Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2026/179

28.1.2026

DECYZJA WYKONAWCZA KOMISJI (UE) 2026/179

z dnia 26 stycznia 2026 r.

na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych przez Brazylię

(notyfikowana jako dokument nr C(2026) 373)

(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 ([1]) (ogólne rozporządzenie o ochronie danych), w szczególności jego art. 45 ust. 3,

a także mając na uwadze, co następuje:

1. WPROWADZENIE

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

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

(3) Jak określono w art. 45 ust. 2 rozporządzenia (UE) 2016/679, przy przyjmowaniu decyzji stwierdzającej odpowiedni stopień ochrony należy opierać się na wszechstronnej analizie porządku prawnego państwa trzeciego, obejmującej zarówno jego przepisy dotyczące podmiotów odbierających dane, jak i ograniczenia oraz zabezpieczenia w zakresie dostępu organów publicznych do danych osobowych. W swojej ocenie Komisja musi ustalić, czy dane państwo trzecie gwarantuje stopień ochrony „zasadniczo odpowiadający" stopniowi ochrony zapewnianemu w Unii Europejskiej ([3]). Oceny spełnienia tego warunku dokonuje się według standardu ustanowionego w przepisach Unii Europejskiej, w szczególności w rozporządzeniu (UE) 2016/679, a także w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej ([4]). Istotne znaczenie pod tym względem ma również dokument w sprawie odpowiedniego stopnia ochrony opracowany przez Europejską Radę Ochrony Danych (EROD), który ma na celu doprecyzowanie wspomnianego standardu i zapewnienie wytycznych ([5]).

([1]) Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Motyw 101 rozporządzenia (UE) 2016/679.
([3]) Motyw 104 rozporządzenia (UE) 2016/679.
([4]) Sprawa C-311/18, Facebook Ireland i Schrems („Schrems II"), ECLI:EU:C:2020:559.
([5]) Europejska Rada Ochrony Danych, dokument w sprawie odpowiedniego stopnia ochrony, WP 254 rev. 01. Dokument dostępny na stronie: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Jak wyjaśnił Trybunał Sprawiedliwości Unii Europejskiej, od państwa trzeciego nie można wymagać zapewnienia poziomu ochrony identycznego z tym, jaki jest zagwarantowany w unijnym porządku prawnym ([6]). W szczególności środki, z których korzysta dane państwo trzecie do zapewnienia ochrony danych osobowych, mogą różnić się od środków stosowanych w Unii, o ile w praktyce skutecznie zapewniają odpowiedni stopień ochrony ([7]). Odpowiedni standard ochrony nie wymaga zatem dokładnego powielenia przepisów unijnych. Przy badaniu odpowiedniości chodzi raczej o stwierdzenie, czy – biorąc pod uwagę istotę praw do prywatności oraz zabezpieczenia służące ochronie danych (w tym ich skuteczne wprowadzenie w życie, egzekwowanie i nadzór nad ich przestrzeganiem), a także okoliczności przekazywania danych osobowych – dany zagraniczny system jako całość zapewnia wymagany stopień ochrony ([8]).

(5) Komisja przeanalizowała prawo i praktykę Federacyjnej Republiki Brazylii („Brazylia"). Na podstawie ustaleń przedstawionych w motywach 7–223 Komisja stwierdza, że Brazylia zapewnia odpowiedni stopień ochrony danych osobowych przekazywanych w ramach zakresu stosowania rozporządzenia (UE) 2016/679 z Unii Europejskiej do Brazylii.

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

2. PRZEPISY MAJĄCE ZASTOSOWANIE DO PRZETWARZANIA DANYCH OSOBOWYCH

2.1. Ramy konstytucyjne Brazylii

(7) Brazylia jest republiką związkową, w której skład wchodzi 26 stanów oraz Dystrykt Federalny, ustanowioną w konstytucji federalnej („konstytucja") ([9]). Brazylijskie stany mają również własne konstytucje, które nie mogą być sprzeczne z konstytucją federalną ([10]). W Brazylii obowiązuje system prezydencki, w którym prezydent i członkowie izb ustawodawczych (tj. Izby Deputowanych i Senatu Federalnego) są wybierani w wyborach bezpośrednich.

