania danych osobowych)

1) Jeżeli administrator danych osobowych wykorzystuje lub przekazuje dane osobowe (dalej „dodatkowe wykorzystywanie lub przekazywanie danych osobowych") bez zgody osoby, której dane dotyczą, zgodnie z art. 15 ust. 3 ustawy lub art. 17 ust. 4 ustawy, uwzględnia on kwestię tego, czy:

1. takie dodatkowe wykorzystywanie lub przekazywanie danych osobowych jest racjonalnie powiązane z pierwotnym celem zbierania tych danych;
2. można przewidzieć dodatkowe wykorzystywanie lub przekazywanie danych osobowych w świetle okoliczności, w jakich dane te zostały zebrane, oraz praktyk przetwarzania;
3. dodatkowe wykorzystywanie lub przekazywanie danych osobowych nie narusza w sposób nieuzasadniony interesów osoby, której dane dotyczą; oraz
4. podjęto działania wymagane do zapewnienia bezpieczeństwa takie jak pseudonimizacja lub szyfrowanie.

([4]) Usługodawcy świadczący usługi informacyjne i komunikacyjne podlegają wyłącznie art. 18 ust. 2 pkt 1 i 2. Pkt 5–9 mają zastosowanie wyłącznie do instytucji publicznych.

2) Administrator danych osobowych podaje z wyprzedzeniem kryteria służące do oceny kwestii, o których mowa w ust. 1 pkt 1–4, uwzględniając je w polityce prywatności określonej w art. 30 ust. 1 ustawy, a urzędnik ds. ochrony prywatności, o którym mowa w art. 31 ust. 1 ustawy, sprawdza, czy administrator danych osobowych wykorzystuje lub przekazuje dodatkowe dane osobowe zgodnie z odpowiednimi normami.

(i) W przypadku gdy administrator danych osobowych przekazuje dane osobowe stronie trzeciej za granicę, musi on poinformować z wyprzedzeniem osoby, których dane dotyczą, o wszelkich kwestiach określonych w art. 17 ust. 2 ustawy oraz uzyskać ich zgodę, z wyjątkiem przypadków, o których mowa w ust. 1 lub 2. Nie zezwala się na zawieranie umów o transgraniczne przekazywanie danych osobowych z naruszeniem przepisów ustawy.

1) Jeżeli dane osobowe są przekazywane w zakresie racjonalnie powiązanym z pierwotnym celem zbierania, zgodnie z art. 17 ust. 4 ustawy. Przepis ten może mieć jednak zastosowanie wyłącznie do spraw zgodnych z normami dotyczącymi dodatkowego wykorzystywania i przekazywania danych osobowych, przewidzianymi w art. 14-2 dekretu wykonawczego. Ponadto administrator danych osobowych musi rozważyć, czy przekazywanie danych osobowych może spowodować niedogodności po stronie osób, których dane dotyczą, oraz czy wprowadził on niezbędne środki w celu zapewnienia bezpieczeństwa, takie jak szyfrowanie.

2) Jeżeli dane osobowe mogą być przekazywane stronie trzeciej w wyjątkowych przypadkach, o którym mowa w art. 18 ust. 2 ustawy (zob. s. 3–5). Jednak nawet w takich przypadkach nie można przekazywać danych osobowych stronie trzeciej, jeżeli przekazanie takich danych może naruszać w sposób nieuzasadniony interesy osoby, której dane dotyczą, lub strony trzeciej. Ponadto osoba przekazująca dane osobowe musi zwrócić się do odbiorcy danych osobowych o ograniczenie celu lub metody wykorzystywania danych osobowych lub wprowadzić środki niezbędne do zapewnienia bezpieczeństwa takich danych, tak aby zapewnić możliwość bezpiecznego przetwarzania danych osobowych.

(ii) W przypadku gdy dane osobowe są przekazywane stronie trzeciej za granicę, stopień ochrony takiego przekazywania może nie być równy stopniowi ochrony zapewnianemu przez ustawę o ochronie danych osobowych Korei ze względu na różnice występujące w systemach ochrony danych osobowych poszczególnych krajów. W związku z tym takie przypadki będą uznawane za „przypadki, w których mogą wystąpić niedogodności po stronie osoby, której dane dotyczą", o których to niedogodnościach mowa w art. 17 ust. 4 ustawy lub „przypadki, w których interes osoby, której dane dotyczą, lub strony trzeciej został w sposób nieuzasadniony naruszony", o którym to interesie mowa w art. 18 ust. 2 ustawy i w art. 14-2 dekretu wykonawczego do tej samej ustawy ([5]). Aby spełnić wymogi tych przepisów, administrator danych osobowych i strona trzecia muszą zatem wyraźnie zapewnić stopień ochrony równy stopniowi ochrony określonemu w ustawie, w tym gwarancję wykonywania przez osobę, której dane dotyczą, przysługujących jej praw w prawnie wiążących dokumentach, takich jak umowy, nawet po przekazaniu danych osobowych za granicę.

3. **Powiadomienie dotyczące danych w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą (art. 20 ustawy)**

<Ustawa o ochronie danych osobowych

(ustawa nr 16930, częściowo zmieniona dnia 4 lutego 2020 r.)>

Artykuł 20 (Powiadomienie dotyczące innych źródeł danych osobowych zebranych od stron trzecich) 1) W przypadku gdy administrator danych osobowych przetwarza dane osobowe zebrane od osób trzecich, powiadamia on niezwłocznie osobę, której dane dotyczą, na jej żądanie, o następujących kwestiach:

1. o źródle zebranych danych osobowych;

2. o celu przetwarzania danych osobowych;

3. o fakcie, że osoba, której dane dotyczą, ma prawo zażądać zawieszenia przetwarzania danych osobowych, jak przewidziano w art. 37.

2) Nie naruszając ust. 1, w przypadku gdy administrator danych osobowych, spełniając kryteria przewidziane w dekrecie prezydenckim z uwzględnieniem rodzajów i ilości przetwarzanych danych osobowych, liczby pracowników, wielkości sprzedaży itp., zbiera dane osobowe od stron trzecich i przetwarza je zgodnie z art. 17 ust. 1 pkt 1, powiadamia on niezwłocznie osobę, której dane dotyczą, o kwestiach wskazanych w ust. 1: pod warunkiem, że przepis ten nie ma zastosowania, w przypadku gdy dane zbierane przez administratora danych osobowych nie zawierają żadnych danych osobowych, takich jak dane kontaktowe, za pomocą których osobie, której dane dotyczą, można przekazać powiadomienie.

([5]) Zgodnie z art. 18 ust. 2 pkt 2 PIPA ma to również zastosowanie w przypadku przekazania danych osobowych stronom trzecim za granicę na podstawie przepisów zawartych w innych ustawach (np. w ustawie o informacjach kredytowych).

3) Niezbędne kwestie dotyczące czasu, metody i procedury przekazywania powiadomienia osobie, której dane dotyczą, zgodnie z ust. 2 zdanie główne, określono w dekrecie prezydenckim.

4) Ust. 1 i ust. 2 zdanie główne nie mają zastosowania w żadnej z następujących okoliczności: z zastrzeżeniem sytuacji, w których jest to w oczywisty sposób nadrzędny wobec praw osób, których dane dotyczą, na mocy niniejszej ustawy:

1. w przypadku gdy dane osobowe, które podlegają wnioskowi o powiadomienie, znajdują się w dokumentacji, o której mowa w którymkolwiek z punktów art. 32 ust. 2;
2. w przypadku gdy takie powiadomienie może spowodować szkodę dla życia lub integralności cielesnej jakiejkolwiek innej osoby lub nieuzasadnione naruszenie interesów majątkowych i innych interesów jakiejkolwiek innej osoby.

(i) Jeżeli administrator danych osobowych otrzyma dane osobowe przekazane z UE na podstawie decyzji UE stwierdzającej odpowiedni stopień ochrony ([6]), musi on powiadomić – bez zbędnej zwłoki i w każdym przypadku nie później niż w ciągu miesiąca od przekazania tych danych – osobę, której dane dotyczą, o danych, o których mowa w pkt 1–5.

1) Imię i nazwisko oraz dane kontaktowe osób, które przekazują i otrzymują dane osobowe.

2) Pozycje lub kategorie przekazanych danych osobowych.

3) Cel zbierania i wykorzystywania danych osobowych (jak ustalił podmiot przekazujący dane zgodnie z pkt 1 niniejszego powiadomienia).

4) Okres zatrzymywania danych osobowych.

5) Informacje na temat praw osoby, której dane dotyczą, związanych z przetwarzaniem danych osobowych, metody wykonywania tych praw i związanej z tym procedury oraz wszelkich niedogodności, jeżeli wykonywanie tych praw je powoduje.

(ii) Ponadto jeżeli administrator danych osobowych przekazuje dane osobowe, o których mowa w pkt (i), stronie trzeciej w Republice Korei lub za granicę, przed przekazaniem takich danych musi on powiadomić osobę, której dane dotyczą, o danych, o których mowa w pkt 1–5.

1) Imię i nazwisko oraz dane kontaktowe osób, które przekazują i otrzymują dane osobowe.

2) Pozycje lub kategorie przekazanych danych osobowych.

3) Kraj, do którego dane osobowe mają zostać przekazane, przewidywana data i metoda przekazania danych osobowych (z ograniczeniem do przypadków, w których dane osobowe mają zostać przekazane stronie trzeciej za granicę).

4) Cel osoby przekazującej dane osobowe oraz podstawa prawna do przekazania danych osobowych.

5) Informacje na temat praw osoby, której dane dotyczą, związanych z przetwarzaniem danych osobowych, metody wykonywania tych praw i związanej z tym procedury oraz wszelkich niedogodności, jeżeli wykonywanie tych praw je powoduje.

(iii) Administrator danych osobowych nie może zastosować przepisów określonych w pkt (i) i (ii) w żadnym z przypadków, o których mowa w pkt 1–4.

1) Jeżeli dane osobowe, o których należy powiadomić, znajdują się w którejkolwiek z dokumentacji, o których mowa w art. 32 ust. 2 ustawy, w zakresie, w jakim interesy chronione niniejszym przepisem są w oczywisty sposób nadrzędne wobec praw osoby, której dane dotyczą, oraz wyłącznie w przypadku, gdy powiadomienie stanowiłoby zagrożenie dla realizacji odpowiednich interesów, np. zagrażając trwającemu postępowaniu przygotowawczemu lub bezpieczeństwu narodowemu.

2) W przypadku gdy i dopóki istnieje prawdopodobieństwo, że powiadomienie może spowodować szkodę dla życia lub integralności cielesnej innej osoby lub nieuzasadnione naruszenie interesów majątkowych innej osoby, o ile te prawa lub interesy są w oczywisty sposób nadrzędne wobec praw osoby, której dane dotyczą.

3) Jeżeli osoba, której dane dotyczą, posiada już informację, że administrator danych osobowych musi wysłać powiadomienie zgodnie z pkt (i) lub (ii).

4) Jeżeli administrator danych osobowych nie dysponuje żadnymi danymi kontaktowymi osoby, której dane dotyczą, lub skontaktowanie się z tą osobą wymaga nadmiernego wysiłku, w tym w kontekście przetwarzania zgodnie z warunkami określonymi w sekcji 3 PIPA. Określając, czy istnieje możliwość skontaktowania się z osobą, której dane dotyczą, lub czy takie skontaktowanie się wymaga nadmiernego wysiłku, należy wziąć pod uwagę możliwość współpracy z podmiotem przekazującym dane w UE.

([6]) Obowiązki, o których mowa w pkt (i), (ii) oraz (iii), mają jednakowe zastosowanie, jeżeli administrator, który otrzymuje dane osobowe z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, przetwarza takie dane na podstawie innych ustaw, jak np. na podstawie ustawy o informacjach kredytowych.

4. **Zakres stosowania szczególnego odstępstwa od przetwarzania danych spseudonimizowanych (art. 28-2, 28-3, 28-4, 28-5, 28-6, 28-7, art. 3 i art. 58-2 ustawy)**

<Ustawa o ochronie danych osobowych

(ustawa nr 16930, częściowo zmieniona dnia 4 lutego 2020 r.)>

Rozdział III Przetwarzanie danych osobowych

SEKCJA 3 Szczególne przykłady dotyczące danych spseudonimizowanych

Artykuł 28-2 (Przetwarzanie danych spseudonimizowanych) 1) Administrator danych osobowych może przetwarzać spseudonimizowane dane osobowe bez zgody osób, których dane dotyczą, do celów statystycznych, do celów badań naukowych i do celów archiwalnych w interesie publicznym itp.

2) Administrator danych osobowych nie uwzględnia informacji, które można wykorzystać do zidentyfikowania określonej osoby fizycznej podczas przekazywania spseudonimizowanych danych osobowych stronie trzeciej zgodnie z ust. 1.

Artykuł 28-3 (Ograniczenie łączenia danych spseudonimizowanych) 1) Nie naruszając art. 28-2, łączenie spseudonimizowanych danych osobowych przetwarzanych przez różnych administratorów danych osobowych do celów statystycznych, do celów badań naukowych i do celów archiwalnych w interesie publicznym itp. przeprowadza wyspecjalizowana instytucja wyznaczona przez Komisję Ochrony Danych Osobowych lub kierownik powiązanej centralnej agencji administracyjnej.

2) Administrator danych osobowych, który zamierza udostępnić połączone dane poza organizację, która je połączyła, uzyskuje zgodę kierownika wyspecjalizowanej instytucji po przetworzeniu danych na spseudonimizowane dane osobowe lub na formę, o której mowa w art. 58-2.

3) Niezbędne kwestie, w tym procedury i metody łączenia danych zgodnie z ust. 1, normy i procedury wyznaczania lub unieważniania wyznaczonych organów zarządczych i nadzorczych wyspecjalizowanej instytucji oraz normy i procedury przekazywania i zatwierdzania zgodnie z ust. 2 określono w dekrecie prezydenckim.

Artykuł 28-4 (Obowiązek wprowadzenia środków bezpieczeństwa w odniesieniu do danych spseudonimizowanych) 1) Przetwarzając spseudonimizowane dane osobowe, administrator danych osobowych wprowadza takie środki techniczne, organizacyjne i fizyczne, jak osobne przechowywanie danych i zarządzanie dodatkowymi danymi niezbędnymi do celów przywrócenia do pierwotnego stanu, jakie mogą być konieczne w celu zapewnienia bezpieczeństwa przewidzianego w dekrecie prezydenckim, tak aby dane osobowe nie zostały utracone, skradzione, ujawnione, sfałszowane, zmienione lub zniszczone.

2) Na potrzeby zarządzania przetwarzaniem spseudonimizowanych danych osobowych administrator danych osobowych, który zamierza przetwarzać takie dane, przygotowuje i przechowuje rejestry dotyczące kwestii przewidzianych w dekrecie prezydenckim, w tym dotyczące celu przetwarzania spseudonimizowanych danych osobowych oraz odbiorcy będącego stroną trzecią w przypadku przekazania takich danych.

Artykuł 28-5 (Czyny zabronione w kontekście przetwarzania spseudonimizowanych danych osobowych) 1) Nie można przetwarzać spseudonimizowanych danych osobowych w celu identyfikacji określonej osoby fizycznej.

2) Jeżeli podczas przetwarzania spseudonimizowanych danych osobowych powstaną dane identyfikujące konkretną osobę fizyczną, administrator danych osobowych zaprzestaje przetwarzania tych danych oraz niezwłocznie odzyskuje i niszczy te informacje.

Artykuł 28-6 (Dodatkowe opłaty z tytułu przetwarzania spseudonimizowanych danych osobowych) 1) Komisja może nałożyć grzywnę w kwocie mniejszej niż 3 % całkowitej sprzedaży na administratora danych osobowych, który przetworzył dane do celów identyfikacji określonej osoby fizycznej, naruszając tym samym art. 28-5 ust. 1: pod warunkiem, że w przypadku braku sprzedaży lub trudności w obliczeniu przychodów ze sprzedaży administrator danych osobowych może podlegać grzywnie w kwocie nieprzekraczającej 400 mln wonów lub 3 % kwoty kapitału, w zależności od tego, która z tych kwot będzie wyższa.

2) Art. 34-2 pkt 3–5 stosuje się odpowiednio do kwestii niezbędnych do nałożenia i pobrania dodatkowych opłat administracyjnych.

Artykuł 28-7 (Zakres stosowania) Art. 20, 21, 27, 34 ust. 1, art. 35–37, art. 39-3, 39-4 oraz od art. 39-6 do art. 39-8 nie mają zastosowania do spseudonimizowanych danych osobowych.

Rozdział I Przepisy ogólne

Artykuł 3 (Zasady ochrony danych osobowych) 1) Administrator danych osobowych określa wyraźnie, do jakich celów przetwarzane są dane osobowe; ponadto administrator danych osobowych zbiera dane osobowe uczciwie i zgodnie z prawem, w minimalnym zakresie, jaki jest niezbędny do osiągnięcia tych celów.

2) Administrator danych osobowych przetwarza dane osobowe w odpowiedni sposób niezbędny do osiągnięcia celów, do których dane te są przetwarzane, i nie wykorzystuje ich w sposób wykraczający poza te cele.

3) Administrator danych osobowych zapewnia, aby dane osobowe były prawidłowe, kompletne i aktualne w zakresie niezbędnym do celów, w których dane te są przetwarzane.

4) Administrator danych osobowych zarządza danymi osobowymi w sposób bezpieczny i zgodny z metodami i innymi rodzajami przetwarzania danych osobowych, z uwzględnieniem możliwości naruszenia praw osób, których dane dotyczą, oraz wagi odnośnych zagrożeń.

5) Administrator danych osobowych podaje do wiadomości publicznej swoją politykę prywatności oraz inne kwestie związane z przetwarzaniem danych osobowych; ponadto gwarantuje prawa osoby, której dane dotyczą, takie jak prawo dostępu do swoich danych osobowych.

6) Administrator danych osobowych przetwarza dane osobowe w taki sposób, aby zminimalizować możliwość naruszenia prywatności osoby, której dane dotyczą.

7) Jeżeli nadal istnieje możliwość osiągnięcia celów zbierania danych osobowych poprzez przetwarzanie danych zanonimizowanych lub spseudonimizowanych, administrator danych osobowych podejmuje wszelkie starania, aby przetwarzać dane osobowe, stosując anonimizację, o ile jest to możliwe, lub pseudonimizację, aby osiągnąć cele zbierania danych osobowych z zastosowaniem anonimizacji.

8) Administrator danych osobowych podejmuje starania, aby zyskać zaufanie osób, których dane dotyczą, wykonując zadania i wypełniając obowiązki przewidziane w niniejszej ustawie i innych powiązanych ustawach.

Rozdział IX Przepisy uzupełniające

Artykuł 58-2 (Zwolnienie ze stosowania) Niniejsza ustawa nie ma zastosowania do danych, które nie identyfikują określonej osoby fizycznej w połączeniu z innymi danymi, uwzględniając w sposób zasadny czas, koszty, technologię itp. <Ten artykuł został dodany na mocy ustawy nr 16930 z dnia 4 lutego 2020 r.>

(i) W rozdziale III sekcja 3 „Szczególne przypadki dotyczące danych spseudonimizowanych" (art. 28-2 do 28-7) zezwala się na przetwarzanie informacji spseudonimizowanych bez zgody osoby, której dane dotyczą, do celów statystycznych, do celów badań naukowych i do celów archiwalnych itp. (art. 28-2), jednak w takich przypadkach obowiązkowe jest stosowanie odpowiednich zabezpieczeń i zakazów koniecznych do zapewnienia ochrony praw osób, których dane dotyczą (art. 28-4 i 28-5), a także możliwe jest nałożenie dodatkowych opłat karnych na osoby dopuszczające się naruszeń (art. 28-6); określone zabezpieczenia przewidziane w inny sposób w PIPA nie mają przy tym zastosowania (art. 28-7).

(ii) Przepisy te nie mają zastosowania do przypadków, w których dane spseudonimizowane są przetwarzane do celów innych niż do celów statystycznych, do celów badań naukowych i do celów archiwalnych itp. Na przykład jeżeli dane osobowe osoby fizycznej z UE, które zostały przekazane do Korei zgodnie z decyzją Komisji Europejskiej stwierdzającą odpowiedni stopień ochrony, zostaną spseudonimizowane do celów innych niż do celów statystycznych, do celów badań naukowych i do celów archiwalnych itp., przepisy szczególne zawarte w rozdziale III sekcja 3 nie mają zastosowania ([7]).

(iii) W przypadku gdy administrator danych osobowych przetwarza dane spseudonimizowane do celów statystycznych, do celów badań naukowych i do celów archiwalnych itp. oraz jeżeli dane spseudonimizowane nie zostały zniszczone po osiągnięciu konkretnego celu przetwarzania zgodnie z art. 37 konstytucji i art. 3 („Zasady ochrony danych osobowych") ustawy, przeprowadza on anonimizację danych w celu zapewnienia, aby dane te nie umożliwiały identyfikacji konkretnej osoby fizycznej, samodzielnie ani w połączeniu z innymi danymi, uwzględniając w sposób zasadny czas, koszty, technologię itp. zgodnie z art. 58-2 PIPA.

5. **Inne działania naprawcze (art. 64 pkt 1, 2 i 4 ustawy)**

<Ustawa o ochronie danych osobowych

(ustawa nr 16930, częściowo zmieniona dnia 4 lutego 2020 r.)>

Artykuł 64 (Działania naprawcze) 1) W przypadku gdy Komisja Ochrony Danych Osobowych stwierdzi istnienie istotnych przesłanek do uznania, że doszło do naruszenia w odniesieniu do danych osobowych, a niepodjęcie działań może spowodować trudną do naprawienia szkodę, może nakazać podmiotowi naruszającemu niniejszą ustawę (z wyłączeniem centralnych agencji administracyjnych, organów samorządu terytorialnego, Zgromadzenia Narodowego, sądów powszechnych, Trybunału Konstytucyjnego oraz Krajowej Komisji Wyborczej) podjęcie któregokolwiek z następujących działań:

1. zaprzestanie naruszenia w odniesieniu do danych osobowych;

2. tymczasowe zaprzestanie przetwarzania danych osobowych;

([7]) Podobnie wyjątek z art. 40-3 ustawy o informacjach kredytowych ma zastosowanie wyłącznie do przetwarzania spseudonimizowanych informacji kredytowych do celów statystycznych, do celów badań naukowych i do celów archiwalnych.

3. podjęcie innych działań niezbędnych do ochrony danych osobowych oraz zapobiegania naruszaniu danych osobowych.

2) W przypadku gdy kierownik powiązanej centralnej agencji administracyjnej stwierdzi istnienie istotnych przesłanek do uznania, że doszło do naruszenia w odniesieniu do danych osobowych, a niepodjęcie działań może spowodować trudną do naprawienia szkodę, kierownik ten może nakazać administratorowi danych osobowych podjęcie któregokolwiek z działań przewidzianych w ust. 1 zgodnie z ustawami wchodzącymi w zakres kompetencji takiej powiązanej centralnej agencji administracyjnej.

4) W przypadku naruszenia niniejszej ustawy przez centralną agencję administracyjną, organy samorządu terytorialnego, Zgromadzenie Narodowe, sąd powszechny, Trybunał Konstytucyjny lub Krajową Komisję Wyborczą Komisja Ochrony Danych Osobowych może zalecić kierownikowi odpowiedniej agencji podjęcie któregokolwiek z działań przewidzianych w ust. 1. W takich przypadkach, po otrzymaniu zalecenia, agencja musi się do niego zastosować, o ile nie uniemożliwiają tego nadzwyczajne okoliczności.

(i) Po pierwsze w orzecznictwie precedensowym ([8]) ([9]) „trudną do naprawienia szkodę" interpretuje się jako przypadek, w którym może dojść do wyrządzenia szkody naruszającej prawa osobiste lub prywatność osoby fizycznej.

(ii) W związku z tym „istotne przesłanki do uznania, że doszło do naruszenia w odniesieniu do danych osobowych, a niepodjęcie działań może spowodować trudną do naprawienia szkodę", w rozumieniu art. 64 ust. 1 i 2, dotyczy przypadków, w których uznaje się, że naruszenie prawa może naruszać prawa i wolności osób fizycznych w odniesieniu do danych osobowych. Przepis ten ma zastosowanie w każdym przypadku naruszenia którychkolwiek z zasad, praw i obowiązków przewidzianych w prawie w celu ochrony danych osobowych ([10]).

