II

(Akty o charakterze nieustawodawczym)

DECYZJE

DECYZJA WYKONAWCZA KOMISJI (UE) 2019/419

z dnia 23 stycznia 2019 r.

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

(notyfikowana jako dokument nr C(2019) 304)

(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) („RODO") ([1]), w szczególności jego art. 45 ust. 3,

po zasięgnięciu opinii Europejskiego Inspektora Ochrony Danych,

1. WPROWADZENIE

(1) W rozporządzeniu (UE) 2016/679 określono zasady dotyczące przekazywania danych osobowych przez administratorów danych lub podmioty przetwarzające w Unii Europejskiej do państw trzecich i organizacji międzynarodowych w zakresie, w jakim takie przekazywanie wchodzi w zakres stosowania rozporządzenia. Zasady dotyczące międzynarodowego przekazywania danych osobowych określono w rozdziale V rozporządzenia, w szczególności w art. 44–50. Przepływ danych osobowych do państw spoza Unii Europejskiej i z tych państw jest niezbędnym warunkiem rozwoju współpracy międzynarodowej i handlu międzynarodowego, przy jednoczesnym zapewnieniu, by nie został naruszony stopień ochrony przysługujący danym osobowym w Unii Europejskiej.

(2) Na podstawie 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. Jak przewidziano w art. 45 ust. 1 i motywie 103 rozporządzenia, przy spełnieniu tego warunku przekazywanie danych osobowych do tego państwa trzeciego, terytorium, sektora lub tej organizacji międzynarodowej może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia.

(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, zarówno w odniesieniu do jego przepisów obejmujących podmioty odbierające dane, jak i do ograniczeń oraz zabezpieczeń w zakresie dostępu organów publicznych do danych osobowych. Przy ocenie należy ustalić, czy dane państwo trzecie daje gwarancje zapewniające odpowiedni stopień ochrony, „zasadniczo odpowiadający" stopniowi ochrony zapewnianemu w Unii Europejskiej (motyw 104 rozporządzenia (UE) 2016/679). Jak wyjaśnił w swoim orzecznictwie Trybunał Sprawiedliwości Unii Europejskiej, w tym przypadku nie jest wymagany identyczny stopień ochrony ([2]). W szczególności środki, z jakich korzysta dane państwo trzecie, mogą różnić się od środków wprowadzonych w Unii Europejskiej, o ile w praktyce skutecznie zapewniają wysoki stopień ochrony ([3]). W związku

([1]) Dz.U. L 119 z 4.5.2016, s. 1.
([2]) Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r., Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, pkt 73.
([3]) Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r., Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, pkt 74.

z powyższym odpowiedni standard ochrony można osiągnąć bez konieczności dokładnego powielenia przepisów unijnych. Przy ustalaniu stopnia ochrony 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 ([4]).

(4) Komisja uważnie przeanalizowała prawo i praktykę Japonii. W oparciu o ustalenia przedstawione w motywach 6–175 Komisja stwierdza, że Japonia zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych do organizacji objętych stosowaniem ustawy o ochronie informacji osobowych ([5]) i podlegających dodatkowym warunkom, o których mowa w niniejszej decyzji. Warunki te zostały określone w przepisach uzupełniających (załącznik I) przyjętych przez Komisję ds. Ochrony Informacji Osobowych ([6]) oraz w oficjalnych oświadczeniach, zapewnieniach i zobowiązaniach rządu Japonii wobec Komisji Europejskiej (załącznik II).

(5) Niniejsza decyzja skutkuje tym, że przekazywanie danych od administratora danych lub podmiotu przetwarzającego w Europejskim Obszarze Gospodarczym (EOG) ([7]) do takich organizacji w Japonii może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia. Niniejsza decyzja nie wpływa na bezpośrednie stosowanie rozporządzenia (UE) 2016/679 w odniesieniu do takich organizacji, jeżeli spełnione są warunki określone w art. 3 tego rozporządzenia.

2. PRZEPISY MAJĄCE ZASTOSOWANIE DO PRZETWARZANIA DANYCH PRZEZ PODMIOTY GOSPODARCZE

2.1. Japońskie ramy ochrony danych

(6) System prawny regulujący kwestie prywatności i ochrony danych w Japonii ma swoje źródło w konstytucji ogłoszonej w 1946 r.

(7) Art. 13 konstytucji stanowi:

„Wszystkich obywateli szanuje się jako jednostki ludzkie. Ich prawa do życia, wolności i dążenia do szczęścia, o ile nie pozostają w sprzeczności z dobrem publicznym, brane są w najwyższym stopniu pod uwagę w działalności ustawodawczej i innych poczynaniach państwa".

(8) Z artykułu tego japoński Sąd Najwyższy wywiódł prawa osób fizycznych w zakresie ochrony informacji osobowych. W wyroku z 1969 r. uznał on prawo do prywatności i ochrony danych za konstytucyjne prawo ([8]). W szczególności Sąd Najwyższy orzekł, że „każda osoba fizyczna ma prawo do ochrony dotyczących jej informacji osobowych przed ich ujawnieniem osobie trzeciej lub podaniem do wiadomości publicznej bez ważnego powodu". W wyroku z dnia 6 marca 2008 r. („Juki-Net") ([9]) Sąd Najwyższy uznał ponadto, że „wolność obywateli w życiu prywatnym jest chroniona przed sprawowaniem władzy publicznej i może być ona postrzegana jako jedna z wolności osoby fizycznej w życiu prywatnym, a każda osoba fizyczna ma prawo do ochrony dotyczących jej informacji osobowych przed ich ujawnieniem osobie trzeciej lub podaniem do wiadomości publicznej bez ważnego powodu" ([10]).

(9) W dniu 30 maja 2003 r. Japonia przyjęła szereg ustaw dotyczących ochrony danych, w tym między innymi:

— ustawę o ochronie informacji osobowych,

— ustawę o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji,

— ustawę o ochronie informacji osobowych znajdujących się w posiadaniu niezależnych agencji administracyjnych.

([4]) 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, sekcja 3.1, s. 6–7.
([5]) Ustawa o ochronie informacji osobowych (ustawa nr 57, 2003 r.).
([6]) Dalsze informacje na temat Komisji ds. Ochrony Informacji Osobowych są dostępne pod adresem: https://www.ppc.go.jp/en/ (w tym dane kontaktowe do przesyłania pytań i skarg: https://www.ppc.go.jp/en/contactus/access/).
([7]) 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.
([8]) Sąd Najwyższy, wyrok Wielkiej Ławy z dnia 24 grudnia 1969 r., Keishu, tom 23, nr 12, s. 1625.
([9]) Sąd Najwyższy, wyrok z dnia 6 marca 2008 r., Minshu, tom 62, nr 3, s. 665.
([10]) Sąd Najwyższy, wyrok z dnia 6 marca 2008 r., Minshu, tom 62, nr 3, s. 665.

(10) Dwie ostatnie ustawy (zmienione w 2016 r.) zawierają przepisy mające zastosowanie do ochrony informacji osobowych przez podmioty sektora publicznego. Przetwarzanie danych wchodzące w zakres stosowania tych ustaw nie stanowi przedmiotu stwierdzenia odpowiedniej ochrony danych zawartego w niniejszej decyzji, ograniczonego do ochrony informacji osobowych przez „podmioty gospodarcze przetwarzające informacje osobowe" w rozumieniu ustawy o ochronie informacji osobowych.

(11) W ostatnich latach ustawę tę znowelizowano. Zmieniona ustawa o ochronie informacji osobowych została ogłoszona w dniu 9 września 2015 r. i weszła w życie w dniu 30 maja 2017 r. W ramach tej nowelizacji wprowadzono szereg nowych zabezpieczeń oraz wzmocniono te istniejące, zbliżając tym samym japoński system ochrony danych do systemu europejskiego. Obejmują one na przykład szereg egzekwowalnych praw indywidualnych lub ustanowienie niezależnego organu nadzorczego (Komisja ds. Ochrony Informacji Osobowych), któremu powierzono działania w zakresie nadzoru i egzekwowania przepisów ustawy o ochronie informacji osobowych.

(12) Przetwarzanie informacji osobowych objęte zakresem niniejszej decyzji podlega nie tylko ustawie o informacji osobowych, ale również przepisom wykonawczym wydanym na jej podstawie. Obejmują one zmianę zarządzenia Rady Ministrów w sprawie egzekwowania przepisów ustawy o ochronie informacji osobowych z dnia 5 października 2016 r. oraz tzw. przepisy wykonawcze do ustawy o ochronie informacji osobowych, przyjęte przez Komisję ds. Ochrony Informacji Osobowych ([11]). Oba zbiory przepisów są prawnie wiążące i egzekwowalne oraz weszły w życie w tym samym czasie co zmieniona ustawa o ochronie informacji osobowych.

(13) Ponadto w dniu 28 października 2016 r. Rada Ministrów Japonii (w skład której wchodzi premier i ministrowie tworzący rząd) wydała „podstawowe zasady polityki", aby „w sposób kompleksowy i integralny promować środki dotyczące ochrony informacji osobowych". Zgodnie z art. 7 ustawy o ochronie informacji osobowych „podstawowe zasady polityki" wydawane są w formie decyzji Rady Ministrów, obejmują kierunki polityki dotyczące egzekwowania przepisów tej ustawy oraz skierowane są zarówno do instytucji rządowych na szczeblu centralnym, jak i samorządowych na szczeblu lokalnym.

(14) Niedawno rząd Japonii zmienił „podstawowe zasady polityki" uchwałą Rady Ministrów przyjętą w dniu 12 czerwca 2018 r. Aby ułatwić międzynarodowe przekazywanie danych, w przedmiotowej uchwale Rady Ministrów przekazano Komisji ds. Ochrony Informacji Osobowych, jako organowi właściwemu w zakresie stosowania i wdrażania ustawy o ochronie informacji osobowych, „prawo do podejmowania działań niezbędnych do zatarcia różnic w systemach oraz działaniach między Japonią a danym państwem obcym na podstawie art. 6 ustawy w celu zapewnienia właściwego przetwarzania informacji osobowych otrzymanych od takiego państwa". Uchwała Rady Ministrów stanowi, że powyższe obejmuje prawo do ustanowienia wzmożonych zabezpieczeń dzięki przyjęciu przez Komisję ds. Ochrony Informacji Osobowych surowszych przepisów uzupełniających, wykraczających poza przepisy określone w ustawie o ochronie informacji osobowych i zarządzeniu Rady Ministrów. Zgodnie z tą uchwałą te surowsze przepisy uzupełniające są wiążące dla japońskich podmiotów gospodarczych i możliwe do wyegzekwowania wobec nich.

(15) Na podstawie art. 6 ustawy o ochronie informacji osobowych i uchwały Rady Ministrów Komisja ds. Ochrony Informacji Osobowych przyjęła w dniu 15 czerwca 2018 r. „Przepisy uzupełniające na podstawie ustawy o ochronie informacji osobowych w zakresie przetwarzania danych osobowych przekazywanych z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony" („przepisy uzupełniające") w celu rozszerzenia ochrony informacji osobowych przekazywanych z Unii Europejskiej do Japonii na podstawie niniejszej decyzji stwierdzającej odpowiedni stopień ochrony. Te przepisy uzupełniające są prawnie wiążące dla japońskich podmiotów gospodarczych i możliwe wobec nich do wyegzekwowania, zarówno przez Komisję ds. Ochrony Informacji Osobowych, jak i sądy, w ten sam sposób, co przepisy ustawy o ochronie informacji osobowych, które uzupełniono przepisami surowszymi lub bardziej szczegółowymi ([12]). Ponieważ japońskie podmioty gospodarcze otrzymujące lub przetwarzające dane osobowe z Unii Europejskiej będą prawnie zobowiązane do przestrzegania przepisów uzupełniających, będą one musiały zapewnić możliwość identyfikowania takich danych osobowych w całym ich „cyklu życia" (np. stosując środki techniczne („tagowanie") lub środki organizacyjne (przechowywanie w specjalnej bazie danych)) ([13]). W kolejnych sekcjach przeanalizowano treść poszczególnych przepisów uzupełniających w ramach oceny artykułów ustawy o ochronie informacji osobowych, którą nimi uzupełniono.

(16) W przeciwieństwie do stanu prawnego sprzed zmiany wprowadzonej w 2015 r., gdy kompetencje w tym zakresie przypadały różnym japońskim ministerstwom w poszczególnych sektorach, ustawa o ochronie informacji osobowych upoważnia Komisję ds. Ochrony Informacji Osobowych do przyjmowania „wytycznych" „w celu zapewnienia właściwego i skutecznego wdrażania działań podejmowanych przez podmioty gospodarcze" w ramach przepisów dotyczących ochrony danych. W swoich wytycznych Komisja ds. Ochrony Informacji Osobowych dokonała

([11]) Dostępne pod adresem: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

([12]) Zob. przepisy uzupełniające (sekcja wprowadzająca).

([13]) Nie jest to sprzeczne z ogólnym wymogiem prowadzenia rejestrów (tylko) przez pewien okres. Nawet jeżeli wśród informacji, które pozyskujący podmiot gospodarczy przetwarzający informacje osobowe ma obowiązek potwierdzić zgodnie z art. 26 ust. 1 ustawy o ochronie informacji osobowych, znajduje się informacja o źródle danych, wymóg wynikający z art. 26 ust. 4 ustawy o ochronie informacji osobowych w związku z art. 18 przepisów Komisji ds. Ochrony Informacji Osobowych dotyczy jedynie określonej formy zapisu (zob. art. 16 przepisów Komisji ds. Ochrony Informacji Osobowych) i nie uniemożliwia podmiotowi gospodarczemu przetwarzającemu informacje osobowe zapewniania identyfikacji danych przez dłuższy okres. Potwierdziła to Komisja ds. Ochrony Informacji Osobowych, która wskazała, że „[i]nformacje o źródle danych UE muszą być przechowywane przez podmiot gospodarczy przetwarzający informacje osobowe tak długo, jak jest to konieczne do przestrzegania przepisów uzupełniających".

wiążącej interpretacji tych przepisów, w szczególności ustawy o ochronie informacji osobowych. Jak wynika z informacji przekazanych przez Komisję ds. Ochrony Informacji Osobowych, wytyczne te stanowią integralną część ram prawnych, które należy interpretować w związku z tekstem ustawy o ochronie informacji osobowych, zarządzenia Rady Ministrów, przepisami przyjętymi przez Komisję ds. Ochrony Informacji Osobowych oraz zestawem pytań i odpowiedzi ([14]) przygotowanym przez tę komisję. Są one zatem „wiążące dla podmiotów gospodarczych". W przypadku gdy wytyczne stanowią, że podmiot gospodarczy „ma obowiązek" lub „nie powinien" działać w określony sposób, Komisja ds. Ochrony Informacji Osobowych uznaje nieprzestrzeganie właściwych przepisów za naruszenie prawa ([15]).

2.2. **Zakres przedmiotowy i podmiotowy**

(17) Zakres stosowania ustawy o ochronie informacji osobowych został określony zdefiniowanymi w niej pojęciami, takimi jak informacje osobowe, dane osobowe i podmiot gospodarczy przetwarzający informacje osobowe. Jednocześnie ustawa przewiduje istotne wyłączenia z zakresu jej stosowania, przede wszystkim w odniesieniu do anonimowo przetwarzanych danych osobowych i określonych rodzajów przetwarzania przez niektóre podmioty. W ustawie o ochronie informacji osobowych nie występuje wprawdzie termin „processing" („przetwarzanie"), stosuje się w niej jednak równoważne pojęcie „handling", które, zgodnie z informacjami otrzymanymi od Komisji ds. Ochrony Informacji Osobowych, obejmuje „wszelkie operacje na danych osobowych", w tym nabywanie, wprowadzanie, gromadzenie, organizowanie, przechowywanie, edytowanie/przetwarzanie, aktualizację, usuwanie, niszczenie lub dostarczanie danych osobowych.

2.2.1. *Definicja informacji osobowych*

(18) Przede wszystkim, jeżeli chodzi o zakres przedmiotowy, w ustawie o ochronie informacji osobowych dokonano rozróżnienia między informacjami osobowymi a danymi osobowymi, przy czym do informacji osobowych zastosowanie mają jedynie niektóre przepisy ustawy. Zgodnie z art. 2 ust. 1 ustawy o ochronie informacji osobowych pojęcie „informacji osobowych" obejmuje wszelkie informacje związane z żyjącą osobą fizyczną, które umożliwiają identyfikację takiej osoby. W definicji wyróżniono dwie kategorie informacji osobowych: (i) kody identyfikujące osoby fizyczne oraz (ii) pozostałe informacje osobowe umożliwiające identyfikację danej osoby fizycznej. Do drugiej kategorii należą również informacje, które same w sobie nie pozwalają na identyfikację, ale po ich „prostym zestawieniu" z innym informacjami umożliwiają identyfikację danej osoby fizycznej. Zgodnie z wytycznymi Komisji ds. Ochrony Informacji Osobowych ([16]) to, czy dane informacje można uznać za umożliwiające ich „łatwe zestawienie", rozstrzyga się w każdym indywidualnym przypadku z uwzględnieniem sytuacji faktycznej („warunków") podmiotu gospodarczego. Powyższe przyjmuje się, jeżeli takie zestawienie przeprowadza (lub może przeprowadzić) przeciętny („zwykły") podmiot gospodarczy za pomocą dostępnych mu środków. Na przykład informacje nie umożliwiają ich „łatwego zestawienia" z innymi informacjami, jeżeli podmiot gospodarczy musi podjąć nietypowe starania lub dopuścić się nielegalnych czynów w celu uzyskania informacji do zestawienia od co najmniej jednego podmiotu gospodarczego.

2.2.2. *Definicja danych osobowych*

(19) Zgodnie z ustawą o ochronie informacji osobowych tylko niektóre formy informacji osobowych wchodzą w zakres pojęcia „danych osobowych". W istocie „dane osobowe" zdefiniowano jako „informacje osobowe stanowiące bazę informacji osobowych", tj. „zbiór informacji" składający się z informacji osobowych „zorganizowanych w systematyczny sposób w celu umożliwienia wyszukiwania określonych informacji osobowych za pomocą komputera" ([17]) lub „uznane w zarządzeniu Rady Ministrów za zorganizowane w systematyczny sposób w celu umożliwienia łatwego wyszukiwania określonych informacji osobowych" (ale „wyłączając informacje, w przypadku których w zarządzeniu Rady Ministrów stwierdzono małe prawdopodobieństwo wystąpienia szkody dla praw i interesów jednostki, mając na względzie metodę wykorzystania tych informacji") ([18]).

(20) Wyjątek ten został szczegółowo określony w art. 3 ust. 1 zarządzenia Rady Ministrów. Zgodnie z tym przepisem spełnione muszą być kumulatywnie trzy następujące warunki: (i) zbiór informacji musi być „wydany w celu

([14]) Komisja ds. Ochrony Informacji Osobowych, pytania i odpowiedzi, 16 lutego 2017 r. (zmienione w dniu 30 maja 2017 r.), dostępne pod adresem: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf W pytaniach i odpowiedziach omówiono szereg kwestii poruszonych w wytycznych dzięki przedstawieniu praktycznych przykładów, takich jak definicja danych wrażliwych, interpretacja pojedynczej zgody, przekazywanie danych osobom trzecim w kontekście przetwarzania w chmurze lub obowiązek prowadzenia rejestru w odniesieniu do przekazywania transgranicznego. Pytania i odpowiedzi są dostępne tylko w języku japońskim.

([15]) Odnosząc się do konkretnego pytania, Komisja ds. Ochrony Informacji Osobowych poinformowała Europejską Radę Ochrony Danych (EROD), że „stosując ustawę ochronie informacji osobowych/przepisy przyjęte przez Komisję ds. Ochrony Informacji Osobowych w poszczególnych rozpoznawanych sprawach, sądy japońskie opierają swo[ją] wykładnię na tych wytycznych, a tym samym w swoich orzeczeniach bezpośrednio odnoszą się do tekstu tych wytycznych. W związku z tym również z tego punktu widzenia wytyczne przyjęte przez Komisję ds. Ochrony Informacji Osobowych są dla podmiotów gospodarczych wiążące. Komisji ds. Ochrony Informacji Osobowych nie jest znany ani jeden przypadek odstąpienia przez sąd od zastosowania tych wytycznych". W tym zakresie odesłała ona Komisję do wyroku dotyczącego problematyki ochrony danych, w którym sąd wyraźnie oparł swój wywód na tych wytycznych (zob. wyrok Sądu Rejonowego w Osace z dnia 19 maja 2006 r., Hanrei Jiho, tom 1948, s. 122, w którym sąd ten orzekł, że podmiot gospodarczy miał obowiązek przeprowadzić kontrolę bezpieczeństwa na podstawie tych wytycznych).

([16]) Wytyczne Komisji ds. Ochrony Informacji Osobowych (wydanie zawierające przepisy ogólne), s. 6.

([17]) Obejmuje to wszelkie elektroniczne zbiory danych. Wytyczne Komisji ds. Ochrony Informacji Osobowych (wydanie zawierające przepisy ogólne, s. 17) zawierają w tym względzie szczegółowe przykłady (np. lista adresów e-mail zapisana w oprogramowaniu klienta).

([18]) Art. 2 ust. 4 i 6 ustawy o ochronie informacji osobowych.

sprzedaży dużej liczbie nieokreślonych osób, a wydanie to nastąpiło bez naruszenia przepisów prawa lub zarządzenia wydanego na ich podstawie"; (ii) zbiór danych musi dawać się do „sprzedaży w każdym czasie dużej liczbie nieokreślonych osób" oraz (iii) zawarte w nim dane osobowe muszą być „dostarczone zgodnie z ich pierwotnym przeznaczeniem bez dodawania innych informacji odnoszących się do danej osoby żyjącej". Zgodnie z wyjaśnieniami Komisji ds. Ochrony Informacji Osobowych ów wąski wyjątek wprowadzono w celu wyłączenia z tego zakresu książek telefonicznych lub podobnego rodzaju zbiorów danych.

(21) W przypadku danych zbieranych w Japonii powyższe rozróżnienie pomiędzy pojęciem „informacje osobowe" a pojęciem „dane osobowe" jest istotne, ponieważ takie informacje nie zawsze stanowią część „bazy informacji osobowych" (np. pojedynczy zbiór danych zbieranych i przetwarzanych ręcznie), w związku z czym zastosowania nie mają przepisy ustawy o ochronie informacji osobowych, które dotyczą wyłącznie danych osobowych ([19]).

(22) Rozróżnienie to nie będzie miało jednak znaczenia dla danych osobowych przekazywanych z Unii Europejskiej do Japonii na podstawie decyzji stwierdzającej odpowiedni stopień ochrony. Ponieważ takie dane będą zazwyczaj przekazywane drogą elektroniczną (co w erze cyfrowej jest powszechnym sposobem wymiany danych, zwłaszcza na bardzo dużą odległość, jaka dzieli UE i Japonię), i w związku z tym staną się częścią elektronicznego zbioru danych podmiotu odbierającego, dane te UE będą zaliczane do kategorii „danych osobowych" w rozumieniu ustawy o ochronie informacji osobowych. W sytuacji wyjątkowej, w której dane osobowe byłyby w inny sposób przekazywane z UE (np. w formie papierowej), będą one nadal objęte zakresem ustawy o ochronie informacji osobowych, jeżeli po przekazaniu staną się one częścią usystematyzowanego „zbioru informacji", umożliwiającego łatwe wyszukiwanie określonych informacji (art. 2 ust. 4 ppkt (ii) ustawy o ochronie informacji osobowych). Zgodnie z art. 3 ust. 2 zarządzenia Rady Ministrów będzie to miało miejsce w przypadku gdy informacje są uporządkowane „według pewnej reguły", a baza danych zawiera narzędzia takie jak np. spis treści lub indeks ułatwiający wyszukiwanie. Odpowiada to definicji „zbioru danych" w rozumieniu art. 2 ust. 1 RODO.

2.2.3. *Definicja zatrzymanych danych osobowych*

(23) Niektóre przepisy ustawy o ochronie informacji osobowych, zwłaszcza art. 27–30 dotyczące praw indywidualnych, mają zastosowanie wyłącznie do określonej kategorii danych osobowych, tj. do „zatrzymanych danych osobowych". W art. 2 ust. 7 ustawy o ochronie informacji osobowych zdefiniowano je jako dane osobowe inne niż dane, które (i) „w zarządzeniu Rady Ministrów uznano za mogące zaszkodzić interesom publicznym lub innym, jeżeli do wiadomości publicznej zostanie podana informacja o ich występowaniu lub braku" albo (ii) „mają zostać usunięte w terminie nie dłuższym niż jeden rok zgodnie z zarządzeniem Rady Ministrów".

(24) Zgodnie z wyjaśnieniem zawartym w art. 4 zarządzenia Rady Ministrów pierwsza z tych dwóch kategorii obejmuje cztery rodzaje wyłączeń ([20]). Wyłączenia te służą podobnym celom do tych, które wymieniono w art. 23 ust. 1 rozporządzenia (UE) 2016/679, mianowicie ochronie osoby, której dane dotyczą (zgodnie z terminologią stosowaną w ustawie o ochronie informacji osobowych „osoba powierzająca dane" [ang. principal]), i wolności innych osób, bezpieczeństwu narodowemu, bezpieczeństwu publicznemu, ściganiu przestępstw oraz innym ważnym celom leżącym w ogólnym interesie publicznym. Ponadto z brzmienia art. 4 ust. 1 lit. (i)–(iv) zarządzenia Rady Ministrów wynika, że ich stosowanie zawsze zakłada, że zachodzi szczególne ryzyko dla jednego z ważnych chronionych interesów ([21]).

(25) Drugą kategorię doprecyzowano w art. 5 zarządzenia Rady Ministrów. W artykule tym, w związku z art. 2 ust. 7 ustawy o ochronie informacji osobowych, z zakresu pojęcia zatrzymanych danych osobowych, a tym samym z praw indywidualnych przewidzianych w ustawie, wyłączono dane osobowe, które „mają zostać usunięte" w terminie sześciu miesięcy. Komisja ds. Ochrony Informacji Osobowych wyjaśniła, że celem tego wyłączenia jest zachęcenie podmiotów gospodarczych do zatrzymywania i przetwarzania danych przez jak najkrótszy okres. Oznaczałoby to jednak, że osoby w UE, których dane dotyczą, nie mogłyby korzystać z ważnych praw z żadnego innego powodu niż okres zatrzymania ich danych przez określony podmiot gospodarczy.

(26) W celu rozwiązania tej sytuacji w sekcji 2 przepisów uzupełniających określono wymóg, aby dane osobowe przekazywane z UE „traktowano jak zatrzymane dane osobowe w rozumieniu art. 2 ust. 7 ustawy, bez względu na termin, w jakim mają one zostać usunięte". Okres zatrzymania danych nie będzie miał zatem wpływu na prawa zapewnione osobom w UE, których dane dotyczą.

([19]) Przykładowo art. 23 ustawy o ochronie danych osobowych dotyczący warunków udostępniania danych osobowych osobom trzecim.

([20]) Mianowicie (i) dane osobowe, „w związku z którymi istnieje prawdopodobieństwo, że podanie do wiadomości publicznej informacji o ich występowaniu lub braku zaszkodzi życiu, zdrowiu lub majątkowi osoby powierzającej dane lub osoby trzeciej"; (ii) dane, „w związku z którymi istnieje prawdopodobieństwo, że podanie do wiadomości publicznej informacji o ich występowaniu lub braku będzie zachęcać lub skłaniać do czynu nielegalnego lub niezgodnego z prawem"; (iii) dane, „w związku z którymi istnieje prawdopodobieństwo, że podanie do wiadomości publicznej informacji o ich występowaniu lub braku będzie stanowić naruszenie bezpieczeństwa narodowego, zaburzy oparte na zaufaniu relacje z państwem obcym lub organizacją międzynarodową albo doprowadzi do niekorzystnych skutków w negocjacjach z państwem obcym lub organizacją międzynarodową"; oraz (iv) dane, „w związku z którymi istnieje prawdopodobieństwo, że podanie do wiadomości publicznej informacji o ich występowaniu lub braku utrudni działania mające na celu zachowanie bezpieczeństwa i porządku publicznego, takie jak zapobieganie przestępstwom, ich zwalczanie oraz prowadzenie dochodzeń w ich sprawie".

([21]) W takich przypadkach powiadomienia osoby fizycznej nie wymaga się. Pozostaje to w zgodności z art. 23 ust. 2 lit. h) RODO, który stanowi, że osoby, których dane dotyczą, nie muszą być informowane o tym ograniczeniu, o ile „nie narusza to celu ograniczenia".

2.2.4. *Definicja przetwarzanych informacji osobowych przetwarzanych anonimowo*

(27) Wymogi dotyczące informacji osobowych przetwarzanych anonimowo, zgodnie z definicją zawartą w art. 2 ust. 9 ustawy o ochronie informacji osobowych, określono w rozdziale IV sekcja 2 ustawy („Obowiązki podmiotu gospodarczego przetwarzającego informacje osobowe przetwarzane anonimowo"). Takie informacje nie podlegają natomiast przepisom rozdziału IV sekcja 1 ustawy, w których określono zabezpieczenia i prawa w zakresie ochrony danych mające zastosowanie do przetwarzania danych osobowych na podstawie ustawy. W konsekwencji, chociaż „informacje osobowe przetwarzane anonimowo" nie podlegają „standardowym" przepisom dotyczącym ochrony danych (wymienionym w rozdziale IV sekcja 1 oraz w art. 42 ustawy o ochronie informacji osobowych), wchodzą one w zakres stosowania tej ustawy, mianowicie jej art. 36–39.

(28) Zgodnie z art. 2 ust. 9 ustawy o ochronie informacji osobowych „informacje osobowe przetwarzane anonimowo" stanowią informacje związane z osobą fizyczną, które zostały „sporządzone w wyniku przetwarzania informacji osobowych" za pomocą środków przewidzianych w tej ustawie (art. 36 ust. 1) i określonych w przepisach przyjętych przez Komisję ds. Ochrony Informacji Osobowych (art. 19) w taki sposób, że niemożliwe jest zidentyfikowanie danej osoby fizycznej ani przywrócenie informacji osobowych.

(29) Z przepisów tych wynika, co potwierdziła także Komisja ds. Ochrony Informacji Osobowych, że proces nadania informacjom osobowym charakteru „anonimowego" nie musi być technicznie nieodwracalny. Zgodnie z art. 36 ust. 2 ustawy o ochronie informacji osobowych podmioty gospodarcze operujące „informacjami osobowymi przetwarzanymi anonimowo" są jedynie zobowiązane do zapobiegania ponownej identyfikacji przez zastosowanie środków w celu zapewnienia bezpieczeństwa „opisów itp. oraz kodów identyfikujących osoby fizyczne, usuwanych z informacji osobowych wykorzystanych do sporządzenia anonimowo przetwarzanych informacji, oraz informacji związanych ze stosowaną metodą przetwarzania".

(30) W związku z tym, że „informacje osobowe przetwarzane anonimowo", zgodnie z definicją zawartą w ustawie o ochronie informacji osobowych, obejmują dane, w przypadku których ponowna identyfikacja osoby fizycznej jest nadal możliwa, mogłoby to oznaczać, że dane osobowe przekazywane z Unii Europejskiej mogłyby utracić część dostępnych zabezpieczeń w wyniku procesu, który zgodnie z rozporządzeniem (UE) 2016/679 byłby uznawany za rodzaj „pseudonimizacji", a nie „anonimizacji" (w związku z czym ich charakter jako danych osobowych pozostałby niezmieniony).

(31) W celu podjęcia tej kwestii w przepisach uzupełniających przewidziano dodatkowe wymogi, które mają zastosowanie wyłącznie do danych osobowych przekazywanych z Unii Europejskiej na podstawie niniejszej decyzji. Zgodnie z sekcją 5 przepisów uzupełniających takie informacje osobowe uznawane są za anonimowo przetwarzane informacje osobowe w rozumieniu ustawy o ochronie informacji osobowych tylko wtedy, „gdy podmiot gospodarczy przetwarzający informacje osobowe stosuje środki umożliwiające nieodwracalną dla kogokolwiek anonimizację osoby fizycznej, w tym dzięki usunięciu informacji o metodzie przetwarzania i tym podobnych powiązanych informacji". Te ostatnie zostały określone w przepisach uzupełniających jako informacje związane z opisami i kodami identyfikującymi osoby fizyczne, usuwane z informacji osobowych wykorzystanych do „sporządzenia anonimowo przetwarzanych informacji osobowych", oraz informacje związane z metodą przetwarzania stosowaną przy usuwaniu tych opisów i kodów identyfikujących osoby fizyczne. Innymi słowy, przepisy uzupełniające nakładają na podmiot gospodarczy sporządzający anonimowo przetwarzane informacje osobowe obowiązek zniszczenia „klucza" umożliwiającego ponowną identyfikację danych. Oznacza to, że dane osobowe pochodzące z Unii Europejskiej będą podlegać przepisom ustawy o ochronie informacji osobowych dotyczącym „informacji osobowych przetwarzanych anonimowo" wyłącznie wówczas, gdy na podstawie rozporządzenia (UE) 2016/679 zostałyby również uznane za informacje anonimowe ([22]).

2.2.5. *Definicja podmiotu gospodarczego przetwarzającego informacje osobowe*

(32) Zakres podmiotowy ustawy o ochronie informacji osobowych obejmuje wyłącznie podmioty gospodarcze przetwarzające informacje osobowe. W art. 2 ust. 5 tej ustawy podmiot gospodarczy przetwarzający informacje osobowe zdefiniowano jako „osobę zapewniającą bazę informacji osobowych itp. wykorzystywanych na potrzeby działalności gospodarczej" z wyłączeniem agencji rządowych i administracyjnych, zarówno na szczeblu centralnym, jak i lokalnym.

(33) Zgodnie z wytycznymi Komisji ds. Ochrony Informacji Osobowych „działalność gospodarcza" oznacza wszelkie „działania zmierzające do prowadzenia, wielokrotnie i w sposób ciągły, społecznie uznawanego przedsiębiorstwa w określonym celu, bez względu na to, czy przynosi ono zysk". Organizacje nieposiadające osobowości prawnej (takie jak stowarzyszenia zwykłe) lub osoby fizyczne uznaje się za podmioty gospodarcze przetwarzające informacje osobowe, jeżeli zapewniają (wykorzystują) one bazy informacji osobowych itp. w związku z prowadzeniem przez nie działalności gospodarczej ([23]). W związku z powyższym pojęcie „działalności gospodarczej" zgodnie z ustawą o ochronie informacji osobowych jest bardzo szerokie w tym względzie, że obejmuje zarówno działania ukierunkowane, jak i działania nieukierunkowane na osiąganie zysku, podejmowane przez wszelkiego rodzaju organizacje i osoby fizyczne. Ponadto „wykorzystywanie na potrzeby działalności gospodarczej" obejmuje również informacje osobowe, które nie są wykorzystywane w (zewnętrznych) relacjach handlowych podmiotu, ale do użytku wewnętrznego, na przykład przy przetwarzaniu danych pracowników.

([22]) Zob. rozporządzenie (UE) 2016/679, motyw 26.
([23]) Wytyczne Komisji ds. Ochrony Informacji Osobowych (wydanie zawierające przepisy ogólne), s. 18.

(34) Jeżeli chodzi o beneficjentów przewidzianych zabezpieczeń, w ustawie o ochronie informacji osobowych nie wprowadzono żadnego rozróżnienia ze względu na przynależność państwową, miejsce zamieszkania lub lokalizację osoby fizycznej. To samo dotyczy możliwości dochodzenia roszczeń przez osoby fizyczne, zarówno przed Komisją ds. Ochrony Informacji Osobowych, jak i w sądach.

2.2.6. *Pojęcie administratora danych i podmiotu przetwarzającego*

(35) W ustawie o ochronie informacji osobowych nie ma wyraźnego rozróżnienia pomiędzy obowiązkami nałożonymi na administratorów danych i na podmioty przetwarzające. Brak takiego rozróżnienia nie wpływa na stopień ochrony, ponieważ wszystkie podmioty gospodarcze przetwarzające informacje osobowe podlegają wszystkim przepisom ustawy. Podmiot gospodarczy przetwarzający informacje osobowe, który powierza przetwarzanie danych osobowych powiernikowi (któremu w RODO odpowiada podmiot przetwarzający), nadal podlega obowiązkom wynikającym z ustawy o ochronie informacji osobowych oraz przepisom uzupełniającym w zakresie powierzonych przez niego danych. Ponadto zgodnie z art. 22 ustawy o ochronie informacji osobowych ma on obowiązek sprawować „niezbędny i właściwy nadzór" nad powiernikiem. Z kolei, jak potwierdziła Komisja ds. Ochrony Informacji Osobowych, powiernika również wiążą wszystkie obowiązki wynikające z ustawy o ochronie informacji osobowych i przepisów uzupełniających.

2.2.7. *Wyłączenia sektorowe*

(36) Art. 76 ustawy o ochronie informacji osobowych przewiduje wyłączenie niektórych rodzajów przetwarzania danych z zakresu stosowania rozdziału IV ustawy, który zawiera główne przepisy dotyczące ochrony danych (podstawowe zasady, obowiązki podmiotów gospodarczych, prawa indywidualne, nadzór sprawowany przez Komisję ds. Ochrony Informacji Osobowych). Przetwarzanie objęte wyłączeniem sektorowym określonym w art. 76 jest również wyłączone z uprawnień Komisji ds. Ochrony Informacji Osobowych, zgodnie z art. 43 ust. 2 ustawy o ochronie informacji osobowych ([24]).

(37) Odpowiednie kategorie dotyczące wyłączenia sektorowego określonego w art. 76 ustawy o ochronie informacji osobowych zdefiniowano za pomocą podwójnego kryterium opartego na rodzaju podmiotu gospodarczego przetwarzającego informacje osobowe i celu przetwarzania. Ściślej rzecz ujmując, wyłączenie ma zastosowanie do: (i) nadawców radiofonii, wydawców gazet, agencji komunikacji i innych organizacji prasowych (w tym wszelkich osób fizycznych prowadzących działalność prasową będącą działalnością gospodarczą), w zakresie, w jakim przetwarzają informacje osobowe do celów prasowych; (ii) osób zawodowo zajmujących się pisaniem, w zakresie, w jakim wykorzystywane są przy tym informacje osobowe; (iii) szkół wyższych i wszelkich innych organizacji lub grup, których celem jest prowadzenie studiów, lub wszelkich osób należących do takich organizacji, w zakresie, w jakim przetwarzają informacje osobowe do celów studiów; (iv) instytucji kościelnych, w zakresie, w jakim przetwarzają informacje osobowe do celów działalności religijnej (w tym wszelkiej działalności z tym związanej) oraz (v) organów politycznych, w zakresie, w jakim przetwarzają informacje osobowe do celów związanych ze swoją działalnością polityczną (w tym wszelkiej działalności z tym związanej). Przetwarzanie informacji osobowych do jednego z celów wymienionych w art. 76 przez innego rodzaju podmioty gospodarcze przetwarzające informacje osobowe oraz przetwarzanie informacji osobowych przez jeden z wymienionych w tym artykule podmiotów gospodarczych do innych celów, np. w kontekście zatrudnienia, pozostaje objęte przepisami rozdziału IV.

(38) Aby zapewnić odpowiedni stopień ochrony danych osobowych przekazywanych z Unii Europejskiej do podmiotów gospodarczych w Japonii, niniejszą decyzją należy objąć wyłącznie przetwarzanie informacji osobowych wchodzących w zakres stosowania rozdziału IV ustawy o ochronie informacji osobowych – tj. przetwarzanie przez podmioty gospodarcze przetwarzające informacje osobowe w zakresie, w jakim sytuacja przetwarzania nie odpowiada jednemu z wyłączeń sektorowych. Jej zakres należy zatem dostosować do zakresu ustawy o ochronie informacji osobowych. Zgodnie z informacjami otrzymanymi od Komisji ds. Ochrony Informacji Osobowych, w przypadku gdy podmiot gospodarczy przetwarzający informacje osobowe objęty niniejszą decyzją przekształci dalej cel wykorzystania danych (w takim zakresie, w jakim jest to dopuszczalne) i zostanie wówczas objęty jednym z wyłączeń sektorowych określonych w art. 76 ustawy o ochronie informacji osobowych, będzie to uznane za przekazywanie międzynarodowe (ze względu na to, że w takich przypadkach przetwarzanie danych osobowych nie byłoby już objęte zakresem rozdziału IV tej ustawy i tym samym pozostawałoby poza zakresem jej zastosowania). To samo dotyczyłoby sytuacji, w której podmiot gospodarczy przetwarzający informacje osobowe przekazuje informacje osobowe podmiotowi objętemu zakresem art. 76 ustawy o ochronie informacji osobowych na potrzeby wykorzystania ich do jednego z celów przetwarzania określonych w tym przepisie. Jeżeli chodzi o dane osobowe przekazane z Unii Europejskiej, stanowiłoby to zatem dalsze przekazanie podlegające właściwym zabezpieczeniom (w szczególności tym określonym w art. 24 ustawy o ochronie informacji osobowych oraz w przepisie uzupełniającym 4). Jeżeli podmiot gospodarczy przetwarzający informacje osobowe opiera się na zgodzie podmiotu ([25]), którego dane dotyczą, byłby obowiązany przekazać mu wszelkie niezbędne informacje, w tym informację o tym, że dane osobowe nie będą już chronione przepisami ustawy o ochronie informacji osobowych.

([24]) Jeżeli chodzi o inne podmioty, Komisja ds. Ochrony Informacji Osobowych w ramach wykonywania swoich uprawnień śledczych i wykonawczych nie uniemożliwia im korzystania z ich prawa do wolności wypowiedzi, wolności nauczania, wolności religii i wolności działalności politycznej (art. 43 ust. 1 ustawy o ochronie informacji osobowych).

([25]) Jak wyjaśniła Komisja ds. Ochrony Informacji Osobowych, w jej wytycznych zgodę interpretuje się jako „wyrażenie przez osobę powierzającą dane woli z takim skutkiem, że akceptuje ona, że jej dane osobowe mogą być przetwarzane z wykorzystaniem metody wskazanej przez podmiot gospodarczy przetwarzający dane osobowe". Wytyczne Komisji ds. Ochrony Informacji Osobowych (wydanie zawierające przepisy ogólne, s. 24) zawierają wyliczenie sposobów wyrażenia zgody, które uznaje się za „zwyczajowe praktyki handlowe w Japonii", tj. porozumienie ustne, formularz zwrotu lub inne dokumenty, porozumienie zawarte za pośrednictwem poczty elektronicznej, zaznaczenie pola na stronie internetowej, kliknięcie na stronie głównej, kliknięcie na przycisk zgody, dotknięcie panelu dotykowego itp. Posłużenie się wszystkimi tymi metodami stanowi wyrażenie w sposób wyraźny zgody.