(8) W konstytucji ochronie prywatności i danych przyznano ochronę jako prawom podstawowym. Dokładniej rzecz ujmując, art. 5 (X) konstytucji chroni intymność i życie prywatne osób fizycznych, art. 5 (XII) gwarantuje tajemnicę korespondencji i komunikacji, w tym danych, a art. 5 (LXXIX) ustanawia prawo do ochrony danych osobowych zarówno w internecie, jak i poza nim ([11]).

(9) Zgodnie z art. 5 konstytucji wszystkie wynikające z niej prawa mają zastosowanie do obywateli Brazylii oraz cudzoziemców zamieszkujących na jej terytorium. W przepisach federalnych doprecyzowano, że każda osoba przebywająca na terytorium Brazylii, niezależnie od miejsca zamieszkania, jest uprawniona do ochrony praw podstawowych ([12]). Zakres ochrony tych praw został dodatkowo rozszerzony w orzecznictwie konstytucyjnym na cudzoziemców mieszkających za granicą, co podkreślono również w odpowiedniej doktrynie prawnej ([13]). W rezultacie każdy cudzoziemiec, niezależnie od tego, czy mieszka w Brazylii, może powoływać się na te konstytucyjne gwarancje ([14]).

([6]) Sprawa C-362/14, Schrems („Schrems I"), ECLI:EU:C:2015:650, pkt 73.
([7]) Schrems I, pkt 74.
([8]) Schrems I, pkt 75.
([9]) Konstytucja Federacyjnej Republiki Brazylii z 1988 r. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.
([10]) Art. 25 konstytucji Federacyjnej Republiki Brazylii z 1988 r.
([11]) Poprawka do konstytucji nr 115 z dnia 10 lutego 2022 r. Dokument dostępny na stronie: http://www.planalto.gov.br/ccivil_03/Constituicao/Emendas/Emc/emc115.htm#art1.
([12]) Zob. na przykład art. 4 (XIII), ustawa nr 13.445 z dnia 24 maja 2017 r., ustawa o migracji. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13445.htm#:~:text=Institui%20a%20Lei%20de%20Migra%C3%A7%C3%A3o.&text=Art.,pol%C3%ADticas%20p%C3%BAblicas%20para%20o%20emigrante.
([13]) Zob. np. FERREIRA FILHO, Manoel Gonçalves, Direitos humanos fundamentais. wyd. 6, São Paulo: Saraiva, 2004 r.
([14]) Orzeczenie wydane przez Superior Tribunal de Justiça, izba czwarta, 2016 r. Dokument dostępny na stronie: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.

(10) W 1992 r. Brazylia ratyfikowała Amerykańską Konwencję Praw Człowieka, zwaną „paktem z San José" ([15]) („konwencja"). Między innymi art. 11 konwencji gwarantuje prawo do prywatności, a art. 8 chroni prawo do rzetelnego procesu sądowego. W 1998 r. Brazylia uznała wiążącą moc orzeczeń Międzyamerykańskiego Trybunału Praw Człowieka w zakresie wykładni i stosowania konwencji ([16]). Trybunał może wydawać orzeczenia dotyczące stosowania praw w kontekście działań podejmowanych przez organy publiczne w Brazylii, w tym organy wykonujące zadania związane z bezpieczeństwem publicznym i obroną ([17]).

2.2. **Ramy ochrony danych w Brazylii**

(11) W 2018 r. Brazylia uchwaliła ogólne przepisy w zakresie ochrony danych, które zapewniają gwarancje wszystkim osobom fizycznym, niezależnie od ich narodowości: ogólną ustawę o ochronie danych – Lei Geral de Proteção de Dados (LGPD) ([18]).

(12) Od czasu uchwalenia ustawę tę wzmocniono i doprecyzowano za pomocą dalszych przepisów. W szczególności ustawą nr 13.853 z 2019 r. utworzono brazylijski organ ochrony danych (Agência Nacional de Proteção de Dados, „ANPD") ([19]), który został uznany za niezależny organ na mocy przepisów przyjętych w 2022 r. ([20]) Kolejne wiążące dekrety uzupełniły te przepisy m.in. w celu aktualizacji statusu ANPD ([21]), dalszego określenia jego składu i procedury mianowania jego dyrektorów ([22]).