(iii) Zgodnie z art. 64 ust. 4 ustawy o ochronie danych osobowych istnieje środek odnoszący się do „naruszenia niniejszej ustawy", tj. działanie przeciwko naruszeniu PIPA.

Na przykład centralna agencja administracyjna, jako organ publiczny związany zasadą praworządności, nie może naruszać przepisów prawa i jest zobowiązana do podjęcia działania naprawczego, w tym do natychmiastowego zaprzestania danej czynności, a w wyjątkowym przypadku także do wypłacenia odszkodowania za szkody, jeżeli mimo wszystko doszło do popełnienia czynu niezgodnego z prawem.

W związku z tym nawet bez interwencji ze strony Komisji Ochrony Danych Osobowych podjętej zgodnie z art. 64 ust. 4 PIPA centralna agencja administracyjna musi podjąć działanie naprawcze wobec naruszeń, jeżeli dowie się o jakimkolwiek naruszeniu prawa.

W szczególności w przypadku gdy Komisja Ochrony Danych Osobowych zaleci podjęcie działania naprawczego, dla centralnej agencji administracyjnej będzie z reguły obiektywnie oczywiste, że naruszyła prawo. Oznacza to, że agencja ta musi przedstawić jasne dowody, że nie naruszyła prawa, aby uzasadnić, dlaczego nie powinna ona zastosować się do zalecenia Komisji Ochrony Danych Osobowych. Zastosowanie się do tego zalecenia jest obowiązkowe, chyba że Komisja Ochrony Danych Osobowych stwierdzi, że faktycznie nie doszło do naruszenia prawa.

Z tego powodu „nadzwyczajne okoliczności", o których mowa w art. 64 ust. 4 ustawy o ochronie danych osobowych, muszą się ograniczać wyłącznie do nadzwyczajnych okoliczności, w których centralna agencja administracyjna dysponuje jasnymi dowodami na to, że nie doszło do „naruszenia tego aktu", takimi jak „przypadki, w których wystąpiły nadzwyczajne okoliczności (faktyczne lub prawne)", o których Komisja Ochrony Danych Osobowych nie wiedziała, wydając swoje zalecenie, oraz pod warunkiem stwierdzenia przez tę Komisję, że faktycznie nie doszło do naruszenia.

6. **Stosowanie PIPA do przetwarzania danych osobowych do celów bezpieczeństwa narodowego, w tym na potrzeby postępowania przygotowawczego w sprawie naruszeń i egzekwowania przepisów zgodnie z PIPA (art. 7-8, 7-9, art. 58, art. 3, art. 4 i art. 62 PIPA)**

<Ustawa o ochronie danych osobowych

(ustawa nr 16930, częściowo zmieniona dnia 4 lutego 2020 r.)>

Artykuł 7-8 (Praca Komisji Ochrony Danych Osobowych) 1) Komisja Ochrony Danych Osobowych zajmuje się: […]

3. kwestiami dotyczącymi postępowania przygotowawczego w sprawie naruszenia prawa osób, których dane dotyczą, oraz powiązanych decyzji;

4. rozpatrywaniem skarg lub prowadzeniem postępowań naprawczych związanych z przetwarzaniem danych osobowych, a także mediacjami w sporach dotyczących danych osobowych;

[…]

([8]) (Orzeczenie Sądu Najwyższego 97Da10215,10222 z dnia 26 stycznia 1999 r.) Ujawnienie za pośrednictwem mediów okoliczności faktycznych w sprawie karnej dotyczących oskarżonego może spowodować niemożliwą do naprawienia szkodę wywołującą negatywne skutki dla cielesnej i psychicznej kondycji nie tylko pokrzywdzonego, tj. powoda, ale także osób w jego otoczeniu, w tym rodzin.

([9]) (Orzeczenie Sądu Apelacyjnego w Seulu nr 2006Na92006 z dnia 16 stycznia 2008 r.) Publikacja szkalującego artykułu może wyrządzić poważną, niemożliwą do naprawienia szkodę na osobie.

([10]) Te same zasady, które określono w pkt (ii), mają zastosowanie do art. 45-4 ustawy o informacjach kredytowych.

Artykuł 7-9 (Kwestie podlegające rozpatrzeniu i rozwiązaniu przez Komisję Ochrony Danych Osobowych) 1) Komisja Ochrony Danych Osobowych rozpatruje i rozwiązuje następujące kwestie: […]

5. kwestie dotyczące wykładni i funkcjonowania prawa związanego z ochroną danych osobowych;

[…]

Artykuł 58 (Częściowe wyłączenie stosowania) 1) Rozdziały III–VII nie mają zastosowania do następujących danych osobowych:

1. danych osobowych zbieranych zgodnie z ustawą o danych statystycznych do celów przetwarzania przez instytucje publiczne;
2. danych osobowych zbieranych lub żądanych do celów przeprowadzenia analizy informacji związanych z bezpieczeństwem narodowym;
3. danych osobowych przetwarzanych tymczasowo, jeżeli jest to pilnie potrzebne ze względów bezpieczeństwa publicznego i ochrony, w tym zdrowia publicznego;
4. danych osobowych zbieranych lub wykorzystywanych przez prasę do jej własnych celów reporterskich, do działalności misyjnej prowadzonej przez organizacje religijne lub do celów nominacji kandydatów przez partie polityczne.

[Ustępy 2 i 3 pominięto.]

4) W przypadku przetwarzania danych osobowych zgodnie z ust. 1, administrator danych osobowych przetwarza dane osobowe w minimalnym zakresie niezbędnym do osiągnięcia zamierzonego celu oraz przez możliwie najkrótszy okres; ponadto administrator danych osobowych podejmuje wszelkie niezbędne kroki, takie jak wdrożenie zabezpieczeń technicznych, zarządczych i fizycznych, rozpatrywanie indywidualnych zażaleń i inne niezbędne działania do celów bezpiecznego zarządzania takimi danymi osobowymi oraz ich odpowiedniego przetwarzania.

Artykuł 3 (Zasady ochrony danych osobowych) 1) Administrator danych osobowych określa wyraźnie, do jakich celów przetwarzane są dane osobowe; ponadto administrator danych osobowych zbiera dane osobowe uczciwie i zgodnie z prawem, w minimalnym zakresie, jaki jest niezbędny do osiągnięcia tych celów.

2) Administrator danych osobowych przetwarza dane osobowe w odpowiedni sposób niezbędny do osiągnięcia celów, do których dane te są przetwarzane, i nie wykorzystuje ich w sposób wykraczający poza te cele.

3) Administrator danych osobowych zapewnia, aby dane osobowe były prawidłowe, kompletne i aktualne w zakresie niezbędnym do celów, w których dane te są przetwarzane.

4) Administrator danych osobowych zarządza danymi osobowymi w sposób bezpieczny i zgodny z metodami i innymi rodzajami przetwarzania danych osobowych, z uwzględnieniem możliwości naruszenia praw osób, których dane dotyczą, oraz wagi odnośnych zagrożeń.

5) Administrator danych osobowych podaje do wiadomości publicznej swoją politykę prywatności oraz inne kwestie związane z przetwarzaniem danych osobowych; ponadto gwarantuje prawa osoby, której dane dotyczą, takie jak prawo dostępu do swoich danych osobowych.

6) Administrator danych osobowych przetwarza dane osobowe w taki sposób, aby zminimalizować możliwość naruszenia prywatności osoby, której dane dotyczą.

7) Jeżeli nadal istnieje możliwość osiągnięcia celów zbierania danych osobowych poprzez przetwarzanie danych zanonimizowanych lub spseudonimizowanych, administrator danych osobowych podejmuje wszelkie starania, aby przetwarzać dane osobowe, stosując anonimizację, o ile jest to możliwe, lub pseudonimizację, aby osiągnąć cele zbierania danych osobowych z zastosowaniem anonimizacji.

8) Administrator danych osobowych podejmuje starania, aby zyskać zaufanie osób, których dane dotyczą, wykonując zadania i wypełniając obowiązki przewidziane w niniejszej ustawie i innych powiązanych ustawach.

Artykuł 4 (Prawa osób, których dane dotyczą) Osobie, której dotyczą dane, przysługują następujące prawa w odniesieniu do przetwarzania jej własnych danych osobowych:

1. prawo do poinformowania o przetwarzaniu takich danych osobowych;
2. prawo do wyrażenia lub niewyrażenia zgody oraz określenia zakresu zgody na przetwarzanie takich danych osobowych;
3. prawo do potwierdzenia, czy dane osobowe są przetwarzane, oraz do zażądania dostępu (w tym przekazania kopii; stosuje się odpowiednio w dalszej części) do takich danych osobowych;
4. prawo do zawieszenia przetwarzania takich danych osobowych, a także do żądania ich korekty, usunięcia i zniszczenia;
5. Prawo do odpowiedniego środka dochodzenia roszczeń, w drodze szybkiej i uczciwej procedury, z tytułu wszelkich szkód wynikających z przetwarzania takich danych osobowych.

Artykuł 62 (Zgłaszanie naruszeń) 1) Osoba, której prawa lub interesy zostaną naruszone w odniesieniu do jej danych osobowych w wyniku przetwarzania danych osobowych przez administratora danych osobowych, może zgłosić takie naruszenia Komisji Ochrony Danych Osobowych.

2) Komisja Ochrony Danych Osobowych może wyznaczyć wyspecjalizowaną instytucję, której zadaniem będzie przyjmowanie i rozpatrywanie zgłoszeń ze skargami zgodnie z ust. 1, jak przewidziano w dekrecie prezydenckim. W takich przypadkach wspomniana wyspecjalizowana instytucja ustanawia i prowadzi centrum informacji na temat naruszeń danych osobowych (zwane dalej „centrum telefonicznym ds. prywatności").

3) Centrum informacji na temat prywatności ma następujące zadania:

1. przyjmuje zgłoszenia ze skargami i udziela konsultacji w zakresie przetwarzania danych osobowych;

2. bada i potwierdza incydenty oraz wysłuchuje opinii powiązanych stron;

3. realizuje zadania powiązane z zadaniami określonymi w pkt 1 i 2.

4) Komisja Ochrony Danych Osobowych może w razie potrzeby oddelegować swojego urzędnika publicznego do wyspecjalizowanej instytucji wyznaczonej na podstawie ust. 2 zgodnie z art. 32-4 ustawy o państwowych urzędnikach publicznych, aby efektywnie zbadać i potwierdzać incydenty, o których mowa w ust. 3 pkt 2.

(i) Zbieranie danych osobowych do celów bezpieczeństwa narodowego regulują ustawy szczególne, które nadają właściwym organom (np. Narodowej Służbie Wywiadu) uprawnienia do przechwytywania informacji lub żądania ich ujawnienia na określonych warunkach i przy zapewnieniu określonych zabezpieczeń (zwane dalej „przepisami dotyczącymi bezpieczeństwa narodowego"). Wspomniane przepisy dotyczące bezpieczeństwa narodowego obejmują na przykład ustawę o ochronie prywatności komunikacji, ustawę o zwalczaniu terroryzmu do celów ochrony obywateli i bezpieczeństwa publicznego lub ustawę o działalności telekomunikacyjnej. Ponadto zbieranie i dalsze przetwarzanie danych osobowych musi być zgodne z wymogami PIPA. Pod tym względem art. 58 ust. 1 pkt 2 PIPA stanowi, że rozdziały III–VII nie mają zastosowania do danych osobowych zbieranych lub żądanych do celów przeprowadzenia analizy informacji związanych z bezpieczeństwem narodowym. Dlatego też ten częściowy wyjątek ma zastosowanie do przetwarzania danych osobowych do celów bezpieczeństwa narodowego.

Jednocześnie rozdział I (Przepisy ogólne), rozdział II (Ustanowienie polityki ochrony danych osobowych itp.), rozdział VIII (Powództwo zbiorowe w sprawie naruszenia przepisów o ochronie danych), rozdział IX (Przepisy uzupełniające) oraz rozdział X (Przepisy dotyczące kar) PIPA mają zastosowanie do przetwarzania takich danych osobowych. Odnosi się to do ogólnych zasad ochrony danych określonych w art. 3 (Zasady ochrony danych osobowych) oraz praw indywidualnych zagwarantowanych w art. 4 PIPA (Prawa osób, których dane dotyczą).

Ponadto art. 58 ust. 4 PIPA stanowi, że informacje takie należy przetwarzać w minimalnym zakresie wymaganym do osiągnięcia zamierzonego celu oraz przez możliwie najkrótszy okres; w przepisie tym wymaga się także wprowadzenia przez administratora danych osobowych środków niezbędnych do zapewnienia bezpiecznego zarządzania danymi i właściwego przetwarzania, takich jak zabezpieczenia techniczne, zarządcze i fizyczne, jak również środków służących odpowiedniemu rozpatrywaniu indywidualnych skarg.

Ponadto zastosowanie mają przepisy regulujące obowiązki i uprawnienia PIPC (w tym art. 60–65 PIPA w sprawie rozpatrywania skarg oraz przyjmowania zaleceń i działań naprawczych), jak również przepisy w sprawie administracyjnych kar pieniężnych i sankcji karnych (art. 70 i nast. PIPA). Zgodnie z art. 7-8 ust. 1 pkt 3 i 4 oraz art. 7-9 ust. 1 pkt 5 PIPA te uprawnienia dochodzeniowe i naprawcze, również wówczas, gdy są wykonywane w kontekście rozpatrywania skarg, obejmują także ewentualne naruszenia przepisów ustaw szczególnych ustanawiających ograniczenia i zabezpieczenia w odniesieniu do zbierania danych osobowych, takich jak ustawy dotyczące bezpieczeństwa narodowego. Biorąc pod uwagę wymogi przewidziane w art. 3 ust. 1 PIPA dotyczące zgodnego z prawem i rzetelnego zbierania danych osobowych, każde takie naruszenie stanowi naruszenie „niniejszej ustawy" w rozumieniu art. 63 i 64, co pozwala PIPC na przeprowadzenie dochodzenia i podjęcie działań naprawczych ([11]). Wykonywanie tych uprawnień przez PIPC uzupełnia uprawnienia Krajowej Komisji Praw Człowieka przewidziane w ustawie o Komisji Praw Człowieka, ale ich nie zastępuje.

Stosowanie podstawowych zasad, praw i obowiązków wynikających z PIPA do przetwarzania danych osobowych do celów bezpieczeństwa narodowego odzwierciedla gwarancje zapisane w konstytucji odnoszące się do ochrony prawa osoby fizycznej do kontrolowania własnych danych osobowych. Jak uznał Trybunał Konstytucyjny, obejmuje to prawo osoby fizycznej ([12]) „do osobistego decydowania o tym, kiedy, komu lub przez kogo oraz w jakim zakresie będą ujawniane lub wykorzystywane jej dane osobiste. Jest to prawo podstawowe ([13]), [...] istniejące w celu ochrony osobistej wolności podejmowania decyzji przed zagrożeniami wynikającymi z rozszerzenia funkcji państwa i rozwoju technologii informacyjno-komunikacyjnych". Wszelkie ograniczenia tego prawa, np. jeśli są niezbędne do zapewnienia ochrony bezpieczeństwa narodowego, wymagają wyważenia praw i interesów osoby fizycznej względem istotnego interesu publicznego i nie mogą naruszać istoty tego prawa (art. 37 ust. 2 konstytucji).

([11]) Więcej informacji na temat działań naprawczych zgodnych z art. 64 można znaleźć w pkt 5 powyżej.
([12]) Wyrok Trybunału Konstytucyjnego, 99HunMa513, 2004HunMa190, z dnia 26 maja 2005 r.
([13]) Wyrok Trybunału Konstytucyjnego, 2003HunMa282, z dnia 21 lipca 2005 r.

W związku z tym, przetwarzając dane osobowe do celów bezpieczeństwa narodowego, administrator (np. NIS) m. in.:

1) określa wyraźnie cele przetwarzania danych osobowych i zbiera dane osobowe uczciwie i zgodnie z prawem, w minimalnym zakresie, jaki jest niezbędny do osiągnięcia tych celów (art. 3 ust. 1 PIPA); w szczególności administrator zbiera i przetwarza dalej dane osobowe na potrzeby wywiązania się z obowiązków przewidzianych w odpowiednich ustawach, takich jak ustawa o Narodowej Służbie Wywiadu;

2) przetwarza dane osobowe w minimalnym zakresie i przez możliwie najkrótszy okres, jakie są niezbędne do osiągnięcia zamierzonego celu (art. 58 ust. 4 PIPA); po osiągnięciu celu przetwarzania administrator nieodwracalnie niszczy dane osobowe, chyba że w stosownym akcie prawnym przewidziano w sposób szczególny ich dalsze zatrzymywanie, w którym to przypadku odnośne dane osobowe są przechowywane i zarządzane osobno od innych danych osobowych, nie mogą być wykorzystywane do innego celu niż cel przewidziany we wspomnianym akcie prawnym, a po upływie okresu zatrzymywania muszą zostać zniszczone;

3) przetwarza dane osobowe w odpowiedni sposób niezbędny do osiągnięcia celów, do których dane te są przetwarzane, i nie wykorzystuje ich w sposób wykraczający poza te cele (art. 3 ust. 2 PIPA);

4) zapewnia, aby dane osobowe były prawidłowe, kompletne i aktualne w zakresie niezbędnym do celów, w których dane te są przetwarzane (art. 3 ust. 3 PIPA);

5) zarządza danymi osobowymi w sposób bezpieczny i zgodny m.in. z metodami i rodzajami przetwarzania danych osobowych, z uwzględnieniem możliwości naruszenia praw osób, których dane dotyczą, oraz wagi odnośnych zagrożeń (art. 3 ust. 4 PIPA);

6) podaje do wiadomości publicznej swoją politykę prywatności oraz inne kwestie związane z przetwarzaniem danych osobowych (art. 3 ust. 5 PIPA);

7) przetwarza dane osobowe w taki sposób, aby zminimalizować możliwość naruszenia prywatności osoby, której dane dotyczą (art. 3 ust. 6 PIPA).

(ii) Zgodnie z art. 58 ust. 4 PIPA administrator (np. organy posiadające kompetencje w zakresie bezpieczeństwa narodowego, takie jak NIS) podejmuje wszelkie niezbędne kroki, takie jak wdrożenie zabezpieczeń technicznych, zarządczych i fizycznych, aby zapewnić zgodność z tymi zasadami oraz odpowiednie przetwarzanie danych osobowych. Może to obejmować np. szczególne działania mające na celu zapewnienie bezpieczeństwa danych osobowych, takie jak ograniczenia dostępu do danych osobowych, kontrola dostępu, logi, zapewnianie pracownikom dedykowanych szkoleń w zakresie m.in. obchodzenia się z danymi osobowymi.

Ponadto, zgodnie z art. 3 ust. 5 i ust. 4 PIPA, osoby, których dane dotyczą, mają m.in. następujące prawa w odniesieniu do danych osobowych przetwarzanych do celów bezpieczeństwa narodowego:

1) prawo do uzyskania potwierdzenia, czy ich dane osobowe są przetwarzane, jak również do uzyskania informacji na temat ich przetwarzania oraz dostępu do tych danych, w tym prawo do przekazania kopii (art. 4 ust. 1 i 3 PIPA);

2) prawo do zawieszenia przetwarzania oraz do korekty, usunięcia i zniszczenia danych osobowych (art. 4 ust. 4 PIPA).

(iii) W celu skorzystania z tych praw osoba, której dane dotyczą, może złożyć wniosek bezpośrednio do administratora lub za pośrednictwem Komisji Ochrony Danych Osobowych, a także może upoważnić swojego przedstawiciela do złożenia takiego wniosku. W przypadku złożenia wniosku przez osobę, której dane dotyczą, administrator przyznaje stosowne prawo bezzwłocznie; administrator może jednak opóźnić przyznanie takiego prawa, ograniczyć je lub odmówić jego przyznania, jeżeli jest to określone szczegółowo w innych ustawach lub niezbędne do zapewnienia zgodności z takimi ustawami tak długo oraz w takim zakresie, w jakim jest to konieczne i proporcjonalne do ochrony ważnego celu leżącego w interesie publicznym (na przykład tak długo oraz w takim zakresie, w jakim przyznanie tego prawa stanowiłoby zagrożenie dla trwającego postępowania przygotowawczego lub bezpieczeństwa narodowego), lub w przypadku gdy przyznanie tego prawa może spowodować szkodę dla życia lub integralności cielesnej strony trzeciej lub nieuzasadnione naruszenie interesów majątkowych i innych interesów strony trzeciej. W przypadku odrzucenia lub ograniczenia wniosku administrator bezzwłocznie zawiadamia osobę, której dane dotyczą, o powodach takiego odrzucenia lub ograniczenia. Administrator opracowuje metodę i procedurę, aby umożliwić osobom, których dane dotyczą, składanie wniosków oraz podawania informacji na temat tych wniosków do wiadomości osób, których dane dotyczą.

Ponadto zgodnie z art. 58 ust. 4 PIPA (wymóg zapewnienia właściwego rozpatrywania skarg indywidualnych) oraz art. 4 ust. 5 PIPA (prawo do odpowiedniego środka dochodzenia roszczeń, w drodze szybkiej i sprawiedliwej procedury, z tytułu wszelkich szkód wynikających z przetwarzania danych osobowych) osoby, których dane dotyczą, mają prawo do dochodzenia roszczeń. Obejmuje to prawo do zgłoszenia domniemanego naruszenia do centrum zgłaszania naruszeń danych osobowych (zgodnie z art. 62 ust. 3 PIPA), wniesienia skargi do PIPC na podstawie art. 62 PIPA w sprawie jakiegokolwiek naruszenia praw lub interesów dotyczących danych osobowych osoby fizycznej oraz do zaskarżenia decyzji lub bezczynności PIPC do sądu na podstawie ustawy o postępowaniu administracyjnosądowym. Ponadto osoby, których dane dotyczą, mogą dochodzić roszczeń na drodze sądowej na mocy ustawy o postępowaniu administracyjnosądowym, jeżeli ich prawa lub interesy zostały naruszone w wyniku decyzji administratora lub zaniechania z jego strony (np. bezprawne zbieranie danych osobowych), lub uzyskać odszkodowanie na podstawie ustawy o odszkodowaniach od państwa. Te drogi dochodzenia roszczeń są dostępne zarówno w przypadku ewentualnych naruszeń przepisów ujętych w ustawach szczególnych określających ograniczenia i zabezpieczenia w odniesieniu do zbierania danych osobowych, takich jak naruszenia przepisów dotyczących bezpieczeństwa narodowego, jak i naruszenia PIPA.

Osoba fizyczna z UE może wnieść skargę do PIPC za pośrednictwem swojego krajowego organu ochrony danych, a PIPC powiadomi tę osobę fizyczną za pośrednictwem jej krajowego organu ochrony danych o zakończeniu dochodzenia i, w stosownych przypadkach, o zastosowanych działaniach naprawczych.

ZAŁĄCZNIK II

18 maja 2021 r.

Jego Ekscelencja Didier Reynders, komisarz do spraw wymiaru sprawiedliwości Komisji Europejskiej

Szanowny Panie Komisarzu!

Z zadowoleniem przyjmuję konstruktywną dyskusję między Koreą a Komisją Europejską w celu stworzenia ram przekazywania danych osobowych między UE a Koreą.

Na wniosek Komisji Europejskiej skierowany do rządu Korei przesyłam w załączeniu dokument zawierający przegląd ram prawnych dotyczących dostępu rządu Korei do informacji.

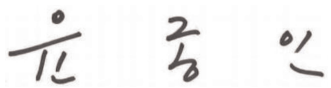
Niniejszy dokument dotyczy wielu koreańskich ministerstw i agencji rządowych; jeżeli chodzi o treść dokumentu, właściwe ministerstwa i agencje (Komisja Ochrony Danych Osobowych, Ministerstwo Sprawiedliwości, Narodowa Służba Wywiadu, Krajowa Komisja Praw Człowieka Korei, Krajowe Centrum Zwalczania Terroryzmu, koreańska jednostka analityki finansowej) odpowiadają za poszczególne obszary wchodzące w zakres ich kompetencji. Właściwe ministerstwa i agencje oraz osoby, które podpisały w ich imieniu dokument, wymieniono poniżej.