2.3. **Zabezpieczenia, prawa i obowiązki**

2.3.1. *Ograniczenie celu*

(39) Dane osobowe powinny być przetwarzane w określonym celu, a następnie wykorzystywane tylko w takim zakresie, w jakim nie jest to niezgodne z celem przetwarzania. Ta zasada ochrony danych zagwarantowana jest w art. 15 i 16 ustawy o ochronie informacji osobowych.

(40) Ustawa ta opiera się na zasadzie, że podmiot gospodarczy obowiązany jest określić cel wykorzystania „w możliwie najbardziej wyraźny sposób" (art. 15 ust. 1), a następnie przestrzegać tego celu przy przetwarzaniu danych.

(41) W tej kwestii w art. 15 ust. 2 ustawy o ochronie informacji osobowych stanowi, że podmiotowi gospodarczemu przetwarzającemu informacje osobowe zakazuje się zmiany początkowego celu, jeżeli zmiana taka „wykraczałaby poza zakres uznawany za racjonalnie istotny dla celu wykorzystania określonego przed zmianą", interpretowanego w wytycznych Komisji ds. Ochrony Informacji Osobowych jako odpowiadający temu, czego osoba, której dane dotyczą, może obiektywnie oczekiwać na podstawie „przyjętych norm społecznych" ([26]).

(42) Ponadto, zgodnie z art. 16 ust. 1 ustawy o ochronie informacji osobowych podmiotom gospodarczym przetwarzającym informacje osobowe zakazuje się przetwarzania tego rodzaju informacji w sposób wykraczający poza „zakres niezbędny do osiągnięcia celu wykorzystania" określonego w art. 15 bez uzyskania wcześniejszej zgody osoby, której dane dotyczą, chyba że zastosowanie mają odstępstwa, o których mowa w art. 16 ust. 3 ([27]).

(43) Jeżeli chodzi o informacje osobowe uzyskane od innego podmiotu gospodarczego, podmiot gospodarczy przetwarzający informacje osobowe może co do zasady określić nowy cel ich wykorzystania ([28]). Aby zapewnić zachowanie przez odbiorcę zgodności z celem, dla którego przekazano dane, zgodnie z sekcją 3 przepisów uzupełniających w odniesieniu do przekazywania danych z Unii Europejskiej wymaga się, aby w przypadku „gdy [podmiot gospodarczy przetwarzający informacje osobowe] otrzymuje dane osobowe z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony" lub gdy taki podmiot „otrzymuje od innego [podmiotu gospodarczego przetwarzającego informacje osobowe] dane osobowe, które wcześniej przekazano z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony" (dalsze przekazywanie), odbiorca był obowiązany „określić cel wykorzystania danych osobowych, o których mowa, w granicach celu wykorzystania, dla którego dane te zostały pierwotnie lub w późniejszym czasie otrzymane". Innymi słowy, przepis ten zapewnia, aby w kontekście przekazywania cel wskazany na podstawie rozporządzenia (UE) 2016/679 nadal określał przetwarzanie oraz aby zmiana tego celu na dowolnym etapie łańcucha przetwarzania w Japonii wymagała zgody osoby w UE, której dane dotyczą. Uzyskanie takiej zgody wymaga wprawdzie, aby podmiot gospodarczy przetwarzający informacje osobowe zwrócił się do osoby, której dane dotyczą, jednak jeżeli jest to niemożliwe, skutkować to będzie po prostu koniecznością zachowania pierwotnego celu.

2.3.2. *Zgodność z prawem i rzetelność przetwarzania*

(44) Dodatkowa ochrona, o której mowa w motywie 43, jest tym bardziej istotna, że przetwarzanie danych osobowych w sposób zgodny z prawem i rzetelny zapewniane jest w japońskim systemie także dzięki zasadzie ograniczenia celu.

(45) Zgodnie z ustawą o ochronie danych osobowych, w przypadku, gdy podmiot gospodarczy przetwarzający informacje osobowe zbiera tego rodzaju informacje, jest on zobowiązany do szczegółowego określenia celu ich wykorzystania ([29]) oraz niezwłocznego poinformowania o tym celu osoby, której dane dotyczą (lub podania tego celu do wiadomości publicznej) ([30]). Co więcej, art. 17 tej ustawy stanowi, że podmiot gospodarczy przetwarzający informacje osobowe nie może pozyskiwać informacji osobowych w wyniku oszustwa ani za pomocą innych niewłaściwych środków. W odniesieniu do niektórych kategorii danych, takich jak informacje osobowe wymagające szczególnej uwagi, do ich uzyskania wymagana jest zgoda osoby, której dane dotyczą (art. 17 ust. 2 ustawy o ochronie informacji osobowych).

([26]) W pytaniach i odpowiedziach wydanych przez Komisję ds. Ochrony Informacji Osobowych przedstawiono szereg przykładów w celu zilustrowania tego pojęcia. Do przykładów sytuacji, w których zmiana mieści się w zakresie racjonalnie istotnym dla celu, zalicza się przede wszystkim wykorzystywanie informacji osobowych otrzymanych od nabywców towarów lub usług w kontekście transakcji handlowej w celu informowania ich o dostępności innych odpowiednich towarów lub usług (np. podmiot prowadzący klub fitness, który rejestruje adresy e-mail członków w celu informowania ich o zajęciach i programach). Jednocześnie w pytaniach i odpowiedziach przytoczono również przykład, w którym zmiana celu wykorzystania jest niedopuszczalna, a mianowicie wówczas, gdy przedsiębiorstwo przesyła informacje na temat swoich towarów i usług na adresy e-mail, które zebrano w celu ostrzegania przed oszustwami i kradzieżami kart członkowskich.

([27]) Wyłączenia te mogą wynikać z innych przepisów ustawowych i wykonawczych lub dotyczyć sytuacji, w których przetwarzanie informacji osobowych jest niezbędne (i) do „ochrony ludzkiego życia, zdrowia lub majątku"; (ii) do „zwiększenia higieny publicznej lub propagowania wychowania zdrowych dzieci"; lub (iii) do „współpracy z agencjami lub organami rządowymi lub z ich przedstawicielami" przy wykonywaniu ich zadań ustawowych. Ponadto kategorie (i) oraz (ii) mają zastosowanie tylko wtedy, gdy istnieją trudności z uzyskaniem zgody osoby, której dane dotyczą, natomiast kategoria (iii) ma zastosowanie tylko wtedy, gdy istnieje ryzyko, że uzyskanie zgody osoby, której dane dotyczą, mogłoby zakłócać wykonywanie takich zadań.

([28]) Niemniej jednak, zgodnie z art. 23 ust. 1 ustawy o ochronie informacji osobowych, do ujawnienia danych osobie trzeciej wymagana jest co do zasady zgoda danej osoby fizycznej. W ten sposób osobie fizycznej umożliwia się pewną kontrolę nad wykorzystaniem dotyczących jej danych przez inny podmiot gospodarczy.

([29]) Zgodnie z art. 15 ust. 1 ustawy o ochronie informacji osobowych takiego określenia należy dokonać „w możliwie najbardziej wyraźny sposób".

([30]) Art. 18 ust. 1 ustawy o ochronie informacji osobowych.

(46) Następnie, jak wyjaśniono w motywach 41 i 42, podmiotowi gospodarczemu przetwarzającemu informacje osobowe zakazuje się przetwarzania informacji osobowych do innych celów, chyba że osoba, której dane dotyczą, wyraziła zgodę na takie przetwarzanie lub gdy zastosowanie ma jedno z odstępstw określonych w art. 16 ust. 3 ustawy o ochronie informacji osobowych.

(47) Wreszcie, jeżeli chodzi o dalsze przekazywanie informacji osobowych osobie trzeciej ([31]), w art. 23 ust. 1 ustawy o ochronie informacji osobowych ograniczono takie ujawnianie do określonych przypadków, przy czym co do zasady wymagana jest wcześniejsza zgoda osoby, której dane dotyczą ([32]). W art. 23 ust. 2, 3 i 4 tej ustawy określono wyjątki od wymogu uzyskania zgody. Wyjątki te mają jednak zastosowanie tylko do danych wrażliwych oraz wymagają od podmiotu gospodarczego, aby z wyprzedzeniem zawiadomił zainteresowane osoby fizyczne o zamiarze ujawnienia ich informacji osobowych osobie trzeciej oraz o możliwości sprzeciwu wobec dalszego ujawniania ([33]).

(48) Jeżeli chodzi o przekazanie danych osobowych z Unii Europejskiej, w pierwszej kolejności muszą być one zebrane i przetwarzane w UE zgodnie z rozporządzeniem (UE) 2016/679. Będzie to zawsze obejmowało z jednej strony zbieranie i przetwarzanie, w tym na potrzeby przekazania z Unii Europejskiej do Japonii, w oparciu o podstawy prawne wymienione w art. 6 ust. 1 rozporządzenia, a z drugiej strony zbieranie w szczególnym, wyraźnym i prawnie uzasadnionym celu oraz zakaz dalszego przetwarzania, w tym przez przekazanie, w sposób niezgodny z takim celem, jak określono w art. 5 ust. 1 lit. b) oraz art. 6 ust. 4 rozporządzenia.

(49) Zgodnie z sekcją 3 przepisów uzupełniających po przekazaniu danych podmiot gospodarczy przetwarzający informacje osobowe i będący ich odbiorcą musi „potwierdzić" szczegółowy cel lub cele stanowiące podstawę przekazania (tzn. cel wskazany na podstawie rozporządzenia (UE) 2016/679) oraz dalej przetwarzać te dane zgodnie z tym celem lub celami ([34]). Oznacza to, że nie tylko początkowy odbiorca takich danych osobowych w Japonii, lecz także każdy przyszły odbiorca danych (w tym powiernik), jest obowiązany zachować zgodność z celem lub celami wskazanymi na podstawie rozporządzenia.

(50) Ponadto, gdyby podmiot gospodarczy przetwarzający informacje osobowe chciał zmienić cel wskazany wcześniej na podstawie rozporządzenia (UE) 2016/679, zgodnie z art. 16 ust. 1 ustawy o ochronie informacji osobowych musiałby co do zasady uzyskać zgodę osoby, której dane dotyczą. Bez uzyskania takiej zgody wszelkie przypadki przetwarzania danych wykraczające poza zakres niezbędny do osiągnięcia celu wykorzystania stanowiłyby naruszenie art. 16 ust. 1, którego przestrzeganie mogłoby być egzekwowane przez Komisję ds. Ochrony Informacji Osobowych lub sądy.

(51) Dlatego też z uwagi na fakt, że zgodnie z rozporządzeniem (UE) 2016/679 do przekazania wymagane są ważna podstawa prawna oraz konkretny cel, których odzwierciedleniem jest cel wykorzystania „potwierdzony" na podstawie ustawy o ochronie informacji osobowych, połączenie właściwych przepisów tej ustawy oraz sekcji 3 przepisów uzupełniających zapewnia ciągłą zgodność przetwarzania unijnych danych w Japonii z prawem.

2.3.3. *Prawidłowość i minimalizacja danych*

(52) Dane powinny być prawidłowe i w razie potrzeby uaktualniane. Powinny być one również adekwatne, stosowne i nienadmierne w stosunku do celów, w których są przetwarzane.

(53) Przestrzeganie tych zasad w japońskim prawie zapewniono w art. 16 ust. 1 ustawy o ochronie informacji osobowych, w którym zakazano przetwarzania informacji osobowych w stopniu wykraczającym poza „zakres niezbędny do osiągnięcia celu wykorzystania". Zgodnie z wyjaśnieniami Komisji ds. Ochrony Informacji Osobowych nie tylko wyklucza to wykorzystanie danych, które są nieadekwatne, oraz nadmierne wykorzystanie danych (w stopniu wykraczającym poza zakres niezbędny do osiągnięcia celu wykorzystania), lecz także oznacza zakaz przetwarzania danych, które nie są istotne dla osiągnięcia celu wykorzystania.

([31]) Chociaż powiernicy są wyłączeni z zakresu pojęcia „osoby trzeciej" do celów stosowania art. 23 (zob. pkt 5), wyłączenie to stosuje się tylko w takim zakresie, w jakim powiernik przetwarza dane osobowe w granicach powierzenia („w zakresie niezbędnym do osiągnięcia celu wykorzystania"), tj. działa jako podmiot przetwarzający.

([32]) Inne (wyjątkowe) okoliczności to: (i) przekazanie informacji osobowych „na podstawie przepisów ustawowych i wykonawczych"; (ii) przypadki, „w których konieczna jest ochrona ludzkiego życia, zdrowia lub majątku, a także gdy istnieją trudności z uzyskaniem zgody osoby powierzającej dane"; (iii) przypadki, „w których szczególnie konieczne jest zwiększenie higieny publicznej lub propagowanie wychowania zdrowych dzieci, a także gdy istnieją trudności z uzyskaniem zgody osoby powierzającej dane" oraz (iv) przypadki, „w których konieczna jest współpraca z instytucjami rządowymi na szczeblu centralnym lub samorządowymi na szczeblu lokalnym, lub osobami, którym powierzyły one wykonywanie działań przewidzianych w przepisach ustawowych i wykonawczych, a także gdy istnieje prawdopodobieństwo, że uzyskanie zgody osoby powierzającej dane zakłóci wykonywanie tego rodzaju działań".

([33]) W przekazywanych informacjach należy wskazać przede wszystkim kategorie danych osobowych, które zostaną udostępnione osobie trzeciej, oraz metodę ich przekazania. Podmiot gospodarczy przetwarzający informacje osobowe jest ponadto zobowiązany do poinformowania osoby, której dane dotyczą, o możliwości sprzeciwu wobec przekazania danych oraz o sposobie jego zgłoszenia.

([34]) Zgodnie z art. 26 ust. 1 ppkt (ii) ustawy o ochronie informacji osobowych po otrzymaniu danych osobowych od osoby trzeciej podmiot gospodarczy przetwarzający informacje osobowe jest zobowiązany do „potwierdzenia" (zweryfikowania) „szczegółów dotyczących pozyskania danych osobowych przez osobę trzecią", w tym szczegółów dotyczących celu, w jakim je pozyskano. Mimo że art. 26 nie stanowi wyraźnie, że podmiot gospodarczy przetwarzający informacje osobowe musi następnie przestrzegać tego celu, jest to wyraźnie wymagane w sekcji 3 przepisów uzupełniających.

(54) Jeżeli chodzi o obowiązek utrzymania prawidłowości i aktualności danych, zgodnie z art. 19 ustawy o ochronie informacji osobowych podmiot gospodarczy przetwarzający informacje osobowe jest zobowiązany do „dążenia, aby dane osobowe były prawidłowe i aktualne w zakresie niezbędnym do osiągnięcia celu wykorzystania". Przepis ten należy interpretować w związku z art. 16 ust. 1 ustawy o ochronie informacji osobowych: zgodnie z wyjaśnieniami otrzymanymi od Komisji ds. Ochrony Informacji Osobowych, jeżeli podmiot gospodarczy przetwarzający informacje osobowe nie spełnia określonych norm dotyczących prawidłowości, przetwarzanie informacji osobowych nie jest uznawane za osiągnięcie celu wykorzystania, w związku z czym uznawane jest za niezgodne z prawem na podstawie art. 16 ust. 1.

2.3.4. *Ograniczenie przechowywania*

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

(56) Zgodnie z art. 19 ustawy o ochronie informacji osobowych podmioty gospodarcze przetwarzające informacje osobowe są zobowiązane do „dążenia […] do niezwłocznego usunięcia danych osobowych, gdy takie wykorzystanie stanie się zbędne". Powyższy przepis należy interpretować w związku z art. 16 ust. 1 ustawy o ochronie informacji osobowych, w którym zakazano przetwarzania informacji osobowych w stopniu wykraczającym poza „zakres niezbędny do osiągnięcia celu wykorzystania". Gdy cel wykorzystania został osiągnięty, przetwarzanie informacji osobowych nie może być dalej uznawane za niezbędne, a tym samym kontynuowane (chyba że podmiot gospodarczy przetwarzający informacje osobowe uzyskał na to zgodę osoby, której dane dotyczą).

2.3.5. *Bezpieczeństwo danych*

(57) 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 oraz koszty ich wdrożenia.

(58) Zasadę tę wdrożono w japońskim prawie za pomocą art. 20 ustawy o ochronie informacji osobowych, który stanowi, że podmiot gospodarczy przetwarzający informacje osobowe „podejmuje niezbędne i stosowne działania na rzecz kontroli bezpieczeństwa danych osobowych, w tym działania zapobiegające wyciekowi, utracie lub uszkodzeniu przetwarzanych danych osobowych". W wytycznych Komisji ds. Ochrony Informacji Osobowych wyjaśniono środki, jakie należy podjąć, w tym metody ustanawiania podstawowych zasad polityki, zasady przetwarzania danych i poszczególne „działania kontrolne" (dotyczące zarówno bezpieczeństwa organizacyjnego, jak i bezpieczeństwa ludzkiego, fizycznego i technologicznego) ([35]). Ponadto w wytycznych Komisji ds. Ochrony Informacji Osobowych i specjalnym zawiadomieniu (dodatek 8 „Treści środków zarządzania bezpieczeństwem, które należy zastosować") opublikowanym przez Komisję ds. Ochrony Informacji Osobowych przedstawiono więcej szczegółów na temat środków dotyczących incydentów bezpieczeństwa związanych na przykład z wyciekiem informacji osobowych, zaliczających się do środków zarządzania bezpieczeństwem podejmowanych przez podmioty gospodarcze przetwarzające informacje osobowe ([36]).

(59) Ponadto, ilekroć dane osobowe są przetwarzane przez pracowników lub podwykonawców, zgodnie z art. 20 i 21 ustawy o ochronie informacji osobowych wymagane jest zapewnienie „niezbędnego i stosownego nadzoru" do celów kontroli bezpieczeństwa. Wreszcie zgodnie z art. 83 ustawy o ochronie informacji osobowych celowy wyciek lub kradzież informacji osobowych są zagrożone karą do jednego roku pozbawienia wolności.

2.3.6. *Przejrzystość*

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

(61) Zgodnie z art. 18 ust. 1 ustawy o ochronie informacji osobowych podmioty gospodarcze przetwarzające informacje osobowe są zobowiązane do udostępnienia osobie, której dane dotyczą, informacji o celu wykorzystania pozyskanych danych osobowych, z wyjątkiem „przypadków, w których cel wykorzystania został z wyprzedzeniem podany do wiadomości publicznej". Ten sam obowiązek stosuje się w przypadku dopuszczalnej zmiany celu (art. 18 ust. 3). Dzięki temu zapewnia się również, że osoba, której dane dotyczą, zostanie poinformowana o fakcie zebrania dotyczących jej danych. Chociaż zgodnie z ustawą o ochronie informacji osobowych podmiot gospodarczy przetwarzający informacje osobowe nie ma co do zasady obowiązku poinformowania osoby, której dane dotyczą, o oczekiwanych odbiorcach informacji osobowych na etapie ich zbierania, zgodnie z art. 23 ust. 2 takie zawiadomienie stanowi warunek niezbędny do jakiegokolwiek dalszego ujawniania informacji osobie trzeciej (odbiorcy), jeżeli następuje ono bez uprzedniej zgody osoby, której dane dotyczą.

([35]) Wytyczne Komisji ds. Ochrony Informacji Osobowych (wydanie zawierające przepisy ogólne), s. 41 oraz s. 86–98.

([36]) Zgodnie z sekcją 3-3-2 wytycznych Komisji ds. Ochrony Informacji Osobowych, jeżeli doszło do takiego wycieku, uszkodzenia lub utraty danych, podmiot gospodarczy przetwarzający informacje osobowe jest zobowiązany do przeprowadzenia wymaganych dochodzeń i przede wszystkim dokonania oceny rozmiaru naruszenia praw i interesów jednostki, a także charakteru i ilości odnośnych informacji osobowych.

(62) Jeżeli chodzi o „zatrzymane dane osobowe", art. 27 ustawy o ochronie informacji osobowych stanowi, że podmiot gospodarczy przetwarzający informacje osobowe informuje osobę, której dane dotyczą, o swojej tożsamości (dane kontaktowe), celu wykorzystania i procedurach odpowiadania na wnioski dotyczące praw indywidualnych osoby, której dane dotyczą, na podstawie art. 28, 29 i 30 tej ustawy.

(63) Zgodnie z przepisami uzupełniającymi dane osobowe przekazywane z Unii Europejskiej będą uznawane za „zatrzymane dane osobowe" bez względu na okres ich zatrzymania (chyba że są objęte wyłączeniami), jak również będą za każdym razem podlegać wymogom przejrzystości przewidzianym w obu wyżej wymienionych przepisach.

(64) Zarówno wymogi określone w art. 18, jak i obowiązek informowania o celu wykorzystania zgodnie z art. 27 ustawy o ochronie informacji osobowych podlegają temu samemu zestawowi wyłączeń, opartych w głównej mierze na względach interesu publicznego oraz ochronie praw i interesów osoby, której dane dotyczą, osób trzecich oraz administratora ([37]). Zgodnie z interpretacją zawartą w wytycznych Komisji ds. Ochrony Informacji Osobowych wyłączenia te obowiązują w szczególnych sytuacjach, w których informacje dotyczące celu wykorzystania mogłyby osłabić prawnie uzasadnione środki podejmowane przez podmiot gospodarczy w celu ochrony określonych interesów (np. zwalczanie oszustw, szpiegostwa przemysłowego, sabotażu).

2.3.7. *Szczególne kategorie danych*

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

(66) „Informacje osobowe wymagające szczególnej uwagi" zdefiniowano art. 2 ust. 3 ustawy o ochronie informacji osobowych. Przepis ten odnosi się do „informacji osobowych obejmujących rasę, przekonania, status społeczny, historię medyczną, uprzednią karalność osoby powierzającej dane, fakt bycia ofiarą przestępstwa lub inne opisy itp. wskazane w zarządzeniu Rady Ministrów jako informacje, których przetwarzanie wymaga szczególnej uwagi, aby nie doprowadzić do nieuczciwej dyskryminacji, uprzedzeń lub innych niekorzystnych okoliczności względem osoby powierzającej dane". Kategorie te odpowiadają w dużym stopniu wykazowi danych wrażliwych określonemu w art. 9 i 10 rozporządzenia (UE) 2016/679. W szczególności „historia medyczna" odpowiada danym dotyczącym zdrowia, natomiast „uprzednia karalność i fakt bycia ofiarą przestępstwa" w znacznym stopniu pokrywają się z kategoriami, o których mowa w art. 10 rozporządzenia (UE) 2016/679. Kategorie, o których mowa w art. 2 ust. 3 ustawy o ochronie informacji osobowych, podlegają dalszej interpretacji przedstawionej w zarządzeniu Rady Ministrów i wytycznych Komisji ds. Ochrony Informacji Osobowych. Zgodnie z interpretacją przedstawioną w sekcji 2.3 pkt 8 wytycznych Komisji ds. Ochrony Informacji Osobowych podkategorie „historii medycznej" wyszczególnione w art. 2 ppkt (ii) oraz (iii) zarządzenia Rady Ministrów obejmują dane genetyczne i biometryczne. Dodatkowo, mimo że wykaz ten nie obejmuje wyraźnie pojęć takich jak „pochodzenie etniczne" i „poglądy polityczne", zawiera odniesienia do „rasy" i „przekonań". Jak wyjaśniono w sekcji 2.3 pkt 1 i 2 wytycznych Komisji ds. Ochrony Informacji Osobowych odniesienie do „rasy" obejmuje „więź lub więzi etniczne z określoną częścią świata", natomiast „przekonania" rozumienie są zarówno jako przekonania religijne, jak i polityczne.

(67) Jak jasno wynika z brzmienia przytoczonego przepisu, wykaz ten nie jest zamknięty, ponieważ możliwe jest dodanie kolejnych kategorii danych, o ile ich przetwarzanie stwarza ryzyko „nieuczciwej dyskryminacji, uprzedzeń lub innych niekorzystnych okoliczności względem osoby powierzającej dane".

(68) Chociaż pojęcie danych „wrażliwych" samo w sobie stanowi konstrukt społeczny w tym względzie, że jest ono zakorzenione w tradycjach kulturowych i prawnych, aspektach moralnych, wyborach politycznych itp. danego społeczeństwa, z uwagi na potrzebę zapewnienia odpowiednich zabezpieczeń w odniesieniu do danych wrażliwych przekazywanych podmiotom gospodarczym w Japonii, Komisja uzyskała zapewnienie, że zgodnie z japońskim prawem szczególne zabezpieczenia przysługujące „informacjom osobowym wymagającym szczególnej uwagi" obejmują również wszystkie kategorie uznawane za „dane wrażliwe" w rozporządzeniu (UE) 2016/679. W tym celu sekcja 1 przepisów uzupełniających stanowi, że podmioty gospodarcze przetwarzający informacje osobowe przetwarzają dane przekazywane z Unii Europejskiej dotyczące seksualności, orientacji seksualnej lub przynależności osoby fizycznej do związków zawodowych „w ten sam sposób, co informacje osobowe wymagające szczególnej uwagi w rozumieniu art. 2 ust. 3 [ustawy o ochronie informacji osobowych]".

([37]) Są to (i) przypadki, w których istnieje prawdopodobieństwo, że poinformowanie osoby, której dane dotyczą, o celu wykorzystania lub jego podanie do wiadomości publicznej „zaszkodzi życiu, zdrowiu, majątkowi lub innym prawom i interesom osoby powierzającej dane lub osoby trzeciej" lub „prawom lub prawnie uzasadnionym interesom […] podmiotu gospodarczego przetwarzającego informacje osobowe"; (ii) przypadki, w których „konieczna jest współpraca z instytucjami rządowymi na szczeblu centralnym lub samorządowymi na szczeblu lokalnym" w związku z wykonywaniem ich zadań ustawowych, a także gdy taka informacja lub ujawnienie zakłóciłyby wykonywanie takich „działań"; (iii) przypadki, w których cel wykorzystania jest jasny na podstawie sytuacji, w której pozyskano dane.

(69) Jeżeli chodzi o dodatkowe zabezpieczenia materialne dotyczące informacji osobowych wymagających szczególnej uwagi, zgodnie z art. 17 ust. 2 ustawy o ochronie informacji osobowych podmioty gospodarcze przetwarzające informacje osobowe nie mogą pozyskiwać, z nielicznymi wyjątkami, tego rodzaju danych bez uprzedniej zgody zainteresowanej osoby fizycznej ([38]). Ponadto ta kategoria informacji osobowych jest wyłączona z możliwości ujawnienia osobie trzeciej na podstawie procedury przewidzianej w art. 23 ust. 2 ustawy o ochronie informacji osobowych (umożliwiającej przekazywanie danych osobom trzecim bez uprzedniej zgody zainteresowanej osoby fizycznej).

2.3.8. *Rozliczalność*

(70) 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.

(71) Jak wspomniano w przypisie 34 (motyw 49), zgodnie z art. 26 ust. 1 ustawy o ochronie informacji osobowych podmioty gospodarcze przetwarzające informacje osobowe są zobowiązane do zweryfikowania tożsamości osoby trzeciej przekazującej im dane osobowe oraz „okoliczności", w jakich pozyskała ona te dane (jeżeli chodzi o dane osobowe objęte niniejszą decyzją, zgodnie z ustawą o ochronie informacji osobowych oraz sekcją 3 przepisów uzupełniających do tych okoliczności zalicza się fakt, że dane pochodzą z Unii Europejskiej oraz cel pierwotnego przekazania danych). Celem tego środka jest między innymi zapewnienie zgodności przetwarzania danych z prawem w całym łańcuchu, w którym uczestniczą podmioty gospodarcze przetwarzające informacje osobowe. Zgodnie z art. 26 ust. 3 ustawy o ochronie informacji osobowych podmioty gospodarcze przetwarzające informacje osobowe są ponadto obowiązane każdorazowo rejestrować datę otrzymania danych oraz (obowiązkowych) informacji otrzymanych od osoby trzeciej na podstawie ust. 1, jak również imienia i nazwiska zainteresowanej osoby fizycznej (osoby, której dane dotyczą), kategorii przetwarzanych danych oraz – w odpowiednim zakresie – faktu, czy osoba, której dane dotyczą, wyraziła zgodę na udostępnienie jej danych osobowych. Zgodnie z art. 18 przepisów przyjętych przez Komisję ds. Ochrony Informacji Osobowych rejestry te muszą być przechowywane przez okres co najmniej od jednego roku do trzech lat, w zależności od okoliczności. W ramach wykonywania swoich zadań Komisja ds. Ochrony Informacji Osobowych może zażądać przedłożenia takich rejestrów ([39]).

(72) Podmioty gospodarcze przetwarzające informacje osobowe mają obowiązek niezwłocznie i we właściwy sposób rozpatrywać skargi zainteresowanych osób fizycznych dotyczące przetwarzania ich informacji osobowych. Aby ułatwić rozpatrywanie skarg, podmioty te wdrażają „system niezbędny do osiągnięcia [tego] celu", co oznacza, że powinny wdrożyć właściwe procedury w swoich organizacjach (na przykład dokonać podziału obowiązków lub zapewnić punkt kontaktowy).

(73) Wreszcie w ustawie o ochronie informacji osobowych ustanowiono ramy dotyczące udziału organizacji sektorowych w zapewnianiu wysokiego stopnia zgodności (zob. rozdział IV sekcja 4). Rolą takich akredytowanych organizacji zajmujących się ochroną informacji osobowych ([40]) jest propagowanie ochrony informacji osobowych przez wspieranie przedsiębiorstw i udostępnianie w tym celu fachowej wiedzy tych organizacji, jak również przyczynianie się do wdrożenia zabezpieczeń, zwłaszcza w drodze rozpatrywania skarg osób fizycznych i udzielania pomocy w rozwiązywaniu związanych z tym konfliktów. W tym celu mogą one zażądać od uczestniczących podmiotów gospodarczych przetwarzających dane osobowe wdrożenia, w stosownych przypadkach, niezbędnych środków ([41]). Ponadto w przypadku naruszenia ochrony danych lub innych incydentów związanych z bezpieczeństwem podmioty gospodarcze przetwarzające informacje osobowe co do zasady informują o tym fakcie Komisję ds. Ochrony Informacji Osobowych i osobę, której dane dotyczą (lub podają tę informację do wiadomości publicznej), oraz podejmują niezbędne działania, w tym środki mające na celu zmniejszenie ewentualnych szkód i uniknięcie ponownego wystąpienia podobnych incydentów ([42]). Chociaż w tym przypadku chodzi o dobrowolne programy, w dniu 10 sierpnia 2017 r. Komisja ds. Ochrony Informacji Osobowych przedstawiła wykaz zawierający nazwy 44 organizacje, z których sama tylko największa – Japońskie Centrum Przetwarzania Informacji i Rozwoju

([38]) Wyłączenia te obejmują: (i) „przypadki wynikające z przepisów ustawowych i wykonawczych"; (ii) „przypadki, w których konieczna jest ochrona ludzkiego życia, zdrowia lub majątku, a także gdy istnieją trudności z uzyskaniem zgody osoby powierzającej dane"; (iii) „przypadki, w których szczególnie konieczne jest zwiększenie higieny publicznej lub propagowanie wychowania zdrowych dzieci, a także gdy istnieją trudności z uzyskaniem zgody osoby powierzającej dane"; (iv) „przypadki, w których konieczna jest współpraca z instytucjami rządowymi na szczeblu centralnym lub samorządowymi na szczeblu lokalnym, lub osobami, którym powierzyły one wykonywanie działań przewidzianych w przepisach ustawowych i wykonawczych, a także gdy istnieje prawdopodobieństwo, że uzyskanie zgody osoby powierzającej dane zakłóci wykonywanie tego rodzaju działań"; oraz (v) przypadki, w których wspomniane informacje osobowe wymagające szczególnej uwagi podawane są do wiadomości publicznej przez osobę, której dane dotyczą, instytucję rządową, instytucję samorządową na szczeblu lokalnym, osobę zaliczającą się do jednej z kategorii wskazanych w art. 76 ust. 1 lub inną osobę wskazaną w przepisach Komisji ds. Ochrony Informacji Osobowych. Kolejna kategoria dotyczy „pozostałych przypadków wskazanych w zarządzeniu Rady Ministrów jako równoważne przypadkom wskazanym w każdym poprzedzającym punkcie" oraz zgodnie z bieżącym zarządzeniem Rady Ministrów obejmuje przede wszystkim widoczne cechy danej osoby (np. zauważalny stan zdrowia) w przypadku, jeżeli dane wrażliwe zostały pozyskane (w sposób niezamierzony) przez obserwację wzrokową, filmowanie lub fotografowanie osoby, której dane dotyczą, np. przy wykorzystaniu kamer telewizji przemysłowej.

([39]) Zgodnie z art. 40 ust. 1 ustawy o ochronie informacji osobowych Komisja ds. Ochrony Informacji Osobowych może, w stopniu niezbędnym do wdrożenia właściwych przepisów tej ustawy, zażądać od podmiotu gospodarczego przetwarzającego informacje osobowe przedłożenia wymaganych informacji lub materiałów związanych z przetwarzaniem informacji osobowych.

([40]) W ustawie o ochronie informacji osobowych przewidziano m.in. zasady akredytacji takich organizacji; zob. art. 47–50 tej ustawy.

([41]) Art. 52 ustawy o ochronie informacji osobowych.

([42]) Zawiadomienie Komisji ds. Ochrony Informacji Osobowych nr 1/2017 w sprawie działań podejmowanych w przypadku naruszenia ochrony danych osobowych lub w przypadku innych incydentów.

(JIPDEC) – zrzeszała 15 436 uczestniczących podmiotów gospodarczych ([43]). Zatwierdzone programy obejmują stowarzyszenia sektorowe, takie jak np. Japońskie Stowarzyszenie Dealerów Papierów Wartościowych, Japońskie Stowarzyszenie Szkół Nauki Jazdy lub Stowarzyszenie Biur Matrymonialnych ([44]).

(74) Co roku zatwierdzone organizacje zajmujące się ochroną informacji osobowych przedkładają sprawozdania ze swojej działalności. Jak wynika z dokumentu pt. „Przegląd stanu wdrożenia ustawy o ochronie informacji osobowych w roku obrachunkowym 2015", opublikowanego przez Komisję ds. Ochrony Informacji Osobowych, akredytowane organizacje zajmujące się ochroną informacji osobowych otrzymały łącznie 442 skargi, w 123 przypadkach zażądały wyjaśnień od podmiotów gospodarczych podlegających ich jurysdykcji, w 41 przypadkach zażądały od tych podmiotów przedłożenia dokumentów oraz wydały 181 instrukcji i dwa zalecenia ([45]).

2.3.9. *Ograniczenia dotyczące dalszego przekazywania danych*

(75) Stopień ochrony zapewnianej danym osobowym przekazywanym z Unii Europejskiej podmiotom gospodarczym w Japonii nie może zostać osłabiony wskutek dalszego przekazywania takich danych odbiorcom z państw trzecich poza Japonią. Takie „dalsze przekazywanie", które z perspektywy japońskiego podmiotu gospodarczego stanowi międzynarodowe przekazywanie danych z Japonii, powinno być dozwolone tylko wtedy, gdy kolejny odbiorca spoza Japonii sam podlega przepisom zapewniającym stopień ochrony zbliżony do ochrony gwarantowanej w japońskim porządku prawnym.

(76) Pierwsze zabezpieczenie przewidziano w art. 24 ustawy o ochronie informacji osobowych, zgodnie z którym co do zasady zakazane jest przekazywanie danych osobowych osobie trzeciej spoza terytorium Japonii bez uprzedniej zgody zainteresowanej osoby fizycznej. W sekcji 4 przepisów uzupełniających zapewniono, aby przy przekazywaniu danych z Unii Europejskiej taka zgoda została wyrażona w szczególnie świadomy sposób, ponieważ wymagane jest, aby zainteresowana osoba fizyczna „otrzymała informacje o okolicznościach związanych z przekazywaniem, które są niezbędne do podjęcia przez osobę powierzającą dane decyzji o wyrażeniu zgody". Na tej podstawie osobę, której dane dotyczą, informuję się o tym, że jej dane zostaną przekazane za granicę (poza zakres stosowania ustawy o ochronie informacji osobowych) oraz o tym, jaki jest kraj przeznaczenia. Pozwoli jej to na ocenę ryzyka naruszenia prywatności związanego z przekazaniem danych. Ponadto, jak można wywieść z art. 23 ustawy o ochronie informacji osobowych (zob. motyw 47), informacje przekazywane osobie powierzającej dane powinny obejmować elementy obligatoryjne, o których mowa w ust. 2, tj. kategorie danych osobowych przekazywanych osobie trzeciej oraz sposób ujawnienia.

(77) W art. 24 ustawy o ochronie informacji osobowych, stosowanym w związku z art. 11-2 przepisów przyjętych przez Komisję ds. Ochrony Informacji Osobowych, przewidziano szereg wyjątków od tej zasady dotyczącej uzyskania zgody. Ponadto zgodnie z art. 24 w przypadku międzynarodowego przekazywania danych stosuje się te same odstępstwa co odstępstwa przewidziane w art. 23 ust. 1 ustawy o ochronie informacji osobowych ([46]).

(78) Aby zapewnić ciągłość ochrony przy przekazywaniu danych osobowych z Unii Europejskiej do Japonii na podstawie niniejszej decyzji, w sekcji 4 przepisów uzupełniających przewidziano zwiększenie stopnia ochrony na potrzeby dalszego przekazywania takich danych przez podmioty gospodarcze przetwarzające informacje osobowe do odbiorców z państw trzecich. Cel ten jest osiągany przez wprowadzenie ograniczeń i ram dotyczących podstaw międzynarodowego przekazywania danych, które podmiot gospodarczy przetwarzający informacje osobowe może wykorzystać jako alternatywę dla zgody. Ściślej rzecz ujmując i bez uszczerbku dla odstępstw określonych w art. 23 ust. 1 ustawy o ochronie informacji osobowych, dane osobowe przekazywane na podstawie niniejszej decyzji mogą podlegać (dalszemu) przekazywaniu bez zgody wyłącznie w dwóch przypadkach: (i) gdy dane przesyłane są do państwa trzeciego, które zostało wskazane przez Komisję ds. Ochrony Informacji Osobowych na podstawie art. 24 ustawy o ochronie informacji osobowych jako państwo zapewniające ochronę w stopniu równoważnym ochronie gwarantowanej w Japonii ([47]); lub (ii) gdy podmiot gospodarczy przetwarzający informacje osobowe i osoba trzecia będąca odbiorcą wspólnie wdrożyły środki zapewniające ochronę w stopniu równoważnym ochronie przewidzianej w ustawie o ochronie informacji osobowych, interpretowanej w związku z przepisami uzupełniającymi, a tego rodzaju środki zostały wdrożone na podstawie umowy lub innej formy wiążących porozumień w ramach grupy przedsiębiorstw. Druga kategoria odpowiada instrumentom stosowanym na podstawie rozporządzenia (UE) 2016/679 w celu zapewnienia odpowiednich zabezpieczeń (zwłaszcza klauzul umownych oraz wiążących reguł korporacyjnych). Ponadto, jak potwierdziła Komisja ds. Ochrony Informacji Osobowych, nawet w takich przypadkach przeniesienie nadal podlega zasadom ogólnym właściwym dla każdego przekazania danych osobowych stronie trzeciej w ramach ustawy o ochronie informacji osobowych (tj. obowiązkowi uzyskania zgody na podstawie art. 23 ust. 1 albo obowiązkowi informacyjnemu z możliwością rezygnacji na

([43]) Według danych opublikowanych na stronie internetowej PrivacyMark JIPDEC z dnia 2 października 2017 r.

([44]) Komisja ds. Ochrony Informacji Osobowych, dokument „Wykaz akredytowanych organizacji zajmujących się ochroną informacji osobowych", dostępny w internecie pod adresem: https://www.ppc.go.jp/personal/nintei/list/ lub https://www.ppc.go.jp/files/pdf/nintei_list.pdf

([45]) Komisja ds. Ochrony Informacji Osobowych, dokument „Przegląd stanu wdrożenia ustawy o ochronie informacji osobowych w roku obrachunkowym 2015", październik 2016 r., dostępny (tylko w języku japońskim) w internecie pod adresem: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

([46]) Zob. przypis 32.

([47]) Zgodnie z art. 11 przepisów przyjętych przez Komisję ds. Ochrony Informacji Osobowych wymaga to nie tylko stosowania standardów materialnych równoważnych standardom przewidzianym w ustawie o ochronie informacji osobowych, których przestrzeganie jest skutecznie nadzorowane przez niezależny organ egzekwowania prawa, lecz także zapewnienia wdrożenia odpowiednich zasad w państwie trzecim.

podstawie z art. 23 ust. 2 tej ustawy). Jeżeli nie można zwrócić się do osoby, której dane dotyczą, z prośbą o wyrażenie zgody lub w celu obowiązkowego poinformowania z wyprzedzeniem na podstawie art. 23 ust. 2 ustawy o ochronie informacji osobowych, przeniesienie nie może nastąpić.

(79) W związku z powyższym z wyjątkiem sytuacji, w których Komisja ds. Ochrony Informacji Osobowych stwierdziła, że dane państwo trzecie zapewnia ochronę w stopniu równoważnym ochronie gwarantowanej ustawą o ochronie informacji osobowych ([48]), wymogi określone w sekcji 4 przepisów uzupełniających wykluczają stosowanie instrumentów przekazywania, które nie stwarzają wiążącej relacji między japońskim podmiotem przekazującym dane a podmiotem z państwa trzeciego odbierającym dane oraz nie gwarantują wymaganego stopnia ochrony. Tak będzie na przykład w przypadku systemu transgranicznych zasad ochrony prywatności APEC (CBPR), w którym uczestniczy japońska gospodarka ([49]), ponieważ zabezpieczenia stosowane w ramach tego systemu nie wynikają z porozumienia wiążącego podmiot przekazujący i podmiot odbierający w kontekście ich relacji dwustronnych, a poziom tych zabezpieczeń jest wyraźnie niższy niż poziom gwarantowany ustawą o ochronie informacji osobowych interpretowaną w związku z przepisami uzupełniającymi ([50]).

(80) Wreszcie kolejne zabezpieczenie na wypadek (dalszego) przekazywania danych wynika z art. 20 i 22 ustawy o ochronie informacji osobowych. Zgodnie z tymi przepisami w przypadku gdy podmiot z państwa trzeciego (podmiot odbierający dane) działa w imieniu podmiotu gospodarczego przetwarzającego informacje osobowe (podmiotu przekazującego dane), tzn. jako podmiot przetwarzający (podwykonawca przetwarzania), podmiot gospodarczy przetwarzający informacje osobowe jest zobowiązany do zapewnienia nadzoru nad takim podmiotem w zakresie bezpieczeństwa przetwarzanie danych.

2.3.10. *Prawa indywidualne*

(81) W ustawie o ochronie informacji osobowych, podobnie jak w unijnych przepisach o ochronie danych, osobom fizycznym zapewniono szereg egzekwowalnych praw. Obejmują one między innymi prawo dostępu („ujawnienia"), prawo do sprostowania i usunięcia danych, a także prawo do sprzeciwu („zaprzestania wykorzystania").

(82) Po pierwsze, zgodnie z art. 28 ust. 1 i 2 ustawy o ochronie informacji osobowych osoba, której dane dotyczą, ma prawo zażądać od podmiotu gospodarczego przetwarzającego informacje osobowe „ujawnieni[a] zatrzymanych danych osobowych, na podstawie których można ją zidentyfikować", a podmiot ten po otrzymaniu takiego żądania „ujawnia […] zatrzymane dane osobowe" osobie, której dane dotyczą. Art. 29 (prawo do korekty) i art. 30 (prawo do zaprzestania wykorzystania) mają tę samą strukturę co art. 28.

(83) Art. 9 zarządzenia Rady Ministrów stanowi, że ujawnienie informacji osobowych, o którym mowa w art. 28 ust. 2 ustawy o ochronie informacji osobowych, odbywa się na piśmie, chyba że podmiot gospodarczy przetwarzający informacje osobowe i osoba, której dane dotyczą, postanowiły inaczej.

(84) Prawa te podlegają trojakiego rodzaju ograniczeniom dotyczącym: praw i interesów ([51]) osoby fizycznej lub osób trzecich, poważnych zakłóceń w działalności gospodarczej podmiotu gospodarczego przetwarzającego informacje osobowe ([52]) oraz przypadków, w których ujawnienie stanowiłoby naruszenie innych przepisów ustawowych i wykonawczych ([53]). Sytuacje, w których ograniczenia te znalazłyby zastosowanie, są podobne do niektórych wyjątków przewidzianych w art. 23 ust. 1 rozporządzenia (UE) 2016/679, w którym dopuszcza się ograniczenie praw osób fizycznych z przyczyn zapewniających „ochronę osoby, której dane dotyczą, lub praw i wolności innych osób" lub osiągnięcie „innych ważnych celów leżących w ogólnym interesie publicznym". Choć kategorie

([48]) Jak dotąd Komisja ds. Ochrony Informacji Osobowych nie przyjęła na podstawie art. 24 ustawy o ochronie informacji osobowych ani jednej decyzji uznającej dane państwo trzecie za zapewniające poziom ochrony równoważny z poziomem ochrony zagwarantowanym w Japonii. Jedyna decyzja, którą Komisja może niebawem przyjąć, dotyczy EOG. Jeżeli chodzi o wydawanie ewentualnych kolejnych decyzji, Komisja będzie ściśle monitorować sytuację i w razie konieczności zastosuje odpowiednie środki mające zapobiec ewentualnym niekorzystnym skutkom dla ciągłości ochrony (zob. motywy 176, 177, 184 i art. 3 ust. 1).

([49]) Jedynie dwa japońskie przedsiębiorstwa zostały jednak certyfikowane w ramach systemu transgranicznych zasad ochrony prywatności APEC (CBPR) (zob. https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). Poza Japonią jedynymi podmiotami gospodarczymi certyfikowanymi w ramach systemu jest niewielka liczba (23) przedsiębiorstw amerykańskich (zob. https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) Nie określono na przykład definicji i szczególnych zabezpieczeń danych wrażliwych ani nie przewidziano obowiązku ograniczonego zatrzymywania danych. Zob. Grupa Robocza Art. 29, opinia 02/2014 w sprawie listy kontrolnej wymogów dla wiążących reguł korporacyjnych składanych do krajowych organów ochrony danych w UE oraz transgranicznych zasad ochrony prywatności składanych do pełnomocników APEC odpowiedzialnych za rozliczalność w zakresie transgranicznych zasad ochrony prywatności, 6 marca 2014 r.

([51]) Według Komisji ds. Ochrony Informacji Osobowych jedynie takie interesy mogą uzasadniać ograniczenie, które „warto objąć ochroną prawną". Ocenę tę należy przeprowadzać indywidualnie dla każdego przypadku „z uwzględnieniem ingerencji w podstawowe prawo do poszanowania życia prywatnego, w tym ochrony danych, uznane w konstytucji i precedensach sądowych". Chronione interesy mogą obejmować np. tajemnice przedsiębiorstwa lub inne tajemnice handlowe.

([52]) Pojęcie „poważnych zakłóceń we właściwym wykonywaniu działalności gospodarczej podmiotu gospodarczego" zilustrowano w wytycznych Komisji ds. Ochrony Informacji Osobowych za pomocą różnych przykładów, np. sytuacji, w której ta sama osoba fizyczna składa identyczne, skomplikowane żądania, które powodują znaczne obciążenie dla podmiotu gospodarczego, ograniczając tym samym jego zdolność do odpowiadania na inne żądania (wytyczne Komisji ds. Ochrony Informacji Osobowych (wydanie zawierające przepisy ogólne), s. 62). Ogólnie rzecz biorąc, Komisja ds. Ochrony Informacji Osobowych potwierdziła, że kategoria ta ogranicza się do przypadków wyjątkowych, wykraczających poza zwykłe niedogodności. W szczególności podmiot gospodarczy przetwarzający informacje osobowe nie może odmówić ujawnienia informacji jedynie z tego powodu, że zwrócono się do niego o przekazanie bardzo dużej ilości danych.

([53]) Jak potwierdziła Komisja ds. Ochrony Informacji Osobowych, regulacje te muszą mieć wzgląd na prawo do prywatności zagwarantowane w konstytucji i tym samym „odzwierciedlać niezbędne i uzasadnione ograniczenia".

przypadków, w których ujawnienie danych stanowiłoby naruszenie „innych przepisów ustawowych i wykonawczych", mogą wydawać się szerokie, w przepisach ustawowych i wykonawczych przewidujących ograniczenia w tym zakresie należy zapewnić poszanowanie konstytucyjnego prawa do prywatności oraz można w nich wprowadzić ograniczenia wyłącznie w zakresie, w jakim wykonywanie tego prawa „nie pozostawałoby w sprzeczności z dobrem publicznym" ([54]). Wymaga to wyważenia istniejących interesów.

(85) Zgodnie z art. 28 ust. 3 ustawy o ochronie informacji osobowych, jeżeli dane, których dotyczy żądanie, nie istnieją lub w przypadku gdy dany podmiot gospodarczy przetwarzający informacje osobowe zdecyduje się nie udzielać dostępu do zatrzymanych danych, jest on zobowiązany do niezwłocznego poinformowania o tym fakcie osoby fizycznej.

(86) Po drugie, zgodnie z art. 29 ust. 1 i 2 ustawy o ochronie informacji osobowych osoba, której dane dotyczą, ma prawo zażądać korekty, dodania lub usunięcie dotyczących jej zatrzymywanych danych osobowych, jeżeli są one nieprawidłowe. Po otrzymaniu takiego żądania podmiot gospodarczy przetwarzający informacje osobowe „przeprowadza niezbędne dochodzenie" i na podstawie uzyskanych wyników „dokonuje korekty itd. treści zatrzymywanych danych".

(87) Po trzecie, zgodnie z art. 30 ust. 1 i 2 ustawy o ochronie informacji osobowych osoba, której dane dotyczą, ma prawo zażądać od podmiotu gospodarczego przetwarzającego informacje osobowe zaprzestania wykorzystywania informacji osobowych lub usunięcia takich informacji, jeżeli ich przetwarzanie stanowi naruszenie art. 16 (w odniesieniu do ograniczenia celu) lub zostały one niewłaściwie pozyskane z naruszeniem art. 17 ustawy o ochronie informacji osobowych (w odniesieniu do pozyskania w wyniku oszustwa lub za pomocą innych niewłaściwych środków lub, w przypadku danych wrażliwych, bez zgody). Podobnie, zgodnie z art. 30 ust. 3 i 4 ustawy o ochronie informacji osobowych, osoba fizyczna ma prawo zażądać od podmiotu gospodarczego przetwarzającego informacje osobowe zaprzestania przekazywania informacji osobie trzeciej, jeżeli stanowiłoby to naruszenie przepisów art. 23 ust. 1 lub art. 24 tej ustawy (w odniesieniu do przekazywania informacji osobie trzeciej, w tym międzynarodowego przekazywania danych).

(88) Po otrzymaniu takiego żądania podmiot gospodarczy przetwarzający informacje osobowe niezwłocznie zaprzestaje ich wykorzystania lub przekazywania osobie trzeciej w stopniu niezbędnym do zaradzenia naruszeniu lub, jeżeli dany przypadek podlega wyłączeniu (zwłaszcza w przypadku gdy zaprzestanie wykorzystania wiązałoby się ze szczególnie wysokimi kosztami) ([55]), wdraża niezbędne alternatywne środki w celu ochrony praw i interesów danej osoby fizycznej.

(89) W odróżnieniu od prawa UE ustawa o ochronie informacji osobowych i właściwe przepisy podustawowe nie zawierają przepisów prawnych szczegółowo odnoszących się do możliwości wniesienia sprzeciwu wobec przetwarzania do celów marketingu bezpośredniego. Niemniej jednak takie przetwarzanie, na mocy tej decyzji, będzie zawsze odbywać się w kontekście przekazywania danych osobowych, które zostały uprzednio zebrane w Unii Europejskiej. Zgodnie z art. 21 ust. 2 rozporządzenia (UE) 2016/679 osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby marketingu bezpośredniego. Ponadto, jak wyjaśniono w motywie 43, zgodnie z sekcją 3 przepisów uzupełniających, podmiot gospodarczy przetwarzający informacje osobowe jest obowiązany przetwarzać dane otrzymane na podstawie niniejszej decyzji w tym samym celu, w jakim zostały one przekazane z Unii Europejskiej, chyba że osoba, której dane dotyczą, wyraziła zgodę na zmianę celu wykorzystania. Dlatego też, jeżeli dane przekazano w jakimkolwiek celu innym niż marketing bezpośredni, podmiot gospodarczy przetwarzający informacje osobowe w Japonii nie będzie miał możliwości przetwarzania danych do celów marketingu bezpośredniego bez zgody osoby w UE, której dane dotyczą.

(90) We wszystkich przypadkach, o których mowa w art. 28 i 29 ustawy o ochronie informacji osobowych, podmiot gospodarczy przetwarzający informacje osobowe jest zobowiązany do niezwłocznego poinformowania osoby fizycznej o wyniku jej żądania oraz dodatkowo do wyjaśnienia każdej (częściowej) odmowy w oparciu o wyjątki ustawowe przewidziane w art. 27–30 (art. 31 ustawy o ochronie informacji osobowych).

([54]) Według interpretacji Sądu Najwyższego art. 13 konstytucji zapewnia prawo do prywatności (zob. motywy 7 i 8 powyżej). Chociaż prawo to może podlegać ograniczeniom w przypadkach, w których „ingeruje ono w dobro publiczne", w wyroku z dnia 6 marca 2008 r. (zob. motyw 8) Sąd Najwyższy jasno stwierdził, że wszelkie ograniczenia (pozwalające w tym przypadku organowi publicznemu na zbieranie i przetwarzanie danych osobowych) należy wyważać w kontekście prawa do prywatności, z uwzględnieniem takich czynników, jak charakter danych, ryzyko, jakie przetwarzanie tych danych stwarza dla osób fizycznych, odpowiednie zabezpieczenia oraz korzyści z przetwarzania danych dla interesu publicznego. Ma to bardzo wiele wspólnego z wyważaniem ograniczeń, jakiego wymaga prawo UE, które dopuszcza jakiekolwiek ograniczenie praw i zabezpieczeń ochrony danych dopiero po uwzględnieniu zasad konieczności i proporcjonalności.

([55]) Aby uzyskać szczegółowe wyjaśnienia na temat tych wyjątków, zob. prof. Katsuya Uga, Article by Article Commentary of the revised Act on the Protection of Personal Information [Komentarz artykuł po artykule na temat zmienionej ustawy o ochronie informacji osobowych], 2015 r., s. 217. Przykładem żądania, które powoduje „znaczne koszty" jest sytuacja, w której tylko niektóre nazwiska wymienione w obszernym wykazie (np. w spisie) są przetwarzane z naruszeniem zasady ograniczenia celu, a spis jest już dostępny w sprzedaży, przez co wycofanie tych egzemplarzy i ich wymiana na nowe byłyby bardzo kosztownym przedsięwzięciem. Jeżeli w ramach tego samego przykładu egzemplarze spisu sprzedano już wielu osobom i zebranie wszystkich z nich jest niemożliwe, „trudne do zrealizowania" byłoby również „zaprzestanie wykorzystania". W tych scenariuszach „niezbędne alternatywne środki" mogłyby obejmować na przykład publikację lub dystrybucję zawiadomienia o korekcie. Takie działania nie wykluczają innych form dochodzenia roszczeń (na drodze sądowej), czy to za naruszenie prywatności, narażenie reputacji (zniesławienie) w wyniku publikacji lub naruszenie innych interesów.

(91) Jeżeli chodzi o warunki składania żądania, zgodnie z art. 32 ustawy o ochronie informacji osobowych (w związku z zarządzeniem Rady Ministrów) podmiot gospodarczy przetwarzający informacje osobowe może określić racjonalne procedury, w tym w odniesieniu do informacji niezbędnych do identyfikacji zatrzymanych danych osobowych. Zgodnie jednak z ust. 4 tego artykułu podmioty gospodarcze przetwarzające informacje osobowe nie mogą „nadmiernie obciążać osoby powierzającej". W niektórych przypadkach podmioty gospodarcze przetwarzające informacje osobowe mogą również nakładać opłaty, o ile ich wysokość pozostaje „w granicach uznawanych za racjonalne przy uwzględnieniu faktycznych kosztów" (art. 33 ustawy o ochronie informacji osobowych).

(92) Wreszcie osoba fizyczna może wnieść sprzeciw wobec przekazywania dotyczących jej informacji osobowych osobie trzeciej na podstawie art. 23 ust. 2 ustawy o ochronie informacji osobowych lub odmówić wyrażenia zgody na podstawie art. 23 ust. 1 (uniemożliwiając tym samym ujawnienie informacji, jeżeli nie jest dostępna żadna inna podstawa prawna). Podobnie osoba fizyczna może zatrzymać przetwarzanie danych do innych celów, odmawiając wyrażenia zgody na podstawie art. 16 ust. 1 ustawy o ochronie informacji osobowych.

(93) W odróżnieniu od prawa Unii ustawa o ochronie informacji osobowych i właściwe przepisy podustawowe nie zawierają przepisów ogólnych odnoszących się do kwestii decyzji wpływających na osobę, której dane dotyczą, i opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych. Kwestia ta została jednak uregulowana w niektórych przepisach sektorowych obowiązujących w Japonii, które są szczególnie istotne dla tego rodzaju przetwarzania. Dotyczy to sektorów, w których przedsiębiorstwa są najbardziej skłonne do korzystania ze zautomatyzowanego przetwarzania danych osobowych przy podejmowaniu decyzji wpływających na osoby fizyczne (np. sektora finansowego). Przykładowo zgodnie z „Kompleksowymi wytycznymi dotyczącymi nadzoru nad głównymi bankami", zmienionymi w czerwcu 2017 r., zainteresowanej osobie fizycznej należy w szczegółowy sposób wyjaśnić powody będące podstawą odrzucenia wniosku o zawarcie umowy kredytu. Przepisy te zapewniają zatem zabezpieczenia w prawdopodobnej ograniczonej liczbie przypadków, w których sam japoński podmiot gospodarczy odbierający dane podjąłby zautomatyzowane decyzje (zamiast unijnego administratora przekazującego dane).

(94) Niezależnie od okoliczności, jeżeli chodzi o dane osobowe zebrane w Unii Europejskiej, wszelkie decyzje opierające się na zautomatyzowanym przetwarzaniu podejmowane są zazwyczaj przez administratora danych w Unii (który ma bezpośrednie powiązanie z zainteresowaną osobą, której dane dotyczą) i podlegają tym samym przepisom rozporządzenia (UE) 2016/679 ([56]). Obejmuje to scenariusze przekazywania, w których za przetwarzanie odpowiada zagraniczny (np. japoński) podmiot gospodarczy działający w charakterze przedstawiciela (podmiotu przetwarzającego) w imieniu unijnego administratora danych (lub działający w charakterze podwykonawcy przetwarzania w imieniu unijnego podmiotu przetwarzającego po otrzymaniu danych od unijnego administratora danych, który je zebrał), który na tej podstawie podejmuje następnie decyzję. Mało prawdopodobne jest zatem, aby fakt, iż ustawa o ochronie informacji osobowych nie zawiera szczegółowych przepisów dotyczących zautomatyzowanego podejmowania decyzji, miał wpływ na stopień ochrony danych osobowych przekazywanych na podstawie niniejszej decyzji.

2.4. **Nadzór i egzekwowanie przepisów**

2.4.1. *Niezależny nadzór*

(95) Aby zagwarantować również w praktyce odpowiedni stopień ochrony danych, należy ustanowić niezależny organ nadzorczy, uprawniony do monitorowania i egzekwowania zgodności z przepisami dotyczącymi ochrony danych. W ramach wykonywanych obowiązków i realizowanych uprawnień organ ten powinien być całkowicie niezależny i bezstronny.

(96) W Japonii organem odpowiedzialnym za monitorowanie i egzekwowanie ustawy o ochronie informacji osobowych jest Komisja ds. Ochrony Informacji Osobowych. Składa się ona z przewodniczącego i ośmiu komisarzy powoływanych przez premiera za zgodą obu izb japońskiego parlamentu (Diet). Kadencja przewodniczącego i wszystkich komisarzy trwa pięć lat, przy czym istnieje możliwość ich ponownego powołania (art. 64 ustawy o ochronie informacji osobowych). Komisarze mogą zostać odwołani wyłącznie z ważnego powodu w razie wystąpienia określonych w zamkniętym katalogu okoliczności ([57]) oraz nie mogą prowadzić aktywnej działalności politycznej. Ponadto zgodnie z ustawą o ochronie informacji osobowych komisarze zatrudnieni w pełnym wymiarze godzin mają obowiązek powstrzymać się od prowadzenia jakiejkolwiek innej działalności zarobkowej lub gospodarczej. Wszyscy komisarze podlegają również przepisom wewnętrznym uniemożliwiającym im uczestnictwo w obradach w razie potencjalnego konfliktu interesów. Wsparcie dla komisji stanowi sekretariat, którym kieruje sekretarz generalny i który utworzono w celu wykonywania zadań powierzonych komisji (art. 70 ustawy o ochronie informacji osobowych). Zarówno komisarzy, jak i wszystkich urzędników sekretariatu obowiązują surowe przepisy dotyczące zachowania tajemnicy (art. 72 i 82 ustawy o ochronie informacji osobowych).

([56]) Natomiast w wyjątkowych przypadkach, w których japoński podmiot 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 podmiot japoński objęty jest zakresem stosowania rozporządzenia (UE) 2016/679 (art. 3 ust. 2) i ma tym samym obowiązek bezpośrednio przestrzegać unijnych przepisów o ochronie danych.

([57]) Zgodnie z art. 65 ustawy o ochronie informacji osobowych odwołanie komisarza wbrew jego woli możliwe jest tylko w następujących przypadkach: (i) wszczęcie postępowania upadłościowego; (ii) wyrok skazujący za naruszenie ustawy o ochronie informacji osobowych lub ustawy o stosowaniu numerów identyfikacyjnych; (iii) wyrok skazujący na karę pozbawienia wolności bez wykonywania pracy lub surowszy wyrok; (iv) niezdolność do wykonywania obowiązków z powodu zaburzeń psychicznych lub fizycznych lub z powodu przewinienia.

(97) Uprawnienia Komisji ds. Ochrony Informacji Osobowych, które są wykonywane przy zachowaniu pełnej niezależności ([58]), przewidziano przede wszystkim w art. 40, 41 i 42 ustawy o ochronie informacji osobowych. Zgodnie z art. 40 Komisja ds. Ochrony Informacji Osobowych może zażądać od podmiotu gospodarczego przetwarzającego informacje osobowe zgłoszenia lub przedłożenia dokumentów dotyczących operacji przetwarzania oraz może również przeprowadzać kontrole, zarówno na miejscu, jak i w zakresie ksiąg i innych dokumentów. Komisja ta może również zapewnić podmiotowi gospodarczemu przetwarzającemu informacje osobowe wytyczne lub doradztwo w kwestii przetwarzania takich informacji, w zakresie wymaganym do wdrożenia ustawy o ochronie informacji osobowych. Komisja ds. Ochrony Informacji Osobowych skorzystała już z tego uprawnienia na mocy art. 41 ustawy o ochronie informacji osobowych, kierując wytyczne do Facebooka po ujawnieniu powiązanej z nim afery Cambridge Analytica.

(98) Przede wszystkim Komisji ds. Ochrony Informacji Osobowych przysługują uprawnienia w zakresie wydawania – w odpowiedzi na skargę lub z własnej inicjatywy – zaleceń i zarządzeń w celu egzekwowania ustawy o ochronie informacji osobowych i innych wiążących przepisów (w tym przepisów uzupełniających) w poszczególnych przypadkach. Uprawnienia te ustanowiono w art. 42 ustawy o ochronie informacji osobowych. Ust. 1 i 2 przewidują dwuetapowy mechanizm, w ramach którego Komisja ds. Ochrony Informacji Osobowych może wydać zarządzenie (wyłącznie) po wcześniejszym wydaniu zalecenia, natomiast ust. 3 przewiduje możliwość bezpośredniego przyjęcia zarządzenia w sytuacjach nagłych.

(99) Chociaż nie wszystkie przepisy rozdziału IV sekcja 1 ustawy o ochronie informacji osobowych zostały wymienione w ust. 42 ust. 1 – w którym określono również zakres stosowania art. 42 ust. 2 – wynika to z faktu, że niektóre z tych przepisów nie dotyczą obowiązków podmiotu gospodarczego przetwarzającego informacje osobowe ([59]), a wszystkie najważniejsze zabezpieczenia zapewniono już w pozostałych wymienionych przepisach. Choć nie wymieniono na przykład art. 15 (zgodnie z którym podmiot gospodarczy przetwarzający informacje osobowe jest zobowiązany do wyznaczenia celu wykorzystania i do przetwarzania odnośnych informacji osobowych wyłącznie w jego zakresie), nieprzestrzeganie zawartego w nim wymogu może stanowić podstawę do wydania zalecenia w związku z naruszeniem art. 16 ust. 1 (w którym podmiotowi gospodarczemu przetwarzającemu informacje osobowe zakazano przetwarzania takich informacji poza zakresem niezbędnym do osiągnięcia celu wykorzystania, chyba że uzyskano zgodę osoby, której dane dotyczą) ([60]). Kolejnym przepisem, którego nie wymieniono w art. 42 ust. 1 tej ustawy, jest art. 19 dotyczący prawidłowości i zatrzymywania danych. Nieprzestrzeganie tego przepisu może być egzekwowane jako naruszenie art. 16 ust. 1 albo w oparciu o naruszenie art. 29 ust. 2, jeżeli dana osoba fizyczna zażądała dokonania korekty lub usunięcia błędnych lub zbędnych danych, a podmiot gospodarczy przetwarzający informacje osobowe odrzucił takie żądanie. Jeżeli chodzi o prawa osób, których dane dotyczą, zgodnie z art. 28 ust. 1, art. 29 ust. 1 oraz art. 30 ust. 1 nadzór sprawowany przez Komisję ds. Ochrony Informacji Osobowych zapewniony jest dzięki przyznaniu jej uprawnień w zakresie egzekwowania odnośnych obowiązków podmiotu gospodarczego przetwarzającego informacje osobowe, o których to obowiązkach mowa w tych artykułach.

(100) Zgodnie z art. 42 ust. 1 ustawy o ochronie informacji osobowych Komisja ds. Ochrony Informacji Osobowych może – w przypadku gdy stwierdzi, że istnieje „potrzeba ochrony praw i interesów jednostki w związku z naruszeniem przez [podmiot gospodarczy przetwarzający informacje osobowe]" określonych przepisów tej ustawy – wydać zalecenie w sprawie „zawieszenia działania stanowiącego naruszenie lub podjęcia innych działań niezbędnych do zaradzenia naruszeniu". Takie zalecenie nie jest wiążące, ale zapewnia możliwość wydania wiążącego zarządzenia na podstawie art. 42 ust. 2 ustawy o ochronie informacji osobowych. Na podstawie tego przepisu, jeżeli zalecenie nie zostanie wykonane „bez prawnie uzasadnionych podstaw", a Komisja ds. Ochrony Informacji Osobowych „uzna, że istnieje nieuchronne ryzyko poważnego naruszenia praw i interesów jednostki", może ona nakazać podmiotowi gospodarczemu przetwarzającemu informacje osobowe podjęcie działania zgodnego z zaleceniem.

(101) W przepisach uzupełniających doprecyzowano i zwiększono uprawnienia Komisji ds. Ochrony Informacji Osobowych w zakresie egzekwowania prawa. Ściślej rzecz ujmując, w przypadkach dotyczących danych odbieranych z Unii Europejskiej Komisja ds. Ochrony Informacji Osobowych zawsze uzna niepodjęcie, bez prawnie uzasadnionych podstaw, przez podmiot gospodarczy przetwarzający informacje osobowe działań zgodnych z zaleceniem wydanym przez komisję na podstawie z art. 42 ust. 1 za bezpośrednie, poważne naruszenie praw i interesów jednostki w rozumieniu art. 42 ust. 2, a zatem za naruszenie uprawniające do wydania wiążącego zarządzenia. Ponadto komisja ta za „prawnie uzasadnione podstawy" niezastosowania się do zalecenia uznaje jedynie „nadzwyczajne zdarzenia [uniemożliwiające zastosowanie się], niezależne od [podmiotu gospodarczego przetwarzającego informacje osobowe], których nie można racjonalnie przewidzieć (na przykład klęski żywiołowe)" lub przypadki, w których konieczność podjęcia działań przewidzianych w zaleceniu „przestała istnieć w związku z podjęciem przez [podmiot gospodarczy przetwarzający informacje osobowe] alternatywnych działań, które pozwoliły w całości zaradzić naruszeniu".

([58]) Zob. art. 62 ustawy o ochronie informacji osobowych.

([59]) Niektóre przepisy dotyczą na przykład dobrowolnych działań podmiotu gospodarczego przetwarzającego informacje osobowe (art. 32, 33 ustawy o ochronie informacji osobowych) lub obowiązku dołożenia należytej staranności, który jako taki nie podlega egzekwowaniu (art. 31, 35, 36 ust. 6, art. 39 ustawy o ochronie informacji osobowych). Niektóre przepisy nie są skierowane do podmiotu gospodarczego przetwarzającego informacje osobowe, a do innych podmiotów. Przykładowo są to art. 23 ust. 4, art. 26 ust. 2 oraz art. 34 ustawy o ochronie informacji osobowych (choć wykonalność art. 26 ust. 2 zapewniono dzięki możliwości nałożenia sankcji karnych zgodnie z art. 88 ppkt (i) tej ustawy).

([60]) Ponadto, jak wyjaśniono w motywie (48), w kontekście przekazywania danych „cel wykorzystania" jest wskazywany przez unijny podmiot eksportujący dane, który pod tym względem podlega obowiązkowi przewidzianemu w art. 5 ust. 1 lit. b) rozporządzenia (UE) 2016/679. Obowiązek ten jest egzekwowany przez właściwy organ ochrony danych w Unii Europejskiej.

(102) Niezastosowanie się do zarządzenia Komisji ds. Ochrony Informacji Osobowych uznawane jest za przestępstwo zgodnie z art. 84 ustawy o ochronie informacji osobowych, a na podmiot gospodarczy przetwarzający informacje osobowe, który zostanie uznany za winny, może zostać nałożona kara pozbawienia wolności w wymiarze do 6 miesięcy z obowiązkiem wykonywania pracy lub kara grzywny w wysokości do 300 000 JPY. Ponadto zgodnie z art. 85 ppkt (i) tej ustawy brak współpracy z Komisją ds. Ochrony Informacji Osobowych lub utrudnianie jej dochodzenia podlega karze grzywny w wysokości do 300 000 JPY. Te sankcje karne stosuje się oprócz sankcji, które mogą być stosowane w przypadkach poważnych naruszeń stawy o ochronie informacji osobowych (zob. motyw 108).

2.4.2. *Dochodzenie roszczeń na drodze sądowej*

(103) W celu zapewnienia odpowiedniej ochrony, a zwłaszcza egzekwowania praw indywidualnych, osoba, której dane dotyczą, powinna mieć możliwość skutecznego dochodzenia roszczeń na drodze administracyjnej lub sądowej, w tym odszkodowania za szkody.

(104) Przed przystąpieniem do dochodzenia roszczeń na drodze administracyjnej lub sądowej lub zamiast takiego dochodzenia osoba fizyczna może zdecydować się złożyć skargę w sprawie przetwarzania dotyczących jej danych osobowych bezpośrednio do administratora. Na podstawie art. 35 ustawy o ochronie informacji osobowych podmioty przetwarzające informacje osobowe dokładają starań, aby takie skargi były rozpatrywane w sposób „odpowiedni i natychmiastowy", oraz ustanawiają w tym celu wewnętrzne systemy rozpatrywania skarg. Ponadto zgodnie z art. 61 pkt (ii) ustawy o ochronie informacji osobowych Komisja ds. Ochrony Informacji Osobowych jest odpowiedzialna za „przeprowadzenie niezbędnej mediacji w związku ze złożoną skargą i zaproponowanie współpracy podmiotowi gospodarczemu, który rozpatruje tę skargę", co w obu aspektach obejmuje skargi wniesione przez cudzoziemców. W tym zakresie ustawodawca japoński powierzył instytucjom rządowym na szczeblu centralnym zadanie podejmowania „działań niezbędnych" do umożliwienia i ułatwienia rozpatrywania skarg przez podmioty gospodarcze przetwarzające informacje osobowe (art. 9), natomiast instytucje samorządowe na szczeblu lokalnym dokładają starań, aby zapewnić mediację w takich przypadkach (art. 13). W tej kwestii osoby fizyczne mogą składać skargi do jednego z 1 700 centrów konsumenckich założonych przez instytucje samorządowe na szczeblu lokalnym na podstawie ustawy w sprawie bezpieczeństwa konsumentów ([61]), a także do Krajowego Centrum Skarg Konsumenckich Japonii. Takie skargi można wnosić w związku z naruszeniem ustawy o ochronie informacji osobowych. Zgodnie z art. 19 podstawowej ustawy konsumenckiej ([62]) instytucje samorządowa na szczeblu lokalnym dokładają starań, aby uczestniczyć w mediacji w przypadku skarg i zapewniać stronom niezbędną wiedzę fachową. Te mechanizmy rozstrzygania sporów wydają się dość skuteczne – spośród ponad 75 000 skarg złożonych w 2015 r. spory rozstrzygnięto w 91,2 % przypadków.

(105) Naruszenia przepisów ustawy o ochronie informacji osobowych przez podmiot gospodarczy przetwarzający informacje osobowe mogą stanowić podstawę do wniesienia powództwa cywilnego, wszczęcia postępowania karnego oraz do nałożenia sankcji karnych. Po pierwsze, jeżeli dana osoba fizyczna uzna, że naruszono jej prawa przewidziane w art. 28, 29 i 30 ustawy o ochronie informacji osobowych, może ona zwrócić się do sądu o wydanie nakazu sądowego, w którym podmiot gospodarczy przetwarzający informacje osobowe zostanie zobowiązany do spełnienia żądania tej osoby na podstawie jednego z powyższych przepisów, tj. do ujawnienia zatrzymanych danych osobowych (art. 28), sprostowania zatrzymanych danych osobowych, które są nieprawidłowe (art. 29), lub zaprzestania niezgodnego z prawem przetwarzania lub przekazywania danych osobie trzeciej (art. 30). Takie działanie można podjąć bez konieczności powoływania się na art. 709 kodeksu cywilnego ([63]) albo w inny sposób na prawo o czynach niedozwolonych ([64]). Przede wszystkim oznacza to, że na osobie fizycznej nie spoczywa obowiązek udowodnienia powstania szkody.

(106) Po drugie, w przypadku gdy zarzucane naruszenie nie dotyczy praw indywidualnych przewidzianych w art. 28, 29 i 30, ale ogólnych zasad lub obowiązków podmiotu gospodarczego przetwarzającego informacje osobowe w zakresie ochrony danych, zainteresowana osoba fizyczna może wytoczyć powództwo cywilne przeciwko podmiotowi gospodarczemu na podstawie przepisów o czynach niedozwolonych japońskiego kodeksu cywilnego, zwłaszcza art. 709. W przypadku sprawy sądowej wytoczonej na podstawie art. 709 oprócz przesłanki winy (winy umyślnej lub niedbalstwa) wykazać należy szkodę, przy czym zgodnie z art. 710 kodeksu cywilnego taka szkoda może być zarówno materialna, jak i niematerialna. Nie ma ograniczeń co do kwoty kompensaty.

(107) W kwestii dostępnych środków ochrony prawnej art. 709 japońskiego kodeksu cywilnego odwołuje się do odszkodowania pieniężnego. W japońskim orzecznictwie artykuł ten jest jednak interpretowany jako przyznający prawo do uzyskania sądowego nakazu powstrzymywania się od działania ([65]). W związku z powyższym, jeżeli osoba, której dane dotyczą, wnosi sprawę na podstawie art. 709 kodeksu cywilnego oraz twierdzi, że jej prawa lub interesy zostały naruszone w wyniku naruszenia przez pozwanego przepisów ustawy o ochronie informacji osobowych, roszczenie może obejmować, oprócz odszkodowania, żądanie wydania nakazu sądowego, przede wszystkim w celu wstrzymania przetwarzania niezgodnego z prawem.

([61]) Ustawa nr 50 z dnia 5 czerwca 2009 r.
([62]) Ustawa nr 60 z dnia 22 sierpnia 2012 r.
([63]) Art. 709 kodeksu cywilnego stanowi główną podstawę wytoczenia powództwa odszkodowawczego. Zgodnie z tym przepisem „kto umyślnie lub wskutek niedbalstwa naruszył jakiekolwiek prawo lub prawnie chroniony interes innych osób, zobowiązany jest do naprawienia wynikłej stąd szkody".
([64]) Wysoki Trybunał w Tokio, wyrok z dnia 20 maja 2015 r. (nieopublikowany); Sąd Rejonowy w Tokio, wyrok z dnia 8 września 2014 r., Westlaw Japan 2014WLJPCA09088002. Zob. również art. 34 ust. 1 i 3 ustawy o ochronie informacji osobowych.
([65]) Zob. Sąd Najwyższy, wyrok z dnia 24 września 2002 r. (Hanrei Times, tom 1106, s. 72).

(108) Po trzecie, oprócz środków służących ochronie interesu prawnego przewidzianych w prawie cywilnym (przepisach o czynach niedozwolonych) osoba, której dane dotyczą, może złożyć w prokuraturze lub w policji sądowej zawiadomienie w sprawie naruszenia ustawy o ochronie informacji osobowych, na podstawie którego mogą zostać nałożone sankcje karne. W rozdziale VII tej ustawy znajduje się szereg przepisów karnych. Najważniejszy z nich (art. 84) dotyczy niestosowania się przez podmiot gospodarczy przetwarzający informacje osobowe do zarządzeń Komisji ds. Ochrony Informacji Osobowych wydanych na podstawie art. 42 ust. 2 i 3. Jeżeli podmiot gospodarczy nie zastosuje się do zarządzenia wydanego przez komisję, jej przewodniczący (oraz każdy inny urzędnik rządowy) ([66]) może przekazać sprawę prokuratorowi lub funkcjonariuszowi policji sądowej, doprowadzając tym samym do wszczęcia postępowania karnego. Za naruszenie zarządzenia komisji grozi kara pozbawienia wolności w wymiarze do sześciu miesięcy z obowiązkiem wykonywania pracy lub kara grzywny w wysokości do 300 000 JPY. Do pozostałych przepisów ustawy o ochronie informacji osobowych, które przewidują sankcje za jej naruszenia mające wpływ na prawa i interesy osób, których dane dotyczą, zalicza się art. 83 (dotyczący „ukradkowego zapewniania lub wykorzystywania" bazy informacji osobowych „w celu czerpania […] nielegalnych korzyści") oraz art. 88 ppkt (i) (dotyczący niedostarczenia przez osobę trzecią właściwych informacji na rzecz podmiotu gospodarczego przetwarzającego informacje osobowe, gdy otrzymuje on dane osobowe zgodnie z art. 26 ust. 1 ustawy o ochronie informacji osobowych, zwłaszcza szczegółowych informacji o własnym, wcześniejszym pozyskaniu takich danych przez osobę trzecią). Kary mające zastosowanie w przypadku takich naruszeń ustawy to, odpowiednio, kara pozbawienia wolności w wymiarze do jednego roku z obowiązkiem wykonywania pracy lub kara grzywny w wysokości do 500 000 JPY (w przypadku art. 83) lub kara grzywny administracyjnej w wysokości do 100 000 JPY (w przypadku art. 88 ppkt (i)). Chociaż już sama groźba sankcji karnej prawdopodobnie będzie mieć duży skutek odstraszający dla zarządu przedsiębiorstwa, który w imieniu podmiotu gospodarczego przetwarzającego informacje osobowe kieruje operacjami przetwarzania, jak również dla osób przetwarzających dane, w art. 87 ustawy o ochronie informacji osobowych doprecyzowano, że w przypadku gdy przedstawiciel, pracownik lub inny zatrudniony w przedsiębiorstwie dopuścił się naruszenia zgodnie z art. 83–85 tej ustawy, „sprawca podlegać będzie odpowiedzialności karnej oraz na tę osobę prawną zostanie nałożona grzywna określona w odpowiednich przepisach". W takim przypadku sankcje, nawet w wysokości maksymalnej, można nałożyć zarówno na pracownika, jak i na przedsiębiorstwo.

(109) Wreszcie osoby fizyczne mogą również dochodzić roszczeń z tytułu działań lub zaniechań Komisji ds. Ochrony Informacji Osobowych. Pod tym względem w japońskim prawie przewidziano szereg możliwości dochodzenia roszczeń na drodze administracyjnej i sądowej.

(110) Jeżeli dana osoba fizyczna jest niezadowolona z przebiegu działań podjętych przez Komisję ds. Ochrony Informacji Osobowych, może ona na podstawie ustawy o skargach administracyjnych złożyć taką skargę ([67]). Jeżeli dana osoba fizyczna uzna natomiast, że Komisja ds. Ochrony Informacji Osobowych powinna była podjąć działania, ale tego nie uczyniła, może ona zgodnie z art. 36-3 tej ustawy zażądać od komisji wydania zarządzenia lub wytycznych administracyjnych, jeżeli uzna, że „zarządzenie lub wytyczne administracyjne niezbędne do skorygowania naruszenia nie zostały przedstawione lub wydane".

(111) Jeżeli chodzi o dochodzenie roszczeń na drodze sądowej, zgodnie z ustawą o sporach administracyjnych osoba fizyczna, która jest niezadowolona z zarządzenia administracyjnego wydanego przez Komisję ds. Ochrony Informacji Osobowych, może wystąpić bezpośrednio do sądu o wydanie nakazu wykonania obowiązku (ang. *mandamus*) ([68]) zobowiązującego komisję do podjęcia dalszych działań ([69]). W niektórych przypadkach sąd może wydać tymczasowy nakaz wykonania określonego obowiązku, aby zapobiec nieodwracalnym szkodom ([70]). Ponadto na podstawie tej samej ustawy osoba fizyczna może dochodzić stwierdzenia nieważności decyzji Komisji ds. Ochrony Informacji Osobowych ([71]).

(112) Wreszcie na podstawie art. 1 ust. 1 ustawy o odszkodowaniu państwowym osoba fizyczna może również wnieść przeciwko Komisji ds. Ochrony Informacji Osobowych powództwo o odszkodowanie wypłacane przez państwo, jeżeli poniosła ona straty w związku z faktem, że zarządzenie wydane przez komisję dla podmiotu gospodarczego było niezgodne z prawem lub komisja nie wykonała swoich uprawnień.

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

(113) Komisja dokonała również oceny ograniczeń i zabezpieczeń, w tym mechanizmów nadzoru i indywidualnego dochodzenia roszczeń, które są dostępne w japońskim prawie w odniesieniu do zbierania i późniejszego wykorzystywania danych osobowych przekazywanych przez organy publiczne podmiotom gospodarczym w Japonii w interesie publicznym, zwłaszcza do celów ścigania przestępstw i na potrzeby bezpieczeństwa narodowego („dostęp rządowy"). W tej kwestii rząd Japonii przekazał Komisji oficjalne oświadczenia, zapewnienia i zobowiązania podpisane na najwyższym szczeblu ministerialnym i na poziomie agencji, zawarte w załączniku II do niniejszej decyzji.

([66]) Art. 239 ust. 2 kodeksu postępowania karnego.
([67]) Ustawa nr 160 z 2014 r.
([68]) Art. 37-2 ustawy o sporach administracyjnych.
([69]) Zgodnie z art. 3 ust. 6 ustawy o sporach administracyjnych pojęcie „postępowanie w przedmiocie wydania *mandamus*" oznacza postępowanie w przedmiocie wydania przez sąd nakazu skierowanego do organu administracji zobowiązującego go do wydania zarządzenia administracyjnego, które organ ten „powinien" był wydać pierwotnie, ale tego nie uczynił.
([70]) Art. 37-5 ustawy o sporach administracyjnych.
([71]) Rozdział II sekcja 1 ustawy o sporach administracyjnych.