Komisja Ochrony Informacji Osobowych przyjmuje wszelkie zapytania dotyczące tego dokumentu oraz będzie koordynować niezbędne odpowiedzi właściwych ministerstw i agencji.

Mam nadzieję, że dokument ten pomoże Komisji Europejskiej w podjęciu decyzji.

Doceniam Pana wielki wkład w tę problematykę.

Z wyrazami szacunku

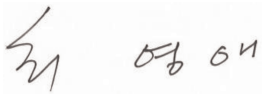


Yoon Jong In
Przewodniczący Komisji Ochrony Danych Osobowych

Niniejszy dokument został sporządzony przez Komisję Ochrony Danych Osobowych oraz następujące zainteresowane ministerstwa i agencje.

Park Jie Won
Prezes (dyrektor), Narodowa Służba Wywiadu

Lee Jung Soo
Dyrektor Generalny, Ministerstwo Sprawiedliwości



Choi Young Ae
Przewodniczący, Krajowa Komisja Praw Człowieka Korei

Kim Hyuck Soo
Dyrektor, Krajowe Centrum Zwalczania Terroryzmu

Kim, Jeong Kag
Komisarz, koreańska jednostka analityki finansowej

Ramy zbierania i wykorzystywania danych osobowych przez koreańskie organy publiczne do celów ścigania przestępstw i do celów dotyczących bezpieczeństwa narodowego

Poniższy dokument zawiera przegląd ram prawnych w zakresie zbierania i wykorzystywania danych osobowych przez koreańskie organy publiczne do celów ścigania przestępstw i do celów bezpieczeństwa narodowego (które to zbieranie i wykorzystywanie danych zwane jest dalej „dostępem rządowym"), w szczególności w odniesieniu do dostępnych podstaw prawnych, obowiązujących warunków (ograniczeń) i zabezpieczeń, a także niezależnego nadzoru i możliwości indywidualnego dochodzenia roszczeń.

1. OGÓLNE ZASADY PRAWNE REGULUJĄCE DOSTĘP RZĄDOWY

1.1. Ramy konstytucyjne

Konstytucja Republiki Korei określa ogólne prawo do prywatności (art. 17) oraz szczególne prawo do prywatności korespondencji (art. 18). Zagwarantowanie tych praw podstawowych jest obowiązkiem państwa ([1]). Ponadto konstytucja stanowi, że prawa i wolności obywateli mogą zostać ograniczone przez prawo wyłącznie wówczas, gdy jest to konieczne ze względów bezpieczeństwa narodowego lub utrzymania porządku publicznego leżącego w interesie publicznym ([2]). Nawet jeżeli takie ograniczenia są nakładane, nie mogą one naruszać istoty wolności ani prawa ([3]). Sądy koreańskie stosowały te przepisy w sprawach dotyczących ingerencji rządu w prywatność. Na przykład Sąd Najwyższy uznał, że monitorowanie osób cywilnych narusza prawo podstawowe – prawo do prywatności – podkreślając, że obywatele mają „prawo do samostanowienia w zakresie danych osobowych" ([4]). W innej sprawie Trybunał Konstytucyjny orzekł, że prywatność jest prawem podstawowym, które zapewnia ochronę przed ingerencją państwa w prywatne życie obywateli i jego obserwacją przez państwo ([5]).

Konstytucja Korei zapewnia ponadto, że nikt nie może zostać aresztowany, zatrzymany, przeszukany, przesłuchany lub że nikomu nie można zająć przedmiotów, z wyjątkiem przypadków przewidzianych w ustawie ([6]). Ponadto przeszukań i zajęć można dokonać wyłącznie na podstawie nakazu wydanego przez sędziego na wniosek prokuratora i z poszanowaniem sprawiedliwości proceduralnej ([7]). W wyjątkowych okolicznościach, tj. jeżeli osoba podejrzana o popełnienie przestępstwa została ujęta podczas popełniania przestępstwa (*flagrante delicto*) lub jeżeli istnieje ryzyko, że osoba podejrzana o popełnienie przestępstwa zagrożonego karą pozbawienia wolności w wymiarze co najmniej trzech lat może zbiec lub zniszczyć dowody, organy śledcze mogą dokonać przeszukania lub zajęcia bez nakazu, w którym to przypadku muszą wystąpić o nakaz *ex post* ([8]). Te ogólne zasady zostały szerzej omówione w ustawach szczegółowych dotyczących postępowania karnego i ochrony komunikacji (zob. dokładny przegląd poniżej).

Jeżeli chodzi o cudzoziemców, konstytucja stanowi, że ich status jest zagwarantowany zgodnie z przepisami prawa międzynarodowego i postanowieniami traktatów ([9]). Kilka umów międzynarodowych, których Korea jest stroną, takich jak Międzynarodowy pakt praw obywatelskich i politycznych (art. 17), Konwencja o prawach osób niepełnosprawnych (art. 22) oraz Konwencja o prawach dziecka (art. 16), zapewnia prawo do prywatności. Co więcej, chociaż co do zasady konstytucja odnosi się do praw „obywateli", Trybunał Konstytucyjny orzekł, że prawa podstawowe przysługują również cudzoziemcom ([10]). W szczególności Trybunał stwierdził, że ochrona godności i wartości osoby jako istoty ludzkiej, jak

([1]) Art. 10 konstytucji Republiki Korei ogłoszonej w dniu 17 lipca 1948 r. (zwanej dalej „konstytucją").
([2]) Art. 37 ust. 2 konstytucji.
([3]) Art. 37 ust. 2 konstytucji.
([4]) Orzeczenie Sądu Najwyższego Korei nr 96DA42789 z dnia 24 lipca 1998 r.
([5]) Orzeczenie Trybunału Konstytucyjnego nr 2002Hun-Ma51 z dnia 30 października 2003 r. Podobnie w orzeczeniu 99Hun-Ma513 i 2004Hun-Ma190 (wersja skonsolidowana) z dnia 26 maja 2005 r. Trybunał Konstytucyjny wyjaśnił, że „prawo do kontrolowania własnych danych osobowych jest prawem osoby, której dane dotyczą, do osobistego decydowania o tym, kiedy, komu, przez kogo i w jakim zakresie informacje o niej zostaną ujawnione lub kiedy, do czyich celów, przez kogo i w jakim zakresie zostaną wykorzystane. Jest to prawo podstawowe, chociaż nie zostało określone w konstytucji, istniejące w celu ochrony osobistej wolności podejmowania decyzji przed zagrożeniami wynikającymi z rozszerzenia funkcji państwa i rozwoju technologii informacyjno-komunikacyjnych".
([6]) Art. 12 ust. 1 zdanie pierwsze konstytucji.
([7]) Art. 16 i art. 12 ust. 3 konstytucji.
([8]) Art. 12 ust. 3 konstytucji.
([9]) Art. 6 ust. 2 konstytucji.
([10]) Orzeczenie Trybunału Konstytucyjnego nr 93Hun-MA120 z dnia 29 grudnia 1994 r. Zob. również np. orzeczenie Trybunału Konstytucyjnego nr 2014Hun-Ma346 (z dnia 31 maja 2018 r.), w którym Trybunał stwierdził, że konstytucyjne prawo obywatela Sudanu przetrzymywanego na lotnisku w celu uzyskania pomocy prawnej zostało naruszone. W innej sprawie Trybunał Konstytucyjny uznał, że swoboda wyboru legalnego miejsca pracy jest ściśle związana z prawem do poszukiwania szczęścia oraz godności i wartości człowieka, a zatem nie jest zastrzeżona wyłącznie dla obywateli, ale może być zapewniona również cudzoziemcom legalnie zatrudnionym w Republice Korei (orzeczenie Trybunału Konstytucyjnego nr 2007Hun-Ma1083 z dnia 29 września 2011 r.).

również prawo do dążenia do szczęścia są prawami każdej istoty ludzkiej, a nie tylko obywateli ([11]). Ponadto Trybunał wyjaśnił, że prawo do kontrolowania informacji o sobie jest uznawane za prawo podstawowe, wywodzące się z prawa do godności i poszukiwania szczęścia oraz prawa do życia prywatnego ([12]). Mimo że orzecznictwo dotychczas nie odnosiło się konkretnie do prawa do prywatności osób niebędących obywatelami Korei, wśród naukowców powszechnie przyjmuje się, że art. 12–22 konstytucji (które obejmują prawo do prywatności oraz wolność osobistą) określają „prawa istoty ludzkiej".

Ponadto konstytucja przewiduje także prawo dochodzenia sprawiedliwego odszkodowania od organów publicznych ([13]). Co więcej, zgodnie z ustawą o Trybunale Konstytucyjnym, każda osoba, której prawa podstawowe zagwarantowane w konstytucji zostały naruszone w wyniku wykonywania władzy państwowej (z wyłączeniem orzeczeń sądów), może wnieść skargę konstytucyjną do Trybunału Konstytucyjnego ([14]).

1.2. **Ogólne przepisy o ochronie danych**

Ogólna ustawa o ochronie danych w Republice Korei, ustawa o ochronie danych osobowych (zwana dalej „PIPA", od ang. Personal Information Protection Act), ma zastosowanie zarówno do sektora prywatnego, jak i do sektora publicznego. Jeżeli chodzi o organy publiczne, w PIPA odniesiono się w szczególności do obowiązku kształtowania polityki w celu zapobiegania „nadużywaniu i niewłaściwemu wykorzystywaniu danych osobowych, jawnemu nadzorowi i śledzeniu itp. oraz wzmocnienia godności istot ludzkich i prywatności osób fizycznych" ([15]).

Przetwarzanie danych osobowych do celów ścigania przestępstw podlega wszystkim wymogom przewidzianym w PIPA. Oznacza to na przykład, że organy ścigania muszą przestrzegać obowiązków dotyczących przetwarzania danych zgodnie z prawem, tj. stosować jedną z podstaw prawnych wymienionych w PIPA w odniesieniu do zbierania, wykorzystywania lub przekazywania danych osobowych (art. 15–18 PIPA), jak również zasady ograniczenia celu (art. 3 ust. 1, 2 PIPA), proporcjonalności/minimalizacji danych (art. 3 ust. 1 i 6 PIPA), ograniczonego zatrzymywania danych (art. 21 PIPA), bezpieczeństwa danych, w tym powiadamiania o naruszeniu ochrony danych (art. 3 ust. 4, art. 29 i 34 PIPA) oraz przejrzystości (art. 3 ust. 1 i 5, art. 20, 30 i 32 PIPA). Do informacji szczególnie chronionych mają zastosowanie szczególne zabezpieczenia (art. 23 PIPA). Ponadto zgodnie z art. 3 ust. 5 i art. 4 PIPA oraz art. od 35 do 39-2 PIPA osoby fizyczne mogą wykonywać swoje prawa w zakresie dostępu, korekty, usunięcia i zawieszenia wobec organów ścigania.

Chociaż PIPA jest w związku z tym w pełni stosowana do przetwarzania danych osobowych do celów ścigania przestępstw, to przewiduje ona wyjątek, gdy dane osobowe są przetwarzane do celów bezpieczeństwa narodowego. Zgodnie z art. 58 ust. 1 pkt 2 PIPA art. 15–50 PIPA nie mają zastosowania do danych osobowych zbieranych lub żądanych do celów przeprowadzenia analizy informacji związanych z bezpieczeństwem narodowym ([16]). Natomiast rozdział I (Przepisy ogólne), rozdział II (Ustanowienie polityki ochrony danych osobowych itp.), rozdział VIII (Powództwo zbiorowe w sprawie naruszenia przepisów o ochronie danych), rozdział IX (Przepisy uzupełniające) oraz rozdział X (Przepisy dotyczące kar) ustawy PIPA nadal mają zastosowanie. Odnosi się to do ogólnych zasad ochrony danych określonych w art. 3 (Zasady ochrony danych osobowych) oraz praw indywidualnych zagwarantowanych w art. 4 PIPA (Prawa osób, których dane dotyczą). Oznacza to, że główne zasady i prawa są zapewnione również w tym obszarze. Ponadto art. 58 ust. 4 PIPA stanowi, że informacje takie należy przetwarzać w minimalnym zakresie wymaganym do osiągnięcia zamierzonego celu oraz przez możliwie najkrótszy okres; w przepisie tym wymaga się także wprowadzenia przez administratora danych osobowych środków niezbędnych do zapewnienia bezpiecznego zarządzania danymi i właściwego przetwarzania, takich jak zabezpieczenia techniczne, zarządcze i fizyczne, jak również środków służących odpowiedniemu rozpatrywaniu indywidualnych skarg.

W zawiadomieniu nr 2021-1 w sprawie przepisów uzupełniających dotyczących wykładni i stosowania ustawy o ochronie danych osobowych Komisja Ochrony Danych Osobowych (zwana dalej „PIPC", od ang. Personal Information Protection Commission) sprecyzowała, w jaki sposób PIPA ma zastosowanie do przetwarzania danych osobowych do celów bezpieczeństwa narodowego w świetle wspomnianego częściowego wyłączenia ([17]). Dotyczy to w szczególności praw osób fizycznych (do dostępu, sprostowania, zawieszenia i usunięcia) oraz podstaw i granic ich ewentualnego ograniczenia. Zgodnie z powiadomieniem stosowanie podstawowych zasad, praw i obowiązków wynikających z PIPA do przetwarzania danych osobowych do celów bezpieczeństwa narodowego odzwierciedla gwarancje przewidziane

([11]) Orzeczenie Trybunału Konstytucyjnego nr 99HeonMa494 z dnia 29 listopada 2001 r.
([12]) Zob. na przykład orzeczenie Trybunału Konstytucyjnego nr 99HunMa513.
([13]) Art. 29 ust. 1 konstytucji.
([14]) Art. 68 ust. 1 ustawy o Trybunale Konstytucyjnym.
([15]) Art. 5 ust. 1 PIPA.
([16]) Art. 58 ust. 1 pkt 2 PIPA.
([17]) Zawiadomienie nr 2021-1 PIPC w sprawie przepisów uzupełniających dotyczących wykładni i stosowania ustawy o ochronie danych osobowych, sekcja III pkt 6.

w konstytucji odnoszące się do ochrony prawa osoby fizycznej do kontrolowania własnych danych osobowych. Wszelkie ograniczenia tego prawa, np. jeśli są niezbędne do zapewnienia ochrony bezpieczeństwa narodowego, wymagają wyważenia praw i interesów osoby fizycznej względem istotnego interesu publicznego i nie mogą naruszać istoty tego prawa (art. 37 ust. 2 konstytucji).

2. DOSTĘP RZĄDOWY DO CELÓW ŚCIGANIA PRZESTĘPSTW

2.1. Właściwe organy publiczne w obszarze ścigania przestępstw

Na podstawie ustawy o postępowaniu karnym (zwanej dalej „CPA", od ang. Criminal Procedure Act), ustawy o ochronie prywatności komunikacji (zwanej dalej „CPPA", od ang. Communications Privacy Protection Act) oraz ustawy o działalności telekomunikacyjnej (zwanej dalej „TBA", od ang. Telecommunications Business Act) policja, prokuratura i sądy mogą zbierać dane osobowe do celów ścigania przestępstw. W zakresie, w jakim w ustawie o Narodowej Służbie Wywiadu nadano te uprawnienia także Narodowej Służbie Wywiadu (zwanej dalej „NIS", od ang. National Intelligence Service), musi ona przestrzegać wyżej wymienionych ustaw ([18]). Ponadto ustawa o zgłaszaniu i wykorzystywaniu określonych informacji o transakcjach finansowych (ang. Act on Reporting and Using Specified Financial Transaction Information, zwana dalej „ARUSFTI") zapewnia instytucjom finansowym podstawę prawną do ujawniania informacji koreańskiej jednostce analityki finansowej (ang. Korea Financial Intelligence Unit, zwana dalej „KOFIU") w celu zapobiegania praniu pieniędzy i finansowaniu terroryzmu. Ta wyspecjalizowana agencja może z kolei udostępnić takie informacje organom ścigania. Te obowiązki w zakresie ujawniania informacji mają jednak zastosowanie wyłącznie do administratorów danych przetwarzających informacje dotyczące kredytów osobistych na podstawie ustawy o informacjach kredytowych i podlegają nadzorowi Komisji Usług Finansowych. Ponieważ przetwarzanie informacji dotyczących kredytów osobistych przez takich administratorów jest wyłączone z zakresu decyzji stwierdzającej odpowiedni stopień ochrony, ograniczenia i zabezpieczenia, które mają zastosowanie na mocy ARUSFTI, nie zostały szczegółowo opisane w niniejszym dokumencie.

2.2. Podstawa prawna i ograniczenia

CPA (zob. 2.2.1), CPPA (zob. 2.2.2) oraz ustawa o działalności telekomunikacyjnej (zob. 2.2.3) stanowią podstawy prawne zbierania danych osobowych na potrzeby ścigania przestępstw oraz określają mające zastosowanie ograniczenia i zabezpieczenia.

2.2.1. *Przeszukanie i zajęcie*

2.2.1.1. Podstawa prawna

Prokuratorzy i wyżsi funkcjonariusze policji sądowej mogą przeprowadzać oględziny przedmiotów, przeszukiwać osoby lub zajmować przedmioty wyłącznie wówczas, gdy 1) dana osoba jest podejrzana o popełnienie przestępstwa (osoba podejrzana o popełnienie przestępstwa); 2) jest to niezbędne do celów postępowania przygotowawczego oraz 3) przedmioty, które mają zostać poddane oględzinom, osoby, które mają zostać przeszukane, oraz wszelkie zajęte przedmioty uznaje się za mające związek ze sprawą ([19]). Podobnie sądy mogą dokonywać przeszukań i zajmować wszelkie przedmioty, które zostaną wykorzystane jako dowody lub podlegają konfiskacie, o ile takie przedmioty lub osoby uważa się za związane z konkretną sprawą ([20]).

2.2.1.2. Ograniczenia i zabezpieczenia

Ogólnym obowiązkiem prokuratorów i funkcjonariuszy policji sądowej jest przestrzeganie praw człowieka przysługujących osobie podejrzanej o popełnienie przestępstwa, jak również wszystkim innym zainteresowanym osobom ([21]). Ponadto środki przymusu służące osiągnięciu celu postępowania przygotowawczego można zastosować jedynie w przypadkach wyraźnie przewidzianych w CPA i w najmniejszym niezbędnym zakresie ([22]).

Funkcjonariusze policji lub prokuratorzy mogą przeprowadzać przeszukania, oględziny lub zajęcia w ramach postępowania przygotowawczego wyłącznie na podstawie nakazu sądowego ([23]). Organ składający wniosek o wydanie nakazu musi przedłożyć materiały uzasadniające podejrzenie, że osoba fizyczna popełniła przestępstwo, że przeszukanie, oględziny lub zajęcie są konieczne oraz że istnieją stosowne przedmioty, które mają zostać zajęte ([24]). Jeżeli chodzi o nakaz, musi on zawierać między innymi imiona i nazwiska osób podejrzanych oraz określenie rodzaju przestępstwa; wskazanie miejsca, osoby lub przedmiotów, które mają zostać przeszukane, lub przedmiotów, które mają zostać zajęte; datę wystawienia oraz okres obowiązywania ([25]). Podobnie, jeżeli w ramach toczącego się postępowania sądowego przeszukania i zajęcia dokonywane są poza jawnym posiedzeniem sądu, należy uprzednio uzyskać nakaz sądowy ([26]). Osobę, której dotyczy nakaz, i jej obrońcę powiadamia się z wyprzedzeniem o przeszukaniu lub zajęciu i mogą być oni obecni podczas wykonywania nakazu ([27]).

([18]) Zob. art. 3 ustawy o NIS (ustawa nr 12948), który odnosi się do postępowań przygotowawczych w sprawie niektórych przestępstw, takich jak rewolucja, zamieszki i przestępstwa związane z bezpieczeństwem narodowym (np. szpiegostwo). W takim kontekście zastosowanie miałyby przewidziane w CPA procedury dotyczące przeszukania i zajęcia, natomiast CPPA regulowałaby zbieranie danych dotyczących komunikacji (zob. część 3 poświęcona przepisom w zakresie dostępu do informacji dotyczących komunikacji do celów bezpieczeństwa narodowego).

([19]) Art. 215 ust. 1 i 2 CPA.

([20]) Art. 106 ust. 1, art. 107 i 109 CPA.

([21]) Art. 198 ust. 2 CPA.

([22]) Art. 199 ust. 1 CPA.

([23]) Art. 215 ust. 1 i 2 CPA.

([24]) Art. 108 ust. 1 rozporządzenia w sprawie postępowania karnego.

([25]) Art. 114 ust. 1 CPA w związku z art. 219 CPA.

([26]) Art. 113 CPA.

([27]) Art. 121 i 122 CPA.

Przy przeprowadzaniu przeszukania lub zajęcia, gdy przedmiotem przeszukania jest dysk komputerowy lub inny nośnik danych, co do zasady zajęte zostają wyłącznie same dane (skopiowane lub wydrukowane), a nie cały nośnik ([28]). Sam nośnik danych może zostać zajęty wyłącznie wówczas, gdy uznano, że wyodrębnione wydrukowanie lub skopiowanie wymaganych danych jest niemożliwe, lub gdy uznano, że nie można zrealizować celu przeszukania w inny sposób ([29]). Osoba, której dotyczy zajęcie, musi być niezwłocznie o nim powiadomiona ([30]). CPA nie przewiduje żadnych wyjątków od tego wymogu powiadomienia.

Przeszukania, oględziny i zajęcia bez nakazu mogą odbyć się jedynie w nielicznych sytuacjach. Po pierwsze, ma to miejsce w przypadku, gdy uzyskanie nakazu jest niemożliwe ze względu na pilny charakter sprawy na miejscu popełnienia przestępstwa ([31]). Następnie należy jednak niezwłocznie uzyskać nakaz ([32]). Po drugie, przeszukania i oględziny bez nakazu można przeprowadzić *in loco*, jeżeli osoba podejrzana o popełnienie przestępstwa została aresztowana lub zatrzymana ([33]). Ponadto prokurator lub wyższy funkcjonariusz policji sądowej może zająć przedmiot bez nakazu, w przypadku gdy został on porzucony przez podejrzanego o popełnienie przestępstwa lub osobę trzecią bądź dobrowolnie przekazany ([34]).

Dowody pozyskane z naruszeniem CPA będą uznane za niedopuszczalne ([35]). Ponadto kodeks karny stanowi, że niezgodne z prawem przeszukanie osób lub miejsca ich zamieszkania, strzeżonego budynku, obiektu, samochodu, statku, samolotu lub zajmowanego pomieszczenia podlega karze pozbawienia wolności do lat trzech ([36]). Przepis ten ma zatem zastosowanie również w przypadku zajęcia przedmiotów, takich jak urządzenia do przechowywania danych, podczas niezgodnego z prawem przeszukania.

2.2.2. *Zbieranie informacji dotyczących komunikacji*

2.2.2.1. Podstawa prawna

Zbieranie informacji dotyczących komunikacji reguluje specjalna ustawa – CPPA. W szczególności CPPA określa powszechny zakaz cenzurowania poczty, zakładania podsłuchu w sieciach telekomunikacyjnych, udostępniania danych potwierdzających komunikację, nagrywania lub podsłuchiwania rozmów, które nie są upubliczniane, między innymi osobami, z wyjątkiem przypadków, gdy podstawą jest CPA, CPPA lub ustawa o sądach wojskowych ([37]). Termin „komunikacja" w rozumieniu CPPA obejmuje zarówno pocztę tradycyjną, jak i telekomunikację ([38]). W tym zakresie w CPPA rozróżnia się „środki ograniczające komunikację" ([39]) i zbieranie „danych potwierdzających komunikację".