3.1. **Ogólne ramy prawne**

(114) W ramach wykonywania władzy publicznej umożliwienie dostępu rządowego w Japonii musi przebiegać przy pełnym poszanowaniu prawa (zasada legalności). Pod tym względem przepisy japońskiej konstytucji zawierają ograniczenia i ramy dotyczące zbierania danych osobowych przez organy publiczne. Jak już wspomniano w odniesieniu do przetwarzania danych przez podmioty gospodarcze, opierając się na art. 13 konstytucji, który przewiduje między innymi ochronę prawa do wolności, japoński Sąd Najwyższy uznał prawo do prywatności i ochrony danych ([72]). Jednym z ważnych aspektów tego prawa jest wolność gwarantująca nieujawnianie informacji osobowych osobie trzeciej bez zezwolenia ([73]). Oznacza to prawo do skutecznej ochrony danych osobowych przed nadużyciami i (przede wszystkim) nielegalnym dostępem. Dodatkową ochronę zapewniono w art. 35 konstytucji dotyczącym prawa wszystkich osób do nienaruszalności domostwa, dokumentów i mienia, chyba że organy publiczne, we wszystkich przypadkach „przeszukania i zajęcia", uzyskały nakaz sądowy wydany z „uzasadnionych przyczyn" ([74]). W wyroku z dnia 15 marca 2017 r. (sprawa GPS) Sąd Najwyższy wyjaśnił, że ów wymóg uzyskania nakazu ma zastosowanie każdorazowo w przypadku gdy rząd narusza („wkracza w") prywatną sferę danej osoby w sposób powstrzymujący jej wolę, posługując się tym samym środkami, które są właściwe dla „obligatoryjnego ścigania". Sędzia może wydać taki nakaz wyłącznie na podstawie konkretnego podejrzenia popełnienia przestępstwa, tj. po otrzymaniu dokumentacji dowodowej, na podstawie której można uznać, że osoba, której dotyczy dochodzenie, popełniła przestępstwo ([75]). W związku z powyższym japońskie władze nie mają prawnych kompetencji do zbierania informacji osobowych za pomocą środków przymusowych w sytuacjach, gdy nie doszło jeszcze do naruszenia prawa ([76]), na przykład aby zapobiec przestępstwu lub innemu zagrożeniu dla bezpieczeństwa (jak w przypadku dochodzenia ze względu na bezpieczeństwo narodowe).

(115) Z zastrzeżeniem praworządności wszelkie przypadki zbierania danych w ramach obowiązkowego dochodzenia muszą być wyraźnie dopuszczone przez prawo (co odzwierciedlono na przykład w art. 197 ust. 1 kodeksu postępowania karnego dotyczącym przymusowego zbierania informacji na potrzeby dochodzenia). Wymóg ten dotyczy również dostępu do informacji elektronicznych.

(116) Przede wszystkim w art. 21 ust. 2 konstytucji zagwarantowano poufność wszystkich środków komunikacji, przy czym zgodnie z przepisami ograniczenia dozwolone są tylko ze względów dotyczących interesu publicznego. W art. 4 ustawy o działalności telekomunikacyjnej, zgodnie z którym zabrania się naruszania poufności komunikacji obsługiwanej przez operatora telekomunikacyjnego, ten wymóg zachowania poufności wdrożono na szczeblu ustawowym. Przepis ten interpretuje się jako zakaz ujawniania informacji ze środków komunikacji, chyba że uzyskano zgodę użytkowników lub jeżeli podstawą jest jedno z wyraźnych zwolnień z odpowiedzialności karnej przewidzianych w kodeksie karnym ([77]).

(117) W konstytucji zagwarantowano również prawo dostępu do sądów (art. 32) oraz prawo do pozwania państwa w celu dochodzenia roszczeń, jeżeli osoba fizyczna poniosła szkodę wskutek nielegalnego działania funkcjonariusza publicznego (art. 17).

(118) Jeżeli chodzi w szczególności o prawo do ochrony danych, w rozdziale III sekcje 1, 2 i 3 ustawy o ochronie informacji osobowych zawarto ogólne zasady w tym zakresie obejmujące wszystkie sektory, w tym sektor publiczny. W szczególności art. 3 tej ustawy stanowi, że wszystkie informacje osobowe należy przetwarzać zgodnie z zasadą poszanowania dóbr osobistych osób fizycznych. Po zebraniu („uzyskaniu") informacji osobowych, w tym na podstawie zapisów elektronicznych, przez organy publiczne ([78]) kwestia przetwarzania tych informacji regulowana jest przez ustawę o ochronie informacji osobowych znajdujących się w posiadaniu organów

([72]) Zob. na przykład Sąd Najwyższy, wyrok z dnia 12 września 2003 r., sprawa nr 1656 (2002 (Ju)). W szczególności Sąd Najwyższy uznał, że „każda osoba fizyczna ma prawo do ochrony dotyczących jej informacji osobowych przed ich ujawnieniem osobie trzeciej lub podaniem do wiadomości publicznej bez ważnego powodu".

([73]) Sąd Najwyższy, wyrok z dnia 6 marca 2008 r. (Juki-net).

([74]) „Uzasadnione przyczyny" istnieją tylko wtedy, gdy uznaje się, że dana osoba fizyczna (podejrzany, oskarżony) popełniła przestępstwo, a przeszukanie i zajęcie są konieczne w związku z dochodzeniem. Zob. Sąd Najwyższy, wyrok z dnia 18 marca 1969 r., sprawa nr 100 (1968 (Shi)).

([75]) Zob. art. 156 ust. 1 przepisów postępowania karnego.

([76]) Należy jednak zauważyć, że ustawa z dnia 15 czerwca 2017 r. o karaniu przestępczości zorganizowanej i kontroli dochodów z przestępstw przewiduje nowy rodzaj przestępstwa, tj. przygotowywanie aktów terrorystycznych i niektóre inne formy przestępczości zorganizowanej. Dochodzenia mogą być wszczynane tylko w przypadku konkretnych podejrzeń, opartych na dowodach, że spełniono wszystkie trzy przesłanki decydujące o istnieniu przestępstwa (udział w zorganizowanej grupie przestępczej, „czynność planowania" oraz „przygotowanie do popełnienia" przestępstwa). Zob. również na przykład art. 38–40 ustawy o zapobieganiu działaniom wywrotowym (ustawa nr 240 z dnia 21 lipca 1952 r.).

([77]) Art. 15 ust. 8 wytycznych w sprawie ochrony informacji osobowych w sektorze telekomunikacyjnym.

([78]) Organy administracji zgodnie z definicją zawartą w art. 2 ust. 1 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji. Zgodnie z informacjami otrzymanymi od japońskiego rządu wszystkie organy publiczne, z wyjątkiem policji prefekturalnej, wchodzą w zakres definicji „organów administracji". Jednocześnie policja prefekturalna działa zgodnie z ramami prawnymi określonymi w prefekturalnych rozporządzeniach w sprawie ochrony informacji osobowych (zob. art. 11 ustawy o ochronie informacji osobowych oraz podstawowe zasady polityki), w których ustanowiono przepisy dotyczące ochrony informacji osobowych równoważne przepisom ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji. Zob. załącznik II, sekcja I.B. Jak wyjaśniła Komisja ds. Ochrony Informacji Osobowych, zgodnie z „polityką podstawową" rozporządzenia te muszą zostać uchwalone na podstawie ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji, zaś Ministerstwo Spraw Wewnętrznych i Komunikacji wydaje komunikaty, aby zapewnić władzom lokalnym niezbędne wskazówki w tym zakresie. Jak podkreśliła Komisja ds. Ochrony Informacji Osobowych, „[w] ramach tych ograniczeń należy w każdej prefekturze ustanowić rozporządzenie o ochronie danych osobowych […] w oparciu o politykę podstawową oraz treść komunikatów".

administracji ([79]). Co do zasady dotyczy to ([80]) również przetwarzania informacji osobowych do celów ścigania przestępstw lub na potrzeby bezpieczeństwa narodowego. Ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji stanowi między innymi, że organy publiczne: (i) mogą zatrzymywać informacje osobowe wyłącznie w zakresie, w jakim jest to niezbędne do wykonywania ich obowiązków; (ii) nie wykorzystują takich informacji do „bezpodstawnego" celu ani nie ujawniają ich osobie trzeciej bez uzasadnienia; (iii) określają cel i nie zmieniają go poza zakres, jaki można racjonalnie uznać za istotny dla pierwotnego celu (ograniczenie celu); (iv) co do zasady nie wykorzystują zatrzymanych informacji osobowych ani nie przekazują ich osobie trzeciej do innych celów oraz, jeżeli uznają to za stosowne, wprowadzają ograniczenia dotyczące celu lub metody wykorzystania przez osoby trzecie; (v) dążą do zapewnienia poprawności informacji (jakości danych); (vi) podejmują środki niezbędne do właściwego zarządzania informacjami oraz mające na celu zapobieganie wyciekowi, utracie lub uszkodzeniu (bezpieczeństwo danych) oraz (vii) dążą do właściwego i sprawnego rozpatrzenia wszelkich skarg dotyczących przetwarzania informacji ([81]).

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

(119) W japońskim prawie ustanowiono szereg ograniczeń w zakresie dostępu do danych osobowych i korzystania z nich na potrzeby ścigania przestępstw, a także mechanizmy nadzoru i dochodzenia roszczeń, które stanowią wystarczające zabezpieczenia dla skutecznej ochrony danych przed niezgodną z prawem ingerencją i ryzykiem nadużycia.

3.2.1. *Podstawa prawna i właściwe ograniczenia/zabezpieczenia*

(120) Zgodnie z japońskimi ramami prawnymi zbieranie informacji elektronicznych do celów ścigania przestępstw jest dopuszczalne na podstawie nakazu (zbieranie przymusowe) lub wniosku o dobrowolne ujawnienie.

3.2.1.1. Obligatoryjne wszczęcie postępowania przygotowawczego na podstawie nakazu sądowego

(121) Jak wskazano w motywie 115, wszelkie przypadki zbierania danych w ramach obligatoryjnego postępowania przygotowawczego muszą być wyraźnie dopuszczane przez prawo i są możliwe wyłącznie na podstawie nakazu sądowego „wydanego z uzasadnionych przyczyn" (art. 35 konstytucji). W odniesieniu do postępowań przygotowawczych dotyczących przestępstw wymóg ten został odzwierciedlony w przepisach kodeksu postępowania karnego. Zgodnie z art. 197 ust. 1 kodeksu postępowania karnego środki przymusowe „nie są stosowane, chyba że w niniejszym kodeksie ustanowiono przepisy szczegółowe". W kwestii zbierania informacji elektronicznych jedyną odpowiednią ([82]) podstawę prawną w tym zakresie stanowią art. 218 (przeszukanie i zajęcie) oraz art. 222-2 kodeksu postępowania karnego, zgodnie z którymi środki przymusowe dotyczące przechwytywania wiadomości elektronicznych bez zgody którejkolwiek ze stron podejmowane są na podstawie przepisów innych ustaw, a mianowicie ustawy o zakładaniu podsłuchów na potrzeby postępowań przygotowawczych („ustawa o zakładaniu podsłuchów"). W obu przypadkach wymagany jest nakaz.

(122) Ściślej rzecz ujmując, zgodnie z art. 218 ust. 1 kodeksu postępowania karnego prokurator, asystent prokuratora lub funkcjonariusz policji sądowej może, jeżeli jest to konieczne do przeprowadzenia postępowania przygotowawczego w sprawie przestępstwa, dokonać przeszukania lub zajęcia (w tym zażądać dokumentacji) po okazaniu nakazu wydanego z wyprzedzeniem przez sędziego ([83]). Taki nakaz zawiera między innymi imię i nazwisko podejrzanego lub oskarżonego, postawione zarzuty ([84]), dokumentację utrwaloną elektromagnetycznie podlegającą zajęciu oraz wskazanie dotyczące „miejsca lub rzeczy", które należy poddać kontroli (art. 219 ust. 1 kodeksu postępowania karnego).

([79]) Informacje osobowe pozyskane przez urzędników organów administracji w trakcie wykonywania swoich obowiązków i znajdujące się w posiadaniu danego organu administracji na użytek organizacyjny wchodzą w zakres definicji „zatrzymanych informacji osobowych" w rozumieniu art. 2 ust. 3 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji, jeżeli są one rejestrowane jako „dokumenty administracyjne". Obejmują one informacje elektroniczne zbierane, a następnie dalej przetwarzane przez takie organy, mając na uwadze, że definicja „dokumentów administracyjnych" zawarta w art. 2 ust. 2 ustawy o dostępie do informacji znajdujących się w posiadaniu organów administracji (ustawa nr 42 z 1999 r.) obejmuje dokumenty utrwalone elektromagnetycznie.

([80]) Zgodnie z art. 53-2 kodeksu postępowania karnego stosowanie rozdziału IV ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji jest jednak wyłączone w odniesieniu do „dokumentów związanych z procesami sądowymi", które zgodnie z otrzymanymi informacjami obejmują informacje elektroniczne pozyskane na podstawie nakazu lub wniosku o dobrowolną współpracę w ramach postępowania przygotowawczego. Podobnie w odniesieniu do informacji zbieranych w obszarze bezpieczeństwa narodowego osoby fizyczne nie będą mogły skutecznie powołać się na swoje prawa przewidziane w ustawie o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji, jeżeli dyrektor organu publicznego ma „uzasadnione przesłanki" do stwierdzenia, że takie ujawnienie „może stanowić zagrożenie dla bezpieczeństwa narodowego" (zob. art. 14 ppkt (iv)). W związku z powyższym organy publiczne są obowiązane dokonać co najmniej częściowego ujawnienia, ilekroć jest to możliwe (art. 15).

([81]) Zob. szczegółowe odesłania do ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji zawarte w załączniku II, sekcja II.A 1) lit. b) ust. 2.

([82]) Podczas gdy zgodnie z art. 220 kodeksu postępowania karnego dozwolone są przeszukanie i zajęcie „na miejscu" bez nakazu, w przypadku gdy prokurator, asystent prokuratora lub funkcjonariusz policji sądowej zatrzymuje podejrzanego/sprawcę w chwili popełniania czynu zabronionego, przepis ten nie dotyczy przekazywania danych, a tym samym celów niniejszej decyzji.

([83]) Zgodnie z art. 222 ust. 1 w zw. z art. 110 kodeksu postępowania karnego nakaz przeszukania/zajęcia dokumentacji należy okazać osobie, która ma zostać objęta tym środkiem.

([84]) Zob. również art. 189 ust. 2 kodeksu postępowania karnego, zgodnie z którym funkcjonariusz policji sądowej przeprowadza postępowanie przygotowawcze dotyczące sprawcy czynu lub bada dotyczące go środki dowodowe, „jeżeli uzna, że doszło do popełnienia przestępstwa". Podobnie zgodnie z art. 155 ust. 1 przepisów postępowania karnego pisemny wniosek o wydanie nakazu zawiera między innymi „postawione zarzuty" oraz „zestawienie faktów na temat przestępstwa".

(123) Jeżeli chodzi o przechwytywanie wiadomości, art. 3 ustawy o zakładaniu podsłuchów stanowi, że takie środki są dopuszczalne tylko wtedy, gdy spełnione są surowe wymogi. W szczególności organy publiczne mają obowiązek z wyprzedzeniem uzyskać nakaz sądowy, który może być wydany jedynie w odniesieniu do postępowań przygotowawczych dotyczących szczególnie poważnych przestępstw (wymienionych w załączniku do ustawy) ([85]) oraz w przypadku gdy „bardzo trudno jest w inny sposób wskazać przestępcę lub wyjaśnić okoliczności/szczegóły dotyczące przestępstwa" ([86]). Zgodnie z art. 5 ustawy o zakładaniu podsłuchów nakaz wydaje się na czas oznaczony, przy czym sąd może ustanowić warunki dodatkowe. Ponadto w ustawie o zakładaniu podsłuchów przewidziano szereg dalszych gwarancji, takich jak niezbędna obecność świadków (art. 12 i 20), zakaz przekazywania informacji przez niektóre grupy uprzywilejowane (np. lekarze, prawnicy) (art. 15), obowiązek zaprzestania stosowania podsłuchów, jeżeli nie ma to już uzasadnienia, nawet w okresie ważności nakazu (art. 18), lub ogólny obowiązek powiadamiania danej osoby oraz umożliwienia dostępu do dokumentacji w terminie 30 dni od dnia, w którym zakończono stosowanie podsłuchów (art. 23 i 24).

(124) W odniesieniu do wszelkich obligatoryjnych środków mających za podstawę wydany nakaz badanie można prowadzić tylko w takim zakresie, w „jakim jest niezbędne do osiągnięcia tego celu", tzn. jeżeli celów ścigania nie można osiągnąć w żaden inny sposób (art. 197 ust. 1 kodeksu postępowania karnego). Chociaż w ustawie bliżej nie określono kryteriów ustalenia stopnia niezbędności, japoński Sąd Najwyższy orzekł, że sędzia, który wydaje nakaz, powinien dokonać ogólnej oceny, uwzględniając przede wszystkim: (i) ciężar przestępstwa i sposób, w jaki zostało ono popełnione; (ii) wartość i znaczenie materiałów, które zostaną zajęte jako środki dowodowe; (iii) prawdopodobieństwo (ryzyko) ukrycia lub zniszczenia środków dowodowych oraz (iv) stopień, w jakim zajęcie może spowodować szkody dla danej osoby fizycznej ([87]).

3.2.1.2. Wniosek o dobrowolne ujawnienie na podstawie „karty z zapytaniem"

(125) Organy publiczne, w granicach swoich uprawnień, mogą również zbierać informacje elektroniczne na podstawie wniosku o dobrowolne ujawnienie. Odnosi się to do nieprzymusowej formy współpracy w przypadku gdy nie można wyegzekwować zastosowania się do wniosku ([88]); jednocześnie można w ten sposób zwolnić organy publiczne z obowiązku uzyskania nakazu sądowego.

(126) Podmiot gospodarczy musi przestrzegać wymogów ustawy o ochronie informacji osobowych w zakresie, w jakim wniosek jest skierowany do podmiotu gospodarczego i dotyczy informacji osobowych. Zgodnie z art. 23 ust. 1 ustawy o ochronie informacji osobowych podmiot gospodarczy może ujawnić informacje osobowe osobom trzecim bez zgody zainteresowanej osoby fizycznej tylko w określonych sytuacjach, w tym w przypadku gdy dane są ujawniane „na podstawie przepisów ustawowych i wykonawczych" ([89]). Jeżeli chodzi o ściganie przestępstw, podstawę prawną dla takich wniosków stanowi art. 197 ust. 2 kodeksu postępowania karnego, zgodnie z którym „organizacje prywatne mogą zostać wezwane do zgłoszenia niezbędnych kwestii związanych z dochodzeniem". Ponieważ zastosowanie „karty z zapytaniem" samo w sobie jest dopuszczalne jedynie w ramach postępowania przygotowawczego, zawsze zakłada ono konkretne podejrzenie już popełnionego przestępstwa ([90]). Ponadto, z uwagi na fakt, że takie postępowania przygotowawcze prowadzi zazwyczaj policja prefekturalna, zastosowanie mają ograniczenia przewidziane w art. 2 ust. 2 ustawy o policji ([91]). Zgodnie z tym przepisem działalność policji jest „ściśle ograniczona" do wypełniania jej zadań i obowiązków (tzn. do zapobiegania przestępstwom, ich zwalczania oraz prowadzenia dochodzeń w ich sprawie). Ponadto policja w ramach wykonywania swoich obowiązków obowiązana jest działać w sposób bezstronny, wolny od uprzedzeń i uczciwy oraz nie może w żadnej sytuacji nadużywać swoich uprawnień „w sposób, który ingeruje w prawa i wolności osoby fizycznej zagwarantowane w konstytucji Japonii" (w tym, jak wskazano powyżej, prawo do prywatności i ochrony danych) ([92]).

(127) Zwłaszcza w odniesieniu do art. 197 ust. 2 kodeksu postępowania cywilnego Agencja Policji Krajowej – jako organ federalny odpowiadający między innymi za wszystkie kwestie dotyczące policji kryminalnej – wydała instrukcje dla

([85]) W załączniku wymieniono 9 rodzajów przestępstw, np. przestępstwa związane z narkotykami i bronią palną, handlem ludźmi i zorganizowanym morderstwem. Należy zauważyć, że nowo wprowadzone przestępstwo, tj. „przygotowywanie aktów terrorystycznych i inne formy przestępczości zorganizowanej" (zob. przypis 76), nie zostało włączone do tego zamkniętego wykazu.

([86]) Zgodnie z art. 23 ustawy o zakładaniu podsłuchów organ prowadzący dochodzenie jest ponadto zobowiązany do pisemnego zawiadomienia o tym fakcie osoby fizycznej, której wiadomości zostały przejęte (i tym samym dołączone do dokumentacji przejęcia).

([87]) Zob. załącznik II, sekcja II.A.1) lit. b) pkt 1.

([88]) Według otrzymanych informacji podmiot gospodarczy, który odmawia współpracy, nie jest ustawowo zagrożony negatywnymi konsekwencjami (w tym sankcjami). Zob. załącznik II, sekcja II.A.2) lit. a).

([89]) Zgodnie z wytycznymi Komisji ds. Ochrony Informacji Osobowych (wydaniem zawierającym przepisy ogólne) art. 23 ust. 1 ppkt (i) stanowi podstawę dla ujawnienia informacji osobowych w odpowiedzi zarówno na nakaz (art. 218 kodeksu postępowania karnego), jak i „kartę z zapytaniem" (art. 197 ust. 2 kodeksu postępowania karnego).

([90]) Oznacza to, że „karta z zapytaniem" może być wykorzystywana wyłącznie w celu zbierania informacji w przypadkach indywidualnych, nie zaś do gromadzenia danych osobowych na dużą skalę. Zob. załącznik II, sekcja I.A.2) lit. b) pkt 1).

([91]) Oraz w rozporządzeniach Prefekturalnej Komisji ds. Bezpieczeństwa Publicznego, zob. art. 189 ust. 1 kodeksu postępowania karnego.

([92]) Zob. również art. 3 ustawy o policji, zgodnie z którym przysięga wypowiadana przy obejmowaniu urzędu przez każdego funkcjonariusza policji zobowiązuje go do „dochowania wierności obowiązkowi, jakim jest obrona i stanie na straży konstytucji i praw Japonii oraz wypełnianie swoich obowiązków w sposób bezstronny, sprawiedliwy, uczciwy i wolny od uprzedzeń".

policji prefekturalnej ([93]) w sprawie „właściwego stosowania zapytań na piśmie w czynnościach dochodzeniowo-śledczych". Zgodnie z tym zawiadomieniem wnioski można składać, korzystając z ustanowionego wcześniej formularza („formularz nr 49" lub tzw. „karta z zapytaniem") ([94]) w sprawie dokumentacji „dotyczącej określonego postępowania przygotowawczego", z kolei informacje objęte wnioskiem muszą być „niezbędne do przeprowadzenia [danego] postępowania przygotowawczego". W każdym przypadku osoba kierująca postępowaniem przygotowawczym „w pełni bada konieczność, treść itp. danego zapytania" oraz musi otrzymać wewnętrzne upoważnienie od urzędnika wysokiego szczebla.

(128) Ponadto w dwóch wyrokach z 1969 r. i 2008 r. ([95]) japoński Sąd Najwyższy ustanowił ograniczenia w odniesieniu do środków nieprzymusowych, które ingerują w prawo do prywatności ([96]). Przede wszystkim Sąd Najwyższy uznał, że takie środki muszą być „racjonalne" i mieścić się w „ogólnie dopuszczalnych granicach", tzn. muszą być one niezbędne do przeprowadzenia postępowania przygotowawczego dotyczącego podejrzanego (gromadzenia środków dowodowych) oraz podejmowane „za pomocą metod właściwych dla osiągnięcia celu postępowania przygotowawczego" ([97]). Z wyroków wynika, że pociąga to ze sobą konieczność analizy proporcjonalności przy uwzględnieniu wszystkich okoliczności sprawy (np. stopnia ingerencji w prawo do prywatności, włączając w to oczekiwania dotyczące prywatności, ciężar przestępstwa, prawdopodobieństwo uzyskania przydatnych środków dowodowych, znaczenie tych środków, ewentualne środki alternatywne w ramach dochodzenia itd.) ([98]).

(129) Oprócz tych ograniczeń w zakresie wykonywania władzy publicznej oczekuje się, że podmioty gospodarcze same będą sprawdzać („potwierdzać") konieczność i „racjonalność" przekazywania danych osoby trzeciej ([99]). Dotyczy to kwestii, czy prawo zabrania im podejmowania współpracy. Takie sprzeczne obowiązki prawne mogą wynikać w szczególności z obowiązków zachowania poufności, takich jak przewidzianych w art. 134 kodeksu karnego (dotyczącym relacji między lekarzem, prawnikiem, duchownym itd. a klientem). Ponadto „każda osoba prowadząca działalność telekomunikacyjną jest podczas pełnienia swoich obowiązków zobowiązana do zachowania tajemnic innych osób, o których dowiedziała się w związku z wiadomościami przetwarzanymi przez operatora telekomunikacyjnego" (art. 4 ust. 2 ustawy o działalności telekomunikacyjnej). Obowiązek ten wsparto sankcją przewidzianą w art. 179 ustawy o działalności telekomunikacyjnej, zgodnie z którym każda osoba dopuszczająca się naruszenia tajemnicy wiadomości przetwarzanych przez operatora telekomunikacyjnego jest winna popełnienia przestępstwa i podlega karze pozbawienia wolności w wymiarze do dwóch lat z obowiązkiem wykonywania pracy lub karze grzywny w wysokości do jednego mln jenów ([100]). Chociaż powyższy wymóg nie jest bezwzględny i w szczególności dopuszczalne są środki naruszające tajemnicę wiadomości, które stanowią „uzasadnione działania" w rozumieniu art. 35 kodeksu karnego, wyjątek ten nie obejmuje odpowiedzi na nieobligatoryjne wnioski organów publicznych w sprawie ujawnienia informacji elektronicznych na podstawie art. 197 ust. 2 kodeksu postępowania karnego ([101]).

3.2.1.3. Dalsze wykorzystanie zebranych informacji

(130) Zebrane przez japońskie organy publiczne informacje osobowe podlegają ustawie o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji. W ustawie uregulowano kwestię przetwarzania

([93]) Zgodnie z art. 30 ust. 1 i art. 31 ust. 2 ustawy o policji „kierownictwo oraz nadzór" nad policją prefekturalną sprawuje dyrektor generalny regionalnych biur policji (jednostek lokalnych Agencji Policji Państwowej).

([94]) Na karcie z zapytaniem należy również wyszczególnić informacje kontaktowe „referenta sprawy" („nazwa sekcji [stanowiska], imię i nazwisko referenta sprawy, numer telefonu do urzędu, numer wewnętrzny itd.").

([95]) Sąd Najwyższy, wyrok z dnia 24 grudnia 1969 r. (1965(A) 1187); wyrok z dnia 15 kwietnia 2008 r. (2007(A) 839).

([96]) Chociaż wyroki te nie dotyczą zbierania informacji elektronicznych, rząd Japonii wyjaśnił, że stosowanie kryteriów opracowanych przez Sąd Najwyższy obejmuje każdy przypadek ingerencji w władzy publicznej w prawo do prywatności, w tym każde „dobrowolnie prowadzone postępowanie przygotowawcze" i tym samym kryteria te są wiążące dla organów japońskich również występujących o dobrowolne ujawnienie informacji. Zob. załącznik II, sekcja II.A.2) lit. b) pkt 1).

([97]) Według otrzymanych informacji czynniki te należy uznać za „racjonalne zgodnie ze społecznie akceptowalnymi zwyczajami". Zob. załącznik II, sekcja II.A.2) lit. b) pkt 1).

([98]) W odniesieniu do podobnych okoliczności w kontekście ścigania obligatoryjnego zob. również Sąd Najwyższy, wyrok z dnia 16 grudnia 1999 r., 1997 (A) 636.

([99]) W odniesieniu do tego zagadnienia władze Japonii wskazały na wytyczne Komisji ds. Ochrony Informacji Osobowych (wydanie zawierające przepisy ogólne) oraz na pkt 5/14 „pytań i odpowiedzi" przygotowanych przez tę komisję na potrzeby stosowania ustawy o ochronie informacji osobowych. Według japońskich władz „ze względu na rosnącą świadomość osób fizycznych w kwestii ich prawa do prywatności oraz biorąc pod uwagę nakład pracy związany z rozpatrywaniem takich wniosków, podmioty gospodarcze zachowują coraz większą ostrożność przy udzielaniu na nie odpowiedzi". Zob. załącznik II, sekcja II.A.2), także w odniesieniu do zawiadomienia Agencji Policji Państwowej z 1999 r. Według otrzymanych informacji faktycznie miały miejsce przypadki, w których podmioty gospodarcze odmówiły współpracy. Przykładowo w sprawozdaniu LINE (najpopularniejszej aplikacji komunikacyjnej w Japonii) z 2017 r. dotyczącym przejrzystości stwierdzono: „Po otrzymaniu wniosków od organów ścigania itp. […] weryfikujemy adekwatność w kontekście legalności, ochrony użytkowników itp. Na podstawie weryfikacji odrzucamy wniosek, jeżeli stwierdzono uchybienie prawne. Jeżeli zakres żądania jest dla celów postępowania przygotowawczego zbyt szeroki, zwracamy się do organów ścigania o wyjaśnienia. Jeżeli w wyjaśnieniu nie podano powodu, pozostawiamy wniosek bez rozpoznania". Sprawozdanie dostępne jest w internecie pod adresem: https://linecorp.com/en/security/transparency/top

([100]) Kara 3 lat pozbawienia wolności z obowiązkiem wykonywania pracy lub kara grzywny w wysokości do 2 mln JPY w przypadku każdej osoby, która „prowadzi działalność telekomunikacyjną".

([101]) Zgodnie z kodeksem karnym „uzasadnione działania" to w szczególności te działania operatora telekomunikacyjnego, które są zgodne ze środkami państwowymi posiadającymi moc prawną (środki przymusowe), np. w razie gdy organy ścigania podejmują środki na podstawie nakazu sądowego. Zob. załącznik II, sekcja II.A.2) lit. b) pkt 2), w odniesieniu do wytycznych dotyczących ochrony informacji osobowych w działalności telekomunikacyjnej.

„zatrzymanych informacji osobowych" oraz nałożono jak dotychczas szereg ograniczeń i zabezpieczeń (zob. motyw 118) ([102]). Ograniczenia – przynajmniej pośrednie – dotyczące wstępnego zbierania informacji wynikają ponadto z tego, że organ administracyjny może zatrzymać informacje osobowe „tylko wtedy, gdy zatrzymanie jest niezbędne do przeprowadzenia czynności podlegających jego jurysdykcji, przewidzianych w przepisach ustawowych i wykonawczych" (art. 3 ust. 1 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji).

3.2.2. *Niezależny nadzór*

(131) W Japonii zbieranie informacji elektronicznych w obszarze ścigania przestępstw wchodzi przede wszystkim ([103]) w zakres obowiązków policji prefekturalnej ([104]), która w tej kwestii podlega nadzorowi różnego szczebla.

(132) Po pierwsze, we wszystkich przypadkach, w których ma miejsce zbieranie informacji za pomocą środków przymusowych, policja musi z wyprzedzeniem uzyskać nakaz sądowy (zob. motyw 121). W związku z powyższym zbieranie informacji w takich przypadkach podlega ocenie *ex ante* przeprowadzanej przez sędziego w oparciu o ścisłą normę „uzasadnionych przyczyn".

(133) Choć w przypadku wniosków o dobrowolne ujawnienie informacji sędzia nie dokonuje oceny *ex ante*, podmioty gospodarcze, które otrzymują takie wnioski, mogą zgłosić sprzeciw, nie narażając się na jakiekolwiek negatywne skutki (podmioty te muszą uwzględnić wpływ ujawnienia na prywatność). Ponadto zgodnie z art. 192 ust. 1 kodeksu postępowania karnego funkcjonariusze policji mają zawsze obowiązek współpracować z prokuratorem (oraz Prefekturalną Komisją ds. Bezpieczeństwa Publicznego) i koordynować z nimi swoje działania ([105]). Z kolei prokurator może przekazać niezbędne instrukcje ogólne, w których określone zostaną normy uczciwego prowadzenia postępowań przygotowawczych, lub wydać określone zarządzenia w odniesieniu do danego postępowania przygotowawczego (art. 193 kodeks postępowania karnego). W przypadku nieprzestrzegania tych instrukcji lub zarządzeń prokuratura może wnieść o wszczęcie postępowania dyscyplinarnego (art. 194 kodeksu postępowania karnego). Policja prefekturalna działa zatem pod nadzorem prokuratora.

(134) Po drugie, zgodnie z art. 62 konstytucji każda z izb japońskiego parlamentu (Diet) może prowadzić postępowania przygotowawcze w sprawach dotyczących kierowania państwem, w tym w zakresie zgodności zbierania informacji przez policję z prawem. W tym celu każda z izb może żądać stawienia się i złożenia zeznań przez świadków lub przedłożenia dokumentów. Te uprawnienia w zakresie zapytań doprecyzowano w ustawie o Diet, w szczególności w rozdziale XII. W szczególności art. 104 ustawy o Diet stanowi, że Rada Ministrów, agencje publiczne i inne organy rządowe „obowiązane są stosować się do wniosków izby i wszelkich jej komitetów w sprawie przedłożenia sprawozdań i dokumentów niezbędnych do celów postępowania przygotowawczego". Odmowa wykonania jest dopuszczalna tylko wtedy, gdy rząd przedstawi wiarygodne uzasadnienie, które Diet uzna za wystarczające, lub jeżeli wydano oficjalne oświadczenie, że przedłożenie sprawozdań lub dokumentów stanowiłoby „poważną szkodę dla interesu narodowego" ([106]). Co więcej, członkowie parlamentu mogą składać na piśmie zapytania Radzie Ministrów (art. 74 i 75 ustawy o Diet), a w przeszłości takie „zapytania na piśmie" dotyczyły również przetwarzania informacji osobowych przez organy administracji ([107]). Funkcję nadzorczą Diet względem władzy wykonawczej wzmacniają obowiązki sprawozdawcze, np. te wynikające z art. 29 ustawy o zakładaniu podsłuchów.

(135) Po trzecie, w zakresie władzy wykonawczej niezależnemu nadzorowi podlega również policja prefekturalna. Dotyczy to w szczególności Prefekturalnych Komisji ds. Bezpieczeństwa Publicznego ustanowionych na szczeblu prefekturalnym w celu zapewnienia zarządzania demokratycznego i neutralności politycznej w policji ([108]). W skład tych komisji wchodzą członkowie powoływani przez gubernatora prefektury za zgodą Zgromadzenia Prefekturalnego (spośród obywateli, którzy nie zajmują w ciągu ostatnich pięciu lat stanowiska funkcjonariusza publicznego w policji) na określoną kadencję (w szczególności odwołanie może nastąpić tylko z ważnego powodu) ([109]). Jeżeli chodzi o uzyskiwanie przez nich informacje, nie podlegają oni instrukcjom i można ich tym samym uznać za całkowicie niezależnych ([110]). Jeżeli chodzi o zadania i uprawnienia Prefekturalnych Komisji ds. Bezpieczeństwa

([102]) W kwestii praw zainteresowanych osób fizycznych zob. sekcję 3.1.
([103]) Prokurator – lub asystent prokuratora na jego polecenie – może co do zasady, jeżeli uzna to za niezbędne, przeprowadzić postępowanie przygotowawcze w sprawie przestępstwa (art. 191 ust. 1 kodeksu postępowania karnego).
([104]) Według otrzymanych informacji Agencja Policji Krajowej nie przeprowadza postępowań przygotowawczych w konkretnych sprawach. Zob. załącznik II, sekcja II.A.1) lit. a).
([105]) Zob. również art. 246 kodeksu postępowania karnego, zgodnie z którym policja ds. sądowych obowiązana jest przesłać akta sprawy prokuratorowi po przeprowadzeniu postępowania przygotowawczego w sprawie przestępstwa („zasada przesyłania we wszystkich sprawach").
([106]) Diet może również żądać od Rady ds. Nadzoru i Oceny Specjalnie Wyznaczonych Tajemnic wszczęcia postępowania wyjaśniającego w sprawie odmowy udzielenia odpowiedzi. Zob. art. 104-II ustawy o Diet.
([107]) Zob. załącznik II, sekcja II.B.4).
([108]) Ponadto, zgodnie z przepisami art. 100 ustawy o autonomii lokalnej, zgromadzenie lokalne jest uprawnione do prowadzenia postępowań wyjaśniających dotyczących działań organów wykonawczych ustanowionych na szczeblu prefekturalnym, w tym działań policji prefekturalnej.
([109]) Zob. art. 39–41 ustawy o policji. W kwestii neutralności politycznej zob. również art. 42 ustawy o policji.
([110]) Zob. załącznik II, sekcja II.B.3) („system niezależnej rady").

Publicznego, zgodnie z art. 38 ust. 3 w związku z art. 2 i art. 36 ust. 2 ustawy o policji są one odpowiedzialne za „ochronę praw i wolności jednostki". W tym celu są one uprawnione do „sprawowania nadzoru" ([111]) nad wszelkimi czynnościami dochodzeniowo-śledczymi policji prefekturalnej, w tym w zakresie zbierania danych osobowych. W szczególności komisje „w stosownych przypadkach mogą wydawać [p]olicji [p]refekturalnej szczegółowe instrukcje lub w sprawach indywidualnych kontroli w związku z przewinieniami funkcjonariuszy policji" ([112]). Jeżeli szef policji prefekturalnej ([113]) otrzymał takie polecenie lub sam dowiedział się o potencjalnym przypadku przewinienia (w tym o naruszeniu przepisów lub zaniedbaniu obowiązków), jest on obowiązany niezwłocznie zbadać sprawę i przekazać wyniki przeprowadzonych w tym zakresie czynności Prefekturalnej Komisji ds. Bezpieczeństwa Publicznego (art. 56 ust. 3 ustawy o policji). Jeżeli komisja uzna to za konieczne, może również wyznaczyć jednego ze swoich członków do przeprowadzenia kontroli stanu wdrożenia. Postępowanie trwa, dopóki komisja nie uzna, że sprawa incydentu została rozwiązana we właściwy sposób.

(136) Ponadto w odniesieniu do właściwego stosowania ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji uprawnienia w zakresie egzekwowania prawa posiada właściwy minister lub szef agencji (np. komisarz generalny Agencji Policji Państwowej), z zastrzeżeniem nadzoru Ministerstwa Spraw Wewnętrznych i Komunikacji. Zgodnie z art. 49 tej ustawy Ministerstwo Spraw Wewnętrznych i Komunikacji „może gromadzić sprawozdania na temat stanu wykonania przepisów niniejszej ustawy" pochodzące od dyrektorów organów administracyjnych (ministrów). Tę funkcję nadzorczą wspomagają dane otrzymywane od 51 „centrów informacji ogólnej" Ministerstwa Spraw Wewnętrznych i Komunikacji (po jednym przypadającym na każdą prefekturę w całej Japonii), z czego każde co roku odpowiada na tysiące zapytań od osób fizycznych ([114]) (co z kolei umożliwia wykrywanie ewentualnych naruszeń prawa). Ministerstwo Spraw Wewnętrznych i Komunikacji może, jeżeli uzna to za niezbędne do zapewnienia zgodności z ustawą, żądać przedłożenia wyjaśnień i materiałów oraz wydawać opinie w sprawie przetwarzania informacji osobowych przez dany organ administracyjny (art. 50 i 51 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji).

3.2.3. *Indywidualne dochodzenie roszczeń*

(137) Oprócz ochrony wynikającej z nadzoru z urzędu osoby fizyczne mają również szereg możliwości dochodzenia roszczeń, zarówno za pośrednictwem niezależnych organów (takich jak Prefekturalne Komisje ds. Bezpieczeństwa Publicznego lub Komisja ds. Ochrony Informacji Osobowych), jak i przed japońskimi sądami.

(138) Po pierwsze, w odniesieniu do informacji osobowych zbieranych przez organy administracyjne te ostatnie są zobligowane do „dążenia do właściwego i sprawnego rozpatrywania wszelkich skarg" dotyczących dalszego przetwarzania tych informacji (art. 48 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji). Chociaż rozdziału IV przywołanej ustawy dotyczącego praw indywidualnych nie stosuje się do informacji osobowych utrwalonych w „dokumentach związanych z procesami sądowymi i zajętymi rzeczami" (art. 53-2 ust. 2 kodeksu postępowania karnego) – które obejmują informacje osobowe zbierane w ramach postępowań przygotowawczych – osoby fizyczne mogą złożyć skargę w celu powołania się na ogólne zasady ochrony danych, takie jak na przykład obowiązek zatrzymania informacji osobowych tylko wtedy, „gdy zatrzymanie jest niezbędne do pełnienia [funkcji w zakresie egzekwowania prawa]" (art. 3 ust. 1 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji).

(139) Ponadto art. 79 ustawy o policji stanowi, że osobom fizycznym, które są zaniepokojone „wykonywaniem obowiązków" przez personel policji, przysługuje prawo skargi do (właściwej) niezależnej Prefekturalnej Komisji ds. Bezpieczeństwa Publicznego. Komisja „skrupulatnie" rozpatruje takie skargi zgodnie z przepisami ustawowymi i regulacjami lokalnymi oraz zawiadamia na piśmie skarżącego o to, co z jego skargi wynikło. Na podstawie uprawnień w zakresie nadzoru i „wydawania poleceń" dotyczących „przewinień pracowników" (art. 38 ust. 3, art. 43-2 ust. 1 ustawy o policji) komisja może zażądać od policji prefekturalnej zbadania okoliczności faktycznych, zastosowania właściwych środków na podstawie wyników postępowania sprawdzającego i przedłożenia sprawozdania z wyników. Jeżeli komisja uzna, że postępowanie przygotowawcze przeprowadzone przez policję było nieodpowiednie, komisja może również przekazać instrukcje w sprawie rozpatrywania skargi.

(140) W celu ułatwienia rozpatrywania skarg Agencja Policji Państwowej wydała „zawiadomienie" skierowane do policji i Prefekturalnych Komisji ds. Bezpieczeństwa Publicznego w sprawie właściwego rozpatrywania skarg dotyczących wykonywania obowiązków przez funkcjonariuszy policji. W dokumencie tym Agencja Policji Państwowej określiła normy dotyczące interpretacji i wdrażania art. 79 ustawy o policji. Policję prefekturalną zobowiązano między

([111]) Zob. art. 5 ust. 3 i art. 38 ust. 3 ustawy o policji.

([112]) Zob. art. 38 ust. 3 i art. 43-2 ust. 1 ustawy o policji. W przypadku „wydania polecenia" w rozumieniu art. 43-2 ust. 1 Prefekturalna Komisja ds. Bezpieczeństwa Publicznego może zlecić wyznaczonemu przez nią komitetowi monitorowanie stanu wdrożenia (ust. 2). Ponadto komisja może zalecić nałożenie kary dyscyplinarnej na szefa policji prefekturalnej lub jego odwołanie (art. 50 ust. 2), jak również podjęcie tych działań wobec innego funkcjonariusza policji (art. 55 ust. 4 ustawy o policji).

([113]) To samo dotyczy nadinspektora w przypadku Policji Metropolitalnej w Tokio (zob. art. 48 ust. 1 ustawy o policji).

([114]) Według otrzymanych informacji w roku obrachunkowym 2017 (kwiecień 2017 r. – marzec 2018 r.) „ogólne centra informacyjne" udzieliły odpowiedzi na łącznie 5 186 zapytań od osób fizycznych.

innymi do ustanowienia „systemu rozpatrywania skarg" oraz rozpatrywania wszystkich skarg i zgłaszania ich „niezwłocznie" właściwej Prefekturalnej Komisji ds. Bezpieczeństwa Publicznego. W zawiadomieniu skargę określa się jako żądanie naprawienia „wszelkich szczególnych niedogodności wyrządzonych bezprawnym lub niewłaściwym postępowaniem" ([115]) lub „zaniechaniem niezbędnych działań przez funkcjonariusza policji podczas wykonywania obowiązków służbowych" ([116]), a także każdego rodzaju „ubolewanie/niezadowolenie z powodu niewłaściwego sposobu wykonywania obowiązków służbowych przez funkcjonariusza policji". Zakres przedmiotowy skargi jest zatem zdefiniowany szeroko i obejmuje wszelkie żądania związane z bezprawnym zbieraniem danych, a skarżącym nie spoczywa obowiązek wykazania jakiejkolwiek szkody doznanej w wyniku działań funkcjonariusza policji. Co istotne, komunikat stanowi, że (m.in.) obcokrajowcom udziela się pomocy przy formułowaniu skargi. Po otrzymaniu skargi Prefekturalne Komisje ds. Bezpieczeństwa Publicznego obowiązane są zapewnić, aby policja prefekturalna zbadała okoliczności faktyczne, wdrożyła środki „zgodnie z wynikami badania" oraz przedłożyła sprawozdanie z wyników. Jeżeli komisja uzna, że badanie było niewystarczające, wydaje ona instrukcję w sprawie rozpatrywania skargi, zgodnie z którą policja prefekturalna ma obowiązek postępować. Na podstawie otrzymanych sprawozdań i zastosowanych środków komisja zawiadamia osobę fizyczną, wskazując między innymi środki, które zastosowano w celu rozpatrzenia skargi. W zawiadomieniu Agencja Policji Państwowej zaznaczyła, że skargi należy rozpatrywać w „uczciwy sposób", a wyniki należy przekazać „w terminie […] uznawanym w świetle norm społecznych i zdrowego rozsądku za właściwy".

(141) Po drugie, z uwagi na fakt, że za granicą z istoty roszczeń trzeba dochodzić w obcym systemie i języku, aby ułatwić dochodzenie roszczeń przez osoby fizyczne z UE, których dane osobowe są przekazywane podmiotom gospodarczym w Japonii, a następnie dostęp do nich mają organy publiczne, rząd Japonii wykorzystał swoje uprawnienia do opracowania szczególnego mechanizmu rozpatrywania i rozstrzygania skarg w powyższym zakresie, którym to systemem zarządza i nad którym nadzór sprawuje Komisja ds. Ochrony Informacji Osobowych. Mechanizm ten opiera się na obowiązku współpracy nałożonym na japońskie organy publiczne zgodnie z ustawą o ochronie informacji osobowych oraz na szczególnej roli Komisji ds. Ochrony Informacji Osobowych w odniesieniu do międzynarodowego przekazywania danych z państw trzecich zgodnie z art. 6 tej ustawy oraz zgodnie z podstawowymi zasadami polityki (ustanowionymi przez rząd Japonii zarządzeniem Rady Ministrów). Mechanizm, o którym mowa, został szczegółowo określony w oficjalnych oświadczeniach, zapewnieniach i zobowiązaniach rządu Japonii, stanowiących załącznik II do niniejszej decyzji. Mechanizm ten jest niezależny od którejkolwiek z przesłanek warunkujących posiadanie legitymacji procesowej. Może z niego skorzystać każda osoba, niezależnie od tego, czy posiada ona status podejrzanej lub oskarżonej o popełnienie przestępstwa.

(142) W ramach tego mechanizmu osoba fizyczna, która podejrzewa, że dotyczące jej dane przekazywane z Unii Europejskiej zostały zebrane lub wykorzystane przez organy publiczne w Japonii (w tym organy odpowiedzialne za ściganie przestępstw) z naruszeniem obowiązujących przepisów, może złożyć skargę do Komisji ds. Ochrony Informacji Osobowych (indywidualnie lub za pośrednictwem swojego organu nadzorczego w rozumieniu art. 51 RODO). Komisja ds. Ochrony Informacji Osobowych ma obowiązek rozpatrzyć skargi oraz w pierwszej kolejności zawiadomienia o tym fakcie właściwych organów publicznych, w tym właściwych organów nadzorczych. Organy te są obowiązane współpracować z Komisją ds. Ochrony Informacji Osobowych „w tym przez zapewnienie niezbędnych informacji i odpowiednich materiałów, dzięki czemu komisja może ocenić, czy zbieranie i późniejsze wykorzystanie informacji osobowych było zgodne z obowiązującymi przepisami" ([117]). Obowiązek ten wynikający z art. 80 ustawy o ochronie informacji osobowych (nakazujący japońskim organom publicznym współpracować z Komisją ds. Ochrony Informacji Osobowych) ma charakter ogólny, a zatem obejmuje również kontrolę stosowania przez te organy wszystkich środków służących wyjaśnieniu danej sprawy. Organy te tym bardziej obowiązane są do takiej współpracy na podstawie pisemnych gwarancji szefów właściwych ministerstw i agencji, co znajduje odzwierciedlenie w załączniku II.

(143) Jeżeli ocena wykaże naruszenie obowiązujących przepisów, „współpraca między danym organem publicznym a Komisją ds. Ochrony Informacji Osobowych obejmuje obowiązek usunięcia naruszenia", co w przypadku niezgodnego z prawem zbierania informacji osobowych polega na usunięciu takich danych. Co istotne, obowiązek ten jest realizowany pod nadzorem Komisji ds. Ochrony Informacji Osobowych, która „potwierdza, przed zakończeniem oceny, że naruszenie udało się w pełni usunąć".

(144) Po zakończeniu oceny Komisja ds. Ochrony Informacji Osobowych zawiadamia w rozsądnym terminie osobę fizyczną o jej wynikach, w tym, w stosownych przypadkach, o podjętych działaniach naprawczych. Jednocześnie Komisja ds. Ochrony Informacji Osobowych informuje osobę fizyczną o możliwości uzyskania potwierdzenia

([115]) Przesłanka „szczególnych niedogodności" wskazuje jedynie, że zachowanie (albo zaniechanie) policji powinno indywidualnie dotyczyć skarżącego, nie zaś, że spoczywa na nim obowiązek wykazania jakiegokolwiek uszczerbku.

([116]) Do tych obowiązków należy również przestrzeganie prawa, w tym określonych prawem wymogów w zakresie zbierania i wykorzystywania danych osobowych. Zob. art. 2 ust. 2 i art. 3 ustawy o policji.

([117]) Przy dokonywaniu oceny Komisja ds. Ochrony Informacji Osobowych może współpracować z Ministerstwem Spraw Wewnętrznych i Komunikacji, które, jak wyjaśniono w motywie 136, może żądać przedłożenia wyjaśnień i materiałów oraz wydawać opinie w sprawie przetwarzania informacji osobowych przez dany organ administracyjny (art. 50 i 51 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji).

wyniku u właściwego organu publicznego oraz danych o tym organie, do którego należy kierować taki wniosek o potwierdzenie. Możliwość uzyskania takiego potwierdzenia, w tym uzasadnienia decyzji właściwego organu, może pomóc osobie fizycznej w podjęciu dalszych działań, włącznie z dochodzeniem roszczeń na drodze sądowej. Szczegółowe informacje na temat wyniku oceny mogą być ograniczone, jeżeli istnieją uzasadnione przesłanki do stwierdzenia, że przekazanie takiej informacji może stanowić zagrożenie dla trwającego postępowania.

(145) Po trzecie, osoba fizyczna, która nie zgadza się z decyzją sędziego o zajęciu (nakazem zajęcia) ([118]) dotyczących jej danych osobowych lub ze środkami podejmowanymi przez policję lub prokuraturę przy wykonywaniu takiej decyzji, może złożyć wniosek o uchylenie lub zmianę decyzji lub takich środków (art. 429 ust. 1, art. 430 ust. 1 i 2 kodeksu postępowania karnego, art. 26 ustawy o zakładaniu podsłuchów) ([119]). Jeżeli sąd badający sprawę stwierdzi, że nakaz lub jego wykonywanie („procedura zajęcia") są niezgodne z prawem, uwzględni on wniosek i nakaże zwrot zajętych artykułów ([120]).

(146) Po czwarte, w ramach bardziej pośredniej formy kontroli sądowej osoba fizyczna, która stwierdzi, że zbieranie dotyczących jej informacji osobowych w ramach postępowania przygotowawczego było niezgodnie z prawem, może powołać się na ten fakt przed sądem karnym. Jeżeli sąd się zgodzi, środki dowodowe zostaną wykluczone i uznane za niedopuszczalne.

(147) Wreszcie zgodnie z art. 1 ust. 1 ustawy o odpowiedzialności odszkodowawczej państwa sąd może przyznać odszkodowanie, jeżeli urzędnik publiczny sprawujący władzę publiczną w imieniu państwa w sposób niezgodny z prawem lub zawiniony (umyślnie lub przez niedbalstwo) wyrządził w ramach wykonywania swoich obowiązków danej osobie fizycznej szkodę. Zgodnie z art. 4 ustawy o odpowiedzialności odszkodowawczej państwa odpowiedzialność państwa za szkody opiera się na przepisach kodeksu cywilnego. W tym zakresie zgodnie z art. 710 kodeksu cywilnego odpowiedzialność ta obejmuje również szkody inne niż na majątkowe, a zatem szkody moralne (na przykład w postaci „urazów psychicznych"). Dotyczy to przypadków, w których prywatność osoby fizycznej została naruszona w wyniku niezgodnego z prawem sprawowania nadzoru lub zbierania dotyczących jej informacji osobowych (na przykład nielegalnego wykonania nakazu) ([121]).

(148) Oprócz odszkodowania pieniężnego osoby fizyczne mogą w określonych warunkach uzyskać również nakaz sądowy (na przykład w sprawie usunięcia danych osobowych zebranych przez organy publiczne) na podstawie praw do prywatności przewidzianych w art. 13 konstytucji ([122]).

(149) W odniesieniu do wszystkich powyższych możliwości dochodzenia roszczeń mechanizm rozstrzygania sporów opracowany przez japoński rząd pozwala osobie fizycznej, która wciąż jest niezadowolona z wyniku postępowania, zgłosić się do Komisji ds. Ochrony Informacji Osobowych, „która informuje osobę fizyczną o różnych możliwościach i szczegółowych procedurach dotyczących uzyskania odszkodowania na podstawie japońskich przepisów ustawowych i wykonawczych". Ponadto Komisja ds. Ochrony Informacji Osobowych „zapewnia osobie fizycznej wsparcie, w tym doradztwo i pomoc w związku z jakimkolwiek dalszym postępowaniem przed właściwym organem administracyjnym lub sądowym".

(150) Dotyczy to korzystania z praw procesowych przewidzianych w kodeksie postępowania karnego. Przykładowo „[j]eżeli ocena wykazała, że osoba fizyczna jest w postępowaniu karnym osobą podejrzaną, Komisja ds. Ochrony Informacji Osobowych zawiadamia ją o tym fakcie" ([123]) oraz o przewidzianej w art. 259 kodeksu postępowania karnego możliwości zwrócenia się do prokuratury z prośbą o zawiadomienie, gdy ta podejmie decyzję, aby nie wszczynać postępowania karnego. Ponadto, jeżeli ocena wykazała, że wszczęto sprawę dotyczącą informacji osobowych osoby fizycznej i została ona zakończona, Komisja ds. Ochrony Informacji Osobowych informuje taką osobę, że z aktami sprawy można się zapoznać zgodnie z art. 53 kodeksu postępowania karnego (oraz art. 4 ustawy o rejestrze zakończonych spraw karnych). Uzyskanie przez osobę fizyczną dostępu do jej akt sprawy

([118]) Dotyczy to również nakazu dotyczących podsłuchów, co do których ustawa o zakładaniu podsłuchów przewiduje szczególny wymóg powiadomienia (art. 23). Zgodnie z tym przepisem organ prowadzący postępowanie ma obowiązek zawiadomić na piśmie o tym fakcie osoby fizyczne, których wiadomości zostały przejęte (i tym samym dołączone do dokumentacji przejęcia). Kolejnym przykładem jest art. 100 ust. 3 kodeksu postępowania karnego, zgodnie z którym sąd, po przejęciu przesyłek pocztowych lub telegramów nadawanych przez lub do oskarżonego, zawiadamia nadawcę lub odbiorcę, chyba że zachodzi ryzyko, że takie powiadomienie utrudni postępowanie. Art. 222 ust. 1 kodeksu postępowania karnego zawiera odesłanie do tego przepisu w zakresie przeszukań i zajęć dokonywanych przez organ prowadzący postępowanie.

([119]) Chociaż taki wniosek nie oznacza automatycznego zawieszenia wykonania decyzji o zajęciu, sąd badający może nakazać zawieszenie do czasu podjęcia rozstrzygnięcia co do istoty sprawy. Zob. art. 429 ust. 2, art. 432 w zw. z art. 424 kodeksu postępowania karnego.

([120]) Zob. załącznik II, sekcja II.A.C pkt 1).

([121]) Zob. załącznik II, sekcja II.C.2).

([122]) Zob. na przykład Sąd Rejonowy w Tokio, wyrok z dnia 24 marca 1988 r. (nr 2925); Sąd Rejonowy w Osace, wyrok z dnia 26 kwietnia 2007 r. (nr 2925). Zgodnie z wyrokiem Sądu Rejonowego w Osace wymagane będzie zrównoważenie szeregu czynników, takich przykładowo jak: (i) charakter i treść przedmiotowych informacji osobowych; (ii) sposób ich zbierania; (iii) straty, jakie poniesienie osoba fizyczna, jeżeli nie dojdzie do usunięcia informacji oraz (iv) interes publiczny, w tym straty, jakie poniesie organ publiczny, jeżeli dojdzie do usunięcia informacji.

([123]) W każdym przypadku po wszczęciu postępowania karnego prokuratura zazwyczaj umożliwia oskarżonemu zapoznanie się z tymi środkami dowodowymi (zob. art. 298–299 kodeksu postępowania karnego). W kwestii ofiar przestępstw zob. art. 316–333 kodeksu postępowania karnego.

jest ważne, ponieważ pomaga jej lepiej zrozumieć prowadzone przeciwko niej postępowanie przygotowawcze, a tym samym przygotować się na ewentualne postępowanie sądowe (np. roszczenie o odszkodowanie), jeżeli uzna ona, że dotyczące jej dane zebrano lub wykorzystano niezgodnie z prawem.

3.3. **Dostęp japońskich organów publicznych do danych w celach związanych z bezpieczeństwem narodowym i wykorzystywanie przez nie tych danych w celach związanych z bezpieczeństwem narodowym**

(151) Według japońskich władz obligatoryjnego składania wniosków o udzielenie informacji ani „zakładania podsłuchów z polecenia organów administracyjnych" poza postępowaniem przygotowawczym w Japonii nie uregulowano. Zatem ze względów bezpieczeństwa narodowego informacje mogą być uzyskiwane wyłącznie ze źródeł, które są swobodnie dostępne dla wszystkich, lub w drodze dobrowolnego ujawnienia. Podmioty gospodarcze, do których zwrócono się o podjęcie dobrowolnej współpracy (w formie ujawnienia informacji elektronicznych), nie są prawnie zobowiązane do przekazania tych informacji ([124]).

(152) Ponadto zgodnie z uzyskanymi informacjami ze względów związanych z bezpieczeństwem narodowym do gromadzenia informacji elektronicznych znajdujących się w posiadaniu japońskich podmiotów gospodarczych uprawnione są tylko cztery instytucje rządowe. Są to: (i) Urząd Wywiadu i Badań Rady Ministrów; (ii) Ministerstwo Obrony; (iii) policja (zarówno Agencja Policji Krajowej ([125]), jak i policja prefekturalna); oraz (iv) Agencja Bezpieczeństwa Publicznego. Jednak Urząd Wywiadu i Badań Rady Ministrów nigdy nie gromadzi informacji bezpośrednio od podmiotów gospodarczych, w tym nie wykorzystuje środków przechwytywania przekazów telekomunikacyjnych. Co prawda uzyskuje on od innych organów rządowych informacje do celów analizy na potrzeby Rady Ministrów, jednak organy te również muszą przestrzegać przepisów prawa, w tym respektować ograniczenia i zabezpieczenia, o których mowa w niniejszej decyzji. Jego działalność nie jest zatem istotna w kontekście przekazywania danych.

3.3.1. *Podstawa prawna i właściwe ograniczenia/zabezpieczenia*

(153) Według otrzymanych informacji Ministerstwo Obrony gromadzi informacje (elektroniczne) na podstawie ustawy o utworzeniu Ministerstwa Obrony. Zgodnie z art. 3 tej ustawy zadaniem Ministerstwa Obrony jest zarządzanie siłami zbrojnymi i wykorzystywanie ich w celu „prowadzenia spraw wojskowych w celu zapewnienia pokoju w kraju i jego suwerenności, a także bezpieczeństwa narodu". Zgodnie z art. 4 ust. 4 Ministerstwo Obrony jest właściwe w zakresie „obrony i straży", w odniesieniu do działań Sił Samoobrony oraz rozmieszczania sił zbrojnych, w tym zbierania informacji niezbędnych do realizacji tych działań. Jest ono uprawnione do gromadzenia informacji (elektronicznych) pochodzących od podmiotów gospodarczych wyłącznie w drodze dobrowolnej współpracy.

(154) Jeżeli chodzi o policję prefekturalną jej zadania i obowiązki obejmują „utrzymywanie bezpieczeństwa i porządku publicznego" (art. 35 ust. 2 w zw. z art. 2 ust. 1 ustawy o policji). W zakresie swojej właściwości policja może gromadzić informacje, ale wyłącznie w sposób dobrowolny, bez użycia przymusu prawnego. Ponadto działania policji są „ściśle ograniczone" do czynności, które są niezbędne do wykonywania jej obowiązków. Poza tym jest ona obowiązana postępować w sposób „bezstronny, wolny od uprzedzeń i sprawiedliwy" i nigdy nie nadużywać swoich uprawnień „w jakikolwiek sposób, który będzie naruszać prawa i wolności osób fizycznych przewidziane w konstytucji Japonii" (art. 2 ustawy o policji).

(155) Wreszcie Agencja Bezpieczeństwa Publicznego może prowadzić postępowania przygotowawcze na podstawie ustawy o zapobieganiu działaniom wywrotowym (Subversive Activities Prevention Act – SAPA) oraz ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa (Act on the Control of Organisations Which Have Committed Acts of Indiscriminate Mass Murder – ACO), jeżeli są one niezbędne do przygotowania wdrożenia środków kontroli wobec określonych organizacji ([126]). Na podstawie obydwu tych ustaw na wniosek dyrektora generalnego Agencji Bezpieczeństwa Publicznego Komisja ds. Badania Bezpieczeństwa Publicznego może wydawać określone „instrukcje" (nadzorcze/zakazujące w ramach ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa ([127]), likwidacyjne/zakazujące w ramach ustawy o zapobieganiu działaniom wywrotowym ([128])), a Agencja Bezpieczeństwa Publicznego może prowadzić postępowania przygotowawcze w tym zakresie ([129]). Według otrzymanych informacji postępowania przygotowawcze zawsze prowadzone są dobrowolnie, co

([124]) W związku z powyższym podmioty gospodarcze mogą się nie zgodzić na tę współpracę, nie ryzykując nałożenia na nie sankcji lub poniesienia innych negatywnych konsekwencji. Zob. załącznik II, sekcja III.A.1).

([125]) Jednak według otrzymanych informacji podstawową rolą Agencji Policji Państwowej jest koordynowanie postępowań przygotowawczych prowadzonych przez poszczególne departamenty policji prefekturalnej oraz wymiana informacji z organami innych państw. Także w tej roli Agencja Policji Krajowej podlega nadzorowi Krajowej Komisji ds. Bezpieczeństwa Publicznego, odpowiedzialnej m.in. za ochronę praw i wolności osób fizycznych (art. 5 ust. 1 ustawy o policji).

([126]) Zob. załącznik II, sekcja III.A.1) pkt 3). Odpowiedni zakres zastosowania obu tych ustaw jest ograniczony, przy czym w ustawie o zapobieganiu działaniom wywrotowym mowa jest o „wywrotowych działaniach terrorystycznych", a w ustawie o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa – o „masowych morderstwach" (tzn. „wywrotowej działalności terrorystycznej" w rozumieniu ustawy o zapobieganiu działaniom wywrotowym, „w wyniku której dochodzi do masowego mordu na wielu osobach").

([127]) Zob. art. 5, 8 ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa. Instrukcja dotycząca nadzoru obejmuje także obowiązek sprawozdawczy w odniesieniu do organizacji, której dotyczą wprowadzone środki. W odniesieniu do gwarancji proceduralnych, w szczególności wymogów przejrzystości i uzyskania wcześniejszego zezwolenia Komisji ds. Badania Bezpieczeństwa Publicznego, zob. art. 12, 13, 15–27 ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa.

([128]) Zob. art. 5, 7 ustawy o zapobieganiu działaniom wywrotowym. W odniesieniu do gwarancji proceduralnych, w szczególności wymogów przejrzystości i uzyskania wcześniejszego zezwolenia Komisji ds. Badania Bezpieczeństwa Publicznego, zob. art. 11–25 ustawy o zapobieganiu działaniom wywrotowym.

([129]) Zob. art. 27 ustawy o zapobieganiu działaniom wywrotowym i art. 29, 30 ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa.

oznacza, że Agencja Bezpieczeństwa Publicznego nie może zmuszać osoby, której dotyczą informacje osobowe, do ich przekazania ([130]). Każdorazowo kontrole i postępowania przygotowawcze prowadzi się wyłącznie w minimalnym zakresie wymaganym do osiągnięcia celu kontroli i w żadnym razie nie są prowadzone „w sposób nieracjonalnie ograniczający" prawa i wolności przewidziane w konstytucji Japonii (art. 3 ust. 1 ustawy o zapobieganiu działaniom wywrotowym/ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa). Ponadto zgodnie z art. 3 ust. 2 ustawy o zapobieganiu działaniom wywrotowym/ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa Agencja Bezpieczeństwa Publicznego nie może w żadnych okolicznościach nadużywać takich środków kontroli ani postępowań prowadzonych w celu przygotowania takich środków. Jeżeli funkcjonariusz Agencji Bezpieczeństwa Publicznego nadużyje swoich uprawnień przewidzianych w odpowiedniej ustawie, zmuszając osobę do czynności, których ta nie ma obowiązku wykonać, lub przeszkadzając w wykonywaniu jej praw, może on podlegać sankcjom karnym zgodnie z art. 45 ustawy o zapobieganiu działaniom wywrotowym lub art. 42 ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa. Wreszcie w obu tych ustawach wyraźnie wskazano, że ich przepisy, w tym te przyznające uprawnienia, „w żadnych okolicznościach nie podlegają wykładni rozszerzającej" (art. 2 ustawy o zapobieganiu działaniom wywrotowym / ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa).

(156) We wszystkich przypadkach dostępu do informacji przez organy rządowe ze względów związanych z bezpieczeństwem narodowym opisanych w niniejszej sekcji zastosowanie znajdują ograniczenia przewidziane przez Sąd Najwyższy Japonii w odniesieniu do dobrowolnego prowadzenia postępowań przygotowawczych, co oznacza, że gromadzenie informacji (elektronicznych) musi odbywać się zgodnie z zasadą konieczności i proporcjonalności („metoda adekwatna") ([131]). Jak w sposób wyraźny potwierdziły władze Japonii, „zbieranie i przetwarzanie informacji odbywa się wyłącznie w zakresie niezbędnym do wykonywania szczególnych obowiązków przez właściwy organ publiczny oraz w związku ze szczególnymi zagrożeniami". W związku z tym „wyklucza to masowe i nieograniczone zbieranie informacji osobowych lub dostęp do nich ze względów bezpieczeństwa narodowego" ([132]).

(157) Ponadto wszelkie zgromadzone informacje osobowe zatrzymane przez organy publiczne do celów bezpieczeństwa narodowego zostają objęte zakresem ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji i tym samym objęte zabezpieczeniami przewidzianymi w tej ustawie w odniesieniu do dalszego przechowywania, wykorzystywania i ujawniania (zob. motyw 118).

3.3.2. *Niezależny nadzór*

(158) Zbieranie informacji osobowych do celów bezpieczeństwa narodowego objęte jest nadzorem na różnych szczeblach, realizowanym przez organy trzech segmentów władzy.

(159) Po pierwsze japońskie zgromadzenie narodowe może, za pośrednictwem swoich specjalistycznych komitetów, badać legalność postępowań przygotowawczych zgodnie ze swoimi uprawnieniami kontroli parlamentarnej (art. 62 konstytucji, art. 104 ustawy o zgromadzeniu narodowym; zob. motyw 134). Tę funkcję nadzorczą wspierają szczególne obowiązki sprawozdawcze w zakresie czynności realizowanych w oparciu o niektóre z wymienionych wyżej podstaw prawnych ([133]).

(160) Po drugie, w obrębie władzy wykonawczej przewidziano szereg mechanizmów nadzorczych.

(161) Jeżeli chodzi o Ministerstwo Obrony, nadzór pełni Biuro Inspektora Generalnego ds. Zgodności z Prawem (Inspector General's Office of Legal Compliance – IGO) ([134]), które utworzono na podstawie art. 29 ustawy o utworzeniu Ministerstwa Obrony jako biuro w ramach tego ministerstwa nadzorowane przez ministra obrony (któremu ono podlega), ale niezależne od departamentów operacyjnych Ministerstwa Obrony. Zadaniem Biura Inspektora Generalnego ds. Zgodności z Prawem jest zapewnianie zgodności z przepisami ustawowymi i wykonawczymi, a także prawidłowego wywiązywania się z obowiązków przez urzędników Ministerstwa Obrony. Do jego uprawnień należy przeprowadzanie tzw. „kontroli obrony", zarówno w regularnych odstępach czasu („regularne kontrole obrony"), jak i w indywidualnych przypadkach („specjalne kontrole obrony"), które w przeszłości obejmowały również właściwe przetwarzanie informacji osobowych ([135]). W ramach takich kontroli urzędnicy Biura Inspektora Generalnego ds. Zgodności z Prawem mogą wchodzić na teren (do biur) instytucji i żądać przedłożenia dokumentów lub informacji, w tym wyjaśnień od zastępcy wiceministra obrony. Kontrola kończy

([130]) Zob. załącznik II, sekcja III.A.1) pkt 3).

([131]) Zob. załącznik II, sekcja III.A.2) lit. b): „Z orzecznictwa Sądu Najwyższego wynika, że wniosek kierowany do podmiotu gospodarczego o podjęcie dobrowolnej współpracy musi być niezbędny do przeprowadzenia postępowania przygotowawczego dotyczącego podejrzenia popełnienia przestępstwa i uzasadniony pod kątem osiągnięcia celu tego postępowania. Chociaż śledztwa prowadzone przez organy śledcze w obszarze bezpieczeństwa narodowego i postępowania przygotowawcze prowadzone przez te organy w obszarze ścigania przestępstw różnią się od siebie pod względem podstawy prawnej i celu, nadrzędne zasady »konieczności przeprowadzenia postępowania przygotowawczego« oraz »odpowiedniości metody« znajdują również zastosowanie w obszarze bezpieczeństwa narodowego i należy ich przestrzegać z odpowiednim uwzględnieniem szczególnych okoliczności każdego przypadku".

([132]) Zob. załącznik II, sekcja III.A.2) lit. b).

([133]) Zob. art. 36 ustawy o zapobieganiu działaniom wywrotowym / art. 31 ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa (w przypadku Agencji Bezpieczeństwa Publicznego).

([134]) Dyrektor Biura Inspektora Generalnego ds. Zgodności z Prawem jest byłym prokuratorem. Zob. załącznik II, sekcja III.B.3).

([135]) Zob. załącznik II, sekcja III.B.3. Zgodnie z przytoczonym przykładem regularne kontrole obrony z 2016 r. w zakresie „świadomości kwestii zgodności z prawem / gotowości do zapewnienia zgodności z prawem" obejmowały między innymi „status ochrony informacji osobowych" (zarządzanie, przechowywanie itd.). W sprawozdaniu na ten temat stwierdzono przypadki niewłaściwego zarządzania danymi oraz wezwano do wprowadzenia usprawnień w tym zakresie. Ministerstwo Obrony opublikowało to sprawozdanie na swojej stronie internetowej.

się sporządzeniem sprawozdania dla ministra obrony, w którym przedstawia się ustalenia i środki poprawy (których wdrożenie można sprawdzić ponownie w drodze dalszej kontroli). Z kolei sprawozdanie stanowi podstawę do wydania przez ministra obrony instrukcji mających na celu wdrożenie środków koniecznych do naprawy sytuacji; zastępca wiceministra odpowiada za wdrożenie takich środków i ma obowiązek przedstawić sprawozdanie z działań następczych.

(162) Jeżeli chodzi o policję prefekturalną, nadzór zapewniają niezależne Prefekturalne Komisje ds. Bezpieczeństwa Publicznego, jak wyjaśniono w motywie 135 w odniesieniu do ścigania przestępstw.

(163) Wreszcie Agencja Bezpieczeństwa Publicznego, jak wskazano powyżej, może prowadzić postępowania przygotowawcze wyłącznie w zakresie koniecznym do wydania instrukcji w sprawie zakazu, likwidacji lub nadzoru na podstawie ustawy o zapobieganiu działaniom wywrotowym/ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa, a w odniesieniu do tych instrukcji niezależna ([136]) Komisja ds. Badania Bezpieczeństwa Publicznego prowadzi nadzór *ex ante*. Ponadto specjalnie wyznaczeni kontrolerzy przeprowadzają regularne/okresowe kontrole (obejmujące kompleksowe badanie działań Agencji Bezpieczeństwa Publicznego) ([137]), a także specjalne kontrole wewnętrzne ([138]) związane z działalnością poszczególnych departamentów/biur itd. Kontrole te mogą zakończyć się wydaniem instrukcji dla dyrektorów właściwych departamentów itp. w celu podjęcia działań naprawczych lub ukierunkowanych na poprawę.

(164) Wymienione mechanizmy nadzoru uzyskują dodatkowe wzmocnienie ze względu na to, że osoby fizyczne mają możliwość spowodowania interwencji Komisji ds. Ochrony Informacji Osobowych jako niezależnego organu nadzorczego (zob. sekcja 168 poniżej). Ponadto zapewniają one odpowiednie zabezpieczenia przed ryzykiem nadużycia przez japońskie władze uprawnień w dziedzinie bezpieczeństwa narodowego, a także przed niezgodnym z prawem zbieraniem informacji elektronicznych.

3.3.3. *Indywidualne dochodzenie roszczeń*

(165) W kwestii dochodzenia roszczeń przez osoby fizyczne, w odniesieniu do informacji osobowych gromadzonych i tym samym „zatrzymywanych" przez organy administracyjne, obowiązkiem tych organów jest „dążyć do właściwego i sprawnego rozpatrzenia wszelkich skarg" dotyczących takiego przetwarzania informacji (art. 48 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji).

(166) Ponadto, w odróżnieniu od postępowań przygotowawczych, osobom fizycznym (w tym cudzoziemcom mieszkającym za granicą) zasadniczo przysługuje prawo do ujawnienia ([139]), korekty (w tym do usunięcia) oraz zawieszenia wykorzystywania/przekazywania informacji na podstawie ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji. Mając powyższe na uwadze, dyrektor organu administracyjnego może odmówić ujawnienia informacji „w przypadku których istnieją uzasadnione przesłanki […] do stwierdzenia, że ujawnienie może stanowić zagrożenie dla bezpieczeństwa narodowego" (art. 14 ppkt (iv) ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji) i może tak uczynić bez ujawniania, że takie informacje istnieją (art. 17 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji). Podobnie, pomimo że osoba fizyczna może zażądać zawieszenia wykorzystywania lub usunięcia informacji zgodnie z art. 36 ust. 1 ppkt (i) ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji, jeżeli organ administracyjny uzyskał informacje niezgodnie z prawem albo jeżeli zatrzymuje/wykorzystuje je w sposób wykraczający poza zakres wymagany do osiągnięcia określonego celu, organ może odrzucić to żądanie, jeżeli uzna, że zawieszenie wykorzystania „może utrudnić właściwą realizację czynności służących osiągnięciu celu, w którym zatrzymano informacje osobowe, z uwagi na charakter tych czynności" (art. 38 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji). Jednak w przypadkach, w których możliwe jest łatwe oddzielenie i wykluczenie elementów objętych wyjątkiem, organy administracyjne są obowiązane do co najmniej częściowego ujawnienia (zob. art. 15 ust. 1 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji) ([140]).

([136]) Zgodnie z ustawą o utworzeniu Komisji ds. Badania Bezpieczeństwa Publicznego, przewodniczący i członkowie Komisji „wykonują swoje uprawnienia w sposób niezależny" (art. 3). Powołuje ich premier za zgodą obu izb Diet. Mogą oni zostać odwołani wyłącznie „z ważnych powodów" (np. skazanie na karę pozbawienie wolności, naruszenie obowiązków, rozstrój zdrowia w sferze fizycznej lub psychicznej, wszczęcie postępowania upadłościowego).

([137]) Rozporządzenie w sprawie okresowych kontroli Agencji Bezpieczeństwa Publicznego (dyrektor generalny Agencji Bezpieczeństwa Publicznego, instrukcja nr 4, 1986).

([138]) Rozporządzenie w sprawie specjalnych kontroli Agencji Bezpieczeństwa Publicznego (dyrektor generalny Agencji Bezpieczeństwa Publicznego, instrukcja nr 11, 2008). Specjalne kontrole przeprowadza się, jeżeli dyrektor generalny Agencji Bezpieczeństwa Publicznego uzna to za konieczne.

([139]) Dotyczy to prawa do otrzymania kopii „zatrzymanych informacji osobowych".

([140]) Zob. również możliwość „uznaniowego ujawnienia" nawet w przypadku, gdy „informacja nieujawniana" objęta jest zakresem „zatrzymanych informacji osobowych", których ujawnienia się żąda (art. 16 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji).

(167) W każdym przypadku organ administracyjny ma obowiązek podjąć decyzję na piśmie w określonym terminie (30 dni, przy czym termin ten może zostać przedłużony o dodatkowe 30 dni w określonych okolicznościach). Jeżeli wniosek został odrzucony, uwzględniony tylko częściowo, albo jeżeli dana osoba z innych względów uzna, że postępowanie organu administracyjnego jest „bezprawne lub niesłuszne", osoba ta może wystąpić o przeprowadzenie kontroli administracyjnej na podstawie ustawy o kontroli skarg administracyjnych ([141]). W takim przypadku dyrektor organu administracyjnego, który podejmuje decyzję w sprawie odwołania, konsultuje się z Radą ds. Oceny Ujawniania Informacji i Ochrony Informacji Osobowych (art. 42, 43 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji), wyspecjalizowanym, niezależnym organem kolegialnym, którego członków powołuje premier za zgodą obu izb Diet. Według otrzymanych informacji Rada ds. Oceny może przeprowadzić badanie ([142]) i tym kontekście zażądać od organu administracyjnego przekazania zatrzymanych informacji osobowych, w tym wszelkich treści niejawnych, a także dalszych informacji i dokumentów. Podczas gdy ostateczne sprawozdanie, które przesyła się skarżącemu oraz organowi administracyjnemu i podaje do wiadomości publicznej, nie jest prawnie wiążące, niemal we wszystkich przypadkach zastosowano się do jego treści ([143]). Ponadto osoba fizyczna może na drodze sądowej zakwestionować rozstrzygnięcie w sprawie odwołania zgodnie z ustawą o sporach administracyjnych. Umożliwia to kontrolę sądową stosowania wyjątków w obszarze bezpieczeństwa narodowego, w tym tego, czy doszło do nadużycia w przypadku zastosowania takie wyjątku bądź czy jest on nadal uzasadniony.

(168) W celu usprawnienia wykonania wymienionych wyżej praw na podstawie ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji Ministerstwo Spraw Wewnętrznych i Komunikacji ustanowiło 51 „centrów informacji ogólnej", które zapewniają skonsolidowane informacje na temat tych praw, obowiązujących procedur dotyczących składania wniosków oraz ewentualnych możliwości dochodzenia roszczeń ([144]). Jeżeli chodzi o organy administracyjne, są obowiązane przekazywać „informacje, które pomagają w określeniu zatrzymanych informacji osobowych" ([145]) oraz podjąć „pozostałe właściwe działania z uwzględnieniem wygody osoby, która zamierza złożyć wniosek" (art. 47 ust. 1 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji).

(169) Zarówno w przypadku postępowań przygotowawczych w obszarze ścigania przestępstw, jak i w dziedzinie bezpieczeństwa narodowego, osoby fizyczne mogą indywidualnie dochodzić roszczeń, kontaktując się bezpośrednio z Komisją ds. Ochrony Informacji Osobowych. Powoduje to wszczęcie szczególnej procedury rozstrzygania sporów, którą japoński rząd opracował dla osób fizycznych z UE, których dane osobowe są przekazywane na podstawie niniejszej decyzji (zob. szczegółowe wyjaśnienia w motywach 141–144 i 149).

(170) Ponadto osoba fizyczna może dochodzić roszczeń na drodze sądowej w formie powództwa o odszkodowanie zgodnie z ustawą o odpowiedzialności odszkodowawczej państwa, które obejmuje także szkody moralne oraz, w określonych warunkach, usunięcie zgromadzonych danych (zob. motyw 147).

4. PODSUMOWANIE: ODPOWIEDNI STOPIEŃ OCHRONY DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UNII EUROPEJSKIEJ PODMIOTOM GOSPODARCZYM Z JAPONII

(171) Komisja uważa, że ustawa o ochronie informacji osobowych wraz z przepisami uzupełniającymi zawartymi w załączniku I oraz oficjalne oświadczenia, zapewnienia i zobowiązania zawarte w załączniku II, zapewnia stopień ochrony danych osobowych przekazywanych z Unii Europejskiej, który zasadniczo odpowiada ochronie zagwarantowanej na mocy rozporządzenia (UE) 2016/679.

(172) Ponadto Komisja stwierdza, że mechanizmy nadzoru i możliwości dochodzenia roszczeń przewidziane w prawie japońskim – rozumiane jako całość – zapewniają możliwość identyfikowania przypadków naruszenia przepisów przez podmioty gospodarcze przetwarzające informacje osobowe będące odbiorcami danych 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 danych na ich temat, a także – ostatecznie – skorygowania lub usunięcia takich danych.

([141]) Ustawa o kontroli skarg administracyjnych (ustawa nr 160 z 2014 r.), w szczególności art. 1 ust. 1.

([142]) Zob. art. 9 ustawy o powołaniu Rady ds. Oceny Ujawniania Informacji i Ochrony Informacji Osobowych (ustawa nr 60 z 2003 r.).

([143]) Według otrzymanych informacji w okresie 13 lat od 2005 r. (gdy ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji weszła w życie) tylko w 2 z ponad 2000 przypadków organ administracyjny nie zastosował się do treści sprawozdania, choć w szeregu przypadków Rada ds. Oceny podważała decyzje administracyjne. Ponadto, jeżeli organ administracyjny podejmie decyzję, która odbiega od ustaleń zawartych w sprawozdaniu, ma obowiązek wyraźnie wskazać przyczyny odstąpienia od tych ustaleń. Zob. załącznik II, sekcja III.C, w odniesieniu do art. 50 ust. 1, pkt (iv) ustawy o kontroli skarg administracyjnych.

([144]) Centra informacji ogólnej – po jednym w każdej prefekturze – udzielają obywatelom wyjaśnień na temat informacji osobowych gromadzonych przez organy publiczne (np. w istniejących bazach danych) oraz właściwych przepisów o ochronie danych (ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji), w tym na temat możliwości realizacji praw do ujawnienia, korekty danych lub zawieszenia ich wykorzystywania. Centra te działają jednocześnie jako punkty kontaktowe w sprawach zapytań/skarg obywateli. Zob. załącznik II, sekcja II.C.4) lit. a).

([145]) Zob. również art. 10, 11 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji w sprawie „rejestru akt z informacjami osobowymi", w których jednak przewidziano daleko idące wyjątki dotyczące „akt z informacjami osobowymi" przygotowanych lub uzyskanych na potrzeby postępowania przygotowawczego albo poruszających kwestie dotyczące bezpieczeństwa i innych istotnych interesów państwa (zob. art. 10 ust. 2 ppkt (i) oraz (ii) ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji).

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

(174) W związku z powyższym, w świetle ustaleń zawartych w niniejszej decyzji, Komisja uważa, że Japonia zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii Europejskiej podmiotom gospodarczym przetwarzającym informacje osobowe w Japonii, które podlegają ustawie o ochronie informacji osobowych, z wyjątkiem przypadków, gdy odbiorca zalicza się do jednej z kategorii wymienionych w art. 76 ust. 1 tej ustawy, a cel przetwarzania w całości lub częściowo odpowiada jednemu z celów przewidzianych w tym przepisie.

(175) Na tej podstawie Komisja stwierdza, że standard ochrony przewidziany w art. 45 rozporządzenia (UE) 2016/679, interpretowany w świetle Karty praw podstawowych Unii Europejskiej, a w szczególności wyroku w sprawie Schrems ([146]), jest spełniony.