Pojęcie środków ograniczających komunikację obejmuje „cenzurę", tj. zbieranie treści pochodzących z poczty tradycyjnej, a także „podsłuch", czyli bezpośrednie przechwytywanie (pozyskiwanie lub nagrywanie) treści przekazów telekomunikacyjnych ([40]). Termin „dane potwierdzające komunikację" odnosi się do „danych na temat rejestrów telekomunikacyjnych", które obejmują datę połączenia telekomunikacyjnego, czas jego rozpoczęcia i zakończenia, liczbę połączeń wychodzących i przychodzących, jak również numer abonenta drugiego rozmówcy, częstotliwość połączeń, pliki dziennika dotyczące korzystania z usług telekomunikacyjnych oraz informacje dotyczące lokalizacji (np. z wież przekaźnikowych, które odbierają sygnały) ([41]).

([28]) Art. 106 ust. 3 CPA.
([29]) Art. 106 ust. 3 CPA.
([30]) Art. 219 CPA w związku z art. 106 ust. 4 CPA.
([31]) Art. 216 ust. 3 CPA.
([32]) Art. 216 ust. 3 CPA.
([33]) Art. 216 ust. 1 i 2 CPA.
([34]) Art. 218 CPA. Jeżeli chodzi o dane osobowe, dotyczy to jedynie ich dobrowolnego udostępnienia przez samą zainteresowaną osobę, a nie przez administratora danych osobowych przechowującego takie dane (co wymagałoby określonej podstawy prawnej zgodnie z ustawą o ochronie danych osobowych). Dobrowolnie okazane przedmioty są dopuszczane jako dowód w postępowaniu sądowym wyłącznie wówczas, gdy nie ma zasadnych wątpliwości co do dobrowolnego charakteru ujawnienia, a wykazanie tego faktu należy do prokuratora. Zob. orzeczenie Sądu Najwyższego 2013Do11233 z dnia 10 marca 2016 r.
([35]) Art. 308-2 CPA.
([36]) Art. 321 kodeksu karnego.
([37]) Art. 3 CPPA. Co do zasady ustawa o sądach wojskowych reguluje zbieranie informacji na temat personelu wojskowego i może mieć zastosowanie do osób cywilnych wyłącznie w ograniczonej liczbie przypadków (postępowanie może zostać wszczęte przed sądem wojskowym np. jeżeli personel wojskowy i osoby cywilne popełniłyby wspólnie przestępstwo lub jeżeli osoba fizyczna popełniłaby przestępstwo przeciwko wojsku, zob. art. 2 ustawy o sądach wojskowych). Przepisy ogólne regulujące przeszukanie i zajęcie są podobne do przepisów ustanowionych w CPA, zob. np. art. 146–149 i 153–156 ustawy o sądach wojskowych. Na przykład korespondencję pocztową można zbierać wyłącznie wówczas, gdy jest to konieczne do przeprowadzenia postępowania przygotowawczego i na podstawie nakazu sądu wojskowego. W zakresie, w jakim zbierane byłyby dane z łączności elektronicznej, zastosowanie mają ograniczenia i zabezpieczenia przewidziane w CPPA.
([38]) Art. 2 ust. 1 CPPA, tj. „przekazywanie lub odbiór wszelkiego rodzaju dźwięków, słów, symboli lub obrazów za pomocą sieci przewodowej, bezprzewodowej, kabla światłowodowego lub innego systemu elektromagnetycznego, w tym telefonu, poczty elektronicznej, usług informacji o członkach, faksów i przywoływania drogą radiową".
([39]) Art. 2 ust. 7 i art. 3 ust. 2 CPPA.
([40]) „Cenzurę" zdefiniowano jako „otwieranie poczty bez zgody zainteresowanej strony lub zapoznawanie się z jej treścią, rejestrowanie jej lub zatrzymywanie za pomocą innych środków" (art. 2 ust. 6 CPPA). „Podsłuch" oznacza „pozyskiwanie lub rejestrowanie treści przekazów telekomunikacyjnych poprzez słuchanie dźwięków lub równoczesne czytanie słów i oglądanie symboli lub obrazów pochodzących z przekazów telekomunikacyjnych za pomocą urządzeń elektronicznych i mechanicznych bez zgody zainteresowanej strony lub zakłócanie ich przekazywania i odbioru" (art. 2 ust. 7 CPPA).
([41]) Art. 2 ust. 11 CPPA.

CPPA określa ograniczenia i zabezpieczenia dotyczące zbierania obu rodzajów danych, a nieprzestrzeganie kilku z tych wymogów podlega sankcjom karnym ([42]).

2.2.2.2. Ograniczenia i zabezpieczenia mające zastosowanie do zbierania treści komunikacji (środki ograniczające komunikację)

Zbieranie treści komunikacji można stosować jedynie jako środek uzupełniający, ułatwiający prowadzenie postępowania przygotowawczego (tj. jako środek ostateczny), i należy dołożyć starań, aby zminimalizować naruszenie poufności komunikacji ([43]). Zgodnie z tą ogólną zasadą środki ograniczające komunikację można stosować wyłącznie wówczas, gdy trudno jest w inny sposób zapobiec popełnieniu przestępstwa, aresztować przestępcę lub zebrać dowody ([44]). Organy ścigania pozyskujące treść komunikacji muszą natychmiast zaprzestać stosowania takich środków, gdy stały dostęp nie jest już uznawany za konieczny, aby tym samym ograniczyć naruszenie prywatności komunikacji do niezbędnego minimum ([45]).

Ponadto środki ograniczające komunikację można stosować wyłącznie wówczas, gdy istnieje istotny powód, aby podejrzewać, że planowane jest popełnienie określonego poważnego przestępstwa wyraźnie wymienionego w CPPA, popełniane jest takie przestępstwo lub zostało ono popełnione. Są to takie przestępstwa jak powstanie, przestępstwa związane z narkotykami, przestępstwa z użyciem materiałów wybuchowych, jak również przestępstwa dotyczące bezpieczeństwa narodowego, stosunków dyplomatycznych lub baz i obiektów wojskowych ([46]). Środek ograniczający komunikację musi być ukierunkowany na konkretne przesyłki pocztowe lub przekazy telekomunikacyjne wysłane lub odebrane przez osobę podejrzaną lub przesyłki pocztowe lub przekazy telekomunikacyjne wysłane lub odebrane przez osobę podejrzaną w ustalonym okresie ([47]).

Nawet jeżeli wymogi te są spełnione, zbieranie danych dotyczących treści może odbywać się wyłącznie na podstawie nakazu sądowego. W szczególności prokurator może zwrócić się do sądu o wydanie zezwolenia na zbieranie danych dotyczących treści odnoszących się do osoby podejrzanej lub osoby, wobec której toczy się postępowanie przygotowawcze ([48]). Podobnie, funkcjonariusz policji sądowej może zwrócić się o udzielenie zezwolenia do prokuratora, który z kolei może wystąpić do sądu o wydanie nakazu ([49]). Wniosek o wydanie nakazu musi być złożony na piśmie i zawierać określone elementy. W szczególności należy w nim określić: 1) istotne przesłanki, które uzasadniają podejrzenie, że jedno z wymienionych przestępstw jest planowane, jest popełniane lub zostało popełnione, a także wszelkie materiały pozwalające stwierdzić istnienie zasadnego podejrzenia; 2) środki ograniczające komunikację, jak również ich przedmiot, zakres, cel i okres obowiązywania; oraz 3) miejsce i sposób wykonania środków ([50]).

Jeżeli wymogi prawne są spełnione, sąd może udzielić pisemnego zezwolenia na zastosowanie środków ograniczających komunikację w odniesieniu do osoby podejrzanej lub osoby, wobec której toczy się postępowanie przygotowawcze ([51]). W nakazie tym określa się rodzaje środków, a także ich przedmiot, zakres, okres obowiązywania oraz miejsce i sposób wykonania ([52]).

Środki ograniczające komunikację można stosować jedynie przez okres dwóch miesięcy ([53]). Jeżeli cel środków zostanie osiągnięty wcześniej w tym okresie, należy natychmiast zaprzestać ich wykonywania. Natomiast jeżeli wymagane warunki są nadal spełnione, wniosek o przedłużenie okresu obowiązywania środków ograniczających komunikację można złożyć w terminie dwóch miesięcy. Wniosek taki musi obejmować materiały wskazujące na zasadność przedłużenia obowiązywania środków ([54]). Okres przedłużenia nie może przekroczyć łącznie jednego roku lub trzech lat w przypadku niektórych szczególnie poważnych przestępstw (np. przestępstw związanych z rewolucją, agresją zewnętrzną, bezpieczeństwem narodowym itp.) ([55]).

Organy ścigania mogą nakazać operatorom sieci komunikacyjnych udzielenie pomocy, przedstawiając im pisemne zezwolenie sądu ([56]). Operatorzy sieci komunikacyjnych są zobowiązani do współpracy i zachowania otrzymanego zezwolenia w swojej dokumentacji ([57]). Mogą oni odmówić współpracy, jeżeli informacje na temat osoby, której dotyczy nakaz, wskazane w pisemnym zezwoleniu sądu (np. numer telefonu tej osoby) są niepoprawne. Ponadto w żadnym wypadku nie mogą oni ujawniać haseł używanych do celów korzystania z usług telekomunikacyjnych ([58]).

([42]) Art. 16 i 17 CPPA. Ma to zastosowanie na przykład do zbierania danych bez nakazu, nierejestrowania, niezaprzestania zbierania danych po ustaniu sytuacji nadzwyczajnej lub nieprzekazania powiadomienia osobie, której to dotyczy.
([43]) Art. 3 ust. 2 CPPA.
([44]) Art. 5 ust. 1 CPPA.
([45]) Art. 2 dekretu wykonawczego do CPPA.
([46]) Art. 5 ust. 1 CPPA.
([47]) Art. 5 ust. 2 CPPA.
([48]) Art. 6 ust. 1 CPPA.
([49]) Art. 6 ust. 2 CPPA.
([50]) Art. 6 ust. 4 CPPA i art. 4 ust. 1 dekretu wykonawczego do CPPA.
([51]) Art. 6 ust. 5 i art. 6 ust. 8 CPPA.
([52]) Art. 6 ust. 6 CPPA.
([53]) Art. 6 ust. 7 CPPA.
([54]) Art. 6 ust. 7 CPPA.
([55]) Art. 6 ust. 8 CPPA.
([56]) Art. 9 ust. 2 CPPA.
([57]) Art. 15-2 CPPA i art. 12 dekretu wykonawczego do CPPA.
([58]) Art. 9 ust. 4 CPPA.

Każda osoba wykonująca środki ograniczające komunikację lub zobowiązana do współpracy musi prowadzić dokumentację określającą cele tych środków, sposób i termin ich wykonania oraz objęte nimi treści ([59]). Organy ścigania stosujące środki ograniczające komunikację również muszą prowadzić dokumentację, w której odnotowują szczegółowe informacje i osiągnięte wyniki ([60]). Funkcjonariusze policji sądowej muszą udostępnić te informacje prokuratorowi w formie sprawozdania po zamknięciu postępowania przygotowawczego ([61]).

Jeżeli prokurator wniesie akt oskarżenia w sprawie, w której zastosowano środki ograniczające komunikację, lub wyda decyzję o odmowie oskarżenia lub aresztowania danej osoby (tj. nie tylko zawieszenie ścigania karnego), musi powiadomić osobę, wobec której zastosowano środki ograniczające komunikację, o fakcie wykonania środków ograniczających komunikację, o organie wykonującym oraz o okresie wykonania. Powiadomienie takie musi być dostarczone na piśmie w terminie 30 dni od wydania decyzji ([62]). Powiadomienie można odroczyć, jeżeli mogłoby poważnie zagrozić bezpieczeństwu narodowemu lub zakłócić bezpieczeństwo publiczne i porządek publiczny lub gdyby mogło spowodować istotną szkodę dla życia i integralności cielesnej innych osób ([63]). W przypadku gdy prokurator lub funkcjonariusz policji sądowej zamierza odroczyć powiadomienie, musi uzyskać zgodę szefa prokuratury okręgowej ([64]). Po ustaniu podstaw do odroczenia powiadomienie musi być dostarczone w terminie 30 dni od tego momentu ([65]).

CPPA określa również szczegółową procedurę zbierania treści komunikacji w sytuacjach nadzwyczajnych. W szczególności organy ścigania mogą pozyskiwać treść komunikacji w przypadku bezpośredniego zagrożenia planowaniem lub popełnieniem przestępstwa w ramach przestępczości zorganizowanej lub innego poważnego przestępstwa, które może bezpośrednio spowodować śmierć lub poważny uszczerbek na zdrowiu, oraz w sytuacji nadzwyczajnej, która uniemożliwia zastosowanie zwykłej procedury (opisanej powyżej) ([66]). W takiej sytuacji nadzwyczajnej funkcjonariusz policji lub prokurator może zastosować środki ograniczające komunikację bez uprzedniego zezwolenia sądu, ale musi wystąpić o takie zezwolenie niezwłocznie po wykonaniu tych środków. Jeżeli organ ścigania nie otrzyma zezwolenia sądu w ciągu 36 godzin od chwili wykonania środków nadzwyczajnych, należy natychmiast zaprzestać ich wykonywania, po czym zazwyczaj następuje zniszczenie zebranych informacji ([67]). Funkcjonariusze policji prowadzący nadzór nadzwyczajny wykonują go pod kontrolą prokuratora lub – w przypadku gdy otrzymanie poleceń od prokuratora z wyprzedzeniem jest niemożliwe ze względu na konieczność podjęcia natychmiastowego działania – policja musi uzyskać zgodę prokuratora niezwłocznie po rozpoczęciu czynności ([68]). Przepisy dotyczące powiadomienia osoby fizycznej opisane powyżej mają zastosowanie także do zbierania treści komunikacji w sytuacjach nadzwyczajnych.

Zbieranie informacji w sytuacjach nadzwyczajnych musi zawsze odbywać się zgodnie z „oświadczeniem o cenzurze/podsłuchu w sytuacji nadzwyczajnej", przy czym organ zajmujący się zbieraniem musi prowadzić rejestr wszystkich środków nadzwyczajnych ([69]). Do wniosku do sądu o wydanie zezwolenia na zastosowanie środków nadzwyczajnych musi być dołączony dokument, w którym wskazano niezbędne środki ograniczające komunikację, objęte nimi treści, osobę, której dotyczą, zakres, okres obowiązywania, miejsce wykonania, metodę oraz wyjaśnienie, w jaki sposób odnośne środki ograniczające komunikację spełniają wymogi określone w art. 5 ust. 1 CPPA ([70]), wraz z dokumentami potwierdzającymi.

W przypadkach gdy środki nadzwyczajne są wykonywane w krótkim czasie, co wyklucza otrzymanie zezwolenia sądu (np. gdy osoba podejrzana zostaje zatrzymana bezpośrednio po rozpoczęciu przechwytywania treści, które w związku z tym ustaje), szef prokuratury właściwej powiadamia sąd właściwy o zastosowaniu środka nadzwyczajnego ([71]). W powiadomieniu należy określić cel, przedmiot, zakres, okres, miejsce i sposób zbierania, a także podstawy niezłożenia wniosku o wydanie zezwolenia przez sąd ([72]). Powiadomienie to umożliwia sądowi, który je otrzymał, zbadanie legalności zbierania treści i musi zostać wprowadzone do rejestru powiadomień o zastosowaniu środków nadzwyczajnych.

([59]) Art. 9 ust. 3 CPPA.
([60]) Art. 18 ust. 1 dekretu wykonawczego do CPPA.
([61]) Art. 18 ust. 2 dekretu wykonawczego do CPPA.
([62]) Art. 9-2 ust. 1 CPPA.
([63]) Art. 9-2 ust. 4 CPPA.
([64]) Art. 9-2 ust. 5 CPPA.
([65]) Art. 9-2 ust. 6 CPPA.
([66]) Art. 8 ust. 1 CPPA.
([67]) Art. 8 ust. 2 CPPA.
([68]) Art. 8 ust. 3 CPPA i art. 16 ust. 3 dekretu wykonawczego do CPPA.
([69]) Art. 8 ust. 4 CPPA.
([70]) Tj., że istnieje istotny powód, aby podejrzewać, że planowane lub popełniane są określone poważne przestępstwa, lub że zostały one popełnione, a zapobiegnięcie popełnieniu przestępstwa, aresztowanie przestępcy lub zebranie dowodów jest niewykonalne w inny sposób.
([71]) Art. 8 ust. 5 CPPA.
([72]) Art. 8 ust. 6–7 CPPA.

Zgodnie z ogólnym wymogiem treść komunikacji pozyskaną w wyniku zastosowania środków ograniczających komunikację na podstawie CPPA można wykorzystać wyłącznie na potrzeby prowadzenia postępowań przygotowawczych w sprawie konkretnych przestępstw wymienionych powyżej, ścigania ich lub zapobiegania im, w postępowaniach dyscyplinarnych dotyczących tych samych przestępstw, w celu dochodzenia roszczeń odszkodowawczych zgłoszonych przez stronę komunikacji lub gdy jest to dozwolone na mocy innych przepisów ([73]).

Szczególne zabezpieczenia mają zastosowanie w przypadku zbierania informacji telekomunikacyjnych przesyłanych przez internet ([74]). Informacje takie można wykorzystać jedynie do prowadzenia postępowań przygotowawczych w sprawie poważnych przestępstw wymienionych w art. 5 ust. 1 CPPA. Aby zatrzymać informacje, należy uzyskać zgodę sądu, który wydał zezwolenie na zastosowanie środków ograniczających komunikację ([75]). Wniosek o zatrzymanie danych musi zawierać informacje na temat środków ograniczających komunikację, podsumowanie wyników zastosowania tych środków, powody zatrzymania (wraz z materiałami potwierdzającymi) oraz przekazy telekomunikacyjne, które mają zostać zatrzymane ([76]). W przypadku braku takiego wniosku pozyskane informacje telekomunikacyjne muszą zostać usunięte w terminie 14 dni od zakończenia stosowania środków ograniczających komunikację ([77]). Jeżeli wniosek został odrzucony, informacje telekomunikacyjne muszą zostać zniszczone w ciągu siedmiu dni ([78]). W przypadku usunięcia informacji telekomunikacyjnych w terminie siedmiu dni należy złożyć sprawozdanie w sądzie, który wydał zezwolenie na zastosowanie środków ograniczających komunikację, podając powody usunięcia, jak również jego szczegóły i termin.

Mówiąc ogólnie, jeżeli informacje zostały pozyskane nielegalnie za pomocą środków ograniczających komunikację, nie zostaną dopuszczone jako dowód w postępowaniu sądowym lub postępowaniu dyscyplinarnym ([79]). Ponadto w CPPA ustanowiono zakaz ujawniania informacji poufnych pozyskanych w trakcie wdrażania środków ograniczających komunikację oraz wykorzystywania zdobytych informacji w celu zaszkodzenia reputacji osób podlegających tym środkom obowiązujący wszystkie osoby korzystające z tych środków ([80]).

2.2.2.3. Ograniczenia i zabezpieczenia mające zastosowanie do zbierania metadanych

Na podstawie CPPA organy ścigania mogą zwracać się do operatorów telekomunikacyjnych o udostępnienie danych potwierdzających komunikację, jeżeli jest to niezbędne do przeprowadzenia postępowania przygotowawczego lub wykonania wyroku ([81]). W przeciwieństwie do zbierania danych dotyczących treści możliwość zbierania danych potwierdzających komunikację nie ogranicza się do konkretnych przestępstw. Podobnie jak w przypadku danych dotyczących treści zbieranie danych potwierdzających komunikację wymaga jednak uzyskania uprzedniego pisemnego zezwolenia sądu, z zastrzeżeniem tych samych warunków, które opisano wcześniej ([82]). Jeżeli ze względu na pilny charakter sprawy niemożliwe jest uzyskanie zezwolenia sądu, dane potwierdzające komunikację można zbierać bez nakazu, w którym to przypadku zezwolenie należy uzyskać niezwłocznie po złożeniu wniosku o udostępnienie danych i przekazać je dostawcy usług telekomunikacyjnych ([83]). W razie nieuzyskania zezwolenia w późniejszym terminie zebrane informacje muszą zostać zniszczone ([84]).

Prokuratorzy, funkcjonariusze policji sądowej i sądy muszą prowadzić rejestr wniosków o udostępnienie danych potwierdzających komunikację ([85]). Ponadto dostawcy usług telekomunikacyjnych muszą dwa razy w roku przedkładać Ministrowi Nauki i Technologii Informacyjno-Komunikacyjnych sprawozdania z ujawniania danych potwierdzających komunikację oraz przechowywać związaną z nimi dokumentację przez siedem lat od dnia, w którym dane zostały ujawnione ([86]).

Osoby fizyczne są co do zasady powiadamiane o fakcie, że zebrano dane potwierdzające komunikację ([87]). Termin dokonania takiego powiadomienia zależy od okoliczności postępowania przygotowawczego ([88]). Po wydaniu postanowienia o wniesieniu aktu oskarżenia lub zaniechaniu ścigania karnego powiadomienie musi zostać dostarczone w terminie 30 dni. Natomiast w sytuacji zawieszenia postępowania karnego powiadomienie musi zostać dostarczone w terminie 30 dni następujących po roku od wydania takiego postanowienia. W każdym razie powiadomienie musi być dostarczone w terminie 30 dni następujących po roku od zebrania informacji.

Powiadomienie można odroczyć wyłącznie w przypadku, gdy istnieje prawdopodobieństwo, że może ono 1) zagrażać bezpieczeństwu narodowemu oraz bezpieczeństwu i porządkowi publicznemu, 2) spowodować śmierć lub uszczerbek

([73]) Art. 12 CPPA.
([74]) Art. 12-2 CPPA.
([75]) Prokurator lub policjant wykonujący środki ograniczające komunikację musi w ciągu 14 dni od zakończenia stosowania środków wybrać przekazy telekomunikacyjne, które mają zostać zatrzymane, i wystąpić do sądu o zezwolenie (funkcjonariusz policji składa wniosek do prokuratora, który następnie składa wniosek do sądu), zob. art. 12-2 ust. 1 i 2 CPPA.
([76]) Art. 12-2 ust. 3 CPPA.
([77]) Art. 12-2 ust. 5 CPPA.
([78]) Art. 12-2 ust. 5 CPPA.
([79]) Art. 4 CPPA.
([80]) Art. 11 ust. 2 dekretu wykonawczego do CPPA.
([81]) Art. 13 ust. 1 CPPA.
([82]) Art. 13 i 6 CPPA.
([83]) Art. 13 ust. 2 CPPA. Tak jak w przypadku pilnych środków ograniczających komunikację konieczne jest sporządzenie dokumentu określającego szczegółowe informacje o sprawie (osoba podejrzana, środki, które mają zostać zastosowane, podejrzewane przestępstwo, jak również pilny charakter sprawy). Zob. art. 37 ust. 5 dekretu wykonawczego do CPPA.
([84]) Art. 13 ust. 3 CPPA.
([85]) Art. 13 ust. 5 i 6 CPPA.
([86]) Art. 13 ust. 7 CPPA.
([87]) Zob. art. 13-3 ust. 7 w związku z art. 9-2 CPPA.
([88]) Art. 13-3 ust. 1 CPPA.

na zdrowiu, 3) utrudnić rzetelne postępowanie sądowe (np. prowadząc do zniszczenia dowodów lub grożenia świadkom) lub 4) zniesławić osobę podejrzaną, poszkodowanych lub inne osoby związane ze sprawą lub naruszyć ich prywatność ([89]). Powiadomienie na podstawie jednej z wyżej wymienionych przyczyn wymaga zezwolenia dyrektora właściwej prokuratury okręgowej ([90]). Powiadomienie musi zostać dostarczone w terminie 30 dni od ustania przyczyn odroczenia ([91]).

Powiadomione osoby mogą złożyć pisemny wniosek do prokuratora lub funkcjonariusza policji sądowej dotyczący przyczyn zbierania danych potwierdzających komunikację ([92]). Wówczas prokurator lub funkcjonariusz policji sądowej musi przedstawić uzasadnienie na piśmie w terminie 30 dni od otrzymania wniosku, chyba że ma zastosowanie jedna z wyżej wymienionych przyczyn (wyjątki odroczenia powiadomienia) ([93]).