5. DZIAŁANIA ORGANÓW OCHRONY DANYCH I INFORMACJE PRZEKAZYWANE KOMISJI

(176) Zgodnie z orzecznictwem Trybunału Sprawiedliwości ([147]), a także jak wskazano w art. 45 ust. 4 rozporządzenia (UE) 2016/679, Komisja powinna ciągle monitorować istotne zmiany zachodzące w państwie trzecim po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony, aby ocenić, czy Japonia nadal zapewnia zasadniczo równoważny stopień ochrony. Taka kontrola jest wymagana w każdym przypadku, gdy Komisja otrzyma informacje budzące uzasadnione wątpliwości w tym względzie.

(177) W związku z powyższym Komisja powinna na bieżąco monitorować sytuację w zakresie ram prawnych i rzeczywistej praktyki w odniesieniu do przetwarzania danych osobowych, podlegających ocenie w niniejszej decyzji, w tym wywiązywanie się japońskich władz z oświadczeń, zapewnień i zobowiązań zawartych w załączniku II. W celu ułatwienia tego procesu oczekuje się, że władze japońskie będą informować Komisję o zmianach w prawie materialnym, które są istotne dla niniejszej decyzji, zarówno w związku z przetwarzaniem danych osobowych przez podmioty gospodarcze, jak i z ograniczeniami i zabezpieczeniami dotyczącymi dostępu organów publicznych do danych osobowych. Powinno to obejmować wszelkie decyzje Komisji ds. Ochrony Informacji Osobowych wydane na mocy art. 24 ustawy o ochronie informacji osobowych, w których uznaje się dane państwo trzecie za zapewniające poziom ochrony równoważny z poziomem ochrony zagwarantowanym w Japonii.

(178) 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 podmiotom gospodarczym w Japonii. Komisja powinna być również informowana o wszelkich sygnałach świadczących o tym, że działania japońskich organów publicznych odpowiedzialnych za zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie przestępstw nie gwarantują wymaganego stopnia ochrony.

(179) 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. 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. Jednocześnie, jak wyjaśnił Trybunał Sprawiedliwości w wyroku sprawie Schrems ([148]) i uznano w art. 58 ust. 5 rozporządzenia, jeżeli organ ochrony danych państwa członkowskiego kwestionuje, również na podstawie skargi, zgodność wydanej przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony z podstawowym prawem osoby do prywatności i ochrony danych, należy zapewnić w prawie krajowym drogę prawną umożliwiającą jej podniesienie tych zarzutów przed sądem krajowym, który w razie wątpliwości jest obowiązany zawiesić postępowanie i wystąpić z pytaniem prejudycjalnym do Trybunału Sprawiedliwości ([149]).

([146]) Zob. przypis 3 powyżej.

([147]) Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r., Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, pkt 76.

([148]) Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r., Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, pkt 65.

([149]) Wyrok Trybunału (wielka izba) z dnia 6 października 2015 r., Maximillian Schrems/Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, 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".

6. OKRESOWY PRZEGLĄD USTALENIA DOTYCZĄCEGO ADEKWATNOŚCI

(180) W zastosowaniu art. 45 ust. 3 rozporządzenia (UE) 2016/679 ([150]) oraz w świetle tego, że stopień ochrony zapewniany w porządku prawnym Japonii może ulec zmianie, Komisja po przyjęciu niniejszej decyzji powinna okresowo sprawdzać, czy ustalenia odnoszące się do adekwatności stopnia ochrony gwarantowanego przez Japonię są nadal faktycznie i prawnie uzasadnione.

(181) W tym celu niniejsza decyzja powinna zostać poddana pierwszemu przeglądowi w ciągu dwóch 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 RODO, podejmie decyzję co do tego, czy dwuletni cykl powinien zostać utrzymany. W każdym przypadku kolejne przeglądy powinny mieć miejsce co najmniej raz na cztery lata ([151]). Przegląd powinien uwzględniać wszystkie aspekty funkcjonowania niniejszej decyzji, w szczególności stosowanie przepisów uzupełniających (przy czym szczególną uwagę należy poświęcić środków ochronnych w związku z dalszym przekazywaniem danych), stosowanie przepisów dotyczących zgody, w tym w razie wycofania, skuteczność nadzoru korzystania przez osoby fizycznej z ich praw, jak również ograniczenia i zabezpieczenia w odniesieniu do dostępu rządowego, w tym mechanizmy dochodzenia roszczeń wskazane w załączniku II do niniejszej decyzji. Przegląd powinien również uwzględniać skuteczność nadzoru i egzekwowania w odniesieniu do przepisów stosowanych zarówno wobec podmiotów gospodarczych przetwarzających informacje osobowe, jak i w obszarze ścigania przestępstw i bezpieczeństwa narodowego.

(182) W celu przeprowadzenia przeglądu Komisja powinna odbyć spotkanie z Komisją ds. Ochrony Informacji Osobowych, której będą towarzyszyć, w stosownych przypadkach, inne japońskie 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 (EROD). W ramach wspólnego przeglądu Komisja powinna wystąpić do Komisji ds. Ochrony Informacji Osobowych 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 ([152]). Komisja powinna również zwracać się o wyjaśnienia dotyczące wszelkich otrzymanych informacji istotnych dla niniejszej decyzji, w tym dotyczące publicznych sprawozdań przygotowanych przez japońskie władze lub inne zainteresowane strony z Japonii, EROD, poszczególne organy ochrony danych, ugrupowania społeczeństwa obywatelskiego, doniesień medialnych i innych dostępnych źródeł informacji.

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

7. ZAWIESZENIE DECYZJI STWIERDZAJACEJ ODPOWIEDNI STOPIEŃ OCHRONY DANYCH OSOBOWYCH

(184) Jeżeli na podstawie regularnych i doraźnych kontroli lub innych dostępnych informacji Komisja stwierdzi, że stopień ochrony zapewniany w porządku prawnym Japonii nie może być dłużej uznawany za zasadniczo równoważny stopniowi ochrony w Unii Europejskiej, powinna ona zawiadomić o tym właściwe organy Japonii oraz wystąpić o zastosowanie właściwych środków w określonym, uzasadnionym terminie. Dotyczy to przepisów mających zastosowanie zarówno do podmiotów gospodarczych, jak i japońskich organów publicznych odpowiedzialnych za ściganie przestępstw lub bezpieczeństwo narodowe. Przykładowo takie postępowanie byłoby uruchamiane w przypadkach, w których dalsze przekazywanie, w tym przekazywanie na podstawie decyzji o uznaniu państwa trzeciego za zapewniające ochronę w stopniu równoważnym ochronie gwarantowanej w Japonii, przyjętych przez Komisję ds. Ochrony Informacji Osobowych na mocy art. 24 ustawy o ochronie informacji osobowych, nie będzie już realizowane w ramach zabezpieczeń zapewniających ciągłość ochrony w rozumieniu art. 44 RODO.

(185) Jeżeli po upływie określonego terminu właściwy japoński organ nie wykaże w zadowalający sposób, że niniejsza decyzja jest nadal oparta na odpowiednim stopniu ochrony, Komisja powinna, w zastosowaniu art. 45 ust. 5 rozporządzenia (UE) 2016/679, wszcząć postępowanie prowadzące do częściowego lub całkowitego zawieszenia lub uchylenia niniejszej decyzji. Ewentualnie Komisja powinna wszcząć procedurę zmiany niniejszej decyzji, zwłaszcza polegającej na poddaniu przekazywania danych dodatkowym warunkom lub ograniczeniu zakresu stwierdzenia odpowiedniego stopnia ochrony wyłącznie do przekazywania danych, co do których zapewniona jest ciągłość ochrony w rozumieniu art. 44 RODO.

([150]) Zgodnie z art. 45 ust. 3 rozporządzenia (UE) 2016/679 „[w] akcie wykonawczym przewiduje się mechanizm okresowego przeglądu – przynajmniej raz na cztery lata – podczas którego uwzględnia się wszelkie mające znaczenie zmiany w państwie trzecim lub organizacji międzynarodowej".

([151]) Zgodnie z art. 45 ust. 3 rozporządzenia (UE) 2016/679 przegląd okresowy musi odbywać się przynajmniej raz na cztery lata. Zob. również EROD, odpowiedni stopień ochrony przekazywanych danych osobowych, WP 254 rev. 01.

([152]) Zob. również załącznik II, sekcja IV: „W ramach okresowego przeglądu decyzji stwierdzającej odpowiedni stopień ochrony Komisja ds. Ochrony Informacji Osobowych i Komisja Europejska będą wymieniać się informacjami dotyczącymi przetwarzana danych na warunkach przewidzianych w ustaleniu dotyczącym adekwatności, w tym określonych w niniejszym oświadczeniu".

(186) Komisja powinna w szczególności wszcząć procedurę zawieszenia lub uchylenia w przypadku wystąpienia przesłanek wskazujących, że przepisy uzupełniające 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 japońskie nie wywiązują się z oświadczeń, zapewnień i zobowiązań zawartych w załączniku II do niniejszej decyzji.

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

(188) W przypadkach należycie uzasadnionej pilnej potrzeby, takiej jak ryzyko poważnego naruszenia praw osób, których dane dotyczą, Komisja powinna rozważyć przyjęcie decyzji o zawieszeniu lub uchyleniu niniejszej decyzji, która powinna obowiązywać ze skutkiem natychmiastowym, zgodnie z art. 93 ust. 3 rozporządzenia (UE) 2016/679 w związku z art. 8 rozporządzenia Parlamentu Europejskiego i Rady 182/2011 ([153]).

8. **UWAGI KOŃCOWE**

(189) Europejska Rada Ochrony Danych opublikowała swoją opinię ([154]), która została uwzględniona podczas przygotowywania niniejszej decyzji.

(190) Parlament Europejski przyjął rezolucję w sprawie strategii w zakresie handlu elektronicznego, w której wezwano Komisję do uznania za priorytet oraz do przyspieszenia przyjmowania decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu do ważnych partnerów handlowych zgodnie z warunkami określonymi w rozporządzeniu (UE) 2016/679 jako podstawowego mechanizmu zabezpieczania przekazywania danych osobowych z Unii Europejskiej ([155]). Parlament Europejski przyjął również rezolucję w sprawie adekwatności ochrony danych osobowych zapewnianej przez Japonię ([156]).

(191) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu utworzonego na podstawie art. 93 ust. 1 RODO,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

1. Do celów art. 45 rozporządzenia (UE) 2016/679 Japonia zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych z Unii Europejskiej podmiotom gospodarczym przetwarzającym informacje osobowe w Japonii z zastrzeżeniem ustawy o ochronie informacji osobowych wraz z przepisami uzupełniającymi zawartymi w załączniku I oraz oficjalnymi oświadczeniami, zapewnieniami i zobowiązaniami zawartymi w załączniku II.

([153]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

([154]) Opinia 28/2018 dotycząca projektu decyzji wykonawczej Komisji stwierdzającej odpowiedni stopień ochrony danych osobowych w Japonii, przyjęta w dniu 5 grudnia 2018 r.

([155]) Parlament Europejski, rezolucja z dnia 12 grudnia 2017 r. „W kierunku strategii w zakresie handlu elektronicznego" (2017/2065(INI)). Zob. przede wszystkim pkt 8 („…przypomina, że dane osobowe mogą być przekazywane do krajów trzecich, bez stosowania zasad ogólnych w umowach handlowych, jeżeli spełnione są obecne i przyszłe wymogi zapisane w […] rozdziale V rozporządzenia (UE) 2016/679; uznaje, że decyzje stwierdzające odpowiedni stopień ochrony, w tym częściowe i dotyczące poszczególnych sektorów, są podstawowym mechanizmem zabezpieczania przekazywania danych osobowych z UE do państwa trzeciego; zauważa, że UE przyjęła decyzje stwierdzające odpowiedni stopień ochrony tylko w odniesieniu do czterech z jej 20 największych partnerów handlowych…"); oraz pkt 9 („wzywa Komisję do uznania za priorytet oraz do przyspieszenia przyjmowania decyzji stwierdzających odpowiedni stopień ochrony, pod warunkiem że państwa trzecie zapewnią, na mocy prawa krajowego lub zobowiązań międzynarodowych, stopień ochrony »zasadniczo odpowiadający« stopniowi gwarantowanemu w UE…").

([156]) Rezolucja Parlamentu Europejskiego z dnia 13 grudnia 2018 r. „Adekwatność ochrony danych osobowych zapewnianej przez Japonię" (2018/2979 (RSP))

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 wymienionych celów, odpowiednio:

a) nadawcy radiofonii, wydawcy gazet, agencje komunikacyjne i inne organizacje prasowe (w tym osoby fizyczne prowadzące działalność prasową), w zakresie, w jakim przetwarzają one dane osobowe do celów prasowych;

b) osoby zawodowo zajmujące się pisaniem, w zakresie, w jakim wykorzystywane są przy tym dane osobowe;

c) szkoły wyższe i wszelkie inne organizacje lub grupy, których celem jest prowadzenie studiów, albo wszelkie osoby należące do takich organizacji lub grup, w zakresie, w jakim przetwarzają one dane osobowe do celów studiów;

d) instytucje kościelne, w zakresie, w jakim przetwarzają one dane osobowe do celów działalności religijnej (w tym wszystkich powiązanych czynności); oraz

e) organy polityczne, w zakresie, w jakim przetwarzają one dane osobowe do celów związanych z ich działalnością polityczną (w tym wszystkich powiązanych czynności).

Artykuł 2

W przypadku gdy właściwe organy w państwach członkowskich wykonują – w celu ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych – swoje uprawnienia na podstawie art. 58 rozporządzenia (UE) 2016/679, co prowadzi do zawieszenia lub ostatecznego zakazu przepływu danych do konkretnego podmiotu gospodarczego w Japonii w zakresie zastosowania określonym w art. 1, dane państwo członkowskie niezwłocznie informuje o tym Komisję.

Artykuł 3

1. Komisja stale monitoruje stosowanie ram prawnych, na których opiera się niniejsza decyzja, w tym warunków, w jakich odbywa się dalsze przekazywanie danych, w celu ustalenia, czy Japonia nadal zapewnia odpowiedni poziom ochrony w rozumieniu art. 1.

2. Państwa członkowskie oraz Komisja informują się nawzajem o przypadkach, w których Komisja ds. Ochrony Informacji Osobowych lub jakikolwiek inny właściwy organ japoński 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 organów publicznych Japonii w prawo osób fizycznych do ochrony ich danych osobowych wykraczają poza to, co jest ściśle niezbędne, lub że nie zapewniono skutecznej ochrony prawnej przed takimi ingerencjami.

4. W ciągu dwóch lat od dnia powiadomienia państw członkowskich o wydaniu niniejszej decyzji, a następnie co najmniej co cztery lata Komisja będzie oceniać ustalenie, o którym mowa w art. 1 ust. 1, na podstawie wszystkich dostępnych informacji, w tym informacji otrzymanych w ramach wspólnego przeglądu, przeprowadzanego wspólnie z właściwymi japońskimi organami.

5. Jeżeli Komisja posiada dowody na to, że odpowiedni stopień ochrony nie jest już zapewniony, Komisja powiadamia o tym właściwe organy Japonii. W razie potrzeby może ona postanowić o zawieszeniu, zmianie albo uchyleniu niniejszej decyzji albo o ograniczeniu jej zakresu, zwłaszcza w przypadku gdy istnieją przesłanki, że:

a) podmioty gospodarcze w Japonii, które otrzymały dane osobowe z Unii Europejskiej na podstawie niniejszej decyzji, nie przestrzegają dodatkowych zabezpieczeń określonych w przepisach uzupełniających zawartych w załączniku I do niniejszej decyzji lub nadzór i egzekwowanie przepisów w tym zakresie są niewystarczające;

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

Komisja może również przedstawić projekt takich środków, jeżeli brak współpracy ze strony rządu Japonii nie pozwala Komisji ustalić, czy ustalenie zawarte w art. 1 ust. 1 niniejszej decyzji zostało podważone.

Artykuł 4

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 23 stycznia 2019 r..

W imieniu Komisji
Věra JOUROVÁ
Członek Komisji

ZAŁĄCZNIK 1

PRZEPISY UZUPEŁNIAJĄCE NA PODSTAWIE USTAWY O OCHRONIE INFORMACJI OSOBOWYCH W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH PRZEKAZYWANYCH Z UE NA PODSTAWIE DECYZJI STWIERDZAJĄCEJ ODPOWIEDNI STOPIEŃ OCHRONY

Spis treści

[Terminy]

„ustawa”	ustawa o ochronie informacji osobowych (ustawa nr 57 z 2003 r.)
„zarządzenie Rady Ministrów”	zarządzenie wykonawcze Rady Ministrów do ustawy o ochronie informacji osobowych (zarządzenie Rady Ministrów nr 507 z 2003 r.)
„przepisy wykonawcze”	przepisy wykonawcze do ustawy o ochronie informacji osobowych (przepisy przyjęte przez Komisję ds. Ochrony Informacji Osobowych nr 3 z 2016 r.)
„wytyczne do przepisów ogólnych”	wytyczne do ustawy o ochronie informacji osobowych (wydanie zawierające przepisy ogólne(zawiadomienie Komisji ds. Ochrony Informacji Osobowych nr 65 z 2015 r.)
„UE”	Unia Europejska, w tym jej państwa członkowskie oraz, w świetle Porozumienia EOG, Islandia, Liechtenstein i Norwegia
„RODO”	rozporządzenie Parlamentu Europejskiego i Rady 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)
„decyzja stwierdzająca odpowiedni stopień ochrony”	decyzja Komisji Europejskiej stwierdzająca, że państwo trzecie lub określone terytorium w tym państwie trzecim itp. zapewnia odpowiedni stopień ochrony danych osobowych na podstawie art. 45 RODO.

W celu prowadzenia wzajemnego i sprawnego przekazywania danych osobowych między Japonią a UE Komisja ds. Ochrony Informacji Osobowych wyznaczyła UE jako państwo obce ustanawiające system ochrony informacji osobowych o ramach równoważnych tym obowiązującym w Japonii w odniesieniu do ochrony praw i interesów jednostki na podstawie art. 24 ustawy, a Komisja Europejska postanowiła jednocześnie, że Japonia zapewnia odpowiedni poziom ochrony danych osobowych na podstawie art. 45 RODO.

Niniejszym postanawia się o ustanowieniu wzajemnego i sprawnego przekazywania danych osobowych między Japonią a UE w sposób zapewniający wysoki poziom ochrony praw i interesów jednostki. W celu zapewnienia wysokiego poziomu ochrony informacji osobowych otrzymywanych z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony oraz w świetle tego, że pomimo wysokiego poziomu zbieżności między tymi dwoma systemami istnieją między nimi pewne istotne różnice, Komisja ds. Ochrony Informacji Osobowych przyjęła niniejsze przepisy uzupełniające w oparciu o przepisy ustawy wdrażającej współpracę z rządami innych państw oraz w celu zapewnienia odpowiedniego przetwarzania informacji osobowych otrzymywanych z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony przez podmiot gospodarczy przetwarzający informacje osobowe oraz właściwego oraz w celu skutecznego wykonywania obowiązków określonych w tych przepisach ([1]).

([1]) Art. 4, 6, 8, 24, 60 i 78 ustawy oraz art. 11 przepisów wykonawczych.

W szczególności art. 6 ustawy przewiduje kompetencję do podejmowania niezbędnych działań ustawodawczych i innych w celu zapewnienia zwiększonej ochrony informacji osobowych i utworzenia systemu dotyczącego informacji osobowych, który byłby zgodny z prawem międzynarodowym, poprzez ustanowienie bardziej rygorystycznych przepisów uzupełniających oraz uszczegóławiających przepisy ustawy i zarządzenia Rady Ministrów. W związku z tym Komisja ds. Ochrony Informacji Osobowych, jako organ właściwy w zakresie ogólnego zarządzania wykonywaniem przepisów ustawy, ma kompetencję do stanowienia, na podstawie art. 6 ustawy, bardziej rygorystycznych regulacji. Realizując je, postanowiła ona przyjąć niniejsze przepisy uzupełniające, zapewniające wyższy poziom ochrony praw i interesów jednostki w odniesieniu do przetwarzania danych osobowych otrzymywanych z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, w tym w odniesieniu do definicji informacji osobowych wymagających szczególnej uwagi zgodnie z art. 2 ust. 3 ustawy oraz zatrzymanych danych osobowych zgodnie z art. 2 ust. 7 ustawy (w tym w odniesieniu do odpowiedniego okresu zatrzymywania danych).

Na tej podstawie przepisy uzupełniające są wiążące dla podmiotu gospodarczego przetwarzającego informacje osobowe, który otrzymuje dane osobowe przekazywane z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, która w związku z tym powinna być z tymi przepisami zgodna. Komisja ds. Ochrony Informacji Osobowych egzekwuje wszelkie prawa i obowiązki, jako prawnie wiążące przepisy, w taki sam sposób jak przepisy ustawy, których uzupełnieniem są te surowsze lub bardziej szczegółowe przepisy. W razie naruszenia praw i obowiązków wynikających z przepisów uzupełniających osoby fizyczne mogą również dochodzić roszczeń na drodze sądowej w taki sam sposób, jak w odniesieniu do przepisów ustawy, których uzupełnieniem są te surowsze lub bardziej szczegółowe przepisy.

Jeżeli chodzi o egzekwowanie przepisów przez Komisję ds. Ochrony Informacji Osobowych, jeżeli podmiot gospodarczy przetwarzający informacje osobowe nie spełnia jednego lub kilku obowiązków wynikających z przepisów uzupełniających, Komisja ds. Ochrony Informacji Osobowych ma kompetencje do przyjęcia środków na podstawie art. 42 ustawy. Jeżeli chodzi ogólnie o informacje osobowe otrzymywane z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, niepodjęcie, bez prawnie uzasadnionej podstawy, przez podmiot gospodarczy przetwarzający informacje osobowe działań zgodnych z zaleceniem otrzymanym na podstawie art. 42 ust. 1 ustawy ([2]) uznaje się za poważne i nieuchronne naruszenie praw i interesów jednostki w rozumieniu art. 42 ust. 2 ustawy.

1. Informacje osobowe wymagające szczególnej uwagi (art. 2 ust. 3 ustawy)

Art. 2 ust. 3 ustawy

3. „Informacje osobowe wymagające szczególnej uwagi" oznaczają w niniejszej ustawie informacje osobowe obejmujące rasę, przekonania, status społeczny, historię medyczną, uprzednią karalność osoby powierzającej dane, fakt bycia ofiarą przestępstwa lub inne opisy itp. wskazane w zarządzeniu Rady Ministrów jako informacje, których przetwarzanie wymaga szczególnej uwagi, aby nie spowodować dyskryminacji, uprzedzeń lub innych niekorzystnych okoliczności względem osoby powierzającej dane.

Art. 2 zarządzenia Rady Ministrów

Opisy te itp., określone zarządzeniem Rady Ministrów na podstawie art. 2 ust. 3 ustawy, to opisy itp., które zawierają którekolwiek z wymienionych poniżej kwestii (z wyjątkiem tych, które są przedmiotem dokumentacji medycznej lub informacji o uprzedniej karalności osoby powierzającej dane)

(i) bycie niepełnosprawnym fizycznie, niepełnosprawnym intelektualnie, cierpienie na zaburzenia psychiczne (w tym zaburzenia rozwojowe) lub bycie w inny sposób funkcjonalnie niepełnosprawnym fizycznie lub umysłowo określone w przepisach wydanych przez Komisję ds. Ochrony Informacji Osobowych;

(ii) wyniki badań lekarskich lub innych badań (dalej: „badania lekarskie itp.") przeprowadzonych w celu zapobiegania i wczesnego wykrywania chorób u osoby powierzającej dane przez lekarza lub inną osobę wykonująca obowiązki w zakresie medycyny (dalej: „lekarz lub inny pracownik medyczny");

(iii) przekazanie przez lekarza lub innego pracownika medycznego osobie powierzającej dane wytycznych dotyczących poprawy kondycji psychicznej i fizycznej lub opieki medycznej lub wydanie recepty na podstawie wyników badań lekarskich itp. lub ze względu na chorobę, obrażenia lub inne zmiany psychiczne i fizyczne;

(iv) aresztowanie, przeszukanie, zajęcie, zatrzymanie, wszczęcie postępowania karnego lub innych procedur związanych z postępowaniem karnym wobec osoby powierzającej dane jako podejrzanej lub oskarżonej;

([2]) Prawnie uzasadniona podstawa oznacza nadzwyczajne zdarzenie niezależne od podmiotu gospodarczego przetwarzającego informacje osobowe, którego nie można racjonalnie przewidzieć (na przykład klęski żywiołowe) lub sytuację, w której konieczność podjęcia działań przewidzianych w zaleceniu wydanym przez Komisję ds. Ochrony Informacji Osobowych na podstawie art. 42 ust. 1 ustawy przestała istnieć w związku z podjęciem przez podmiot gospodarczy przetwarzający informacje osobowe alternatywnych działań, które w całości pozwoliły zaradzić naruszeniu.

(v) przeprowadzenie postępowania przygotowawczego, działań w zakresie obserwacji i ochrony wobec osoby powierzającej dane, jako nieletniego przestępcy lub podejrzanego na podstawie art. 3 ust. 1 ustawy o przestępczości nieletnich, jej przesłuchanie zakończone wydaniem orzeczenia, zastosowanie wobec niej środka zabezpieczającego lub przeprowadzenie innej procedury w ramach ochrony nieletnich.

Art. 5 przepisów wykonawczych

Fizyczna i umysłowa niepełnosprawność funkcjonalna określona w przepisach Komisji ds. Ochrony Informacji Osobowych zgodnie z art. 2 ppkt (i) zarządzenia oznacza formy niepełnosprawności wymienione poniżej:

(i) niepełnosprawność fizyczną określoną w tabeli załączonej do ustawy o dobrobycie osób niepełnosprawnych fizycznie (ustawa nr 283 z 1949 r.)

(ii) niepełnosprawność intelektualną, o której mowa w ustawie o dobrobycie osób niepełnosprawnych intelektualnie (ustawa nr 37 z 1960 r.)

(iii) zaburzenia psychiczne, o których mowa w ustawie o zdrowiu psychicznym i dobrostanie osób z zaburzeniami psychicznymi (ustawa nr 123 z 1950 r.) (w tym zaburzenia rozwojowe, o których mowa w art. 2 ust. 1 ustawy o pomocy dla osób z zaburzeniami rozwojowymi, z wyłączeniem niepełnosprawności intelektualnej na mocy ustawy o dobrobycie osób niepełnosprawnych intelektualnie)

(iv) chorobę dla której nie ma przyjętych metod leczenia lub inne specyficzne choroby, których poważny charakter określony w zarządzeniu Rady Ministrów wydanym na podstawie art. 4 ust. 1 ustawy o kompleksowym wsparciu osób niepełnosprawnych w zakresie życia codziennego i społecznego (ustawa nr 123 z 2005 r.) jest równoważny temu określonemu przez Ministra Zdrowia, Pracy i Opieki Społecznej na podstawie wspomnianego ustępu.

Jeżeli dane osobowe otrzymywane z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony zawierają dane dotyczące życia seksualnego lub orientacji seksualnej osoby fizycznej lub przynależności do związków zawodowych, które określono w RODO jako szczególne kategorie danych osobowych, podmioty gospodarcze przetwarzające informacje osobowe są obowiązane przetwarzać te dane osobowe w taki sam sposób jak informacje osobowe wymagające szczególnej uwagi w rozumieniu art. 2 ust. 3 ustawy.

2. Zatrzymane dane osobowe (art. 2 ust. 7 ustawy)

Art. 2 ust. 7 ustawy

7. „Zatrzymane dane osobowe" w niniejszej ustawie oznaczają dane osobowe, które podmiot gospodarczy przetwarzający informacje osobowe ma prawo ujawnić, poprawić, uzupełnić lub usunąć ich treść, zaprzestać ich wykorzystywania, wymazać je oraz zaprzestać ich przekazywania osobom trzecim, a które nie są ani informacjami określonymi w zarządzeniu Rady Ministrów jako mogące zaszkodzić interesom publicznym lub innym interesom w przypadku ujawnienia informacji o ich występowaniu lub braku, ani informacjami, które mają zostać usunięte po okresie nie dłuższym niż rok, określonym w zarządzeniu Rady Ministrów.

Art. 4 zarządzenia Rady Ministrów

Dane określone w zarządzeniu Rady Ministrów, o którym mowa w art. 2 ust. 7, to dane zdefiniowane poniżej:

(i) dane osobowe, w związku z którymi istnieje prawdopodobieństwo, że podanie do wiadomości publicznej informacji o ich występowaniu bądź braku zaszkodzi życiu, zdrowiu lub majątkowi osoby powierzającej dane lub osoby trzeciej;

(ii) dane osobowe, w związku z którymi istnieje prawdopodobieństwo, że podanie do wiadomości publicznej informacji o ich występowaniu lub braku będzie zachęcać lub skłaniać do czynu bezprawnego lub niesprawiedliwego czynu;

(iii) dane osobowe, w związku z którymi istnieje prawdopodobieństwo, że podanie do wiadomości publicznej informacji o ich występowaniu lub braku będzie stanowić naruszenie bezpieczeństwa narodowego, zaburzy oparte na zaufaniu relacje z państwem obcym lub organizacją międzynarodową albo doprowadzi do niekorzystnych skutków w negocjacjach z państwem obcym lub organizacją międzynarodową;

(iv) dane osobowe, w związku z którymi istnieje prawdopodobieństwo, że podanie do wiadomości publicznej informacji o ich występowaniu lub braku utrudni działania mające na celu zachowanie bezpieczeństwa i porządku publicznego, takie jak zapobieganie przestępstwom, ich zwalczanie oraz prowadzenie dochodzeń w ich sprawie.

Art. 5 zarządzenia Rady Ministrów

Przewidziany w zarządzeniu Rady Ministrów okres, o którym mowa w art. 2 ust. 7 ustawy, wynosi sześć miesięcy.

Dane osobowe otrzymane z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony należy traktować jako zatrzymane dane osobowe w rozumieniu art. 2 ust. 7 ustawy, bez względu na okres, po upływie którego mają one zostać usunięte.

Jeżeli dane osobowe otrzymane z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony objęte są zakresem danych osobowych określonych w zarządzeniu Rady Ministrów jako „mogące zaszkodzić interesom publicznym lub innym interesom w przypadku ujawnienia informacji o ich występowaniu lub braku", nie wymaga się traktowania takich danych jako zatrzymanych danych osobowych (zob. art. 4 zarządzenia Rady Ministrów; Wytyczne do przepisów ogólnych, „2-7. „Zatrzymane dane osobowe").

3. Określenie celu wykorzystania, ograniczenie ze względu na cel wykorzystania (art. 15 ust. 1, art. 16, ust. 1 i art. 26 ust. 1 i 3 ustawy)

Art. 15 ust. 1 ustawy

1. Przy przetwarzaniu informacji osobowych podmiot gospodarczy przetwarzający informacje osobowe określa, w możliwie najbardziej wyraźny sposób, cel wykorzystania informacji osobowych (zwany dalej „celem wykorzystania").

Art. 16 ust. 1 ustawy

1. Bez uzyskania uprzedniej zgody osoby powierzającej dane podmiot gospodarczy przetwarzający informacje osobowe nie przetwarza informacji osobowych w stopniu wykraczającym poza zakres niezbędny do osiągnięcia celu wykorzystania tych informacji określonego zgodnie z przepisami poprzedniego artykułu.

Art. 26 ust. 1 i 3 ustawy

1. Po otrzymaniu danych osobowych od osoby trzeciej podmiot gospodarczy przetwarzający informacje osobowe potwierdza poniższe szczegóły na podstawie przepisów Komisji ds. Ochrony Informacji Osobowych: (pominięto)

   (i) (pominięto)

   (ii) okoliczności, w których osoba trzecia, o której mowa, uzyskała te dane osobowe

3. Po potwierdzeniu szczegółów, o których mowa w ust.1, podmiot gospodarczy przetwarzający informacje osobowe rejestruje, na podstawie przepisów Komisji ds. Ochrony Informacji Osobowych, dzień otrzymania tych danych osobowych, szczegóły potwierdzenia, o którym mowa, oraz inne szczegóły określone w przepisach Komisji ds. Ochrony Informacji Osobowych.

W przypadku gdy podmioty gospodarcze przetwarzające informacje osobowe przetwarzają informacje osobowe w stopniu wykraczającymi poza zakres niezbędny do osiągnięcia celu wykorzystania tych informacji, o którym mowa w art. 15 ust. 1 ustawy, obowiązane są uprzednio uzyskać zgodę osoby powierzającej dane (art. 16 ust. 1 ustawy). Po otrzymaniu danych osobowych od osoby trzeciej podmioty gospodarcze przetwarzające informacje osobowe potwierdzają, zgodnie z przepisami wykonawczymi, szczegóły takie jak okoliczności, w których osoba trzecia, o której mowa, uzyskała te dane osobowe, oraz rejestrują te szczegóły (art. 26 ust. 1 i 3 ustawy).

W przypadku gdy podmiot gospodarczy przetwarzający informacje osobowe otrzymuje dane osobowe z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, okoliczności dotyczące uzyskania tych danych osobowych, które należy potwierdzić i zarejestrować zgodnie z art. 26 ust. 1 i 3, obejmują cel wykorzystania, w związku z którym otrzymano te dane z UE.

Analogicznie w przypadku gdy podmiot gospodarczy przetwarzający informacje osobowe otrzymuje od innego podmiotu gospodarczego przetwarzającego informacje osobowe dane osobowe uprzednio przekazane z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, okoliczności dotyczące uzyskania wspomnianych danych osobowych, które należy potwierdzić i zarejestrować zgodnie z art. 26 ust. 1 i 3, obejmują cel wykorzystania, w związku z którym otrzymano te dane z UE.

W powyższych przypadkach podmiot gospodarczy przetwarzający informacje osobowe jest obowiązany określić cel wykorzystania tych danych osobowych w zakresie celu wykorzystania, w związku z którym dane te pierwotnie lub wtórnie otrzymał, zgodnie z tym, co potwierdzono i zarejestrowano zgodnie z art. 26 ust. 1 i 3, oraz do wykorzystania tych danych w tym zakresie (na podstawie art. 15 ust. 1 i art. 16 ust. 1 ustawy).

4. Ograniczenie przekazywania danych osobie trzeciej w państwie obcym (art. 24 ustawy; art. 11-2 przepisów wykonawczych)

Art. 24 ustawy

Z wyjątkiem przypadków określonych w poszczególnych podpunktach ust. 1 poprzedniego artykułu podmiot gospodarczy przetwarzający informacje osobowe, przekazując dane osobowe osobie trzeciej (z wyłączeniem osób ustanawiających system zgodny ze standardami określonymi w przepisach Komisji ds. Ochrony Informacji Osobowych jako niezbędny do ciągłego podejmowania działań równoważnych tym, jakie podmiot gospodarczy przetwarzający informacje osobowe podejmuje w odniesieniu do przetwarzania danych osobowych na podstawie przepisów niniejszej sekcji; w dalszej części niniejszego artykułu tak samo) w państwie obcym (tzn. państwie lub regionie położonym poza terytorium Japonii; dalej tak samo) (z wyłączeniem tych określonych w przepisach Komisji ds. Ochrony Informacji Osobowych jako państwa obce ustanawiające system ochrony informacji osobowych o ramach równoważnych tym obowiązującym w Japonii w odniesieniu do ochrony praw i interesów jednostki; w dalszej części niniejszego artykułu tak samo) uzyskuje uprzednio zgodę osoby powierzającej dane na przekazanie danych osobie trzeciej w państwie obcym. W tym przypadku postanowienia poprzedniego artykułu nie mają zastosowania.

Art. 11-2 przepisów wykonawczych

Standardy określone w przepisach Komisji ds. Ochrony Informacji Osobowych, o których mowa w art. 24 ustawy, powinny podlegać któremukolwiek z poniższych podpunktów:

(i) podmiot gospodarczy przetwarzający informacje osobowe oraz osoba, która otrzymuje przekazywane dane osobowe, zapewniły w odniesieniu do przetwarzania danych osobowych przez osobę, która otrzymuje te dane, wdrożenie, w odpowiedni i racjonalny sposób, środków zgodnych z treścią przepisów rozdziału IV sekcji 1 ustawy;

(ii) osoba otrzymująca dane osobowe została uznana na podstawie norm międzynarodowych dotyczących przetwarzania informacji osobowych.

W przypadku przekazywania osobie trzeciej w państwie obcym danych osobowych, które podmiot gospodarczy przetwarzający informacje osobowe otrzymał z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, podmiot ten uzyskuje uprzednią zgodę osoby powierzającej dane na przekazanie danych osobie trzeciej w państwie obcym na podstawie art. 24 ustawy po otrzymaniu informacji o okolicznościach przekazania niezbędnych do podjęcia decyzji o wyrażeniu zgody przez osobę powierzającą dane, z wyjątkiem przypadków objętych jednym z poniższych podpunktów (i)–(iii):

(i) jeżeli osoba trzecia znajduje się w państwie określonym w przepisach Komisji ds. Ochrony Informacji Osobowych jako państwo obce ustanawiające system ochrony informacji osobowych o ramach równoważnych tym obowiązującym w Japonii w odniesieniu do ochrony praw i interesów jednostki;

(ii) jeżeli podmiot gospodarczy przetwarzający informacje osobowe i osoba trzecia otrzymująca dane osobowe wspólnie wdrożyły, w odniesieniu do przetwarzania danych osobowych przez osobę trzecią, środki zapewniające poziom ochrony równoważny temu, który zapewnia ustawa w związku z niniejszymi przepisami wykonawczymi, w odpowiedni i racjonalny sposób (tj. umownie, na podstawie innego prawnie wiążącego porozumienia lub wiążących uzgodnień w ramach grupy przedsiębiorstw).

(iii) w przypadkach objętych poszczególnymi podpunktami art. 23 ust. 1 ustawy

5. Informacje przetwarzane anonimowo (art. 2 ust. 9 i art. 36 ust. 1 i 2 ustawy)

Art. 2 ust. 9 ustawy

9. „Informacje przetwarzane anonimowo" oznaczają w niniejszej ustawie informacje dotyczące osoby fizycznej, które można sporządzić na podstawie przetwarzania informacji osobowych, tak aby nie były możliwe ani identyfikacja określonej osoby w wyniku działań określonych w poniższych podpunktach zgodnie z podziałem informacji osobowych określonym w każdym z tych podpunktów, ani odtworzenie informacji osobowych.

(i) informacje osobowe wchodzące w zakres ust. 1 ppkt (i);

Usuwanie części opisów itp. zawartych w informacjach osobowych (w tym zastąpienie takiej części opisów itp. innymi opisami itp. przy użyciu metody nieobejmującej regularnych schematów, które umożliwiłyby przywrócenie tej części opisów itp.);

(ii) informacje osobowe wchodzące w zakres ust. 1 ppkt (ii);

Usuwanie wszystkich indywidualnych kodów identyfikacyjnych zawartych w informacjach osobowych (w tym zastąpienie takich kodów innymi opisami itp. przy użyciu metody nieobejmującej regularnych schematów, które umożliwiłyby przywrócenie indywidualnych kodów identyfikacyjnych)

Art. 36 ust. 1 ustawy

1. Przy sporządzaniu informacji przetwarzanych anonimowo (ograniczonych do tych, które stanowią informacje przetwarzane anonimowo stanowiące bazę danych osobowych itp.; dalej tak samo) podmiot gospodarczy przetwarzający informacje osobowe przetwarza te informacje zgodnie ze standardami określonymi w przepisach Komisji ds. Ochrony Informacji Osobowych jako niezbędne do uniemożliwienia identyfikacji określonej osoby i przywrócenia informacji osobowych wykorzystanych do ich sporządzenia.

Art. 19 przepisów wykonawczych

Standardy określone w przepisach wykonawczych Komisji ds. Ochrony Informacji Osobowych na mocy art. 36 ust. 1 ustawy są następujące:

(i) usuwanie całości lub części tych opisów itp., które umożliwiają identyfikację określonej osoby fizycznej, zawartych w informacjach osobowych (w tym zastąpienie takich opisów itp. innymi opisami itp. przy użyciu metody nieobejmującej regularnych schematów, które umożliwiłyby przywrócenie całości lub części opisów itp.);

(ii) usuwanie wszystkich indywidualnych kodów identyfikacyjnych zawartych w informacjach osobowych (w tym zastąpienie takich kodów innymi opisami itp. przy użyciu metody nieobejmującej regularnych schematów, które umożliwiłyby przywrócenie indywidualnych kodów identyfikacyjnych);

(iii) usuwanie tych kodów (ograniczonych do kodów wiążących między sobą różne informacje, które są w rzeczywistości przetwarzane przez podmiot gospodarczy przetwarzający informacje osobowe), które łączą informacje osobowe i informacje uzyskane w wyniku zastosowania środków wobec informacji osobowych (w tym zastąpienie rzeczonych kodów innymi kodami, które nie pozwalają na powiązanie informacji osobowych, o których mowa, z informacjami uzyskanymi dzięki zastosowaniu środków wobec informacji osobowych, przy użyciu metody nieobejmującej regularnych schematów, które umożliwiłyby przywrócenie tych kodów);

(iv) usuwanie idiosynkratycznych opisów itp. (w tym zastąpienie takich opisów itp. innymi opisami itp. przy użyciu metody nieobejmującej regularnych schematów, które umożliwiłyby przywrócenie idiosynkratycznych opisów itp.);

(v) oprócz działań określonych w każdym poprzedzającym punkcie, podejmowanie odpowiednich działań w oparciu o wyniki, z uwzględnieniem atrybutu itp. bazy informacji osobowych itp. takich jak różnica między opisami itp. zawartymi w informacji osobowych i opisami itp. zawartymi w innych informacji osobowych stanowiących bazę informacji osobowych itp., które obejmują wspomniane informacje osobowe.

Art. 36 ust. 2 ustawy

2. Podmiot gospodarczy przetwarzający informacje osobowe, który sporządził informacje przetwarzane anonimowo, podejmuje działania w celu kontroli bezpieczeństwa takich informacji, zgodnie ze standardami określonymi w przepisach wykonawczych Komisji ds. Ochrony Informacji Osobowych jako niezbędne, by zapobiec wyciekowi informacji związanych z tymi opisami itp. i kodami identyfikacyjnymi usuniętymi z informacji osobowych wykorzystanych do sporządzenia informacji przetwarzanych anonimowo, a także informacji dotyczących metody przetwarzania stosowanej zgodnie z przepisami poprzedniego ustępu.

Art. 20 przepisów wykonawczych

Standardy określone w przepisach wykonawczych Komisji ds. Ochrony Informacji Osobowych na mocy art. 36 ust. 2 ustawy są następujące:

(i) wyraźne określenie organu i zakresu odpowiedzialności osoby przetwarzającej informacje dotyczące tych opisów itp. oraz indywidualnych kodów identyfikacyjnych, które zostały usunięte z informacji osobowych wykorzystywanych do sporządzania informacji przetwarzanych anonimowo i informacji dotyczących metody przetwarzania przeprowadzonego zgodnie z przepisami art. 36 ust. 1 (ograniczone do tych elementów, które umożliwiają przywrócenie informacji osobowych za pomocą takich informacji) (zwane dalej w niniejszym artykule „informacjami dotyczącymi metody przetwarzania itp.");

(ii) określenie zasad i procedur postępowania z informacjami dotyczącymi metody przetwarzania itp., właściwego obchodzenia się z informacjami dotyczącymi metody przetwarzania itp. zgodnie z zasadami i procedurami, oceny sytuacji w zakresie obchodzenia się z informacjami oraz – w oparciu o wyniki takiej oceny – podejmowania niezbędnych działań w celu poprawy sytuacji;

(iii) podejmowanie koniecznych i odpowiednich działań mających na celu uniemożliwienie osobie, która nie posiada odpowiednich uprawnień, przetwarzania informacji dotyczących metody przetwarzania itp.

Informacje osobowe otrzymane z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony oznaczają informacje przetwarzane anonimowo w rozumieniu art. 2 ust. 9 ustawy wyłącznie w przypadku, gdy podmiot gospodarczy przetwarzający informacje osobowe podejmuje środki, które powodują dla każdego nieodwracalność anonimizacji poszczególnych osób, w tym poprzez usunięcie informacji dotyczących metody przetwarzania itp. (tj. informacji o tych opisach itp. i indywidualnych kodów identyfikacyjnych, które zostały usunięte z informacji osobowych wykorzystanych do sporządzenia anonimowo przetwarzanych informacji i informacji dotyczących metody przetwarzania przeprowadzonego zgodnie z przepisami art. 36 ust. 1 ustawy (ograniczone do tych elementów, które umożliwiają przywrócenie informacji osobowych za pomocą takich powiązanych informacji)).

ZAŁĄCZNIK 2

Jej Ekscelencja Věra Jourová, komisarz do spraw sprawiedliwości, konsumentów i równouprawnienia płci, Komisja Europejska

Ekscelencjo,

z zadowoleniem przyjmuję konstruktywną dyskusję między Japonią a Komisją Europejską w celu stworzenia ram wzajemnego przekazywania danych osobowych między Japonią a UE.

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

Niniejszy dokument dotyczy wielu japońskich ministerstw i agencji rządowych; jeżeli chodzi o treść dokumentu, właściwe ministerstwa i agencje (sekretariat Rady Ministrów, Agencja Policji Krajowej, Komisja ds. Ochrony Informacji Osobowych, Ministerstwo Spraw Wewnętrznych i Komunikacji, Ministerstwo Sprawiedliwości, Agencja Bezpieczeństwa Publicznego, Ministerstwo Obrony) odpowiadają za poszczególne obszary wchodzące w zakres ich kompetencji. Właściwe ministerstwa i agencje oraz osoby, które podpisały w ich imieniu dokument, wymieniono poniżej.

Komisja ds. 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 Pani wielki wkład w tę problematykę.

Z wyrazami szacunku

Yoko Kamikawa

Minister Sprawiedliwości

Niniejszy dokument został sporządzony przez Ministerstwo Sprawiedliwości oraz następujące zainteresowane ministerstwa i agencje.

Koichi Hamano

Radca, Sekretariat Rady Ministrów

Schunichi Kuryu

Komisarz Generalny Agencji Policji Krajowej

Mari Sonoda

Sekretarz Generalny, Komisja ds. Ochrony Informacji Osobowych

Mitsuru Yasuda

Wiceminister, Ministerstwo Spraw Wewnętrznych i Komunikacji

Seimei Nakagawa

Agencja Bezpieczeństwa Publicznego

Kenichi Takahashi

Wiceminister Obrony do spraw Administracyjnych

14 września 2018 r.

Zbieranie i wykorzystywanie informacji osobowych przez japońskie 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 (w formie elektronicznej) przez japońskie 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, w tym niezależnego nadzoru i możliwości indywidualnego dochodzenia roszczeń. Dokument ten skierowany jest do Komisji Europejskiej, aby sformułować zobowiązanie i zapewnić, że dostęp rządowy do informacji osobowych przekazywanych z UE do Japonii będzie ograniczony do tego, co jest konieczne i proporcjonalne, oraz będzie objęty niezależnym nadzorem, a zainteresowane osoby fizyczne będą mogły dochodzić roszczeń w razie naruszenia ich podstawowego prawa do prywatności i ochrony danych. W dokumencie przewidziano również utworzenie nowego mechanizmu dochodzenia roszczeń, zarządzanego przez Komisję ds. Ochrony Informacji Osobowych, którego celem będzie rozpatrywanie skarg osób fizycznych z UE dotyczących dostępu rządowego do ich danych osobowych przekazywanych z UE do Japonii.

I. **Ogólne zasady prawne regulujące dostęp rządowy**

W ramach wykonywania władzy publicznej umożliwienie dostępu rządowego musi przebiegać przy pełnym poszanowaniu prawa (zasada legalności). W Japonii informacje osobowe są chronione zarówno w sektorze prywatnym, jak i w sektorze publicznym, w ramach mechanizmu wielowarstwowego.

A. Ramy konstytucyjne i zastrzeżenie praworządności

Art. 13 konstytucji i orzecznictwo uznają prawo do prywatności za prawo konstytucyjne. W tym względzie Sąd Najwyższy orzekł, iż jest rzeczą naturalną, że osoby fizyczne nie chcą, aby inne osoby znały, bez należytego uzasadnienia, ich informacje osobowe, oraz że oczekiwania te należy chronić ([1]). Dalsze środki ochrony zagwarantowano w art. 21 ust. 2 konstytucji, który zapewnia przestrzeganie tajemnicy komunikacji, oraz art. 35 konstytucji, zgodnie z którym każdy ma prawo do nienaruszalności dokumentów i mienia przed rewizją i zajęciem, chyba że został wydany nakaz, co oznacza, że zbieranie informacji osobowych, w tym dostęp, za pomocą środków przymusowych zawsze wymaga wydania nakazu sądowego. Nakaz taki może zostać wydany jedynie w celu przeprowadzenia postępowania przygotowawczego dotyczącego popełnionego już przestępstwa. W związku z tym w japońskich ramach prawnych zbieranie informacji za pomocą środków przymusowych do celów bezpieczeństwa narodowego (a nie prowadzenia postępowania przygotowawczego w sprawie karnej) nie jest dozwolone.

Co więcej, zgodnie z zasadą zastrzeżenia praworządności, przymusowe zbieranie informacji każdorazowo wymaga podstawy prawnej. Jeżeli chodzi o nieobowiązkowe/dobrowolne zbieranie informacji, uzyskuje się je ze swobodnie dostępnego źródła lub otrzymuje na podstawie wniosku o dobrowolne ujawnienie, tj. wniosku, który nie podlega wyegzekwowaniu w stosunku do osoby fizycznej lub prawnej posiadającej informacje. Jest to jednak dopuszczalne tylko w takim zakresie, w jakim organ publiczny jest właściwy do prowadzenia postępowania wyjaśniającego, biorąc pod uwagę, że każdy organ publiczny może działać wyłącznie w prawem określonych granicach jego właściwości administracyjnej (niezależnie od tego, czy jego działalność ingeruje w prawa i wolności osób fizycznych). Zasada ta ma zastosowanie do możliwości zbierania informacji osobowych przez dany organ.

B. Szczegółowe zasady dotyczące ochrony informacji osobowych

Ustawa o ochronie informacji osobowych oraz ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji, które mają swoją podstawę w konstytucji i doprecyzowują ją, gwarantują prawo do ochrony informacji osobowych zarówno w sektorze prywatnym, jak i publicznym.

Art. 7 ustawy o ochronie informacji osobowych stanowi, że Komisja ds. Ochrony Informacji Osobowych opracowuje „podstawową politykę ochrony informacji osobowych" („polityka podstawowa"). Polityka podstawowa, przyjmowana decyzją Rady Ministrów Japonii jako organu centralnego japońskiego rządu (premier i ministrowie państwa), określa kierunki ochrony informacji osobowych w Japonii. W ten sposób Komisja ds. Ochrony Informacji Osobowych, jako niezależny organ nadzorczy, pełni funkcję „centrum dowodzenia" japońskiego systemu ochrony informacji osobowych.

Organy administracyjne, które zbierają informacje osobowe – niezależnie od tego, czy czynią to za pomocą środków przymusowych, czy też nie – co do zasady ([2]) obowiązane są spełniać wymogi określone w ustawie o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji. Ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji to ogólna ustawa regulująca przetwarzanie „przechowywanych informacji osobowych" ([3]) przez „organy administracyjne" (w rozumieniu art. 2 ust. 1 tej ustawy). W związku z tym obejmuje ona również

([1]) Sąd Najwyższy, wyrok z dnia 12 września 2003 r. (2002 (Ju) nr 1656).

([2]) Wyjątki dotyczące rozdziału 4 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji można znaleźć poniżej na stronie 16.

([3]) „Zatrzymane informacje osobowe" w art. 2 ust. 5 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji oznaczają informacje osobowe przygotowane lub uzyskane przez pracownika organu administracyjnego w ramach pełnienia przez niego obowiązków służbowych i znajdujące się w posiadaniu danego organu administracyjnego do wykorzystania do celów organizacyjnych przez jego pracowników.

przetwarzanie danych w obszarze ścigania przestępstw i w obszarze bezpieczeństwa narodowego. Spośród organów publicznych uprawnionych do korzystania z dostępu rządowego wszystkie organy, z wyjątkiem policji prefekturalnej, są krajowymi organami rządowymi, które są objęte zakresem pojęcia „organy administracyjne". Przetwarzanie informacji osobowych przez policję prefekturalną jest regulowane rozporządzeniami prefekturalnymi ([4]), które określają zasady ochrony informacji osobowych oraz prawa i obowiązki równoważne z tymi określonymi w ustawie o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji.

II. **Dostęp rządowy do celów ścigania przestępstw**

A. Podstawa prawna i ograniczenia

1. Zbieranie informacji osobowych za pomocą środków przymusu

a) Podstawa prawna

Zgodnie z art. 35 konstytucji każdy ma prawo do nienaruszalności swego domostwa, dokumentów i mienia przed wtargnięciem, rewizją i zajęciem, chyba że z uzasadnionych przyczyn został wydany nakaz określający szczegółowo miejsce podlegające rewizji oraz rzeczy podlegające zajęciu. W związku z tym przymusowe zbieranie informacji elektronicznych przez organy publiczne w ramach postępowania przygotowawczego dotyczącego sprawy karnej może odbywać się wyłącznie na podstawie nakazu sądowego. Odnosi się to zarówno do zbierania zapisów elektronicznych zawierających informacje (osobowe), jak i do przechwytywania komunikacji w czasie rzeczywistym (tzw. podsłuchów). Jedynym wyjątkiem od tej zasady (który nie jest jednak istotny w kontekście elektronicznego przekazywania informacji osobowych z zagranicy) jest art. 220 ust. 1 kodeksu postępowania karnego ([5]), zgodnie z którym w razie aresztowania podejrzanego lub „sprawcy rażącego przestępstwa" prokurator, asystent prokuratora lub funkcjonariusz policji sądowej może, w razie konieczności, dokonać przeszukania i zajęcia „w miejscu zatrzymania".

Zgodnie z art. 197 ust. 1 kodeksu postępowania karnego przymusowe środki ścigania „nie są stosowane, chyba że przepisy szczególne niniejszego kodeksu stanowią inaczej". Jeżeli chodzi o przymusowe zbieranie informacji elektronicznych, odpowiednia podstawa prawna w tym zakresie to art. 218 ust. 1 kodeksu postępowania karnego (zgodnie z którym prokurator, asystent prokuratora lub funkcjonariusz policji sądowej może – jeżeli to konieczne do przeprowadzenia postępowania przygotowawczego dotyczącego przestępstwa – przeprowadzić przeszukanie, zajęcie lub kontrolę na podstawie nakazu wydanego przez sędziego) oraz art. 222-2 kodeksu postępowania karnego (zgodnie z którym przymusowe środki przechwytywania komunikacji elektronicznej bez zgody którejkolwiek ze stron będą wykonywane na podstawie innych ustaw). Ten ostatni przepis odnosi się do ustawy o zakładaniu podsłuchów na potrzeby postępowań przygotowawczych (ustawa o podsłuchach), która w art. 3 ust. 1 określa warunki, zgodnie z którymi komunikacja dotycząca niektórych poważnych przestępstw może być podsłuchiwana na podstawie nakazu wydanego przez sędziego ([6]).

Jeżeli chodzi o policję, organem ścigania jest we wszystkich przypadkach policja prefekturalna, natomiast Agencja Policji Krajowej nie wykonuje w tym zakresie żadnych funkcji na podstawie kodeksu postępowania karnego.

b) Ograniczenia

Przymusowe zbieranie informacji elektronicznych jest ograniczone konstytucją i statutami kompetencyjnymi, zgodnie z wykładnią zawartą w orzecznictwie, która w szczególności określa kryteria stosowane przez sądy podczas wydawania nakazu sądowego. Ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji ustanawia również szereg ograniczeń w zakresie zarówno zbierania informacji, jak i ich przetwarzania (przy czym regulacje lokalne nakładają zasadniczo te same kryteria na policję prefekturalną).

1) Ograniczenia wynikające z konstytucji i statutu kompetencyjnego

Zgodnie z art. 197 ust. 1 kodeksu postępowania karnego środki przymusowe nie są stosowane, chyba że przepisy szczególne kodeksu stanowią inaczej. Art. 218 ust. 1 kodeksu postępowania karnego stanowi natomiast, że zajęcie itp. może być przeprowadzone na podstawie nakazu wydanego przez sędziego jedynie „jeżeli jest to konieczne do

([4]) W każdej prefekturze obowiązują odrębne „regulacje prefekturalne" w zakresie ochrony informacji osobowych przez policję prefekturalną. Regulacje te nie zostały przetłumaczone na języki angielski.

([5]) Art. 220 ust. 1 kodeksu postępowania karnego przewiduje, że w przypadku gdy prokurator, asystent prokuratora lub funkcjonariusz policji sądowej aresztuje podejrzanego, może, w razie konieczności, zastosować następujące środki: a) wejście do miejsca zamieszkania innej osoby itp. w celu poszukiwania podejrzanego; b) przeszukanie, zajęcie lub kontrola na miejscu w chwili zatrzymania.

([6]) Przepis ten przewiduje w szczególności, że „prokurator lub policja sądowa mogą – w przypadkach wchodzących w zakres którejkolwiek z poniższych pozycji, gdy zachodzą okoliczności pozwalające podejrzewać, że będzie miała miejsce komunikacja dotycząca ustaleń, przygotowań, zmowy dotyczącej działań następczych takich jak niszczenie dowodów itp., instrukcji i innych informacji dotyczących przestępstw określonych w każdej z wymienionych pozycji (zwanych dalej »serią przestępstw« w drugiej i trzeciej pozycji), a także komunikacja obejmująca sprawy związane z przestępstwem (zwana dalej »komunikacją dotyczącą przestępstw« w niniejszym ustępie), a także w przypadkach, w których niezwykle trudno jest zidentyfikować przestępcę lub w inny sposób ustalić okoliczności/szczegóły dotyczące popełnienia przestępstwa – prowadzić podsłuch komunikacji dotyczącej przestępstw, na podstawie sądowego nakazu założenia podsłuchu, który to nakaz określa numer telefonu i inne numery/kody w celu identyfikacji źródła lub miejsca przeznaczenia rozmowy telefonicznej, które podejrzany wykorzystuje na podstawie umowy z operatorami telekomunikacyjnymi itp. (z wyjątkiem komunikacji, które można uznać za niebudzące podejrzeń jako »komunikacja dotycząca przestępstw«), a w odniesieniu do komunikacji, co do których istnieją podstawy, by podejrzewać, że są wykorzystywane jako »komunikacja dotycząca przestępstw«, możliwe jest prowadzenie podsłuchu komunikacji dotyczącej przestępstw za pomocą tych środków komunikacji".

przeprowadzenia postępowania przygotowawczego w sprawie przestępstwa". Chociaż kryteria oceny niezbędności nie zostały doprecyzowane w aktach rangi ustawowej, Sąd Najwyższy ([7]) orzekł, że przy ocenie konieczności zastosowania środków sędzia powinien dokonać ogólnej oceny, biorąc pod uwagę w szczególności następujące elementy:

a) wagę przestępstwa i sposób jego popełnienia;

b) wartość i znaczenie materiałów zajętych jako dowody;

c) prawdopodobieństwo ukrycia lub zniszczenia zajętych materiałów;

d) zakres niedogodności spowodowanych zajęciem;

e) inne powiązane warunki.

Ograniczenia wynikają również z wymogu zawartego w art. 35 konstytucji, dotyczącego wykazania „uzasadnionej przyczyny". W ramach standardu wymagającego wskazania „uzasadnionej przyczyny" nakazy sądowe można wydawać, jeżeli: [1] istnieje konieczność prowadzenia postępowania przygotowawczego w sprawie karnej (zob. wyrok Sądu Najwyższego z dnia 18 marca 1969 r. (1968 (Shi) nr 100), o którym mowa powyżej); [2] w danym przypadku uznaje się, że podejrzany (oskarżony) popełnił przestępstwo (art. 156 ust. 1 kodeksu postępowania karnego) ([8]). [3] Sądowy nakaz ścigania w odniesieniu do osoby innej niż oskarżony oraz rzeczy, miejsca zamieszkania lub innego miejsca pobytu takiej osoby należy wydawać wyłącznie wtedy, gdy zachodzi uzasadnione przypuszczenie, że rzeczy, które mają zostać zajęte, istnieją (art. 102 ust. 2 kodeksu postępowania karnego). Jeżeli sędzia uzna, że przedstawione przez organy ścigania dowody w postaci dokumentów nie stanowią wystarczającej podstawy do uznania, że mogło dojść do popełnienia przestępstwa, oddali wniosek o wydanie nakazu. W tym względzie należy zauważyć, że zgodnie z ustawą o karalności przestępczości zorganizowanej i kontroli dochodów z przestępstw „działania przygotowawcze do popełnienia" planowanego przestępstwa (np. przygotowanie pieniędzy na popełnienie przestępstwa terrorystycznego) same w sobie stanowią przestępstwo i w związku z tym mogą być przedmiotem przymusowego postępowania przygotowawczego na podstawie nakazu.

Jeżeli nakaz sądowy dotyczy natomiast przeprowadzenia postępowania przygotowawczego w sprawie osoby innej niż podejrzany lub oskarżony oraz rzeczy, miejsca zamieszkania lub innego miejsca pobytu takiej osoby, nakaz ten należy wydać wyłącznie wtedy, gdy zachodzi uzasadnione przypuszczenie, że rzeczy, które mają zostać zajęte, istnieją (art. 102 ust. 2 oraz art. 222 ust. 1 kodeksu postępowania karnego).

W szczególności, jeżeli chodzi o przechwytywanie komunikacji do celów prowadzenia postępowań przygotowawczych w sprawach karnych na podstawie ustawy o podsłuchach, przechwytywanie to można prowadzić wyłącznie po spełnieniu rygorystycznych wymogów określonych w art. 3 ust. 1. Zgodnie z tym przepisem przechwytywanie zawsze wymaga uprzedniego nakazu sądowego, który może zostać wydany jedynie w szczególnych sytuacjach ([9]).

2) Ograniczenia wynikające z ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji

Jeżeli chodzi o zbieranie ([10]) i dalsze przetwarzanie informacji osobowych (w szczególności ich zatrzymywanie, zarządzanie nimi i wykorzystywanie ich) przez organy administracyjne, ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji ustanawia w szczególności następujące ograniczenia:

a) Zgodnie z art. 3 ust. 1 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji organy administracyjne mogą przechowywać informacje osobowe jedynie wówczas, gdy zatrzymanie jest niezbędne do wykonywania obowiązków wchodzących w zakres ich właściwości zgodnie z przepisami ustawowymi i wykonawczymi. W chwili zatrzymania są one również obowiązane określić (w miarę możliwości) cel wykorzystania informacji osobowych. Zgodnie z art. 3 ust. 2 i 3 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji organy administracyjne nie zatrzymują informacji osobowych wykraczających poza zakres niezbędny do osiągnięcia celu ich wykorzystania oraz nie zmieniają celu ich wykorzystania ponad to, co można w sposób uzasadniony uznać za właściwe dla celu pierwotnego.

b) Art. 5 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji stanowi, że dyrektor organu administracyjnego dokłada starań, aby utrzymać dokładność i aktualność zatrzymanych informacji osobowych w zakresie niezbędnym do osiągnięcia celu ich wykorzystania.

c) Art. 6 ust. 1 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji stanowi, że dyrektor organu administracyjnego wprowadza środki niezbędne w celu zapobiegania wyciekom, utracie lub zniszczeniu zatrzymanych informacji osobowych oraz w celu właściwego zarządzania tymi informacjami.

d) Zgodnie z art. 7 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji żaden pracownik (w tym żaden były pracownik) nie może ujawniać uzyskanych informacji osobowych innej osobie bez uzasadnionego powodu ani wykorzystywać takich informacji do celu niegodziwego.

([7]) Wyrok z dnia 18 marca 1969 r. (1968 (Shi) nr 100).

([8]) Art. 156 ust. 1 kodeksu postępowania karnego stanowi: „Występując z wnioskiem, o którym mowa w ust. 1 poprzedniego artykułu, wnioskodawca dostarcza materiały, na podstawie których powinno się uznać, że podejrzany lub oskarżony popełnił przestępstwo".

([9]) Zob. przypis 6.

([10]) Art. 3 ust. 1 i 2 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji ograniczają zakres zatrzymania, a tym samym również zbierania informacji osobowych.

e) Art. 8 ust. 1 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji stanowi ponadto, że dyrektor organu administracyjnego nie może wykorzystywać lub dostarczać innej osobie zatrzymanych informacji osobowych do celów innych niż określony cel stosowania, chyba że przepisy ustawowe i wykonawcze stanowią inaczej. Podczas gdy art. 8 ust. 2 zawiera wyjątki od tej reguły w szczególnych sytuacjach, mają one zastosowanie jedynie wówczas, gdy takie wyjątkowe ujawnienie nie wywoła „niesprawiedliwego" naruszenia praw i interesów osoby, której dane dotyczą, lub osoby trzeciej.

f) Zgodnie z art. 9 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji, jeżeli zatrzymane informacje osobowe przekazuje się innej osobie, dyrektor organu administracyjnego nakłada w razie potrzeby ograniczenia dotyczące celu lub sposobu wykorzystania tych informacji lub wszelkie inne niezbędne ograniczenia; może również wymagać od osoby otrzymującej informacje wprowadzenia środków niezbędnych do zapobiegania wyciekowi i właściwego zarządzania informacjami.

g) Art. 48 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji stanowi, że dyrektor organu administracyjnego dokłada starań, by sprawnie i właściwie rozpatrzyć wszystkie wnioski dotyczące postępowania z informacjami osobowymi.

2. Zbieranie informacji osobowych za pomocą wniosków o dobrowolną współpracę (Dobrowolne prowadzenie postępowań przygotowawczych)

a) Podstawa prawna

Oprócz stosowania środków przymusowych informacje osobowe uzyskuje się również ze źródła, które jest swobodnie dostępne, lub na podstawie wniosku o dobrowolne ujawnienie, w tym przez podmioty gospodarcze przechowujące takie informacje.

Jeżeli chodzi o ten ostatni sposób, art. 197 ust. 2 kodeksu postępowania karnego uprawnia prokuraturę i policję sądową do dokonywania pisemnych zapytań w kwestiach dotyczących postępowania (tzw. „karty z zapytaniem"). Na podstawie kodeksu postępowania karnego osoby, do których skierowano zapytanie, są proszone o przekazanie informacji organom śledczym. Nie ma jednak sposobu, aby zmusić je do takiego przekazania informacji, jeżeli urzędy publiczne lub organizacje publiczne lub prywatne, które otrzymały zapytanie, odmówią wykonania swoich obowiązków w tym zakresie. Jeżeli nie odpowiedzą one na zapytanie, nie można nałożyć na nie kary ani innych sankcji. Jeżeli organy śledcze uznają, że wymagane informacje są niezbędne, mogą uzyskać takie informacje w drodze przeszukania i zajęcia na podstawie nakazu sądowego.

Ze względu na rosnącą świadomość osób fizycznych w kwestii ich prawa do prywatności oraz biorąc pod uwagę nakład pracy związany z rozpatrywaniem takich wniosków, podmioty gospodarcze zachowują coraz większą ostrożność przy udzielaniu na nie odpowiedzi ([11]). Przy podejmowaniu decyzji o współpracy podmioty gospodarcze biorą w szczególności pod uwagę charakter wymaganych informacji, stosunki tych podmiotów z osobą, której dotyczą informacje, narażenie ich reputacji, ryzyko sporów prawnych itp.

b) Ograniczenia

Jeżeli chodzi o przymusowe zbieranie informacji elektronicznych, dobrowolne prowadzenie postępowań przygotowawczych jest ograniczone przez konstytucję, zgodnie z interpretacją orzecznictwa, oraz przez statut kompetencyjny. Ponadto w pewnych sytuacjach podmioty gospodarcze nie są prawnie upoważnione do ujawniania informacji. Ustawa ustanawia również szereg ograniczeń mających zastosowanie zarówno do zbierania informacji, jak i ich przetwarzania (przy czym regulacje lokalne nakładają zasadniczo te same kryteria na policję prefekturalną).

1) Ograniczenia wynikające z konstytucji i statutu kompetencyjnego

Mając na uwadze cel art. 13 konstytucji, Sąd Najwyższy nałożył ograniczenia wobec prowadzenia postępowań przygotowawczych przez organy śledcze dwoma decyzjami – (1965 (A) nr 1187) z 24 grudnia 1969 r. i (2007 (A) nr 839) z 15 kwietnia 2008 r. Decyzje te dotyczyły wprawdzie przypadków, w których informacje osobowe (w formie obrazów) były zbierane za pomocą fotografii/filmowania, jednak ustalenia mają również zastosowanie do dobrowolnych (nieprzymusowych) postępowań przygotowawczych, które zasadniczo naruszają prywatność osoby fizycznej. Mają zatem zastosowanie i należy ich przestrzegać w odniesieniu do zbierania informacji osobowych w drodze dobrowolnego postępowania przygotowawczego, uwzględniając szczególne okoliczności każdego przypadku.

Według tych decyzji zgodność z prawem dobrowolnego postępowania przygotowawczego zależy od spełnienia trzech kryteriów, a mianowicie:

— „podejrzenie popełnienia przestępstwa" (tj. należy ocenić, czy popełniono przestępstwo),

— „konieczność przeprowadzenia postępowania przygotowawczego" (tj. należy ocenić, czy wniosek nie wykracza poza to, co jest niezbędne do celów postępowania przygotowawczego), oraz

([11]) Zob. również powiadomienie wydane przez Agencję Policji Krajowej 7 grudnia 1999 r. (poniżej w akapicie 9), w którym również pojawia się to stwierdzenie.

— „odpowiedniość metod" (tj. należy ocenić, czy dobrowolne postępowanie przygotowawcze jest właściwe lub racjonalne, aby osiągnąć cel postępowania przygotowawczego) ([12]).

Ogólnie, przy uwzględnieniu trzech kryteriów wymienionych powyżej, zgodność z prawem dobrowolnego postępowania przygotowawczego ocenia się ze względu na fakt, czy można je uznać za racjonalne według społecznie akceptowalnej konwencji.

Wymóg, zgodnie z którym postępowanie przygotowawcze powinno być „niezbędne", wynika bezpośrednio z art. 197 kodeksu postępowania karnego i został potwierdzony w wytycznych wydanych przez Agencję Policji Krajowej dla policji prefekturalnej, dotyczących stosowania „kart z zapytaniem". W powiadomieniu Agencji Policji Krajowej z dnia 7 grudnia 1999 r. przewidziano szereg ograniczeń proceduralnych, w tym wymóg stosowania „karty z zapytaniem" wyłącznie jeżeli jest to konieczne do celów postępowania przygotowawczego. Ponadto art. 197 ust. 1 kodeksu postępowania karnego ma zastosowanie wyłącznie do postępowań karnych, może być zatem stosowany wyłącznie w przypadku, gdy istnieje konkretne podejrzenie dotyczące już popełnionego przestępstwa. Ta podstawa prawna nie ma w związku z tym zastosowania do zbierania i wykorzystywania informacji osobowych, w przypadku gdy nie doszło jeszcze do naruszenia prawa.

2) Ograniczenia dotyczące niektórych podmiotów gospodarczych

W niektórych obszarach obowiązują dodatkowe ograniczenia na podstawie ochrony przewidzianej w innych przepisach.

Po pierwsze organy śledcze i operatorzy telekomunikacyjni przechowujący informacje osobowe mają obowiązek przestrzegania tajemnicy komunikacji, jak przewidziano w art. 21 ust. 2 konstytucji ([13]). Na operatorów telekomunikacyjnych nałożono również ten sam obowiązek w art. 4 ustawy o działalności telekomunikacyjnej ([14]). Zgodnie z wytycznymi dotyczącymi ochrony informacji osobowych w działalności telekomunikacyjnej, wydanymi przez Ministerstwo Spraw Wewnętrznych i Komunikacji na podstawie konstytucji i ustawy o działalności telekomunikacyjnej, w przypadku gdy chodzi o tajemnicę komunikacji, operatorzy telekomunikacyjni mają zakaz ujawniania osobom trzecim informacji osobowych dotyczących tajemnicy komunikacji, z wyjątkiem sytuacji gdy uzyskali zgodę osoby, której dotyczą te informacje, lub jeżeli mogą powołać się na jedną z „uzasadnionych przyczyn" związanych z nieprzestrzeganiem przepisów kodeksu karnego. Uzasadnione przyczyny dotyczą „uzasadnionych działań" (art. 35 kodeksu karnego), „obrony własnej" (art. 36 kodeksu karnego) i „przeciwdziałania powstałemu zagrożeniu" (art. 37 kodeksu karnego). Zgodnie z kodeksem karnym „uzasadnione działania" to wyłącznie te działania operatora telekomunikacyjnego, które są zgodne z przymusowymi środkami państwowymi, co wyklucza dobrowolne postępowanie przygotowawcze. W związku z tym, jeżeli organy śledcze zwrócą się o informacje osobowe na podstawie „karty z zapytaniem" (art. 197 ust. 2 kodeksu postępowania karnego), operator telekomunikacyjny ma zakaz ujawniania takich danych.

Po drugie podmioty gospodarcze mają obowiązek odrzucenia wniosków o dobrowolną współpracę, jeżeli prawo zabrania im ujawniania informacji osobowych. Obejmuje to między innymi przypadki, gdy podmiot ma obowiązek przestrzegania poufności informacji, np. zgodnie z art. 134 kodeksu karnego ([15]).

3) Ograniczenia oparte na ustawie o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji

Jeżeli chodzi o zbieranie informacji osobowych przez organy administracyjne i dalsze ich przetwarzanie, ustawa przewiduje ograniczenia, jak wyjaśniono powyżej w sekcji II.A.1) lit. b) pkt 2. Równoważne ograniczenia wynikają z regulacji prefekturalnych mających zastosowanie do policji prefekturalnej.

B. Nadzór

1. Nadzór sądowy

W przypadku zbierania informacji osobowych za pomocą środków przymusowych wymagany jest nakaz sądowy ([16]), podlega ono zatem wcześniejszej analizie sądowej. Jeżeli postępowanie przygotowawcze jest niezgodne z prawem, sędzia może wykluczyć materiał dowodowy zebrany w trakcie tego postępowania z następującego po nim postępowania przed sądem karnym. Osoba fizyczna może złożyć wniosek o takie wykluczenie w dotyczącym jej postępowaniu przed sądem karnym, twierdząc, że takie postępowanie przygotowawcze było niezgodne z prawem.

([12]) Odpowiednimi czynnikami służącymi ocenie „odpowiedniości metod" jest waga przestępstwa i pilny charakter sprawy.

([13]) Art. 21 ust. 2 konstytucji stanowi: „Nie stosuje się cenzury ani nie narusza się tajemnicy jakichkolwiek środków komunikacji".

([14]) Art. 4 ustawy o działalności telekomunikacyjnej stanowi: „1. Zabrania się naruszania poufności komunikacji obsługiwanej przez operatora telekomunikacyjnego. 2. Zabrania się każdej osobie prowadzącej działalność telekomunikacyjną ujawniania informacji uzyskanych podczas pełnienia obowiązków w związku z komunikacją obsługiwaną przez operatora telekomunikacyjnego. Zakaz ten ma zastosowanie również po zakończeniu pełnienia obowiązków przez taką osobę".

([15]) Art. 134 kodeksu karnego stanowi: „1. Jeżeli lekarz, farmaceuta, dystrybutor produktów leczniczych, położna, prawnik, adwokat, notariusz lub dowolna inna osoba, która wcześniej wykonywała taki zawód, ujawni bez uzasadnionego powodu poufne informacje dotyczące innej osoby, które uzyskała w trakcie wykonywania swojego zawodu, podlega karze więzienia z możliwością wykonywania pracy do 6 miesięcy lub grzywnie w wysokości do 100 000 jenów. 2. Powyższy przepis ma zastosowanie również w przypadku, gdy osoba, która wykonuje lub wykonywała obowiązki w zakresie posługi religijnej, ujawni bez uzasadnionego powodu poufne informacje dotyczące innej osoby, które uzyskała w trakcie wykonywania takich czynności religijnych".

([16]) Informacje na temat wyjątku od tej zasady znajdują się w przypisie 5.

2. Nadzór oparty na ustawie o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji

W Japonii minister lub szef każdego ministerstwa lub agencji ma uprawnienia do wykonywania czynności w zakresie nadzoru i egzekwowania przepisów na podstawie ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji, natomiast Minister Spraw Wewnętrznych i Komunikacji może prowadzić postępowania wyjaśniające w sprawie egzekwowania przepisów tej ustawy przez wszystkie pozostałe ministerstwa.

Minister Spraw Wewnętrznych i Komunikacji może zwrócić się do dyrektora organu administracyjnego o przedłożenie materiałów i wyjaśnień dotyczących przetwarzania informacji osobowych przez ten organ administracyjny na podstawie art. 50 ustawy, jeżeli uzna to za konieczne – na przykład na podstawie postępowania wyjaśniającego w sprawie sytuacji w zakresie egzekwowania przepisów ustawy ([17]), rozpatrywania wniosków lub zapytań skierowanych do jednego z centrów informacji ogólnej podlegających ministerstwu. Minister może kierować do dyrektora organu administracyjnego opinie na temat przetwarzania informacji osobowych w tym organie administracyjnym, jeżeli uzna to za konieczne do osiągnięcia celu tej ustawy. Ponadto minister może zwrócić się na przykład o przegląd środków za pomocą działań, które może podjąć zgodnie z art. 50 i 51 ustawy, kiedy zachodzi podejrzenie, że doszło do naruszenia lub niewłaściwego zastosowania przepisów tej ustawy. Ułatwia to zapewnienie spójnego stosowania i przestrzegania ustawy.

3. Nadzór ze strony komisji ds. bezpieczeństwa publicznego

Jeżeli chodzi o administrację policyjną, Agencja Policji Krajowej podlega nadzorowi Krajowej Komisji ds. Bezpieczeństwa Publicznego, natomiast policja prefekturalna podlega nadzorowi jednej z Prefekturalnych Komisji ds. Bezpieczeństwa Publicznego ustanowionych w każdej prefekturze. Każdy z tych organów nadzoru zapewnia zarząd policją na demokratycznych zasadach i przy zachowaniu neutralności politycznej.

Krajowa Komisja ds. Bezpieczeństwa Publicznego odpowiada za sprawy podlegające jej jurysdykcji zgodnie z ustawą o policji i innymi ustawami. Obejmuje to mianowanie komisarza generalnego Agencji Policji Krajowej i lokalnych funkcjonariuszy policji wyższego szczebla, jak również ustanowienie kompleksowej polityki określającej podstawowe kierunki lub środki w odniesieniu do zarządu Agencją Policji Krajowej.

Prefekturalne Komisje ds. Bezpieczeństwa Publicznego składają się z członków reprezentujących obywateli danej prefektury na podstawie ustawy o policji i zarządzają policją prefekturalną jako niezależne rady. Członków powołuje gubernator prefektury za zgodą Zgromadzenia Prefekturalnego na podstawie art. 39 ustawy o policji. Kadencja członków trwa trzy lata, a ich odwołanie wbrew ich woli możliwe jest wyłącznie z określonych powodów wymienionych w ustawie (takich jak niezdolność do wykonywania obowiązków, naruszenie obowiązków, przewinienie służbowe itp.), co zapewnia ich niezależność (zob. art. 40 i 41 ustawy o policji). Ponadto, aby zagwarantować neutralność polityczną członków, art. 42 ustawy o policji zabrania członkowi komisji pełnienia jednocześnie funkcji członka organu prawodawczego, obejmowania funkcji wykonawczych w partii politycznej lub dowolnym innym organie politycznym, lub też czynnego angażowania się w ruchy polityczne. Każda komisja podlega wprawdzie jurysdykcji właściwego gubernatora prefektury, ale nie wiąże się to z nadaniem gubernatorowi uprawnień do wydawania instrukcji dotyczących wypełniania jej zadań.

Zgodnie z art. 38 ust. 3 w związku z art. 2 i art. 36 ust. 2 ustawy o policji Prefekturalne Komisje ds. Bezpieczeństwa Publicznego są odpowiedzialne za „ochronę praw i wolności jednostki". W tym celu, m.in. na regularnych spotkaniach odbywających się trzy lub cztery razy w miesiącu, szefowie policji prefekturalnych przekazują im sprawozdania dotyczące działalności w ramach ich jurysdykcji. Komisje zapewniają wytyczne w tych kwestiach przez ustanawianie kompleksowych zasad polityki.

Ponadto, w ramach funkcji nadzorczej, w konkretnych indywidualnych przypadkach Prefekturalne Komisje ds. Bezpieczeństwa Publicznego mogą wydawać policji prefekturalnej instrukcje, gdy uznają to za konieczne w związku z kontrolą działań policji prefekturalnej lub przewinień jej pracowników. Komisje mogą również, jeżeli uznają to za konieczne, zlecić wyznaczonemu członkowi komisji przeprowadzenie kontroli stanu wdrożenia wydanych instrukcji (art. 43-2 ustawy o policji).

([17]) Aby zapewnić przejrzystość i ułatwić nadzór prowadzony przez Ministra Spraw Wewnętrznych i Komunikacji, od dyrektora organu administracyjnego wymaga się, zgodnie z art. 11 ustawy, rejestrowania każdego elementu zapisanego w art. 10 ust. 1 ustawy, jak na przykład nazwy organu administracyjnego przechowującego akta, celu wykorzystania akt, metody zbierania informacji osobowych itp. (tzw. „rejestr akt z informacjami osobowymi"). Akta z informacjami osobowymi wchodzące w zakres art. 10 ust. 2 ustawy, takie jak akta przygotowane lub uzyskane w ramach postępowania przygotowawczego lub dotyczące spraw związanym z bezpieczeństwem narodowym, nie są objęte obowiązkiem powiadamiania ministra i zamieszczania w rejestrze publicznym. Zgodnie z art. 7 ustawy o zarządzaniu rejestrami i archiwami publicznymi od dyrektora organu administracyjnego zawsze wymaga się jednak rejestrowania klasyfikacji, tytułu, okresu zatrzymywania i lokalizacji miejsca przechowywania itp. dokumentów administracyjnych („Rejestr do celów zarządzania aktami zawierającymi dokumenty administracyjne"). Informacje dotyczące indeksowania obu rejestrów publikowane są na stronie internetowej i umożliwiają osobom fizycznym sprawdzenie, jakiego rodzaju informacje zawierają akta i który organ administracyjny przechowuje dane informacje.

4. Nadzór ze strony Diet

Diet może badać sprawy dotyczące działań organów publicznych i w tym celu wymagać przedstawienia dokumentów i zeznań świadków (art. 62 konstytucji). W tym kontekście właściwa komisja śledcza w Diet może zbadać stosowność prowadzonych przez policję działań związanych ze zbieraniem informacji.

Kompetencje te zostały szczegółowo określone w ustawie o Diet. Zgodnie z art. 104 Diet może zobowiązać Radę Ministrów i agencje publiczne do sporządzania sprawozdań i dokumentów niezbędnych do prowadzenia postępowania. Ponadto członkowie Diet mogą składać „zapytania na piśmie" na podstawie art. 74 ustawy o Diet. Takie zapytania musi zatwierdzić przewodniczący Izby, a Rada Ministrów, co do zasady, ma obowiązek udzielić odpowiedzi na piśmie w terminie siedmiu dni (w przypadku gdy nie ma możliwości udzielenia odpowiedzi w tym terminie, należy podać uzasadnienie i wyznaczyć nowy termin – art. 75 ustawy o Diet). W przeszłości zapytania na piśmie składane przez Diet dotyczyły również przetwarzania informacji osobowych przez administrację ([18]).

C. Indywidualne dochodzenie roszczeń

Zgodnie z art. 32 konstytucji Japonii żadna osoba nie może zostać pozbawiona prawa dostępu do wymiaru sprawiedliwości. Ponadto art. 17 konstytucji gwarantuje każdej osobie prawo do pozwania państwa lub podmiotu publicznego w celu dochodzenia roszczeń (na podstawie przepisów prawa) w przypadku, gdy osoba ta poniosła szkodę w wyniku niezgodnego z prawem działania funkcjonariusza publicznego.

1. Dochodzenie roszczeń na drodze sądowej z tytułu przymusowego zbierania informacji na podstawie nakazu (art. 430 kodeksu postępowania karnego)

Zgodnie z art. 430 ust. 2 kodeksu postępowania karnego osoba fizyczna, która jest niezadowolona ze środków zastosowanych przez funkcjonariusza policji w związku z zajęciem rzeczy (w tym, jeżeli zawierają one informacje osobowe) na podstawie nakazu, może złożyć wniosek (tzw. „quasi-complaint") do właściwego sądu o uchylenie lub zmianę tych środków.