2.2.3. *Dobrowolne ujawnianie informacji przez operatorów telekomunikacyjnych*

W art. 83 ust. 3 TBA dopuszczono możliwość dobrowolnego zastosowania się przez operatorów telekomunikacyjnych do wniosku (złożonego w związku z procesem sądowym w postępowaniu karnym, postępowaniem przygotowawczym lub w celu wykonania wyroku) sądu, prokuratora lub szefa organu ścigania prowadzącej o ujawnienie „danych dotyczących komunikacji". W kontekście TBA „dane dotyczące komunikacji" obejmują imię i nazwisko, numer rejestracyjny mieszkańca, adres i numer telefonu użytkowników, terminy rozpoczęcia lub zakończenia abonamentu, jak również kody identyfikacyjne użytkowników (tj. kody używane do identyfikacji prawowitego użytkownika systemów komputerowych lub sieci komunikacyjnych) ([94]). Do celów TBA za użytkowników uważa się wyłącznie osoby fizyczne, które bezpośrednio korzystają z usług koreańskiego dostawcy telekomunikacyjnego ([95]). W związku z tym sytuacje, w których osoby fizyczne z UE, których dane zostały przekazane do Republiki Korei, zostałyby uznane za użytkowników na podstawie TBA, będą prawdopodobnie bardzo ograniczone, ponieważ osoby te zazwyczaj nie zawarłyby bezpośredniej umowy z koreańskim operatorem telekomunikacyjnym.

Wnioski o uzyskanie danych dotyczących komunikacji na podstawie TBA muszą być składane na piśmie i muszą zawierać uzasadnienie wniosku oraz wskazanie związku z danym użytkownikiem i zakresu danych objętych wnioskiem ([96]). Jeżeli dostarczenie pisemnego wniosku nie jest możliwe ze względu na pilny charakter sprawy, wniosek takie należy dostarczyć niezwłocznie po ustaniu przyczyny tego pilnego charakteru ([97]). Operatorzy telekomunikacyjni, którzy stosują się do wniosków o ujawnienie danych dotyczących komunikacji, muszą zatrzymać ewidencję zawierającą rejestry wskazujące, że dane dotyczące komunikacji zostały udostępnione, jak również powiązane materiały, takie jak pisemny wniosek ([98]). Ponadto operatorzy telekomunikacyjni muszą dwa razy w roku przedkładać Ministrowi Nauki i Technologii Informacyjno-Komunikacyjnych sprawozdania z przekazywania danych dotyczących komunikacji ([99]).

Operatorzy telekomunikacyjni nie mają obowiązku stosowania się do wniosków o ujawnienie danych dotyczących komunikacji na podstawie TBA. Przedsiębiorca musi zatem ocenić każdy wniosek w świetle obowiązujących wymogów ochrony danych na mocy PIPA. W szczególności operator telekomunikacyjny musi wziąć pod uwagę interesy osoby, której dane dotyczą, i nie może ujawnić informacji, jeżeli mogłoby to naruszyć w sposób nieuzasadniony interes tej osoby lub strony trzeciej ([100]). Ponadto, zgodnie z zawiadomieniem nr 2021-1 w sprawie przepisów uzupełniających dotyczących wykładni i stosowania ustawy o ochronie danych osobowych, osoba objęta wnioskiem musi zostać poinformowana o ujawnieniu informacji. W wyjątkowych okolicznościach powiadomienie takie można odroczyć, w szczególności w przypadku gdy i dopóki istnieje prawdopodobieństwo, że powiadomienie zagrażałoby toczącemu się postępowaniu przygotowawczemu lub że może spowodować szkodę dla życia lub integralności cielesnej innej osoby, o ile te prawa lub interesy są w oczywisty sposób nadrzędne wobec praw osoby, której dane dotyczą ([101]).

W 2016 r. Sąd Najwyższy potwierdził, że dobrowolne przekazywanie danych dotyczących komunikacji przez operatorów telekomunikacyjnych bez nakazu na podstawie TBA samo w sobie nie narusza prawa użytkownika usługi telekomunikacyjnej do prywatności informacji. Jednocześnie Sąd Najwyższy wyjaśnił, że takie naruszenie miałoby miejsce, gdyby było zupełnie oczywiste, że agencja występująca z wnioskiem nadużyła swoich uprawnień, aby złożyć wniosek o ujawnienie danych dotyczących komunikacji, naruszając w ten sposób interesy osoby, której te dane dotyczą, lub strony trzeciej ([102]). Ogólnie rzecz ujmując, każdy wniosek o dobrowolne ujawnienie informacji złożony przez organ ścigania musi być zgodny z zasadami zgodności z prawem, konieczności i proporcjonalności wynikającymi z koreańskiej konstytucji (art. 12 ust. 1 i art. 37 ust. 2).

([89]) Art. 13-3 ust. 2 CPPA.
([90]) Art. 13-3 ust. 3 CPPA.
([91]) Art. 13-3 ust. 4 CPPA.
([92]) Art. 13-3 ust. 5 CPPA.
([93]) Art. 13-3 ust. 6 CPPA.
([94]) Art. 83 ust. 3 TBA.
([95]) Art. 2 ust. 9 TBA.
([96]) Art. 83 ust. 4 TBA.
([97]) Art. 83 ust. 4 TBA.
([98]) Art. 83 ust. 5 TBA.
([99]) Art. 83 ust. 6 TBA.
([100]) Art. 18 ust. 2 PIPA.
([101]) Zawiadomienie nr 2021-1 PIPC w sprawie przepisów uzupełniających dotyczących wykładni i stosowania ustawy o ochronie danych osobowych, sekcja III pkt 2 ppkt (iii).
([102]) Orzeczenie Sądu Najwyższego nr 2012Da105482 z dnia 10 marca 2016 r.

2.3. **Nadzór**

Nadzór nad organami ścigania sprawowany jest za pomocą różnych mechanizmów stosowanych zarówno wewnętrznie, jak i przez organy zewnętrzne.

2.3.1. *Kontrolowanie własnej działalności*

Zgodnie z ustawą o audycie w sektorze publicznym organy publiczne zachęca się do powołania wewnętrznego organu ds. kontrolowania własnej działalności, którego zadaniem jest m.in. przeprowadzanie kontroli legalności ([103]). Szefowie takich organów audytowych muszą mieć zagwarantowaną niezależność w możliwie największym zakresie ([104]). W szczególności są oni powoływani spoza danego organu (np. byli sędziowie, profesorowie) na okres od dwóch do pięciu lat i mogą zostać odwołani wyłącznie z uzasadnionych powodów (np. gdy nie są w stanie wykonywać swoich obowiązków ze względu na stan psychiczny lub fizyczny lub gdy podlegają środkom dyscyplinarnym) ([105]). Podobnie audytorzy są powoływani na podstawie szczegółowych warunków określonych w ustawie ([106]). Sprawozdania z audytu mogą zawierać zalecenia lub wnioski o odszkodowanie lub dokonanie korekty, jak również nagany i zalecenia lub wnioski o zastosowanie środków dyscyplinarnych ([107]). W terminie 60 dni od zakończenia audytu są one przekazywane szefowi organu publicznego objętego audytem, a także Komisji Kontroli i Audytu (zob. pkt 2.3.2) ([108]). Organ, którego dotyczy sprawozdanie, musi wdrożyć wymagane środki i przedstawić wyniki Komisji Kontroli i Audytu ([109]). Ponadto wyniki audytu są zazwyczaj udostępniane społeczeństwu ([110]). Odmowa kontrolowania własnej działalności lub jego utrudnianie podlega administracyjnym karom pieniężnym ([111]). W obszarze ścigania przestępstw, aby zapewnić zgodność z wyżej wymienionymi przepisami, Agencja Policji Krajowej prowadzi system Inspektora Generalnego służący do przeprowadzania audytów wewnętrznych, w tym w odniesieniu do ewentualnych naruszeń praw człowieka ([112]).

2.3.2. *Komisja Kontroli i Audytu*

Komisja Kontroli i Audytu (zwana dalej „BAI", od ang. Board of Audit and Inspection) może przeprowadzać kontrole działań organów publicznych i na podstawie takich kontroli wydawać zalecenia, wnosić o zastosowanie środków dyscyplinarnych lub złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa ([113]). BAI została ustanowiona przy prezydencie Republiki Korei, ale zachowuje niezależny status w odniesieniu do swoich obowiązków ([114]). Ponadto w ustawie ustanawiającej BAI wymaga się, aby komisja ta uzyskała jak największą niezależność w zakresie powoływania, odwoływania i organizacji swoich pracowników, jak również opracowywania swojego budżetu ([115]). Przewodniczący BAI jest powoływany przez prezydenta za zgodą Zgromadzenia Narodowego ([116]). Sześciu pozostałych komisarzy jest powoływanych przez prezydenta na czteroletnią kadencję na podstawie rekomendacji przewodniczącego ([117]). Komisarze (w tym przewodniczący) muszą dysponować określonymi kwalifikacjami wymienionymi w ustawie ([118]) i mogą zostać odwołani wyłącznie w przypadku impeachmentu, skazania na karę pozbawienia wolności lub niezdolności do wykonywania obowiązków z powodu długotrwałej niepełnosprawności intelektualnej lub fizycznej ([119]). Ponadto komisarze mają zakaz uczestniczenia w działalności politycznej oraz jednoczesnego pełnienia funkcji w Zgromadzeniu Narodowym, agencjach administracyjnych, organizacjach podlegających audytowi i kontroli BAI lub zajmowania innych urzędów lub stanowisk, za które otrzymują wynagrodzenie ([120]).

BAI przeprowadza corocznie audyt ogólny, ale może również przeprowadzać audyty specjalne w sprawach będących przedmiotem szczególnego zainteresowania. Podczas przeprowadzania kontroli BAI może zażądać przedłożenia dokumentów i wezwać osoby fizyczne do stawiennictwa ([121]). W ramach audytu BAI bada dochody i wydatki państwa, ale

([103]) Art. 3 i 5 ustawy o audycie w sektorze publicznym.
([104]) Art. 7 ustawy o audycie w sektorze publicznym.
([105]) Art. 8-11 ustawy o audycie w sektorze publicznym.
([106]) Art. 16 i nast. ustawy o audycie w sektorze publicznym.
([107]) Art. 23 ust. 2 ustawy o audycie w sektorze publicznym.
([108]) Art. 23 ust. 1 ustawy o audycie w sektorze publicznym.
([109]) Art. 23 ust. 3 ustawy o audycie w sektorze publicznym.
([110]) Art. 26 ustawy o audycie w sektorze publicznym.
([111]) Art. 41 ustawy o audycie w sektorze publicznym.
([112]) Zob. w szczególności jednostki podlegające dyrektorowi generalnemu ds. audytu i kontroli: https://www.police.go.kr/eng/knpa/org/org01.jsp
([113]) Art. 24 i art. 31–35 ustawy o Komisji Kontroli i Audytu (zwanej dalej „ustawą o BAI").
([114]) Art. 2 ust. 1 ustawy o BAI.
([115]) Art. 2 ust. 2 ustawy o BAI.
([116]) Art. 4 ust. 1 ustawy o BAI.
([117]) Art. 5 ust. 1 i art. 6 ustawy o BAI.
([118]) Na przykład co najmniej dziesięcioletni staż pracy w charakterze sędziego, prokuratora lub radcy prawnego, co najmniej ośmioletni staż pracy w charakterze funkcjonariusza państwowego, profesora lub pracownika na wyższym stanowisku na uniwersytecie, co najmniej dziesięcioletni staż pracy w spółce notowanej na giełdzie lub instytucji z udziałem skarbu państwa (w tym co najmniej pięcioletni staż pracy na stanowisku kierowniczym), zob. art. 7 ustawy o BAI.
([119]) Art. 8 ustawy o BAI.
([120]) Art. 9 ustawy o BAI.
([121]) Zob. np. art. 27 ustawy o BAI.

także sprawuje ogólny nadzór nad wypełnianiem obowiązków przez organy publiczne i urzędników publicznych w celu usprawnienia funkcjonowania administracji publicznej ([122]). Sprawowany przez nią nadzór wykracza zatem poza aspekty budżetowe i obejmuje również kontrolę zgodności z prawem.

2.3.3. *Zgromadzenie Narodowe*

Zgromadzenie Narodowe może przeprowadzać śledztwa i kontrole dotyczące organów publicznych ([123]). W trakcie śledztwa lub kontroli Zgromadzenie Narodowe może zażądać ujawnienia dokumentów i wezwać świadków ([124]). Każdy, kto dopuści się krzywoprzysięstwa w czasie śledztwa prowadzonego przez Zgromadzenie Narodowe, podlega sankcjom karnym (kara pozbawienia wolności do lat dziesięciu) ([125]). Przebieg i wyniki kontroli mogą być udostępniane publicznie ([126]). Jeżeli Zgromadzenie Narodowe stwierdzi, że doszło do niezgodnego z prawem lub niewłaściwego działania, może zażądać od odnośnego organu publicznego podjęcia działań naprawczych, w tym przyznania odszkodowania, zastosowania środków dyscyplinarnych i usprawnienia procedur wewnętrznych ([127]). Po otrzymaniu takiego żądania organ musi niezwłocznie podjąć działania i poinformować Zgromadzenie Narodowe o ich wyniku ([128]).

2.3.4. *Komisja Ochrony Danych Osobowych*

Komisja Ochrony Danych Osobowych (zwana dalej „PIPC") sprawuje nadzór nad przetwarzaniem danych osobowych przez organy ścigania zgodnie z PIPA. Ponadto, zgodnie z art. 7-8 ust. 3 i 4 oraz art. 7-9 ust. 5 PIPA, nadzór PIPC obejmuje również ewentualne naruszenia przepisów określających ograniczenia i zabezpieczenia w odniesieniu do zbierania danych osobowych, w tym przepisów ustanowionych w ustawach szczegółowych regulujących zbieranie (elektronicznych) materiałów dowodowych do celów ścigania przestępstw (zob. pkt 2.2). Biorąc pod uwagę wymogi przewidziane w art. 3 ust. 1 PIPA dotyczące zgodnego z prawem i rzetelnego zbierania danych osobowych, każde takie naruszenie stanowi także naruszenie PIPA, co pozwala PIPC na przeprowadzenie dochodzenia i podjęcie działań naprawczych ([129]).

Wykonując swoją funkcję nadzorczą, PIPC ma dostęp do wszystkich istotnych informacji ([130]). PIPC może wydać zalecenia dla organu ścigania w celu zwiększenia poziomu ochrony danych osobowych w ramach prowadzonych przez niego czynności przetwarzania, nakazać podjęcie działań naprawczych (np. zawieszenie przetwarzania danych lub wprowadzenie środków niezbędnych do zapewnienia ochrony danych osobowych) lub zalecić organowi zastosowanie środków dyscyplinarnych ([131]). Ponadto przewidziano sankcje karne za niektóre naruszenia PIPA, takie jak bezprawne wykorzystywanie lub ujawnianie danych osobowych stronom trzecim lub niezgodne z prawem przetwarzanie informacji szczególnie chronionych ([132]). W tym kontekście PIPC może przekazać sprawę do właściwego organu ścigania (w tym prokuratury) ([133]).

2.3.5. *Krajowa Komisja Praw Człowieka*

Krajowa Komisja Praw Człowieka (zwana dalej „NHRC", od ang. National Human Rights Commission) – niezależny organ, którego zadaniem jest ochrona i promowanie praw podstawowych ([134]) – jest uprawniona do badania i usuwania naruszeń określonych w art. 10–22 konstytucji, dotyczących między innymi prawa do prywatności i prawa do prywatności korespondencji. W skład NHRC wchodzi 11 komisarzy powołanych na podstawie nominacji: Zgromadzenia Narodowego (czterech), prezydenta (czterech) oraz prezesa Sądu Najwyższego (trzech) ([135]). Aby zostać powołanym, komisarz musi: 1) przepracować co najmniej dziesięć lat na uniwersytecie lub w autoryzowanym instytucie badawczym na stanowisku co najmniej profesora nadzwyczajnego; 2) przez co najmniej dziesięć lat wykonywać zawód sędziego, prokuratora lub radcy prawnego; 3) przez co najmniej dziesięć lat angażować się w działalność na rzecz praw człowieka (np. w organizacji nienastawionej na zysk, organizacji pozarządowej lub organizacji międzynarodowej); lub 4) otrzymać rekomendację od grup społeczeństwa obywatelskiego ([136]). Przewodniczącego powołuje prezydent spośród komisarzy,

([122]) Art. 20 i 24 ustawy o BAI.
([123]) Art. 128 ustawy o Zgromadzeniu Narodowym oraz art. 2, 3 i 15 ustawy o kontroli i nadzorowaniu administracji państwowej. Obejmuje to coroczne kontrole działalności rządu ogółem, jak również śledztwa w konkretnych sprawach.
([124]) Art. 10 ust. 1 ustawy o kontroli i nadzorowaniu administracji państwowej. Zob. także art. 128 i 129 ustawy o Zgromadzeniu Narodowym.
([125]) Art. 14 ustawy o składaniu zeznań, wydawaniu opinii itp. przed Zgromadzeniem Narodowym.
([126]) Art. 12-2 ustawy o kontroli i nadzorowaniu administracji państwowej.
([127]) Art. 16 ust. 2 ustawy o kontroli i nadzorowaniu administracji państwowej.
([128]) Art. 16 ust. 3 ustawy o kontroli i nadzorowaniu administracji państwowej.
([129]) Zob. zawiadomienie PIPC nr 2021-1 w sprawie przepisów uzupełniających dotyczących wykładni i stosowania ustawy o ochronie danych osobowych.
([130]) Art. 63 PIPA.
([131]) Art. 61 ust. 2, art. 65 ust. 1, art. 65 ust. 2 oraz art. 64 ust. 4 PIPA.
([132]) Art. 70–74 PIPA.
([133]) Art. 65 ust. 1 PIPA.
([134]) Art. 1 ustawy o Krajowej Komisji Praw Człowieka (zwanej dalej „ustawą o NHRC").
([135]) Art. 5 ust. 1 i 2 ustawy o NHRC.
([136]) Art. 5 ust. 3 ustawy o NHRC.

a następnie wymagane jest zatwierdzenie przez Zgromadzenie Narodowe ([137]). Komisarze (w tym przewodniczący) są powoływani na odnawialną trzyletnią kadencję i mogą zostać odwołani wyłącznie w przypadku skazania na karę pozbawienia wolności lub gdy nie są w stanie dłużej wykonywać swoich obowiązków z powodu długotrwałej niepełnosprawności intelektualnej lub fizycznej (w takim przypadku dwie trzecie komisarzy musi wyrazić zgodę na odwołanie) ([138]). Komisarze NHRC nie mogą pełnić jednocześnie funkcji w Zgromadzeniu Narodowym, radach samorządu terytorialnego ani w żadnych organach administracji państwowej lub samorządowej (jako urzędnicy publiczni) ([139]).

NHRC może wszcząć dochodzenie z urzędu lub na wniosek osoby fizycznej. W ramach prowadzonego dochodzenia NHRC może zażądać przedłożenia odpowiednich materiałów, przeprowadzić kontrolę i wezwać osoby fizyczne do złożenia zeznań ([140]). Po przeprowadzeniu dochodzenia NHRC może wydawać zalecenia dotyczące poprawy lub skorygowania określonych polityk i praktyk, które to zalecenia może podać do wiadomości publicznej ([141]). Organy publiczne mają obowiązek powiadomić NHRC o planie wdrożenia takich zaleceń w terminie 90 dni od ich otrzymania ([142]). Ponadto w przypadku niewdrożenia zaleceń odnośny organ musi poinformować o tym komisję ([143]). NHRC może z kolei ujawnić takie zaniechanie Zgromadzeniu Narodowemu lub podać je do wiadomości publicznej. Organy publiczne co do zasady stosują się do zaleceń NHRC i mają ku temu silną motywację, ponieważ wdrożenie zaleceń jest przedmiotem oceny w ramach ogólnej oceny dokonywanej przez Biuro Koordynacji Polityki Rządu podlegające kancelarii premiera.

2.4. **Indywidualne dochodzenie roszczeń**

2.4.1. *Mechanizmy dochodzenia roszczeń dostępne na mocy PIPA*

Zgodnie z PIPA osoby fizyczne mogą wykonywać swoje prawa dostępu do danych osobowych przetwarzanych przez organy ścigania, ich korekty i usunięcia oraz zawieszenia zgody na ich przetwarzanie. Wniosek o dostęp można złożyć bezpośrednio do właściwego organu lub pośrednio, za pośrednictwem PIPC ([144]). Właściwy organ może ograniczyć dostęp lub odmówić dostępu wyłącznie wówczas, gdy przewiduje tak prawo, jeżeli dostęp mógłby spowodować szkodę dla życia lub integralności cielesnej strony trzeciej lub prawdopodobnie doprowadziłby do nieuzasadnionego naruszenia prawa do użytkowania nieruchomości i innych interesów innej osoby (tj. gdy interesy innej osoby przeważałyby nad interesami osoby składającej wniosek) ([145]). W przypadku odmowy dostępu należy poinformować osobę fizyczną o przyczynach odmowy oraz o sposobie odwołania się ([146]). Podobnie wniosek o korektę lub usunięcie danych może zostać odrzucony, jeżeli przewidziano tak w innych przepisach, i wówczas osoba fizyczna musi otrzymać informacje o przyczynach odmowy i możliwości odwołania się ([147]).

Jeśli chodzi o dochodzenie roszczeń, osoby fizyczne mogą wnieść skargę do PIPC między innymi za pośrednictwem centrum telefonicznego ds. prywatności prowadzonego przez Koreańską Agencję ds. Internetu i Bezpieczeństwa ([148]). Ponadto osoba fizyczna może prowadzić mediacje za pośrednictwem Komisji ds. Mediacji w Sporach Dotyczących Danych Osobowych ([149]). Te środki dochodzenia roszczeń są dostępne zarówno w przypadku ewentualnych naruszeń przepisów ujętych w ustawach szczególnych określających ograniczenia i zabezpieczenia w odniesieniu do zbierania danych osobowych (pkt 2.2), jak i naruszeń przepisów PIPA. Ponadto na podstawie ustawy o postępowaniu administracyjnosądowym osoby fizyczne mogą odwołać się od decyzji lub wnieść skargę na bezczynność PIPC (zob. pkt 2.4.3).

([137]) Art. 5 ust. 5 ustawy o NHRC.
([138]) Art. 7 ust. 1 i art. 8 ustawy o NHRC.
([139]) Art. 10 ustawy o NHRC.
([140]) Art. 36 ustawy o NHRC. Zgodnie z art. 36 ust. 7 ustawy można odmówić przedłożenia materiałów lub przedmiotów, jeżeli naruszałoby to tajemnicę państwową, co mogłoby mieć istotny wpływ na bezpieczeństwo państwa lub stosunki dyplomatyczne albo stanowiłoby poważną przeszkodę w prowadzeniu postępowania przygotowawczego lub sądowego. W takich przypadkach Komisja może w razie konieczności zażądać od szefa właściwej agencji (który musi działać w dobrej wierze) dalszych informacji, aby umożliwić sprawdzenie, czy odmowa udzielenia informacji jest uzasadniona.
([141]) Art. 25 ust. 1 ustawy o NHRC.
([142]) Art. 25 ust. 3 ustawy o NHRC.
([143]) Art. 25 ust. 4 ustawy o NHRC.
([144]) Art. 35 ust. 2 PIPA.
([145]) Art. 35 ust. 4 PIPA.
([146]) Art. 42 ust. 2 dekretu wykonawczego do PIPA.
([147]) Art. 36 ust. 1–2 PIPA i art. 43 ust. 3 dekretu wykonawczego do PIPA.
([148]) Art. 62 PIPA.
([149]) Art. 40–50 PIPA i od art. 48-2 do 57 dekretu wykonawczego do PIPA.