Osoba fizyczna może złożyć taki wniosek bez konieczności oczekiwania na zakończenie sprawy. Jeżeli sąd uzna, że zajęcie nie było konieczne lub że istnieją inne powody uznania zajęcia za niezgodne z prawem, może nakazać uchylenie lub zmianę takich środków.

2. Dochodzenie roszczeń na drodze sądowej na podstawie kodeksu postępowania cywilnego i ustawy o odpowiedzialności odszkodowawczej państwa

Osoby fizyczne, które uznają, że naruszono ich prawo do prywatności przysługujące im na podstawie art. 13 konstytucji, mogą wytoczyć powództwo cywilne, żądając usunięcia informacji osobowych zebranych w toku postępowania przygotowawczego.

Ponadto osoba fizyczna może wytoczyć powództwo odszkodowawcze na podstawie ustawy o odpowiedzialności odszkodowawczej państwa w połączeniu z odpowiednimi artykułami kodeksu cywilnego, jeżeli uzna, że doszło do naruszenia jej prawa do prywatności i że poniosła szkodę w wyniku zbierania dotyczących jej informacji osobowych lub nadzoru ([19]). Biorąc pod uwagę, że „szkoda", która może być przedmiotem roszczenia odszkodowawczego, nie ogranicza się do szkody majątkowej (art. 710 kodeksu cywilnego), może ona również obejmować „urazy psychiczne". Sędzia oceni kwotę zadośćuczynienia za doznaną krzywdę na podstawie „swobodnej oceny uwzględniającej różne czynniki w poszczególnych przypadkach" ([20]).

Art. 1 ust. 1 ustawy o odpowiedzialności odszkodowawczej państwa przyznaje prawo do odszkodowania w przypadku, gdy (i) urzędnik publiczny, który sprawuje władzę publiczną w imieniu państwa lub podmiotu publicznego (ii) w ramach wykonywania swoich obowiązków (iii) umyślnie lub przez niedbalstwo (iv) w sposób niezgodny z prawem (v) wyrządził szkodę innej osobie.

Osoba fizyczna składa pozew zgodnie z kodeksem postępowania cywilnego. Zgodnie z obowiązującymi przepisami osoba taka może złożyć pozew do sądu właściwego dla miejsca, w którym popełniono czyn niedozwolony.

([18]) Zob. np. zapytanie na piśmie do Izby Radców nr 92 z dnia 27 marca 2009 r. dotyczące przetwarzania informacji zebranych w związku z postępowaniami przygotowawczymi, w których doszło do naruszeń obowiązków zachowania poufności przez organy policji i prokuratury.

([19]) Przykładem takiego powództwa jest „Sprawa dotycząca wykazu Agencji Obrony" (Sąd Rejonowy w Niigata, wyrok z dnia 11 maja 2006 r., (2002(Wa) Nr 514)). W tym przypadku urzędnik Agencji Obrony opracował, przechowywał i rozprowadzał wykaz osób, które złożyły wnioski o ujawnienie dokumentów administracyjnych do Agencji Obrony. W wykazie znajdowały się opisy informacji osobowych powoda. Podkreślając, że doszło do naruszenia jego prywatności, prawa do informacji itp., powód domagał się od pozwanego wypłaty odszkodowania za szkody na podstawie art. 1 ust. 1 ustawy o odpowiedzialności odszkodowawczej państwa. Sąd uwzględnił ten wniosek częściowo i przyznał skarżącemu częściowe odszkodowanie.

([20]) Sąd Najwyższy, wyrok z dnia 5 kwietnia 1910 r. (1910 (O) nr 71).

3. Indywidualne dochodzenie roszczeń z tytułu niezgodnego z prawem/niewłaściwego prowadzenia postępowania przygotowawczego przez policję: skarga do Prefekturalnej Komisji ds. Bezpieczeństwa Publicznego (art. 79 ustawy o policji)

Zgodnie z art. 79 ustawy o policji ([21]), jak wyjaśniono dokładniej w instrukcji szefa Agencji Policji Krajowej skierowanej do policji prefekturalnej i Prefekturalnych Komisji ds. Bezpieczeństwa Publicznego ([22]), osoby fizyczne mogą złożyć pisemną skargę ([23]) do właściwej Prefekturalnej Komisji ds. Bezpieczeństwa Publicznego na wszelkie bezprawne lub niewłaściwe postępowanie funkcjonariusza policji podczas wykonywania jego obowiązków; obejmuje to obowiązki związane ze zbieraniem i wykorzystywaniem informacji osobowych. Komisja skrupulatnie rozpatruje takie skargi zgodnie z przepisami ustawowymi i regulacjami lokalnymi oraz powiadamia skarżącego o wyniku postępowania na piśmie.

W oparciu o swoje uprawnienia nadzorcze zgodnie z art. 38 ust. 3 ustawy o policji, Prefekturalna Komisja ds. Bezpieczeństwa Publicznego wydaje policji prefekturalnej instrukcje w sprawie zbadania stanu faktycznego, wdrożenia niezbędnych środków zgodnie z wynikami badania oraz przedłożenia Komisji sprawozdania z wyników. Jeżeli Komisja uzna to za konieczne, może również wydać instrukcje w sprawie rozpatrywania skargi, na przykład jeżeli uzna, że postępowanie przygotowawcze przeprowadzone przez policję jest niewystarczające. Wdrożenie zostało opisane w zawiadomieniu wydanym przez Agencję Policji Krajowej skierowanym do szefów policji prefekturalnej.

Zawiadomienie skarżącego o wyniku postępowania przygotowawczego odbywa się również w świetle sprawozdań policji dotyczących postępowania oraz środków zastosowanych na wniosek Komisji.

4. Indywidualne dochodzenie roszczeń na podstawie ustawy o ochronie informacji osobowych i kodeksu postępowania karnego

a) Ustawa o ochronie informacji osobowych

Zgodnie z art. 48 ustawy o ochronie informacji osobowych organy administracyjne muszą dążyć do właściwego i sprawnego rozpatrzenia wszelkich skarg dotyczących przetwarzania informacji osobowych. Aby osobom fizycznym zapewnić skonsolidowane informacje (np. na temat dostępnych praw do ujawnienia, korekty oraz zawieszenia wykorzystywania informacji na podstawie ustawy o ochronie informacji osobowych) oraz jako punkt kontaktowy w sprawach zapytań, Ministerstwo Spraw Wewnętrznych i Komunikacji utworzyło w każdej prefekturze Centra Informacji Ogólnej w zakresie Ujawniania Informacji i Ochrony Informacji Osobowych w oparciu o art. 47 ust. 2 ustawy o ochronie informacji osobowych. Zapytania mogą również kierować nierezydenci. Na przykład w roku obrachunkowym 2017 (kwiecień 2017 r. – marzec 2018 r.) łączna liczba przypadków, w których centra informacji ogólnej odpowiedziały na pytania itp., wyniosła 5186.

W art. 12 i 27 ustawy o ochronie informacji osobowych przyznaje się osobom fizycznym prawo do zwrócenia się o ujawnienie i korektę zatrzymanych informacji osobowych. Ponadto zgodnie z art. 36 ustawy o ochronie informacji osobowych osoby fizyczne mogą zażądać zawieszenia wykorzystania lub usunięcia swoich zatrzymanych informacji osobowych, jeżeli organ administracyjny nie uzyskał tych informacji zgodnie z prawem albo zatrzymuje lub wykorzystuje takie informacje z naruszeniem prawa.

Jeżeli jednak chodzi o informacje osobowe zebrane (na podstawie nakazu lub „karty z zapytaniem") i zatrzymane na potrzeby postępowań przygotowawczych ([24]), takie informacje zasadniczo należą do kategorii „informacji osobowych utrwalonych w dokumentach związanych z procesami sądowymi i zajętymi rzeczami". Takie informacje osobowe są zatem wyłączone z zakresu stosowania praw indywidualnych określonych w rozdziale 4 ustawy o ochronie informacji osobowych na podstawie art. 53-2 kodeksu postępowania karnego ([25]). Przetwarzanie takich informacji osobowych oraz

([21]) Art. 79 ustawy o policji (fragment).
1. Każdy, kto chce złożyć skargę na wykonywanie obowiązków przez personel policji prefekturalnej, może wnieść skargę na piśmie do Prefekturalnej Komisji ds. Bezpieczeństwa Publicznego, korzystając z procedury opisanej w zarządzeniu Krajowej Komisji ds. Bezpieczeństwa Publicznego.
2. Prefekturalna Komisja ds. Bezpieczeństwa Publicznego, do której wpłynęła skarga, o której mowa w poprzednim akapicie, skrupulatnie ją rozpatruje zgodnie z ustawami i regulacjami lokalnymi oraz powiadamia skarżącego o wyniku na piśmie; wyjątek stanowią następujące przypadki:
1) skarga może zostać uznana za wniesioną w celu utrudnienia zgodnego z prawem wykonywania obowiązków policji prefekturalnej;
2) aktualne miejsce zamieszkania skarżącego jest nieznane;
3) skarga może zostać uznana za wniesioną wspólnie z innymi skarżącymi i inni skarżący już zostali powiadomieni o wyniku rozpatrzenia wspólnej skargi.

([22]) Agencja Policji Krajowej, Zawiadomienie w sprawie właściwego rozpatrywania skarg dotyczących wykonywania obowiązków przez funkcjonariuszy policji, 13 kwietnia 2001 r., z załącznikiem 1 „Normy dotyczące interpretacji i wdrażania art. 79 ustawy o policji".

([23]) Zgodnie z zawiadomieniem Agencji Policji Krajowej (zob. poprzedni przypis) osoby fizyczne mające trudności w sformułowaniu skargi na piśmie otrzymują pomoc. Obejmuje to wyraźnie cudzoziemców.

([24]) Z drugiej strony istnieją dokumenty, które nie są sklasyfikowane jako „dokumenty związane z procesami sądowymi", ponieważ same w sobie nie są informacjami uzyskanymi na podstawie nakazu, zapytań na piśmie lub czynności dochodzeniowo-śledczych, lecz są tworzone na podstawie takich dokumentów. Miałoby to miejsce w przypadku, gdy informacje prywatne nie podlegają art. 45 ust. 1 ustawy o ochronie informacji osobowych, a w związku z czym takie informacje nie byłyby wyłączone z zakresu stosowania rozdziału 4 ustawy o ochronie informacji osobowych.

([25]) Art. 53-2 ust. 2 kodeksu postępowania karnego stanowi, że przepisów rozdziału IV ustawy o ochronie informacji osobowych nie stosuje się do informacji osobowych utrwalonych w dokumentach związanych z procesami sądowymi i zajętymi rzeczami.

prawa osoby fizycznej do dostępu do danych i ich korekty podlegają jednak specjalnym przepisom zgodnie z kodeksem postępowania karnego i ustawą o rejestrze zakończonych spraw karnych (zob. poniżej) ([26]). Wyłączenie to jest uzasadnione różnymi czynnikami, takimi jak ochrona prywatności zainteresowanych osób, poufność postępowań oraz właściwe prowadzenie postępowania karnego. W związku z tym nadal mają zastosowanie przepisy rozdziału 2 ustawy o ochronie informacji osobowych regulujące zasady postępowania z takimi informacjami.

b) Kodeks postępowania karnego

Zgodnie z kodeksem postępowania karnego możliwość dostępu do informacji osobowych zbieranych na potrzeby postępowania przygotowawczego zależy zarówno od etapu postępowania, jak i od roli osoby fizycznej w postępowaniu (osoba podejrzana, oskarżona, ofiara itp.).

W drodze wyjątku od zasady zawartej w art. 47 kodeksu postępowania karnego stanowiącej, że dokumentów związanych z procesem sądowym nie podaje się do wiadomości publicznej przed rozpoczęciem procesu (ponieważ mogłoby to naruszyć honor lub prywatność zainteresowanych osób fizycznych oraz utrudnić postępowanie), dostęp ofiary przestępstwa jest co do zasady dozwolony w uzasadnionym zakresie, biorąc pod uwagę cel przepisu zawartego w art. 47 kodeksu postępowania karnego ([27]).

Jeżeli chodzi o osoby podejrzane, zazwyczaj dowiadują się, że są objęte postępowaniem przygotowawczym, podczas przesłuchania przez policję sądową lub prokuratura. Jeżeli następnie prokurator postanowi nie wszczynać postępowania, niezwłocznie powiadamia o tym fakcie osobę podejrzaną (art. 259 kodeksu postępowania karnego).

Ponadto po wszczęciu postępowania prokurator umożliwia osobie oskarżonej lub jej pełnomocnikowi zapoznanie się z dowodami przed zwróceniem się o ich zbadanie przez sąd (art. 299 kodeksu postępowania karnego). Umożliwia to oskarżonemu sprawdzenie własnych informacji osobowych zebranych w trakcie postępowania przygotowawczego.

Ochrona informacji osobowych zebranych w ramach postępowania przygotowawczego, dotyczących osoby podejrzanej, oskarżonej lub jakiejkolwiek innej osoby (np. ofiary przestępstwa) jest również zagwarantowana dzięki obowiązkowi zachowania poufności (art. 100 ustawy o krajowej służbie publicznej) oraz groźbie kary w przypadku wycieku poufnych informacji w ramach wykonywania obowiązków służby publicznej (art. 109 ppkt (xii) ustawy o krajowej służbie publicznej).

5. Indywidualne dochodzenie roszczeń z tytułu bezprawnego/nieprawidłowego prowadzenia postępowań przygotowawczych przez organy publiczne: skarga do Komisji ds. Ochrony Informacji Osobowych

Zgodnie z art. 6 ustawy o ochronie informacji osobowych rząd podejmuje, we współpracy z rządami państw trzecich, niezbędne działania mające na celu stworzenie zgodnego z przepisami międzynarodowymi systemu dotyczącego informacji osobowych poprzez wspieranie współpracy z organizacjami międzynarodowymi i innymi systemami międzynarodowymi. Na podstawie tego przepisu w podstawowych zasadach polityki dotyczącej ochrony informacji osobowych (przyjętych uchwałą Rady Ministrów) przekazano Komisji ds. Ochrony Informacji Osobowych, jako organowi właściwemu w zakresie ogólnego wykonywania przepisów ustawy o ochronie informacji osobowych, prawo do podejmowania działań niezbędnych do zatarcia różnic w systemach oraz działaniach między Japonią a danym państwem obcym w celu zapewnienia właściwego przetwarzania informacji osobowych otrzymanych od takiego państwa.

Ponadto, jak przewidziano w art. 61 ppkt (i) i (ii) ustawy o ochronie informacji osobowych, Komisji ds. Ochrony Informacji Osobowych powierza się zadanie formułowania i propagowania podstawowych zasady polityki, a także mediacji w przypadku skarg złożonych przeciwko podmiotom gospodarczym. Wreszcie organy administracyjne pozostają w ścisłym kontakcie i współpracują ze sobą (art. 80 ustawy o ochronie informacji osobowych).

W oparciu o te przepisy Komisja ds. Ochrony Informacji Osobowych rozpatruje skargi osób fizycznych w następujący sposób:

a) Osoba, która podejrzewa, że jej dane przekazane z UE zostały zebrane lub wykorzystane przez organy publiczne w Japonii, w tym organy odpowiedzialne za działania, o których mowa w rozdziale II i III niniejszego „oświadczenia", z naruszeniem obowiązujących przepisów, w tym również tych, które podlegają niniejszemu „oświadczeniu", może złożyć skargę do Komisji ds. Ochrony Informacji Osobowych (indywidualnie lub za pośrednictwem swojego organu ochrony danych).

b) Komisja ds. Ochrony Informacji Osobowych rozpatruje skargę, korzystając między innymi ze swoich uprawnień na mocy art. 6, art. 61 ppkt (ii) i art. 80 ustawy o ochronie informacji osobowych, oraz informuje o skardze właściwe organy publiczne, w tym właściwe organy nadzorcze.

([26]) Zgodnie z kodeksem postępowania karnego i ustawą o rejestrze zakończonych spraw karnych dostęp do zajętych rzeczy i ich korekta, a także dokumenty / informacje osobowe dotyczące postępowań karnych podlegają wyjątkowemu i odrębnemu systemowi przepisów, który ma na celu ochronę prywatności zainteresowanych osób, poufności postępowań oraz właściwego prowadzenia postępowania karnego itp.

([27]) Ściślej rzecz ujmując, dostęp do informacji dotyczących obiektywnych dowodów jest co do zasady dozwolony w przypadku ofiar przestępstw w odniesieniu do rejestrów innych niż sądowe w sprawach odbywających się z udziałem ofiar, o których mowa w art. 316-33 kodeksu postępowania karnego, co służy zapewnieniu lepszej ochrony ofiar przestępstw.

Organy te są obowiązane współpracować z Komisją ds. Ochrony Informacji Osobowych na mocy art. 80 ustawy o ochronie informacji osobowych, zapewniając między innymi niezbędne informacje i odpowiednie materiały, dzięki którym komisja może ocenić, czy zbieranie i późniejsze wykorzystanie informacji osobowych było zgodne z obowiązującymi przepisami. Przeprowadzając swoją ocenę, Komisja ds. Ochrony Informacji Osobowych współpracuje z Ministerstwem Spraw Wewnętrznych i Komunikacji.

c) Jeżeli ocena wykaże naruszenie obowiązujących przepisów, współpraca między danym organem publicznym a Komisją ds. Ochrony Informacji Osobowych obejmuje obowiązek usunięcia naruszenia.

W przypadku niezgodnego z prawem zbierania informacji osobowych na mocy obowiązujących przepisów obejmuje to usunięcie zebranych informacji osobowych.

W przypadku naruszenia obowiązujących przepisów Komisja ds. Ochrony Informacji Osobowych potwierdza również, przed zakończeniem oceny, że naruszenie udało się w pełni usunąć.

d) Po zakończeniu oceny Komisja ds. Ochrony Informacji Osobowych zawiadamia w rozsądnym terminie osobę fizyczną o jej wynikach, w tym, w stosownych przypadkach, o podjętych działaniach naprawczych. W zawiadomieniu tym Komisja ds. Ochrony Informacji Osobowych informuje osobę fizyczną o możliwości uzyskania potwierdzenia wyniku u właściwego organu publicznego oraz o tym, do którego organu należy kierować taki wniosek o potwierdzenie.

Szczegółowe informacje na temat wyniku oceny mogą być ograniczone, jeżeli istnieją uzasadnione przesłanki do stwierdzenia, że przekazanie takiej informacji może stanowić zagrożenie dla trwającego postępowania.

W przypadku gdy skarga dotyczy zbierania lub wykorzystywania danych osobowych w ramach ścigania przestępstw, jeżeli ocena wykazała, że wszczęto postępowanie, w którym wykorzystano informacje osobowe osoby fizycznej, a następnie postępowanie to zakończono, Komisja ds. Ochrony Informacji Osobowych informuje taką osobę, że z aktami sprawy można się zapoznać zgodnie z art. 53 kodeksu postępowania karnego oraz art. 4 ustawy o rejestrze zakończonych spraw karnych.

Jeżeli ocena wykazała, że osoba fizyczna jest w postępowaniu karnym osobą podejrzaną, Komisja ds. Ochrony Informacji Osobowych zawiadamia ją o tym fakcie oraz o możliwości złożenia wniosku zgodnie z art. 259 kodeksu postępowania karnego.

e) Jeżeli mimo to osoba fizyczna jest niezadowolona z wyniku postępowania, może się zgłosić się do Komisji ds. Ochrony Informacji Osobowych, która informuje osobę fizyczną o różnych możliwościach i szczegółowych procedurach dotyczących uzyskania odszkodowania na podstawie japońskich przepisów ustawowych i wykonawczych. Komisja ds. Ochrony Informacji Osobowych zapewnia osobie fizycznej wsparcie, w tym doradztwo i pomoc w związku z jakimkolwiek dalszym postępowaniem przed właściwym organem administracyjnym lub sądowym.

III. **Dostęp rządowy do celów bezpieczeństwa narodowego**

A. Podstawa prawna i ograniczenia dotyczące zbierania informacji osobowych

1. Podstawa prawna zbierania informacji przez zainteresowane ministerstwo/agencję

Jak wskazano powyżej, zbieranie informacji osobowych do celów bezpieczeństwa narodowego przez organy administracyjne musi wchodzić w zakres ich jurysdykcji administracyjnej.

W Japonii nie istnieje prawo umożliwiające zbieranie informacji za pomocą środków przymusowych wyłącznie do celów bezpieczeństwa narodowego. Zgodnie z art. 35 konstytucji przymusowe zbieranie informacji osobowych jest możliwe wyłącznie na podstawie nakazu wydanego przez sąd w celu przeprowadzenia postępowania przygotowawczego w sprawie przestępstwa. Taki nakaz można zatem wydać wyłącznie na potrzeby postępowania przygotowawczego. Oznacza to, że w japońskim systemie prawnym nie zezwala się na zbieranie informacji / dostęp do informacji za pomocą środków przymusowych ze względów bezpieczeństwa narodowego. Zamiast tego w dziedzinie bezpieczeństwa narodowego zainteresowane ministerstwa lub agencje mogą uzyskiwać informacje wyłącznie ze źródeł, które są swobodnie dostępne lub otrzymywać informacje od podmiotów gospodarczych lub osób fizycznych w drodze dobrowolnego ujawnienia. Podmioty gospodarcze, do których zwrócono się o podjęcie dobrowolnej współpracy, nie są prawnie zobowiązane do przekazania tych informacji i w związku z tym nie są zagrożone negatywnymi konsekwencjami, jeżeli odmawiają współpracy.

W dziedzinie bezpieczeństwa narodowego odpowiedzialnych jest szereg różnych resortów i agencji.

1) Sekretariat Rady Ministrów

Sekretariat Rady Ministrów zbiera informacje i prowadzi badania w zakresie ważnych strategii politycznych Rady Ministrów ([28]), o których mowa w art. 12-2 ustawy o Radzie Ministrów ([29]). Sekretariat Rady Ministrów nie ma jednak uprawnień do zbierania informacji osobowych bezpośrednio od podmiotów gospodarczych. Sekretariat zbiera, łączy, analizuje i ocenia informacje pochodzące ze źródeł otwartych, od innych organów publicznych itp.

2) Agencja Policji Krajowej/policja prefekturalna

W każdej prefekturze policja prefekturalna ma kompetencje w zakresie zbierania informacji w ramach swojej jurysdykcji zgodnie z art. 2 ustawy o policji. Może się zdarzyć, że Agencja Policji Państwowej bezpośrednio zbiera informacje w zakresie swojej właściwości na mocy ustawy o policji. Dotyczy to w szczególności działalności Biura Bezpieczeństwa Agencji Policji Krajowej oraz Departamentu Spraw Zagranicznych i Wywiadu. Zgodnie z art. 24 ustawy o policji Biuro Bezpieczeństwa zajmuje się sprawami dotyczącymi policji bezpieczeństwa ([30]), a Departament Spraw Zagranicznych i Wywiadu jest odpowiedzialny za sprawy dotyczące cudzoziemców, jak również obywateli Japonii, którzy prowadzą działalność z siedzibą za granicą.

3) Agencja Bezpieczeństwa Publicznego

Stosowanie ustawy o zapobieganiu działaniom wywrotowym oraz ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa, mieści się głównie w kompetencjach Agencji Bezpieczeństwa Publicznego. Jest to agencja Ministerstwa Sprawiedliwości.

Ustawa o zapobieganiu działaniom wywrotowym i ustawa o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa stanowią, że przepisy administracyjne (tj. środki nakazujące ograniczenie działalności takich organizacji, ich rozwiązanie itp.) mogą być przyjmowane na mocy konstytucji, na ściśle określonych warunkach, przeciwko organizacjom popełniającym pewne poważne czyny („wywrotowe działania terrorystyczne" lub „zbrodnie masowego morderstwa") z naruszeniem „bezpieczeństwa publicznego" lub „podstawowego systemu społecznego". „Wywrotowe działania terrorystyczne" wchodzą w zakres stosowania ustawy o zapobieganiu działaniom wywrotowym (zob. art. 4 dotyczący działań takich jak powstanie, podżeganie do agresji zewnętrznej, zabójstwo z zamiarem politycznym itp.), natomiast ustawa o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa, odnosi się do „zbrodni masowego morderstwa" (zob. art. 4 tej ustawy). Jedynie precyzyjnie określone organizacje, które stwarzają konkretne wewnętrzne lub zewnętrzne zagrożenia dla bezpieczeństwa publicznego, mogą podlegać przepisom tych ustaw.

W tym celu ustawy te zapewniają podstawy prawne śledztwa. Podstawowe uprawnienia śledcze urzędników Agencji Bezpieczeństwa Publicznego są określone w art. 27 ustawy o zapobieganiu działaniom wywrotowym i w art. 29 ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa. Zgodnie z tymi przepisami urzędnicy Agencji Bezpieczeństwa Publicznego prowadzą śledztwa w zakresie, w jakim są one niezbędne w odniesieniu do powyższych przepisów dotyczących kontroli organizacji (np. w przeszłości jako przedmiot śledztwa przedstawiano ugrupowania skrajnej lewicy, sektę *Aum Shinrikyo* i określone ugrupowania krajowe ściśle powiązane z Koreą Północną). Postępowania te nie mogą opierać się jednak na środkach przymusowych, a zatem organizacja posiadająca informacje osobowe nie może być zmuszona do przekazania takich informacji.

Zbieranie i wykorzystywanie informacji dobrowolnie ujawnionych urzędnikom Agencji Bezpieczeństwa Publicznego podlega odpowiednim ograniczeniom i zabezpieczeniom przewidzianym przez prawo, takim jak, między innymi, gwarantowana przez konstytucję tajemnica wiadomości oraz przepisy dotyczące przetwarzania informacji osobowych zgodnie z ustawą o ochronie informacji osobowych.

4) Ministerstwo Obrony

Jeśli chodzi o zbieranie informacji przez Ministerstwo Obrony, ministerstwo to zbiera informacje w oparciu o art. 3 i 4 ustawy o utworzeniu Ministerstwa Obrony w zakresie niezbędnym do wykonywania jego kompetencji administracyjnych, w tym w odniesieniu do obrony i straży, działań podejmowanych przez Siły Samoobrony, a także rozmieszczania Sił Samoobrony Naziemnej, Morskiej i Lotniczej. Ministerstwo Obrony może zbierać informacje do tych celów wyłącznie w drodze dobrowolnej współpracy i ze źródeł swobodnie dostępnych. Nie zbiera ono informacji na temat ogółu społeczeństwa.

2. Ograniczenia i zabezpieczenia

a) Ograniczenia ustawowe

1) Ogólne ograniczenia wynikające z ustawy o ochronie informacji osobowych

Ustawa o ochronie informacji osobowych to ustawa ogólna, która ma zastosowanie do zbierania i przetwarzania informacji osobowych przez organy administracyjne we wszystkich dziedzinach działalności takich organów. W związku z tym ograniczenia i zabezpieczenia opisane w sekcji II.A.1) lit. b) pkt 2 mają zastosowanie również do zatrzymywania, przechowywania, wykorzystywania itp. informacji osobowych w dziedzinie bezpieczeństwa narodowego.

([28]) Zajmuje się tym Urząd Wywiadu i Badań Rady Ministrów na podstawie art. 4 zarządzenia w sprawie organizacji Sekretariatu Rady Ministrów.

([29]) Obejmuje to „zbieranie i badanie informacji wywiadowczych w zakresie ważnych strategii politycznych Rady Ministrów".

([30]) Policja bezpieczeństwa jest odpowiedzialna za działania w zakresie zwalczania przestępczości związane z bezpieczeństwem publicznym i z interesem kraju. Obejmuje to zwalczanie przestępczości oraz zbieranie informacji na temat niezgodnych z prawem działań związanych z ugrupowaniami skrajnej lewicy, skrajnej prawicy i szkodliwymi działaniami przeciwko Japonii.

2) Szczególne ograniczenia dotyczące policji (zarówno Agencji Policji Krajowej, jak i policji prefekturalnej)

Jak określono powyżej w sekcji poświęconej zbieraniu informacji do celów ścigania przestępstw policja może zbierać informacje wyłącznie w zakresie swoich kompetencji, a przy tym, zgodnie z art. 2 ust. 2 ustawy o policji, może podejmować działania jedynie w zakresie „ściśle ograniczonym" do wykonywania jej obowiązków i w sposób „bezstronny, wolny od uprzedzeń i sprawiedliwy". Ponadto swoich uprawnień „nigdy nie może nadużywać w jakikolwiek sposób, który ingeruje w prawa i wolności osoby fizycznej zagwarantowane w konstytucji Japonii".

3) Szczególne ograniczenia mające zastosowanie do Agencji Bezpieczeństwa Publicznego

Zarówno art. 3 ustawy o zapobieganiu działaniom wywrotowym, jak i art. 3 ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa, stanowią, że w ramach tych aktów postępowania prowadzone są wyłącznie w minimalnym zakresie wymaganym do osiągnięcia celu i nie są prowadzone w sposób nieracjonalnie ograniczający podstawowe prawa człowieka. Ponadto zgodnie z art. 45 ustawy o zapobieganiu działaniom wywrotowym i art. 42 ustawy o kontroli organizacji, które dopuściły się zbrodni masowego morderstwa, nadużycie uprawnień przez urzędnika Agencji Bezpieczeństwa Publicznego stanowi przestępstwo podlegające surowszym sankcjom karnym niż „ogólne" nadużycia uprawnień w innych dziedzinach sektora publicznego.

4) Szczególne ograniczenia dotyczące Ministerstwa Obrony

Jeśli chodzi o zbieranie/porządkowanie informacji przez Ministerstwo Obrony, o czym mowa w art. 4 ustawy o utworzeniu Ministerstwa Obrony, działalność tego ministerstwa w zakresie zbierania informacji ogranicza się do czynności, które są niezbędne do wykonywania jego obowiązków w zakresie 1) obrony i straży, 2) działań Sił Samoobrony oraz 3) organizacji, liczby personelu, struktury, wyposażenia i rozmieszczenia Sił Samoobrony Naziemnej, Morskiej i Lotniczej.

b) Inne ograniczenia

Jak już wyjaśniono w sekcji II.A.2) lit. b) ppkt (1), z orzecznictwa Sądu Najwyższego wynika, że kierowany do podmiotu gospodarczego wniosek o podjęcie dobrowolnej współpracy musi być niezbędny do przeprowadzenia postępowania przygotowawczego dotyczącego podejrzenia popełnienia przestępstwa i uzasadniony pod kątem osiągnięcia celu tego postępowania.

Chociaż śledztwa prowadzone przez organy śledcze w obszarze bezpieczeństwa narodowego i postępowania przygotowawcze prowadzone przez te organy w obszarze ścigania przestępstw różnią się od siebie pod względem podstawy prawnej i celu, nadrzędne zasady „konieczności przeprowadzenia postępowania przygotowawczego" oraz „odpowiedniości metody" znajdują również zastosowanie w obszarze bezpieczeństwa narodowego i należy ich przestrzegać z odpowiednim uwzględnieniem szczególnych okoliczności każdego przypadku.

Dzięki połączeniu powyższych ograniczeń zbieranie i przetwarzanie informacji odbywa się wyłącznie w zakresie niezbędnym do wykonywania szczególnych obowiązków przez właściwy organ publiczny oraz w związku ze szczególnymi zagrożeniami. Wyklucza to masowe i nieograniczone zbieranie informacji osobowych i dostęp do nich ze względów bezpieczeństwa narodowego.

B. Nadzór

1. Nadzór oparty na ustawie o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji

Jak wyjaśniono w sekcji II.B.2, w japońskim sektorze publicznym minister lub szef każdego ministerstwa lub agencji posiada uprawnienia do nadzorowania i egzekwowania zgodności z ustawą o ochronie informacji osobowych w swoim ministerstwie lub agencji. Ponadto Minister Spraw Wewnętrznych i Komunikacji może zbadać stan wykonania ustawy, zwrócić się do każdego ministra o przedstawienie materiałów i wyjaśnień w oparciu o art. 49 i 50 ustawy oraz skierować opinie do każdego ministra na podstawie art. 51 ustawy. Może na przykład wystąpić o przegląd środków poprzez działania na podstawie art. 50 i 51 ustawy.

2. Nadzór Komisji ds. Bezpieczeństwa Publicznego nad policją

Jak wyjaśniono powyżej w sekcji II „Zbieranie informacji do celów ścigania przestępstw", niezależne Prefekturalne Komisje ds. Bezpieczeństwa Publicznego nadzorują działania policji prefekturalnej.

Jeżeli chodzi o Agencję Policji Krajowej, funkcje nadzorcze pełni Krajowa Komisja ds. Bezpieczeństwa Publicznego. Zgodnie z art. 5 ustawy o policji komisja odpowiada w szczególności za „ochronę praw i wolności osoby fizycznej". W tym celu ustanawia w szczególności kompleksową politykę określającą przepisy dotyczące zarządzania działaniami określonymi w poszczególnych pozycjach w art. 5 ust. 4 ustawy o policji oraz określa inne podstawowe instrukcje lub środki, które należy stosować w celu prowadzenia wymienionych działań. Krajowa Komisja ds. Bezpieczeństwa Publicznego jest równie niezależna, jak Prefekturalne Komisje ds. Bezpieczeństwa Publicznego.

3. Nadzór Biura Inspektora Generalnego ds. Zgodności z Prawem nad Ministerstwem Obrony

Biuro Inspektora ds. Przestrzegania Prawa to niezależne biuro Ministerstwa Obrony, pod bezpośrednim nadzorem Ministra Obrony zgodnie z art. 29 ustawy o utworzeniu Ministerstwa Obrony. Biuro Inspektora ds. Przestrzegania Prawa może przeprowadzać kontrole przestrzegania przez urzędników Ministerstwa Obrony przepisów ustawowych i wykonawczych. Kontrole te określa się mianem „kontroli obronności".

Biuro Inspektora ds. Przestrzegania Prawa przeprowadza kontrole jako urząd niezależny, aby zapewnić przestrzeganie przepisów prawa w całym ministerstwie, w tym również przez Siły Samoobrony. Biuro wykonuje swoje obowiązki niezależnie od jednostek operacyjnych Ministerstwa Obrony. Po przeprowadzeniu kontroli Biuro Inspektora ds. Przestrzegania Prawa niezwłocznie przedstawia bezpośrednio ministrowi obrony swoje sprawozdanie zawierające ustalenia pokontrolne oraz niezbędne środki usprawniające. Na podstawie sprawozdania Biura Inspektora ds. Przestrzegania Prawa minister obrony może zarządzić wdrożenie zaproponowanych środków naprawczych. Za wdrożenie tych środków odpowiada zastępca wiceministra, który ma obowiązek złożyć ministrowi obrony sprawozdanie ze stanu ich wdrożenia.

Ze względów dodatkowej przejrzystości wyniki kontroli obronności publikuje się obecnie na stronie internetowej Ministerstwa Obrony (chociaż prawo tego nie wymaga).

Kontrole obronności mogą być trojakiego rodzaju:

(i) stałe kontrole obronności, tj. przeprowadzane okresowo ([31]);

(ii) kontrole obronności mające na celu określenie efektywności zastosowanych środków naprawczych; oraz

(iii) kontrole specjalne obronności przeprowadzane w niektórych sprawach na zarządzenie Ministra Obrony.

W ramach takich kontroli Generalny Inspektor może zwracać się do właściwego urzędu o przedstawienie sprawozdań i dokumentów, może wchodzić do pomieszczeń w celu przeprowadzenia kontroli, występować do zastępcy wiceministra o wyjaśnienia itd. Ze względu na charakter zadań kontrolnych Biura Inspektora ds. Przestrzegania Prawa na czele tego urzędu stoją najwyżsi rangą prawnicy (były prokurator naczelny).

4. Nadzór nad Agencją Bezpieczeństwa Publicznego

Agencja Bezpieczeństwa Publicznego przeprowadza zarówno kontrole stałe, jak i specjalne działalności poszczególnych jej biur i jednostek (Biuro Wywiadu Bezpieczeństwa Publicznego, jednostek wywiadu bezpieczeństwa publicznego oraz jednostek im podporządkowanych itp.). W celu stałej kontroli jako inspektorów wyznacza się zastępcę dyrektora generalnego lub dyrektora. Kontrole takie dotyczą również zarządzania informacjami osobowymi.

5. Nadzór sprawowany przez Diet

Jeżeli chodzi o zbieranie informacji do celów ścigania przestępstw, Diet, za pośrednictwem właściwej komisji, może badać, czy informacje w obszarze bezpieczeństwa narodowego są zbierane zgodnie z prawem. Uprawnienia śledcze Diet wynikają z art. 62 konstytucji oraz art. 74 i 104 ustawy o Diet.

C. Indywidualne dochodzenie roszczeń

Roszczeń można dochodzić indywidualnie tak samo, jak w obszarze ścigania przestępstw. Dotyczy to również nowego mechanizmu dochodzenia roszczeń, zarządzanego i nadzorowanego przez Komisję ds. Ochrony Informacji Osobowych, w zakresie rozpoznawania i rozstrzygania o skargach wniesionych przez obywateli UE. W tym zakresie zob. odpowiednie fragmenty sekcji II.C.

Ponadto w dziedzinie bezpieczeństwa narodowego dostępne są szczególne sposoby indywidualnego dochodzenia roszczeń.

Dane osobowe zbierane przez organ administracyjny do celów bezpieczeństwa narodowego podlegają przepisom rozdziału 4 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji. Chodzi tu o prawo do żądania ujawnienia (art. 12), prawo do korekty (w tym uzupełnienia lub wykreślenia) (art. 27) zatrzymanych informacji osobowych osoby fizycznej, a także prawo do wystąpienia o zawieszenie wykorzystywania informacji

([31]) Przykładem kontroli obszaru problemowego objętego niniejszym oświadczeniem może być „stała" kontrola obronności przeprowadzona w 2016 r., która dotyczyła „podnoszenia świadomości/gotowości w zakresie przestrzegania przepisów prawa". Ochrona informacji osobowych była tutaj jedną z najistotniejszych kwestii poddanych kontroli. Dokładniej rzecz biorąc, kontrola ta dotyczyła stanu zarządzania, przechowywania itp. informacji osobowych. W swoim sprawozdaniu Biuro Inspektora ds. Przestrzegania Prawa zidentyfikowało pewne wymagające działań naprawczych nieprawidłowości w zarządzaniu informacjami osobowymi, takie jak brak ochrony danych przy pomocy hasła. Sprawozdanie to udostępniono na stronie internetowej Ministerstwa Obrony.

osobowych w razie uzyskania przez organ administracyjny tych informacji w sposób bezprawny (art. 36). W związku z powyższym w obszarze bezpieczeństwa narodowego korzystanie z takich praw podlega pewnym ograniczeniom: wnioski o ujawnienie, korektę lub zawieszenie nie będą rozpatrywane, jeżeli dotyczą „informacji, co do których dyrektor organu administracyjnego ma uzasadnione podstawy, by sądzić, że ujawnienie to prawdopodobnie wywoła szkodę dla bezpieczeństwa narodowego, nadwyręży wzajemne zaufanie w stosunkach z innym państwem lub organizacją międzynarodową lub utrudni negocjacje z innym państwem lub organizacją międzynarodową" (art. 14 ppkt (iv)). Nie każde zatem dobrowolne zbieranie informacji dotyczących bezpieczeństwa narodowego jest objęte tym wyłączeniem, gdyż każdorazowo wymaga to przeprowadzenia szczegółowej oceny ryzyka związanego z ich ujawnieniem.

Ponadto, jeżeli wniosek danej osoby został odrzucony ze względu na to, że informacje uznaje się za niepodlegające ujawnieniu w rozumieniu art. 14 pkt (iv), osoba ta może złożyć odwołanie administracyjne o ponowne zbadanie takiej decyzji, twierdząc np., że w rozpatrywanej sprawie nie spełniono warunków określonych w art. 14 ppkt (iv). Wówczas przed podjęciem decyzji dyrektor organu administracyjnego rozpatrującego sprawę występuje do Rady ds. Oceny Ujawniania Informacji i Ochrony Informacji Osobowych. Rada oceni to odwołanie w sposób niezależny. Rada jest wysoce wyspecjalizowanym i niezależnym organem, którego członków powołuje premier za zgodą obu Izb Diet spośród osób wyróżniających się gruntowną wiedzą fachową ([32]). Rada ma szerokie uprawnienia śledcze, w tym może zwracać się o dokumenty i ujawnienie istotnych w sprawie informacji osobowych. Rada obraduje przy drzwiach zamkniętych oraz stosuje procedurę indeksu Vaughna ([33]). Następnie Rada sporządza pisemne sprawozdanie, które przekazuje osobie, której sprawa dotyczy ([34]). Ustalenia zawarte w sprawozdaniu podaje się do wiadomości publicznej. Choć sprawozdanie nie jest formalnie wiążące prawnie, prawie wszystkie organy administracyjne stosują się do niego ([35]).

Konkludując, zgodnie z art. 3 ust. 3 ustawy o sporach administracyjnych osoba fizyczna może zaskarżyć decyzję organu administracyjnego odmawiającą ujawnienia informacji osobowych.

IV. **Przegląd okresowy**

W ramach okresowego przeglądu decyzji stwierdzającej odpowiedni stopień ochrony Komisja ds. Ochrony Informacji Osobowych i Komisja Europejska będą wymieniać się informacjami dotyczącymi przetwarzana danych na warunkach przewidzianych w ustaleniu dotyczącym adekwatności, w tym określonych w niniejszym oświadczeniu.

([32]) Zob. art. 4 ustawy o powołaniu Rady ds. Oceny Ujawniania Informacji i Ochrony Informacji Osobowych.
([33]) Zob. art. 9 ustawy o powołaniu Rady ds. Oceny Ujawniania Informacji i Ochrony Informacji Osobowych.
([34]) Zob. art. 16 ustawy o powołaniu Rady ds. Oceny Ujawniania Informacji i Ochrony Informacji Osobowych.
([35]) W ostatnich 3 latach nie było przypadku, w którym dany organ administracyjny podjąłby decyzję niezgodną z wnioskami Rady. W przeszłości odnotowano bardzo mało spraw, w których organ podjął taką decyzję: od 2005 r. (kiedy ustawa o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji weszła w życie) spośród 2 000 spraw łącznie miały miejsce jedynie dwa takie przypadki. Jeżeli organ administracyjny ustali/rozstrzygnie niezgodnie z wnioskami Rady, zgodnie z art. 50 ust. 1 pkt 4 ustawy o kontroli skarg administracyjnych w brzmieniu nadanym nowym art. 42 ust. 2 ustawy o ochronie informacji osobowych znajdujących się w posiadaniu organów administracji, organ ten w sposób wyraźny wskazuje motywy podjęcia takiej decyzji.