2.4.2. *Skarga do Krajowej Komisji Praw Człowieka*

NHRC rozpatruje skargi osób fizycznych (zarówno Koreańczyków, jak i cudzoziemców) dotyczące naruszeń praw człowieka przez organy publiczne ([150]). Składanie skarg do NHRC przez osoby fizyczne nie jest obwarowane żadnymi stałymi wymogami ([151]). W rezultacie NHRC rozpatrzy skargę, nawet jeśli dana osoba nie jest w stanie wykazać faktycznej szkody na etapie sprawdzania dopuszczalności. W kontekście zbierania danych osobowych do celów ścigania przestępstw osoba fizyczna nie musiałaby zatem wykazywać, że koreańskie organy publiczne faktycznie uzyskały dostęp do jej danych osobowych, aby skarga była dopuszczalna przed NHRC. Osoba fizyczna może również wnieść o rozstrzygniecie skargi w drodze mediacji ([152]).

W celu zbadania skargi NHRC może wykorzystać swoje uprawnienia dochodzeniowe, w tym zażądać przedstawienia odpowiednich materiałów, przeprowadzić kontrolę i wezwać osoby fizyczne do złożenia zeznań ([153]). Jeżeli dochodzenie wykaże, że doszło do naruszenia odpowiednich przepisów, NHRC może zalecić wprowadzenie środków zaradczych lub skorygowanie bądź ulepszenie wszelkich stosownych ustaw, instytucji, polityk lub praktyk ([154]). Zaproponowane środki zaradcze mogą obejmować mediację, zaprzestanie naruszania praw człowieka, odszkodowanie i środki zapobiegające ponownemu wystąpieniu takich samych lub podobnych naruszeń ([155]). W przypadku bezprawnego zbierania informacji osobowych na podstawie obowiązujących przepisów środki zaradcze obejmują usunięcie zebranych danych osobowych. Jeżeli istnieje wysokie prawdopodobieństwo, że naruszenie ma charakter ciągły, oraz istnieje prawdopodobieństwo, że niepodjęcie działań spowoduje trudne do naprawienia szkody, NHRC może przyjąć środki naprawcze w trybie pilnym ([156]).

Chociaż NHRC nie ma uprawnień do nakazania usunięcia naruszeń, jej decyzje (np. decyzja o umorzeniu postępowania w sprawie skargi) ([157]) i zalecenia mogą zostać zaskarżone przed sądami koreańskimi na podstawie ustawy o postępowaniu administracyjnosądowym (zob. pkt 2.4.3 poniżej) ([158]). Ponadto jeżeli z ustaleń NHRC wynika, że organ publiczny zebrał dane osobowe bezprawnie, osoba fizyczna może korzystać przed sądami koreańskimi z dalszych środków dochodzenia roszczeń wobec tego organu publicznego, np. kwestionując zbieranie danych na podstawie ustawy o postępowaniu administracyjnosądowym, składając skargę konstytucyjną na podstawie ustawy o Trybunale Konstytucyjnym lub ubiegając się o odszkodowanie za szkody na podstawie ustawy o odszkodowaniach od państwa (zob. pkt 2.4.3 poniżej).

2.4.3. *Dochodzenie roszczeń na drodze sądowej*

Osoby fizyczne mogą powoływać się na ograniczenia i zabezpieczenia opisane w poprzednich punktach, aby dochodzić roszczeń przed sądami koreańskimi za pośrednictwem różnych metod.

Po pierwsze, zgodnie z ustawą o postępowaniu karnym dana osoba fizyczna i jej pełnomocnik mogą być obecni przy wykonywaniu nakazu przeszukania lub zajęcia, a zatem mogą również wnieść sprzeciw w czasie wykonywania nakazu ([159]). Ponadto w CPA przewidziano mechanizm tzw. „quasi-skargi", który umożliwia osobom fizycznym złożenie do sądu właściwego wniosku o unieważnienie lub zmianę decyzji podjętej przez prokuratora lub policjanta w sprawie zajęcia ([160]). Umożliwia to osobom fizycznym zakwestionowanie środków zastosowanych w celu wykonania nakazu zajęcia.

([150]) Chociaż art. 4 ustawy o NHRC odnosi się do obywateli i cudzoziemców zamieszkałych na terytorium Republiki Korei, termin „zamieszkały" odzwierciedla raczej pojęcie jurysdykcji niż terytorium. Dlatego też, jeśli podstawowe prawa osoby fizycznej spoza Korei są naruszane przez instytucje krajowe w Korei, osoba ta może wnieść skargę do NHRC. Zob. np. odpowiednie pytanie na stronie internetowej NHRC zawierającej odpowiedzi na często zadawane pytania, dostępnej pod adresem: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Będzie to miało miejsce w przypadku, gdy dane osobowe cudzoziemca przekazane do Korei są bezprawnie udostępniane koreańskim organom publicznym.

([151]) Skarga musi co do zasady zostać złożona w ciągu jednego roku od naruszenia, ale NHRC może wciąż podjąć decyzję o rozpatrzeniu skargi złożonej po tym okresie, o ile nie upłynął termin przedawnienia wynikający z przepisów prawa karnego lub cywilnego (art. 32 ust. 1 pkt 4 ustawy o NHRC).

([152]) Art. 42 i nast. ustawy o NHRC.

([153]) Art. 36 i 37 ustawy o NHRC.

([154]) Art. 44 ustawy o NHRC.

([155]) Art. 42 ust. 4 ustawy o NHRC.

([156]) Art. 48 ustawy o NHRC.

([157]) Na przykład jeżeli NHRC wyjątkowo nie jest w stanie przeprowadzić kontroli określonych materiałów lub obiektów, są one związane z tajemnicami państwowymi, które mogą mieć istotny wpływ na bezpieczeństwo państwa lub stosunki dyplomatyczne, lub jeżeli kontrola stanowiłaby poważną przeszkodę dla postępowania przygotowawczego lub toczącego się procesu (zob. przypis 166) i jeżeli uniemożliwia to NHRC przeprowadzenie dochodzenia niezbędnego do oceny zasadności otrzymanego wniosku, NHRC informuje daną osobę fizyczną o przyczynach odrzucenia skargi, zgodnie z art. 39 ustawy o NHRC. W takim przypadku osoba ta może odwołać się od decyzji NHRC na podstawie ustawy o postępowaniu administracyjnosądowym.

([158]) Zob. np. orzeczenie Sądu Apelacyjnego w Seulu nr 2007Nu27259 z dnia 18 kwietnia 2008 r., potwierdzone orzeczeniem Sądu Najwyższego nr 2008Du7854 z dnia 9 października 2008 r.; orzeczenie Sądu Apelacyjnego w Seulu nr 2017Nu69382 z 2 lutego 2018 r.

([159]) Art. 121 i 219 CPA.

([160]) Art. 417 CPA w związku z art. 414 ust. 2 CPA. Zob. również orzeczenie Sądu Najwyższego nr 97Mo66 z dnia 29 września 1997 r.

Ponadto osoby fizyczne mogą uzyskać odszkodowanie przed sądami koreańskimi. Na podstawie ustawy o odszkodowaniach od państwa osoby fizyczne mogą ubiegać się o odszkodowanie za szkody wyrządzone przez urzędników publicznych wykonujących swoje oficjalne obowiązki z naruszeniem prawa ([161]). Powództwo na podstawie ustawy o odszkodowaniach od państwa można wnieść do wyspecjalizowanej rady ds. odszkodowań lub bezpośrednio do koreańskich sądów ([162]). Jeśli poszkodowany jest cudzoziemcem, ustawa o odszkodowaniach od państwa ma zastosowanie, o ile kraj pochodzenia tej osoby również zapewnia prawo do odszkodowania obywatelom koreańskim ([163]). Zgodnie z orzecznictwem warunek ten jest spełniony, jeśli wymogi dotyczące ubiegania się o odszkodowanie w tym drugim kraju „nie są w znacznym stopniu rozbieżne między Koreą a takim krajem" i „nie są zasadniczo bardziej rygorystyczne niż te określone przez Koreę, a ponadto nie wykazują żadnych istotnych i zasadniczych różnic" ([164]). Kodeks cywilny reguluje odpowiedzialność państwa w zakresie odszkodowań, a w konsekwencji odpowiedzialność państwa obejmuje szkody niemajątkowe (np. cierpienia psychiczne) ([165]).

Jeżeli chodzi o naruszenia przepisów o ochronie danych osobowych, w PIPA przewidziano dodatkowy środek ochrony prawnej. Zgodnie z art. 39 PIPA każdy, kto poniósł szkodę w wyniku naruszenia PIPA lub utraty, kradzieży, ujawnienia, fałszerstwa, zmiany lub uszkodzenia jej danych osobowych, może dochodzić odszkodowania przed sądem. Nie ma takiego wymogu wzajemności jak w przypadku ustawy o odszkodowaniach od państwa.

Oprócz odszkodowania za szkody na podstawie ustawy o postępowaniu administracyjnosądowym można skorzystać z administracyjnych środków dochodzenia roszczeń z tytułu działań lub zaniechań organów administracji. Każda osoba fizyczna może zaskarżyć decyzję (tj. wykonanie lub odmowę wykonania uprawnień publicznych w konkretnej sprawie) lub zaniechanie (długotrwałe niepodejmowanie przez organ administracji określonego działania wbrew zobowiązaniu prawnemu), co może prowadzić do uchylenia/zmiany niezgodnej z prawem decyzji, do stwierdzenia nieważności (tj. stwierdzenia, że decyzja nie wywołuje skutków prawnych lub nie istnieje w porządku prawnym) lub stwierdzenia, że zaniechanie jest niezgodne z prawem ([166]). Zaskarżenie decyzji administracyjnej jest możliwe tylko wtedy, gdy bezpośrednio wpływa ona na prawa i obowiązki obywatelskie ([167]). Obejmuje to środki służące zbieraniu danych osobowych, czy to bezpośrednio (np. w drodze przechwytywania komunikacji), czy w drodze żądania ujawnienia (np. wobec dostawcy usług).

Odwołanie od decyzji administracyjnej można najpierw wnieść do administracyjnych komisji odwoławczych ustanowionych przy niektórych organach publicznych (np. NIS, NHRC) lub do Centralnej Administracyjnej Komisji Odwoławczej ustanowionej przy Komisji Antykorupcyjnej i Praw Obywatelskich ([168]). Takie odwołanie administracyjne stanowi alternatywny, mniej formalny sposób zakwestionowania decyzji lub zaniechania organu publicznego. Można jednak również wnieść pozew bezpośrednio do sądów koreańskich na podstawie ustawy o postępowaniu administracyjnym.

Wniosek o uchylenie/zmianę decyzji na podstawie ustawy o postępowaniu administracyjnosądowym może złożyć każda osoba mająca interes prawny w ubieganiu się o uchylenie/zmianę lub w przywróceniu jej praw w drodze uchylenia/zmiany, jeżeli decyzja już nie obowiązuje ([169]). Również o stwierdzenie nieważności może wystąpić osoba mająca interes prawny w takim stwierdzeniu, natomiast o stwierdzenie, że zaniechanie jest niezgodne z prawem, wystąpić może każda osoba, która złożyła wniosek o wydanie decyzji i ma interes prawny w dochodzeniu stwierdzenia takiej niezgodności z prawem ([170]). Zgodnie z orzecznictwem Sądu Najwyższego „interes prawny" jest rozumiany jako „interes prawnie chroniony", tj. bezpośredni i konkretny interes chroniony przepisami ustawowymi i wykonawczymi, na których opierają się decyzje administracyjne (niebędący ogólnym pośrednim i abstrakcyjnym interesem społeczeństwa) ([171]). Osoby fizyczne mają zatem taki interes prawny w przypadku naruszenia ograniczeń i zabezpieczeń, które mają zastosowanie do zbierania ich danych osobowych na potrzeby ścigania przestępstw (na mocy przepisów szczególnych lub PIPA). Wyrok kończący postępowanie w sprawie wydany na podstawie ustawy o postępowaniu administracyjnosądowym jest wiążący dla stron ([172]).

Ponadto wniosek o uchylenie/zmianę decyzji oraz wniosek o stwierdzenie niezgodności z prawem zaniechania należy złożyć w terminie 90 dni od dnia, w którym dana osoba fizyczna dowiedziała się o decyzji/zaniechaniu, i co do zasady

([161]) Art. 2 ust. 1 ustawy o odszkodowaniach od państwa.

([162]) Art. 9 i 12 ustawy o odszkodowaniach od państwa. W ustawie ustanawia się rady okręgowe (którym przewodniczy zastępca prokuratora odpowiedniej prokuratury), radę centralną (której przewodniczy wiceminister sprawiedliwości) i radę specjalną (której przewodniczy wiceminister obrony narodowej, odpowiedzialną za odszkodowania za szkody wyrządzone przez personel wojskowy lub cywilnych pracowników wojska). Powództwa o odszkodowanie są z zasady rozpatrywane przez rady okręgowe, które w określonych okolicznościach mogą przekazywać sprawy do rady centralnej lub specjalnej, np. jeśli dochodzone odszkodowanie przekracza określoną kwotę lub gdy osoba fizyczna wnioskuje o ponowne rozpatrzenie sprawy. Członków wszystkich rad powołuje minister sprawiedliwości (np. spośród urzędników publicznych Ministerstwa Sprawiedliwości, urzędników sądowych, prawników i osób posiadających wiedzę fachową w dziedzinie odszkodowań od państwa) i członkowie ci podlegają przepisom szczególnym dotyczącym konfliktu interesów (zob. art. 7 dekretu wykonawczego do ustawy o odszkodowaniach od państwa).

([163]) Art. 7 ustawy o odszkodowaniach od państwa.

([164]) Orzeczenie Sądu Najwyższego nr 2013Da208388 z dnia 11 czerwca 2015 r.

([165]) Zob. art. 8 ustawy o odszkodowaniach od państwa, jak również art. 751 kodeksu cywilnego.

([166]) Art. 2 i 4 ustawy o postępowaniu administracyjnosądowym.

([167]) Orzeczenie Sądu Najwyższego nr 98Du18435 z dnia 22 października 1999 r., orzeczenie Sądu Najwyższego nr 99Du1113 z dnia 8 września 2000 r. oraz orzeczenie Sądu Najwyższego nr 2010Du3541 z dnia 27 września 2012 r.

([168]) Art. 6 ustawy o odwołaniach administracyjnych i art. 18 ust. 1 ustawy o postępowaniu administracyjnosądowym.

([169]) Art. 12 ustawy o postępowaniu administracyjnosądowym.

([170]) Art. 35 i 36 ustawy o postępowaniu administracyjnosądowym.

([171]) Orzeczenie Sądu Najwyższego nr 2006Du330 z dnia 26 marca 2006 r.

([172]) Art. 30 ust. 1 ustawy o postępowaniu administracyjnosądowym.

nie później niż w ciągu roku od dnia wydania decyzji lub wystąpienia zaniechania, chyba że istnieją uzasadnione przyczyny zwłoki ([173]). Zgodnie z orzecznictwem Sądu Najwyższego pojęcie „uzasadnionych przyczyn" należy interpretować szeroko i wymaga ono oceny, czy w świetle wszystkich okoliczności sprawy wniesienie skargi po terminie jest dopuszczalne społecznie ([174]). Obejmuje to (między innymi) przyczyny opóźnień, za które dana strona nie może być odpowiedzialna (tj. sytuacje, które są poza kontrolą skarżącego, na przykład gdy nie został on powiadomiony o zbieraniu jego danych osobowych) lub siłę wyższą (np. klęski żywiołowe, wojny).

Ponadto osoby fizyczne mogą wnieść skargę konstytucyjną do Trybunału Konstytucyjnego ([175]). Zgodnie z ustawą o Trybunale Konstytucyjnym każda osoba, której prawa podstawowe zagwarantowane w konstytucji zostały naruszone w wyniku wykonywania lub niewykonania władzy państwowej (z wyłączeniem orzeczeń sądów), może wnieść skargę konstytucyjną. Jeśli dostępne są inne środki ochrony prawnej, należy je wyczerpać w pierwszej kolejności. Zgodnie z orzecznictwem Trybunału Konstytucyjnego cudzoziemcy mogą wnieść skargę konstytucyjną w zakresie, w jakim ich prawa podstawowe są uznawane na mocy konstytucji koreańskiej (zob. wyjaśnienia w pkt 1.1) ([176]). Skargę konstytucyjną należy wnieść w terminie 90 dni od chwili, w której dana osoba dowiedziała się o naruszeniu, oraz w terminie jednego roku od jego wystąpienia. Ponieważ procedura przewidziana w ustawie o postępowaniu administracyjnosądowym ma zastosowanie do postępowania sądowego na mocy ustawy o Trybunale Konstytucyjnym ([177]), skarga będzie nadal dopuszczalna, jeśli występują „uzasadnione przyczyny" zgodnie z wykładnią dokonaną w orzecznictwie Sądu Najwyższego, o którym mowa powyżej.

Jeżeli w pierwszej kolejności konieczne jest wyczerpanie innych środków ochrony prawnej, skargę konstytucyjną należy wnieść w terminie 30 dni od zapadnięcia prawomocnego orzeczenia w sprawie tego środka ([178]). Trybunał Konstytucyjny może uchylić akt organu administracji rządowej, który spowodował naruszenie, lub potwierdzić, że określone zaniechanie jest niezgodne z konstytucją ([179]). W takim przypadku właściwy organ jest zobowiązany do wdrożenia środków w celu zastosowania się do orzeczenia Trybunału.

3. DOSTĘP RZĄDOWY DO CELÓW BEZPIECZEŃSTWA NARODOWEGO

3.1. Właściwe organy publiczne w obszarze bezpieczeństwa narodowego

Republika Korei posiada dwie wyspecjalizowane agencje wywiadowcze: Narodową Służbę Wywiadu (ang. National Intelligence Service, NIS) i Dowództwo Wsparcia Bezpieczeństwa Wojskowego (ang. Defense Security Support Command). Dane osobowe do celów bezpieczeństwa narodowego mogą zbierać również policja i prokuratura.

NIS, ustanowiona ustawą o Narodowej Służbie Wywiadu (zwaną dalej „ustawą o NIS"), należy do zakresu kompetencji prezydenta i działa pod jego nadzorem ([180]). W szczególności NIS zbiera, kompiluje i rozpowszechnia informacje o państwach obcych (i o Korei Północnej) ([181]), informacje wywiadowcze związane z zadaniami w zakresie zwalczania szpiegostwa (w tym szpiegostwa wojskowego i przemysłowego), terroryzmu i działalności międzynarodowych grup przestępczych, dane wywiadowcze dotyczące niektórych rodzajów przestępstw przeciwko bezpieczeństwu publicznemu i narodowemu (np. rewolucja wewnątrz kraju, podżeganie do agresji zewnętrznej) oraz dane wywiadowcze związane z zadaniem polegającym na zapewnieniu cyberbezpieczeństwa oraz zapobieganiu lub przeciwdziałaniu cyberatakom i cyberzagrożeniom ([182]). Ustawa o NIS, w której ustanowiono NIS i określono jej zadania, zawiera również ogólne zasady, które wyznaczają ramy wszystkich działań Służby. Co do zasady NIS musi zachować neutralność polityczną oraz chronić wolność i prawa osób fizycznych ([183]). Zadaniem dyrektora NIS jest opracowanie ogólnych wytycznych określających zasady, zakres i procedury wykonywania przez NIS obowiązków dotyczących zbierania i wykorzystywania danych, a następnie przedstawienie ich Zgromadzeniu Narodowemu ([184]). Zgromadzenie Narodowe (za pośrednictwem Komisji ds. Wywiadu) może zażądać skorygowania lub uzupełnienia wytycznych, jeżeli uzna, że są one niezgodne z prawem lub niesprawiedliwe. Ogólnie rzecz biorąc, podczas wykonywania swoich obowiązków dyrektor i personel NIS nie mogą nadużywać swojej władzy publicznej w celu zmuszenia jakiejkolwiek instytucji, organizacji lub osoby fizycznej do czynności, których ta nie ma obowiązku wykonać, ani nie może utrudniać jakiejkolwiek osobie wykonywania przysługujących jej praw ([185]). Ponadto cenzura poczty, przechwytywanie przekazów telekomunikacyjnych, zbieranie informacji dotyczących lokalizacji, zbieranie danych potwierdzających komunikację, nagrywanie lub

([173]) Art. 20 ustawy o postępowaniu administracyjnosądowym. Termin ten ma również zastosowanie do wniosku o stwierdzenie niezgodności z prawem zaniechania, zob. art. 38 ust. 2 ustawy o postępowaniu administracyjnosądowym.
([174]) Orzeczenie Sądu Najwyższego nr 90Nu6521 z dnia 28 czerwca 1991 r.
([175]) Art. 68 ust. 1 ustawy o Trybunale Konstytucyjnym.
([176]) Orzeczenie Trybunału Konstytucyjnego nr 99HeonMa194 z dnia 29 listopada 2001 r.
([177]) Art. 40 ustawy o Trybunale Konstytucyjnym.
([178]) Art. 69 ustawy o Trybunale Konstytucyjnym.
([179]) Art. 75 ust. 3 ustawy o Trybunale Konstytucyjnym.
([180]) Art. 2 i art. 4 ust. 2 ustawy o NIS.
([181]) Pojęcie to nie obejmuje danych dotyczących osób fizycznych, lecz dane dotyczące informacji ogólnych o państwach obcych (tendencje, rozwój sytuacji) oraz o działalności podmiotów państwowych z państw trzecich.
([182]) Art. 3 ust. 1 ustawy o NIS.
([183]) Art. 3 ust. 1, art. 6 ust. 2, art. 11 i 21. Zob. również przepisy dotyczące konfliktu interesów, w szczególności art. 10 i 12.
([184]) Art. 4 ust. 2 ustawy o NIS.
([185]) Art. 13 ustawy o NIS.

podsłuchiwanie prywatnych rozmów przez NIS musi się odbywać w zgodzie z CPPA, ustawą o informacjach dotyczących lokalizacji lub CPA ([186]). Każde nadużycie władzy lub zbieranie danych z naruszeniem tych przepisów jest zagrożone sankcjami karnymi ([187]).

Dowództwo Wsparcia Bezpieczeństwa Wojskowego jest agencją wywiadu wojskowego podlegającą Ministerstwu Obrony. Odpowiada za sprawy dotyczące bezpieczeństwa w wojsku, prowadzenie postępowań przygotowawczych w sprawach o przestępstwa związane z wojskiem (z zastrzeżeniem ustawy o sądach wojskowych) oraz za wywiad wojskowy. Ogólnie rzecz biorąc, Dowództwo Wsparcia Bezpieczeństwa Wojskowego nie prowadzi nadzoru nad osobami cywilnymi, chyba że jest to niezbędne do wykonywania jego funkcji wojskowych. Może prowadzić postępowania przygotowawcze wobec personelu wojskowego, cywilnych pracowników wojska, osób odbywających szkolenie wojskowe, osób odbywających służbę wojskową w rezerwie lub poborowych oraz jeńców wojennych ([188]). Zbierając informacje dotyczące komunikacji do celów bezpieczeństwa narodowego, Dowództwo Wsparcia Bezpieczeństwa Wojskowego podlega ograniczeniom i zabezpieczeniom określonym w CPPA i dekrecie wykonawczym do CPPA.

3.2. **Podstawa prawna i ograniczenia**

CPPA, ustawa o zwalczaniu terroryzmu do celów ochrony obywateli i bezpieczeństwa publicznego (zwana dalej „ustawą o zwalczaniu terroryzmu") oraz TBA zapewniają podstawy prawne do zbierania danych osobowych do celów bezpieczeństwa narodowego oraz określają obowiązujące ograniczenia i zabezpieczenia ([189]). Te ograniczenia i zabezpieczenia, które opisano w poniższych sekcjach, gwarantują, że zbieranie i przetwarzanie informacji jest ograniczone do tego, co jest absolutnie niezbędne do osiągnięcia uzasadnionego celu. Wyklucza to jakiekolwiek masowe i nieograniczone zbieranie danych osobowych do celów bezpieczeństwa narodowego.

3.2.1. *Zbieranie informacji dotyczących komunikacji*

3.2.1.1. Zbieranie informacji dotyczących komunikacji przez agencje wywiadowcze

3.2.1.1.1. Podstawa prawna

CPPA upoważnia agencje wywiadowcze do zbierania danych dotyczących komunikacji i wymaga od dostawców usług komunikacyjnych realizowania wniosków tych agencji ([190]). Jak opisano w pkt 2.2.2.1, w CPPA rozróżnia się zbieranie treści komunikacji (tj. „środki ograniczające komunikację", takie jak środki obejmujące „podsłuchy" lub „cenzurę" ([191])) i zbieranie „danych potwierdzających komunikację" ([192]).

Próg zbierania tych dwóch rodzajów danych jest różny, ale obowiązujące procedury i zabezpieczenia są w dużej mierze identyczne ([193]). Zbieranie danych potwierdzających komunikację (metadanych) może mieć miejsce w celu zapobiegania zagrożeniom dla bezpieczeństwa narodowego ([194]). Wyższy próg obowiązuje w przypadku korzystania ze środków ograniczających komunikację (tj. zbierania treści komunikacji), które można stosować wyłącznie w przypadku, gdy spodziewane jest poważne zagrożenie dla bezpieczeństwa narodowego, a zbieranie danych wywiadowczych jest niezbędne do zapobieżenia takiemu zagrożeniu (tj. gdy istnieje poważne zagrożenie dla bezpieczeństwa narodowego, a zbieranie danych jest niezbędne do zapobieżenia mu) ([195]). Ponadto dostęp do treści komunikacji można wykorzystywać wyłącznie jako środek ostateczny w celu ochrony bezpieczeństwa narodowego, a ponadto należy podjąć starania w celu zminimalizowania naruszenia prywatności komunikacji ([196]). Nawet w przypadku uzyskania odpowiedniej zgody/odpowiedniego zezwolenia należy natychmiast zaprzestać stosowania środków ograniczających komunikację, jeżeli przestaną być potrzebne, zapewniając w ten sposób ograniczenie do minimum wszelkich naruszeń poufności komunikacji danej osoby fizycznej ([197]).

3.2.1.1.2. Ograniczenia i zabezpieczenia mające zastosowanie do zbierania informacji dotyczących komunikacji obejmującej co najmniej jednego obywatela Korei

Zbieranie informacji dotyczących komunikacji (zarówno treści, jak i metadanych), w przypadku gdy jedna osoba lub obie osoby fizyczne uczestniczące w komunikacji są obywatelami Korei, może odbywać się wyłącznie za zgodą Prezesa

([186]) Art. 14 ustawy o NIS.
([187]) Zob. również art. 22 i 23 ustawy o NIS.
([188]) Art. 1 ustawy o sądach wojskowych.
([189]) Prowadząc postępowania przygotowawcze w sprawie przestępstw związanych z bezpieczeństwem narodowym, policja i NIS działają na podstawie CPA, natomiast Dowództwo Wsparcia Bezpieczeństwa Wojskowego podlega ustawie o sądach wojskowych.
([190]) Art. 15-2 CPPA.
([191]) Art. 2 ust. 6 i 7 CPPA.
([192]) Art. 2 ust. 11 CPPA.
([193]) Zob. również art. 13-4 ust. 2 CPPA i art. 37 ust. 4 dekretu wykonawczego do CPPA, zgodnie z którymi procedury mające zastosowanie do zbierania treści komunikacji mają również odpowiednio zastosowanie do zbierania danych potwierdzających komunikację.
([194]) Art. 13-4 CPPA.
([195]) Art. 7 ust. 1 CPPA.
([196]) Art. 3 ust. 2 CPPA.
([197]) Art. 2 dekretu wykonawczego do CPPA.

Sądu Apelacyjnego ([198]). Agencja wywiadowcza musi złożyć pisemny wniosek do prokuratora lub prokuratury apelacyjnej ([199]). We wniosku należy wskazać powody zbierania danych (tj. spodziewane poważne zagrożenie dla bezpieczeństwa narodowego lub konieczność zbierania danych w celu zapobieżenia zagrożeniom dla bezpieczeństwa narodowego), wraz z materiałami potwierdzającymi te powody i wskazującymi zasadność zbierania, jak również szczegóły wniosku (tj. cele, osobę lub osoby fizyczne, których dotyczy wniosek, zakres, okres zbierania danych, jak również sposób i miejsce zbierania danych) ([200]). Prokurator/prokuratura apelacyjna występuje następnie o zgodę do Prezesa Sądu Apelacyjnego ([201]). Prezes może wydać pisemną zgodę tylko wtedy, gdy uzna wniosek za zasadny, a odrzuci go, jeżeli uzna go za bezpodstawny ([202]). W nakazie określa się rodzaj, cel, zakres, miejsce i sposób zbierania danych oraz treści objęte zbieraniem ([203]).

W przypadku gdy środek ma na celu prowadzenie śledztwa w sprawie aktu zmowy zagrażającej bezpieczeństwu narodowemu oraz w sytuacji nadzwyczajnej, która uniemożliwia zastosowanie wspomnianych procedur, zastosowanie mają przepisy szczególne ([204]). Jeżeli te warunki są spełnione, agencje wywiadowcze mogą stosować środki nadzoru bez uprzedniej zgody sądu ([205]). Jednak natychmiast po zastosowaniu środków nadzwyczajnych agencja wywiadowcza musi zwrócić się do sądu o udzielenie zezwolenia. Jeżeli zezwolenie sądu nie zostanie uzyskane w ciągu 36 godzin od chwili podjęcia działań, należy ich natychmiast zaprzestać ([206]). Zbieranie informacji w sytuacjach nadzwyczajnych musi zawsze odbywać się zgodnie z „oświadczeniem o cenzurze/podsłuchu w sytuacji nadzwyczajnej", przy czym agencja wywiadowcza zajmująca się zbieraniem musi prowadzić rejestr wszystkich środków nadzwyczajnych ([207]).

W przypadku szybkiego zakończenia nadzoru, co wyklucza możliwość uzyskania zezwolenia sądu, właściwa prokuratura apelacyjna musi przesłać zawiadomienie o środkach nadzwyczajnych przygotowane przez agencję wywiadowczą do prezesa sądu właściwego, który prowadzi rejestr środków nadzwyczajnych ([208]). Umożliwia to sądowi zbadanie legalności zbierania danych.

3.2.1.1.3. Ograniczenia i zabezpieczenia mające zastosowanie do zbierania informacji dotyczących komunikacji obejmującej wyłącznie osoby niebędące obywatelami Korei.

Aby zbierać dane dotyczące komunikacji wyłącznie między osobami niebędącymi obywatelem Korei, agencje wywiadowcze muszą uzyskać uprzednią pisemną zgodę prezydenta ([209]). Takie dane dotyczące komunikacji można zbierać do celów bezpieczeństwa narodowego wyłącznie wówczas, gdy należą do jednej z kilku wymienionych kategorii, tj. komunikacji między urzędnikami państwowymi lub innymi osobami z państw wrogich Republice Korei, zagranicznymi agencjami, grupami lub obywatelami podejrzanymi o prowadzenie działalności antykoreańskiej ([210]) lub członkami grup na Półwyspie Koreańskim w praktyce pozostających poza jurysdykcją Republiki Korei, oraz ich grup parasolowych mających siedzibę w innych państwach ([211]) Jeżeli natomiast jedna strona komunikacji jest obywatelem Korei, a druga nie jest obywatelem Korei, wymagana będzie zgoda sądu zgodnie z procedurą opisaną w pkt 3.2.1.1.2.

Szef agencji wywiadowczej musi przedłożyć dyrektorowi NIS plan zakładanych działań ([212]). Dyrektor NIS sprawdza, czy plan jest odpowiedni, a jeśli tak, przedkłada go prezydentowi do zatwierdzenia ([213]). Plan musi zawierać takie same informacje jak te wymagane w przypadku wniosku o udzielenie przez sąd zezwolenia na zbieranie informacji o obywatelach Korei (jak opisano powyżej) ([214]). W szczególności należy w nim wskazać powody zbierania danych (tj. spodziewane poważne zagrożenie dla bezpieczeństwa narodowego lub konieczność zbierania danych w celu zapobiegania zagrożeniom dla bezpieczeństwa narodowego), główne powody podejrzenia, wraz z materiałami potwierdzającymi te

([198]) Art. 7 ust. 1 pkt 1 CPPA. Sądem właściwym jest sąd apelacyjny właściwy dla miejsca zamieszkania lub siedziby jednej strony lub obu stron podlegających nadzorowi.
([199]) Art. 7 ust. 3 dekretu wykonawczego do CPPA.
([200]) Art. 7 ust. 3 i art. 6 ust. 4 CPPA.
([201]) Art. 7 ust. 4 dekretu wykonawczego do CPPA. Wniosek prokuratora do sądu musi określać główne podstawy podejrzeń oraz, w zakresie, w jakim wniosek obejmuje szereg zgód jednocześnie – ich uzasadnienie (zob. art. 4 dekretu wykonawczego do CPPA).
([202]) Art. 7 ust. 3, art. 6 ust. 5 i art. 6 ust. 9 CPPA.
([203]) Art. 7 ust. 3 i art. 6 ust. 6 CPPA.
([204]) Art. 8 CPPA.
([205]) Art. 8 ust. 1 CPPA.
([206]) Art. 8 ust. 2 CPPA.
([207]) Art. 8 ust. 4 CPPA. Więcej informacji na temat środków nadzwyczajnych w kontekście ścigania przestępstw przedstawiono w pkt 2.2.2.2 powyżej.
([208]) Art. 8 ust. 5 i 7 CPPA. W powiadomieniu należy wskazać cel, przedmiot, zakres, okres, miejsce i sposób przeprowadzania nadzoru, jak również powód niezłożenia wniosku przed zastosowaniem środka (art. 8 ust. 6 CPPA).
([209]) Art. 7 ust. 1 pkt 2 CPPA.
([210]) Dotyczy to do działań, które zagrażają istnieniu i bezpieczeństwu narodu, ładowi demokratycznemu lub przetrwaniu i wolności ludności.
([211]) Ponadto, jeżeli jedną ze stron jest osoba opisana w art. 7 ust. 1 pkt 2 CPPA, a druga strona jest nieznana lub nie można jej określić, zastosowanie ma procedura przewidziana w art. 7 ust. 1 pkt 2.
([212]) Art. 8 ust. 1 dekretu wykonawczego do CPPA. Dyrektora NIS powołuje prezydent po zatwierdzeniu przez parlament (art. 7 ustawy o NIS).
([213]) Art. 8 ust. 2 dekretu wykonawczego do CPPA.
([214]) Art. 8 ust. 3 dekretu wykonawczego do CPPA w związku z art. 6 ust. 4 CPPA.

powody i wskazującymi zasadność zbierania, jak również szczegóły wniosku (tj. cele, osobę lub osoby fizyczne, których dotyczy wniosek, zakres, okres zbierania danych, jak również sposób i miejsce zbierania danych). W przypadku występowania o szereg zgód jednocześnie, należy podać ich cel i podstawy ([215]).

W sytuacjach nadzwyczajnych ([216]) należy uzyskać uprzednią zgodę ministra odpowiedzialnego za daną agencję wywiadowczą. Jednak w tym przypadku agencja wywiadowcza musi zwrócić się o zgodę do prezydenta niezwłocznie po zastosowaniu środków nadzwyczajnych. Jeżeli agencja wywiadowcza nie uzyska zgody w ciągu 36 godzin od złożenia wniosku, zbierania danych należy natychmiast zaprzestać ([217]). W takich przypadkach zebrane dane są zawsze niszczone.

3.2.1.1.4 Ogólne ograniczenia i zabezpieczenia

Wzywając podmioty prywatne do współpracy, agencje wywiadowcze muszą przedstawić im nakaz sądowy/zgodę prezydenta lub odpis oświadczenia o cenzurze w sytuacji nadzwyczajnej, które podmiot wezwany do współpracy musi przechowywać w swoich rejestrach ([218]). Podmioty, których agencje wywiadowcze wezwały do ujawnienia informacji na podstawie CPPA, mogą odmówić ich udostępnienia, jeżeli upoważnienie lub oświadczenie o cenzurze w sytuacji nadzwyczajnej odnosi się do niewłaściwego identyfikatora (np. numeru telefonu należącego do innej osoby fizycznej niż osoba, która została zidentyfikowana). Ponadto nigdy nie można ujawniać haseł używanych do prowadzenia komunikacji ([219]).

Agencje wywiadowcze mogą powierzyć wykonanie środków ograniczających komunikację lub zbieranie danych potwierdzających komunikację urzędowi pocztowemu lub dostawcy usług telekomunikacyjnych (zgodnie z definicją zawartą w ustawie o działalności telekomunikacyjnej) ([220]). Zarówno dana agencja wywiadowcza, jak i dostawca otrzymujący wniosek o współpracę muszą przez trzy lata przechowywać zapisy wskazujące cel złożenia wniosku o zastosowanie środków, datę wykonania lub współpracy oraz przedmiot środków (np. poczta, telefon, e-mail) ([221]). Dostawcy usług telekomunikacyjnych udostępniający dane potwierdzające komunikację muszą przechowywać rejestry przez siedem lat i dwa razy w roku przedkładać Ministrowi Nauki i Technologii Informacyjno-Komunikacyjnych stosowne sprawozdania ([222]).

Ponadto agencje wywiadowcze muszą przedkładać dyrektorowi NIS sprawozdania na temat zebranych przez siebie informacji i wyników działań nadzorczych ([223]). Jeśli chodzi o zbieranie danych potwierdzających komunikację, należy przechowywać rejestry dotyczące faktu złożenia wniosku o takie dane, jak również samego pisemnego wniosku oraz instytucji, która działała na jego podstawie ([224]).

Zbieranie treści komunikacji i danych potwierdzających komunikację może trwać maksymalnie cztery miesiące, a jeżeli w międzyczasie zostanie osiągnięty zamierzony cel, musi zostać natychmiast przerwane ([225]). Jeżeli warunki, w związku z którymi uzyskano zgodę, utrzymują się, okres ten można przedłużyć o maksymalnie cztery miesiące za zgodą sądu lub prezydenta. Wniosek o uzyskanie zezwolenia na przedłużenie stosowania środków nadzoru należy sporządzić na piśmie, podając uzasadnienie wniosku o przedłużenie i załączając materiały potwierdzające ([226]).

W zależności od podstawy prawnej zbierania danych, osoby fizyczne są zazwyczaj powiadamiane o zbieraniu informacji na temat ich komunikacji. W szczególności niezależnie od tego, czy zbierane informacje dotyczą treści komunikacji czy danych potwierdzających komunikację, oraz niezależnie od tego, czy informacje uzyskano w drodze zwykłej procedury czy w sytuacji nadzwyczajnej, szef agencji wywiadowczej musi powiadomić daną osobę o zastosowanym środku nadzoru na piśmie w terminie 30 dni od daty zakończenia nadzoru ([227]). Powiadomienie musi zawierać: 1) informację

([215]) Art. 8 ust. 3 i art. 4 dekretu wykonawczego do CPPA.
([216]) Tzn. gdy środek jest skierowany przeciwko aktowi zmowy zagrażającej bezpieczeństwu narodowemu, nie ma wystarczająco dużo czasu na uzyskanie zgody prezydenta, a nieprzyjęcie środków nadzwyczajnych może naruszyć bezpieczeństwo narodowe (art. 8 ust. 8 CPPA).
([217]) Art. 8 ust. 9 CPPA.
([218]) Art. 9 ust. 2 CPPA i art. 12 dekretu wykonawczego do CPPA.
([219]) Art. 9 ust. 4 CPPA.
([220]) Art. 13 dekretu wykonawczego do CPPA.
([221]) Art. 9 ust. 3 CPPA i art. 17 ust. 2 dekretu wykonawczego do CPPA. Okres ten nie ma zastosowania do danych potwierdzających komunikację (zob. art. 39 dekretu wykonawczego do CPPA).
([222]) Art. 13 ust. 7 CPPA i art. 39 dekretu wykonawczego do CPPA.
([223]) Art. 18 ust. 3 dekretu wykonawczego do CPPA.
([224]) Art. 13 ust. 5 i art. 13-4 ust. 3 CPPA.
([225]) Art. 7 ust. 2 CPPA.
([226]) Art. 7 ust. 2 CPPA i art. 5 dekretu wykonawczego do CPPA.
([227]) Art. 9-2 ust. 3 CPPA. Zgodnie z art. 13-4 CPPA dotyczy to zbierania zarówno treści komunikacji, jak i danych potwierdzających komunikację.

o zbieraniu danych, 2) nazwę agencji stosującej środki oraz 3) okres stosowania. Jeżeli jednak istnieje prawdopodobieństwo, że powiadomienie zagroziłoby bezpieczeństwu narodowemu lub życiu i bezpieczeństwu fizycznemu ludzi, powiadomienie można odroczyć ([228]). Powiadomienie musi zostać dostarczone w terminie 30 dni od ustania przyczyn odroczenia ([229]).

Ten wymóg powiadomienia ma jednak zastosowanie wyłącznie do zbierania informacji, w przypadku gdy przynajmniej jedna ze stron jest obywatelem Korei. W związku z tym osoby niebędące obywatelami Korei będą powiadamiane tylko w przypadku zbierania informacji o ich kontaktach z obywatelami Korei. Nie ma zatem wymogu powiadamiania w przypadku zbierania danych dotyczących komunikacji wyłącznie między osobami niebędącymi obywatelami Korei.

Treść wszelkich komunikatów, jak również dane potwierdzające komunikację uzyskane w drodze nadzoru na podstawie CPPA można wykorzystywać wyłącznie: 1) w celu prowadzenia postępowań przygotowawczych w sprawie określonych przestępstw, ścigania ich lub zapobiegania im, 2) w postępowaniu dyscyplinarnym, 3) w postępowaniu sądowym, jeżeli strona związana z daną komunikacją powołuje się na nie w roszczeniu o odszkodowanie lub 4) na podstawie innych przepisów ([230]).

3.2.1.2. Zbieranie informacji dotyczących komunikacji przez policję/prokuraturę do celów bezpieczeństwa narodowego

Policja/prokurator może pozyskiwać informacje dotyczące komunikacji (zarówno treść komunikacji, jak i dane potwierdzające komunikację) do celów bezpieczeństwa narodowego na tych samych warunkach, jak te opisane w pkt 3.2.1.1. W przypadku działań w sytuacjach nadzwyczajnych ([231]) stosuje się procedurę, którą opisano wcześniej w odniesieniu do zbierania treści komunikacji na potrzeby ścigania przestępstw w sytuacjach nadzwyczajnych (tj. art. 8 CPPA).

3.2.2. *Zbieranie informacji na temat osób podejrzanych o terroryzm*

3.2.2.1. Podstawa prawna

Ustawa o zwalczaniu terroryzmu upoważnia dyrektora NIS do zbierania informacji o osobach podejrzanych o terroryzm ([232]). „Osoba podejrzana o terroryzm" oznacza członka grupy terrorystycznej ([233]); osobę, która propaguje działalność grupy terrorystycznej (przez promowanie i rozpowszechnianie idei lub taktyk grupy terrorystycznej), pozyskuje lub przekazuje środki na działalność terrorystyczną ([234]) lub angażuje się w inne działania polegające na przygotowywaniu aktów terrorystycznych, zmowie, propagandzie lub podżeganiu do terroryzmu bądź osobę, co do której istnieją uzasadnione podejrzenia, że prowadziła taką działalność ([235]). Co do zasady każdy urzędnik publiczny wykonujący przepisy ustawy o zwalczaniu terroryzmu musi przestrzegać praw podstawowych zapisanych w konstytucji koreańskiej ([236]).

Ustawa o zwalczaniu terroryzmu sama w sobie nie określa konkretnych uprawnień, ograniczeń ani gwarancji dotyczących zbierania informacji o osobach podejrzanych o terroryzm, lecz odwołuje się do procedur zawartych w innych ustawach. Po pierwsze, na podstawie ustawy o zwalczaniu terroryzmu dyrektor NIS może zbierać 1) informacje dotyczące wjazdu na terytorium Republiki Korei i wyjazdu z niej, 2) informacje dotyczące transakcji finansowych oraz 3) informacje dotyczące komunikacji. W zależności od rodzaju poszukiwanych informacji właściwe wymogi proceduralne określono odpowiednio w ustawie o imigracji i ustawie celnej, ARUSFTI lub CPPA ([237]). W przypadku zbierania informacji dotyczących wjazdu do Korei i wyjazdu z niej ustawa o zwalczaniu terroryzmu odwołuje się do procedur

([228]) Art. 9-2 ust. 4 CPPA.
([229]) Art. 13-4 ust. 2 i art. 9-2 ust. 6 CPPA.
([230]) Art. 5 ust. 1–2, ust. 12 i 13-5 CPPA.
([231]) Tzn. gdy środek jest skierowany przeciwko aktowi zmowy zagrażającej bezpieczeństwu narodowemu, oraz w sytuacji nadzwyczajnej, która uniemożliwia zastosowanie zwykłej procedury uzyskania zgody (art. 8 ust. 1 CPPA).
([232]) Art. 9 ustawy o zwalczaniu terroryzmu.
([233]) „Grupa terrorystyczna" oznacza grupę terrorystyczną wskazaną przez Organizację Narodów Zjednoczonych (art. 2 ust. 2 ustawy o zwalczaniu terroryzmu).
([234]) „Terroryzm" zdefiniowano w art. 2 ust. 1 ustawy o zwalczaniu terroryzmu jako działanie prowadzone w celu utrudnienia wykonywania władzy przez państwo, organy samorządu terytorialnego lub rząd państwa obcego (w tym władze lokalne i organizacje międzynarodowe) lub w celu zmuszenia ich do podjęcia działań, do których nie są zobowiązane, lub w celu stworzenia zagrożenia dla społeczeństwa. Obejmuje to: a) zabójstwo lub stworzenie zagrożenia dla życia osoby poprzez spowodowanie obrażeń ciała lub zatrzymanie, uwięzienie, porwanie lub wzięcie osoby jako zakładnika; b) niektóre rodzaje działań skierowanych przeciwko statkowi powietrznemu (np. spowodowanie wypadku, porwanie lub uszkodzenie statku powietrznego w locie); c) niektóre rodzaje działań związanych ze statkami (np. zajęcie statku lub konstrukcji morskiej znajdującej się w eksploatacji, zniszczenie statku lub konstrukcji morskiej znajdującej się w eksploatacji lub spowodowanie ich uszkodzeń w stopniu zagrażającym ich bezpieczeństwu, w tym uszkodzenie ładunku załadowanego na statek lub konstrukcję morską znajdującą się w eksploatacji); d) umieszczenie, zdetonowanie lub użycie w jakikolwiek inny sposób broni biochemicznej, wybuchowej lub zapalającej bądź takiego urządzenia z zamiarem spowodowania śmierci, poważnego uszczerbku na zdrowiu lub poważnych szkód majątkowych lub wywołanie takiego skutku w niektórych rodzajach pojazdów lub obiektów (np. w pociągach, tramwajach, pojazdach silnikowych, parkach publicznych i na stacjach, w obiektach służących do dostarczania energii elektrycznej, gazu lub usług telekomunikacyjnych itp.); e) niektóre rodzaje działań związanych z materiałami jądrowymi, materiałami promieniotwórczymi lub obiektami jądrowymi (np. wywoływanie szkód dla życia i zdrowia ludzkiego lub mienia bądź w inny sposób zakłócanie bezpieczeństwa publicznego poprzez zniszczenie reaktora jądrowego lub manipulowanie materiałami promieniotwórczymi w sposób niewłaściwy itp.).
([235]) Art. 2 ust. 3 ustawy o zwalczaniu terroryzmu.
([236]) Art. 3 ust. 3 ustawy o zwalczaniu terroryzmu.
([237]) Art. 9 ust. 1 ustawy o zwalczaniu terroryzmu.

określonych w ustawie o imigracji i ustawie celnej. Obecnie jednak w ustawach tych nie przewidziano takich uprawnień. W odniesieniu do zbierania informacji o komunikacji i informacji o transakcjach finansowych ustawa o zwalczaniu terroryzmu odsyła do ograniczeń i zabezpieczeń przewidzianych w CPPA (które szczegółowo opisano poniżej) oraz w ARUSFTI (które, jak wyjaśniono w sekcji 2.1, nie mają znaczenia dla oceny na potrzeby decyzji stwierdzającej odpowiedni stopień ochrony).

Ponadto w art. 9 ust. 3 ustawy o zwalczaniu terroryzmu określono, że dyrektor NIS może zwrócić się do administratora danych osobowych ([238]) lub dostawcy informacji dotyczących lokalizacji ([239]) o udostępnienie danych osobowych lub informacji o lokalizacji osoby podejrzanej o terroryzm. Możliwość ta jest ograniczona do wniosków o dobrowolne ujawnienie, na które administratorzy danych osobowych i dostawcy informacji o lokalizacji nie mają obowiązku odpowiadać, a w każdym razie mogą to zrobić wyłącznie zgodnie z ustawą PIPA i ustawą o informacjach dotyczących lokalizacji (zob. pkt 3.2.2.2 poniżej).

3.2.2.2. Ograniczenia i zabezpieczenia mające zastosowanie do dobrowolnego ujawniania informacji na podstawie ustawy PIPA i ustawy o informacji dotyczących lokalizacji

Wnioski o dobrowolną współpracę na podstawie ustawy o zwalczaniu terroryzmu muszą być ograniczone do informacji o osobach podejrzanych o terroryzm (zob. pkt 3.2.2.1 powyżej). Każdy taki wniosek złożony przez NIS musi być zgodny z zasadami zgodności z prawem, konieczności i proporcjonalności wynikającymi z konstytucji koreańskiej (art. 12 ust. 1 i art. 37 ust. 2) ([240]), jak również z wymogami PIPA dotyczącymi zbierania danych osobowych (art. 3 ust. 1 PIPA, zob. pkt 1.2 powyżej). Ustawa o bezpieczeństwie sieci i informacji stanowi ponadto, że NIS nie może nadużywać swojej władzy publicznej w celu zmuszenia jakiejkolwiek instytucji, organizacji lub osoby fizycznej do czynności, których ta nie ma obowiązku wykonać, ani nie może utrudniać jakiejkolwiek osobie wykonywania przysługujących jej praw ([241]). Naruszenie tego zakazu może wiązać się z sankcjami karnymi ([242]).

Administratorzy danych osobowych i dostawcy informacji dotyczących lokalizacji otrzymujący wnioski od NIS na podstawie ustawy o zwalczaniu terroryzmu nie muszą się do nich stosować. Mogą się do nich zastosować dobrowolnie, ale wolno im to zrobić jedynie zgodnie z PIPA i ustawą o informacjach dotyczących lokalizacji. Jeśli chodzi o zgodność z przepisami PIPA, administrator danych musi w szczególności wziąć pod uwagę interesy osoby, której dane dotyczą, i nie może ujawnić informacji, jeżeli mogłoby to naruszyć w sposób nieuzasadniony interes tej osoby lub strony trzeciej ([243]). Ponadto, zgodnie z zawiadomieniem nr 2021-1 w sprawie przepisów uzupełniających dotyczących wykładni i stosowania ustawy o ochronie danych osobowych, osoba objęta wnioskiem musi zostać poinformowana o ujawnieniu informacji. W wyjątkowych okolicznościach powiadomienie takie można odroczyć, w szczególności w przypadku gdy i dopóki istnieje prawdopodobieństwo, że powiadomienie zagrażałoby toczącemu się postępowaniu przygotowawczemu lub że może spowodować szkodę dla życia lub integralności cielesnej innej osoby, o ile te prawa lub interesy są w oczywisty sposób nadrzędne wobec praw osoby, której dane dotyczą ([244]).

3.2.2.3. Ograniczenia i zabezpieczenia na podstawie CPPA

Zgodnie z ustawą o zwalczaniu terroryzmu agencje wywiadowcze mogą pozyskiwać informacje dotyczące komunikacji (zarówno treść komunikacji, jak i dane potwierdzające komunikację) wyłącznie wtedy, gdy jest to konieczne do prowadzenia działań antyterrorystycznych, tj. działań związanych z zapobieganiem i przeciwdziałaniem terroryzmowi. Procedury określone w CPPA opisane w pkt 3.2.1 mają zastosowanie do zbierania informacji dotyczących komunikacji do celów zwalczania terroryzmu.

3.2.3. *Dobrowolne ujawnianie informacji przez operatorów telekomunikacyjnych*

Zgodnie z TBA operatorzy telekomunikacyjni mogą wykonać wniosek o ujawnienie „danych dotyczących komunikacji" złożony przez agencję wywiadowczą, która zamierza zebrać te informacje w celu zapobieżenia zagrożeniu dla bezpieczeństwa narodowego ([245]). Każdy taki wniosek musi być zgodny z zasadami zgodności z prawem, konieczności i proporcjonalności wynikającymi z konstytucji koreańskiej (art. 12 ust. 1 i art. 37 ust. 2) ([246]), jak również z wymogami PIPA dotyczącymi zbierania danych osobowych (art. 3 ust. 1 PIPA, zob. pkt 1.2 powyżej). Ponadto zastosowanie mają te same ograniczenia i zabezpieczenia, co w przypadku dobrowolnego ujawnienia na potrzeby ścigania przestępstw (zob. pkt 2.2.3) ([247]).

([238]) Zgodnie z definicją zawartą w art. 2 PIPA, tj. instytucja publiczna, osoba prawna, organizacja, osoba fizyczna itp., która w sposób bezpośredni lub pośredni przetwarza dane osobowe, aby obsługiwać dokumenty zawierające dane osobowe do celów urzędowych lub biznesowych.

([239]) Zgodnie z definicją zawartą w art. 5 ustawy o ochronie, wykorzystaniu itp. informacji dotyczących lokalizacji (zwanej dalej „ustawą o informacjach dotyczących lokalizacji"), tj. każdy, kto uzyskał od Koreańskiej Komisji Telekomunikacyjnej zezwolenie na prowadzenie działalności związanej z informacjami dotyczącymi lokalizacji.

([240]) Zob. również art. 3 ust. 2 i 3 ustawy o zwalczaniu terroryzmu.

([241]) Art. 11 ust. 1 ustawy o NIS.

([242]) Art. 19 ustawy o NIS.

([243]) Art. 18 ust. 2 PIPA.

([244]) Zawiadomienie nr 2021-1 PIPC w sprawie przepisów uzupełniających dotyczących wykładni i stosowania ustawy o ochronie danych osobowych, sekcja III pkt 2 ppkt (iii).

([245]) Art. 83 ust. 3 TBA.

([246]) Zob. również art. 3 ust. 2 i 3 ustawy o zwalczaniu terroryzmu.

([247]) W szczególności wniosek musi zostać złożony na piśmie i zawierać uzasadnienie, jak również powiązanie z danym użytkownikiem i zakres żądanych informacji, a przedsiębiorca telekomunikacyjny musi rejestrować takie wnioski i dwa razy w roku przedkładać sprawozdanie Ministrowi Nauki i Technologii Informacyjno-Komunikacyjnych.

Przedsiębiorca telekomunikacyjny nie jest zobowiązany do uwzględnienia wniosku, ale może to zrobić dobrowolnie i wyłącznie zgodnie z PIPA. W tym względzie do przedsiębiorców telekomunikacyjnych mają zastosowanie te same obowiązki, w tym w odniesieniu do powiadamiania osób fizycznych, co w przypadku wniosków otrzymanych od organów ścigania w sprawach karnych, jak wyjaśniono szczegółowo w sekcji 2.2.3.

3.3. **Nadzór**

Działalność koreańskich agencji wywiadowczych nadzoruje szereg różnych organów. Nadzór nad Dowództwem Wsparcia Bezpieczeństwa Wojskowego prowadzi Ministerstwo Obrony Narodowej, zgodnie z rozporządzeniem ministra w sprawie wdrożenia audytu wewnętrznego. NIS podlega nadzorowi ze strony władzy wykonawczej, Zgromadzenia Narodowego i innych niezależnych organów, jak wyjaśniono szczegółowo poniżej.

3.3.1. *Urzędnik ds. ochrony praw człowieka*

W przypadku zbierania przez agencje wywiadowcze informacji na temat osób podejrzanych o terroryzm ustawa o zwalczaniu terroryzmu przewiduje nadzór ze strony Komisji ds. Zwalczania Terroryzmu i urzędnika ds. ochrony praw człowieka ([248]).

Komisja ds. Zwalczania Terroryzmu m.in. opracowuje politykę dotyczącą działań w zakresie zwalczania terroryzmu i nadzoruje wdrażanie środków służących zwalczaniu terroryzmu, a także działania różnych właściwych organów zajmujących się zwalczaniem terroryzmu ([249]). Komisji przewodniczy premier, a w jej skład wchodzi szereg ministrów i szefów agencji rządowych, m.in. minister spraw zagranicznych, minister sprawiedliwości, minister obrony narodowej, minister spraw wewnętrznych i bezpieczeństwa, dyrektor NIS, komisarz generalny Agencji Policji Krajowej oraz przewodniczący Komisji Usług Finansowych ([250]). Podczas prowadzenia śledztw antyterrorystycznych i śledzenia osób podejrzanych o terroryzm w celu zebrania informacji lub materiałów niezbędnych do działań antyterrorystycznych dyrektor NIS musi składać sprawozdania przewodniczącemu Komisji ds. Zwalczania Terroryzmu (tj. premierowi) ([251]).

Ustawą o zwalczaniu terroryzmu ustanowiono ponadto instytucję urzędnika ds. ochrony praw człowieka w celu ochrony praw podstawowych osób fizycznych przed naruszaniem tych praw w wyniku działań antyterrorystycznych ([252]). Urzędnika ds. ochrony praw człowieka powołuje przewodniczący Komisji ds. Zwalczania Terroryzmu spośród osób, które spełniają kwalifikacje wymienione w dekrecie wykonawczym do ustawy o zwalczaniu terroryzmu (tj. każdy, kto posiada uprawnienia radcy prawnego z co najmniej dziesięcioletnim doświadczeniem zawodowym lub posiada wiedzę specjalistyczną w dziedzinie praw człowieka i pracuje lub pracował (przynajmniej) jako profesor nadzwyczajny przez co najmniej dziesięć lat, lub pracował jako wyższy urzędnik publiczny w agencjach państwowych lub organach samorządu terytorialnego, lub posiada co najmniej dziesięcioletnie doświadczenie zawodowe w dziedzinie praw człowieka, np. w organizacji pozarządowej) ([253]). Urzędnik ds. ochrony praw człowieka jest powoływany na dwa lata (z możliwością przedłużenia kadencji) i może zostać usunięty ze stanowiska tylko z określonych, ograniczonych przyczyn i z ważnego powodu, np. jeżeli zostanie oskarżony w sprawie karnej związanej z jego obowiązkami, gdy ujawnia informacje poufne lub z powodu długotrwałej niepełnosprawności intelektualnej lub fizycznej ([254]).

Jeśli chodzi o uprawnienia, urzędnik ds. ochrony praw człowieka może wydawać zalecenia dotyczące zwiększenia ochrony praw człowieka przez agencje zaangażowane w działania antyterrorystyczne oraz rozpatrywać wnioski publiczne (zob. pkt 3.4.3) ([255]). W przypadku gdy można w sposób uzasadniony stwierdzić naruszenie praw człowieka w trakcie wykonywania obowiązków służbowych, urzędnik ds. ochrony praw człowieka może zalecić szefowi odpowiedzialnej agencji skorygowanie takiego naruszenia ([256]). Odpowiedzialna agencja musi natomiast powiadomić urzędnika ds. ochrony praw człowieka o działaniach podjętych w celu wykonania takiego zalecenia ([257]). Jeśli agencja nie wdroży zalecenia urzędnika ds. ochrony praw człowieka, sprawa zostaje przekazana Komisji, w tym jej przewodniczącemu – premierowi. Do tej pory nie odnotowano przypadków niewdrożenia zaleceń urzędnika ds. ochrony praw człowieka.

3.3.2. *Zgromadzenie Narodowe*

Jak opisano w pkt 2.3.2, Zgromadzenie Narodowe może prowadzić śledztwa i kontrole wobec organów publicznych i w tym kontekście żądać ujawnienia dokumentów oraz wezwać świadków. Jeżeli chodzi o kwestie wchodzące w zakres kompetencji NIS, taki nadzór parlamentarny sprawuje Komisja ds. Wywiadu Zgromadzenia Narodowego ([258]). Dyrektor NIS, który nadzoruje wykonywanie obowiązków przez agencję, składa sprawozdania Komisji ds. Wywiadu (a także

([248]) Art. 7 ustawy o zwalczaniu terroryzmu.
([249]) Art. 5 ust. 3 ustawy o zwalczaniu terroryzmu.
([250]) Art. 3 ust. 1 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu.
([251]) Art. 9 ust. 4 ustawy o zwalczaniu terroryzmu.
([252]) Art. 7 ustawy o zwalczaniu terroryzmu.
([253]) Art. 7 ust. 1 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu.
([254]) Art. 7 ust. 3 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu.
([255]) Art. 8 ust. 1 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu.
([256]) Art. 9 ust. 1 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu. Urzędnik ds. ochrony praw człowieka samodzielnie podejmuje decyzje o wydaniu zaleceń, ale ma obowiązek zgłaszać je przewodniczącemu Komisji ds. Zwalczania Terroryzmu.
([257]) Art. 9 ust. 2 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu.
([258]) Art. 36 i art. 37 ust. 1 pkt 16 ustawy o Zgromadzeniu Narodowym.

prezydentowi) ([259]). Komisja ds. Wywiadu może również z własnej inicjatywy zażądać sprawozdania w konkretnej sprawie, a dyrektor NIS musi to zrobić bezzwłocznie ([260]). Dyrektor może odmówić udzielenia odpowiedzi lub złożenia zeznań przed Komisją ds. Wywiadu wyłącznie w przypadku tajemnicy państwowej dotyczącej kwestii wojskowych, dyplomatycznych lub związanych z Koreą Północną, w przypadku których publiczne ujawnienie mogłoby mieć poważny wpływ na losy państwa ([261]). W takim przypadku Komisja ds. Wywiadu może zażądać od premiera wyjaśnień. Jeżeli nie otrzyma takiego wyjaśnienia w ciągu siedmiu dni od złożenia wniosku, odmowa odpowiedzi lub złożenia zeznań nie będzie już możliwa.

Jeżeli Zgromadzenie Narodowe stwierdzi, że doszło do niezgodnego z prawem lub niewłaściwego działania, może zażądać od danego organu publicznego podjęcia działań naprawczych, w tym przyznania odszkodowania, zastosowania środków dyscyplinarnych i usprawnienia procedur wewnętrznych ([262]). Po otrzymaniu takiego żądania organ musi niezwłocznie podjąć działania i poinformować Zgromadzenie Narodowe o ich wyniku. Zgodnie z CCPA w przypadku stosowania środków ograniczających komunikację (tj. zbierania treści komunikacji) obowiązują przepisy szczególne dotyczące nadzoru parlamentarnego ([263]). Zgromadzenie Narodowe może zwrócić się do szefów agencji wywiadowczych o sprawozdanie na temat każdego konkretnego środka ograniczającego komunikację. Ponadto może ono przeprowadzać kontrole na miejscu urządzeń podsłuchowych. Agencje wywiadowcze, które zebrały informacje dotyczące treści, i operatorzy, którzy ujawnili te informacje do celów bezpieczeństwa narodowego, muszą ponadto złożyć sprawozdanie z takiego ujawnienia na wniosek Zgromadzenia Narodowego.

3.3.3. *Komisja Kontroli i Audytu*

Komisja Kontroli i Audytu pełni te same funkcje nadzorcze w odniesieniu do agencji wywiadowczych co w obszarze ścigania przestępstw (zob. pkt 2.3.2) ([264]).

3.3.4. *Komisja Ochrony Danych Osobowych*

Jeśli chodzi o przetwarzanie danych do celów bezpieczeństwa narodowego, w tym na etapie zbierania danych, dodatkowy nadzór sprawuje PIPC. Jak wyjaśniono bardziej szczegółowo w pkt 1.2, obejmuje on ogólne zasady i obowiązki określone w art. 3 i art. 58 ust. 4 PIPA, jak również wykonywanie praw indywidualnych zagwarantowanych w art. 4 PIPA. Ponadto, zgodnie z art. 7-8 ust. 3 i 4 oraz art. 7-9 ust. 5 PIPA, nadzór PIPC obejmuje również ewentualne naruszenia przepisów zawartych w przepisach szczególnych określających ograniczenia i zabezpieczenia w odniesieniu do zbierania danych osobowych, np. w CPPA, ustawie o zwalczaniu terroryzmu oraz TBA. Biorąc pod uwagę zawarte w art. 3 ust. 1 PIPA wymogi dotyczące zgodnego z prawem i rzetelnego gromadzenia danych osobowych, każde naruszenie tych ustaw stanowi naruszenie PIPA. PIPC jest zatem uprawniona do prowadzenia dochodzeń ([265]) w sprawie naruszenia przepisów regulujących dostęp do danych do celów bezpieczeństwa narodowego oraz zasad przetwarzania danych określonych w PIPA, a także do wydawania zaleceń dotyczących usprawnień, nakazywania podjęcia działań naprawczych, zalecania środków dyscyplinarnych oraz informowania odpowiednich organów dochodzeniowych o podejrzeniu popełnienia przestępstwa ([266]).

3.3.5. *Krajowa Komisja Praw Człowieka*

Nadzór prowadzony przez NRHC ma zastosowanie w taki sam sposób do agencji wywiadowczych, jak do innych organów rządowych (zob. pkt 2.3.2).

3.4. **Indywidualne dochodzenie roszczeń**

3.4.1. *Skarga do urzędnika ds. ochrony praw człowieka*

Jeżeli chodzi o zbieranie danych osobowych w kontekście działań służących zwalczaniu terroryzmu, szczególną drogę ochrony prawnej zapewnia urzędnik ds. ochrony praw człowieka, ustanowiony w ramach Komisji ds. Zwalczania Terroryzmu. Urzędnik ds. ochrony praw człowieka rozpatruje wnioski publiczne związane z naruszeniem praw człowieka w wyniku działań antyterrorystycznych ([267]). Może zalecić działania naprawcze, a właściwa agencja musi poinformować urzędnika o wszelkich środkach podjętych w celu realizacji takiego zalecenia. Składanie skarg do urzędnika ds. ochrony praw człowieka przez osoby fizyczne nie jest obwarowane żadnymi stałymi wymogami. W rezultacie urzędnik ds. ochrony praw człowieka rozpatrzy skargę, nawet jeśli dana osoba nie jest w stanie wykazać faktycznej szkody na etapie sprawdzania dopuszczalności.

([259]) Art. 18 ustawy o NIS.
([260]) Art. 15 ust. 2 ustawy o NIS.
([261]) Art. 17 ust. 2 ustawy o NIS. „Tajemnice państwowe" oznaczają „fakty, dobra lub wiedzę zaklasyfikowane jako tajemnice państwowe, do których dostęp ma tylko ograniczona liczba osób i których nie można ujawniać żadnemu innemu państwu ani organizacji, aby uniknąć poważnej szkody dla bezpieczeństwa narodowego", zob. art. 13 ust. 4 ustawy o NIS.
([262]) Art. 16 ust. 2 ustawy o kontroli i nadzorowaniu administracji państwowej.
([263]) Art. 15 CPPA.
([264]) Podobnie jak w przypadku Komisji ds. Wywiadu Zgromadzenia Narodowego, dyrektor NIS może odmówić odpowiedzi BAI jedynie w sprawach stanowiących tajemnicę państwową i jeżeli podanie ich do wiadomości publicznej miałoby poważny wpływ na bezpieczeństwo narodowe (art. 13 ust. 1 ustawy o NIS).
([265]) Art. 63 PIPA.
([266]) Art. 61 ust. 2, art. 65 ust. 1, art. 65 ust. 2 oraz art. 64 ust. 4 PIPA.
([267]) Art. 8 ust. 1 pkt 2 dekretu wykonawczego do ustawy o zwalczaniu terroryzmu.

3.4.2. *Mechanizmy dochodzenia roszczeń dostępne na mocy PIPA*

Zgodnie z PIPA osoby fizyczne mogą wykonywać swoje prawa dostępu do danych osobowych przetwarzanych do celów bezpieczeństwa narodowego, ich korekty i usunięcia oraz zawieszenia zgody na ich przetwarzanie ([268]). Wnioski o skorzystanie z tych praw można składać bezpośrednio do agencji wywiadu lub pośrednio poprzez PIPC. Agencja wywiadowcza może ograniczyć wykonanie prawa lub odmówić wykonania prawa tak długo oraz w takim zakresie, w jakim jest to konieczne i proporcjonalne do ochrony ważnego celu leżącego w interesie publicznym (na przykład tak długo oraz w takim zakresie, w jakim przyznanie prawa zagroziłoby trwającemu postępowaniu przygotowawczemu lub bezpieczeństwu narodowemu) lub gdy przyznanie prawa może spowodować szkodę dla życia lub integralności cielesnej strony trzeciej. W przypadku odrzucenia lub ograniczenia wniosku należy bezzwłocznie powiadomić daną osobę fizyczną o przyczynach takiego odrzucenia.

Ponadto zgodnie z art. 58 ust. 4 PIPA (wymóg zapewnienia właściwego rozpatrywania skarg indywidualnych) oraz art. 4 ust. 5 PIPA (prawo do odpowiedniego środka dochodzenia roszczeń, w drodze szybkiej i sprawiedliwej procedury, z tytułu wszelkich szkód wynikających z przetwarzania danych osobowych) osoby fizyczne mają prawo do wniesienia środka zaskarżenia. Obejmuje to prawo do zgłoszenia domniemanego naruszenia do centrum telefonicznego ds. prywatności prowadzonego przez Koreańską Agencję ds. Internetu i Bezpieczeństwa oraz złożenia skargi do PIPC ([269]). Te środki dochodzenia roszczeń są dostępne zarówno w przypadku ewentualnych naruszeń przepisów ujętych w ustawach szczególnych określających ograniczenia i zabezpieczenia w odniesieniu do zbierania danych osobowych do celów bezpieczeństwa narodowego, jak i naruszeń PIPA. Jak wyjaśniono w zawiadomieniu nr 2021-1, osoba fizyczna z UE może wnieść skargę do PIPC za pośrednictwem swojego krajowego organu ochrony danych. W takim przypadku PIPC powiadomi osobę fizyczną za pośrednictwem jej krajowego organu ochrony danych o zakończeniu dochodzenia (w tym, w stosownych przypadkach, o zastosowanych działaniach naprawczych). Decyzje lub bezczynność PIPC można następnie zaskarżyć w sądach koreańskich na podstawie ustawy o postępowaniu administracyjnym.

3.4.3. *Skarga do Krajowej Komisji Praw Człowieka*

Możliwość indywidualnego dochodzenia roszczeń przed NHRC ma zastosowanie w taki sam sposób w przypadku agencji wywiadowczych, jak w przypadku innych organów rządowych (zob. pkt 2.4.2).

3.4.4. *Dochodzenie roszczeń na drodze sądowej*

Podobnie jak w przypadku działań organów ścigania w sprawach karnych, osoby fizyczne mogą dochodzić roszczeń wobec agencji wywiadowczych w odniesieniu do naruszeń wyżej wymienionych ograniczeń i zabezpieczeń na drodze sądowej, korzystając z różnych środków.

Po pierwsze, osoby fizyczne mogą uzyskać odszkodowanie na podstawie ustawy o odszkodowaniach od państwa. Na przykład w jednej sprawie przyznano odszkodowanie za bezprawny nadzór prowadzony przez Dowództwo Wsparcia Wojskowego (poprzednik Dowództwa Wsparcia Bezpieczeństwa Wojskowego) ([270]).

Po drugie, ustawa o postępowaniu administracyjnosądowym pozwala osobom fizycznym zakwestionować decyzje i zaniechania agencji administracyjnych, w tym agencji wywiadowczych ([271]).

Osoby fizyczne mogą również złożyć na podstawie ustawy o Trybunale Konstytucyjnym skargę konstytucyjną do Trybunału Konstytucyjnego w sprawie środków zastosowanych przez agencje wywiadowcze.

([268]) Art. 3 ust. 5 oraz art. 4 ust. 1, 3 i 4 PIPA.
([269]) Art. 62 i art. 63 ust. 2 PIPA.
([270]) Orzeczenie Sądu Najwyższego nr 96Da42789 z dnia 24 lipca 1998 r.
([271]) Art. 3 i 4 ustawy o postępowaniu administracyjnosądowym.