(13) Jak opisano bardziej szczegółowo w motywach 125–141 niniejszej decyzji, ANPD jest organem odpowiedzialnym za wykładnię i egzekwowanie przepisów LGPD. W tym kontekście regularnie wydaje on wiążące rozporządzenia co do interpretacji i zastosowania prawa. Na przykład przyjął szereg rozporządzeń mających na celu dalszy rozwój systemu sankcji i określenie zasad powiadamiania o naruszeniu ochrony danych ([23]). ANPD zapewnia dalsze wytyczne dotyczące stosowania i wykładni przepisów LGPD za pośrednictwem dokumentów i przewodników, takich jak te przyjęte w odniesieniu do interpretacji podstawy prawnej (np. prawnie uzasadnionego interesu) i kluczowych pojęć wynikających z LGPD (np. sankcje, inspektor ochrony danych).

([15]) Wykaz sygnatariuszy i ratyfikacja, Amerykańska Konwencja Praw Człowieka. Dokument dostępny na stronie: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm.

([16]) Deklaracja Brazylii dotycząca konwencji. Dokument dostępny na stronie: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm#Brazil.

([17]) Zob. np. sprawa Escher i in. przeciwko Brazylii, wyrok z dnia 6 lipca 2009 r. Dokument dostępny na stronie: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf.

([18]) Ustawa nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych. Dokument dostępny na stronie: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm, a w języku angielskim na stronie: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf.

([19]) Ustawa nr 13.853 z dnia 8 lipca 2019 r. zmieniająca LGPD m.in. w celu utworzenia organu ochrony danych – Autoridade Nacional de Proteção de Dados (ANPD). Dokument dostępny na stronie: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2.

([20]) Ustawa nr 14.460 z dnia 25 października 2022 r. przekształcająca ANPD w organ o statusie szczególnym. Dokument dostępny na stronie: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7.

([21]) Dekret nr 1.317 z dnia 17 września 2025 r. zmieniający LGPD w celu przekształcenia Agência Nacional de Proteção de Dados. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

([22]) Dekret nr 10.474 z dnia 26 sierpnia 2020 r. ustanawiający ANPD i jego skład. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226; dekret nr 11.758 z 30 października 2023 r. zmieniający skład ANPD. Dokument dostępny na stronie: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11758.htm; dekret z dnia 5 listopada 2020 r. w sprawie mianowania dyrektorów ANPD. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/decretos-de-5-de-novembro-de-2020-286734594.

([23]) Zob. wykaz rozporządzeń ANPD. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes, a w szczególności rozporządzenie nr 4 z dnia 24 lutego 2024 r. w sprawie stosowania sankcji administracyjnych. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077; oraz rozporządzenie nr 15 z dnia 24 kwietnia 2024 r. w sprawie powiadamiania o naruszeniu ochrony danych. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

(14) W ramach zaangażowania na rzecz promowania i ochrony danych na szczeblu międzynarodowym w 2023 r. brazylijski ANPD przystąpił do Globalnego Zgromadzenia ds. Prywatności, do którego należą również wszystkie organy ochrony danych z Unii Europejskiej ([24]). Brazylia przystąpiła także, w charakterze obserwatora, do Komitetu ds. Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych ([25]). Brazylia odegrała ponadto wiodącą rolę w szeregu postępów poczynionych przez Organizację Narodów Zjednoczonych (ONZ) w zakresie prawa do prywatności. Wraz z Niemcami Brazylia przedstawiła rezolucje ONZ w sprawie prawa do prywatności w epoce cyfrowej, przyjęte przez Zgromadzenie Ogólne ONZ w latach 2013 i 2014 ([26]). W rezolucjach tych wskazano między innymi, że „bezprawna lub arbitralna inwigilacja lub przechwytywanie komunikacji, a także bezprawne lub arbitralne gromadzenie danych osobowych, jako działania wysoce inwazyjne, naruszają prawo do prywatności i wolności wypowiedzi i mogą być sprzeczne z założeniami społeczeństwa demokratycznego". Rezolucje wzywają państwa do przeglądu przepisów dotyczących gromadzenia danych w celu dostosowania ich do prawa międzynarodowego w zakresie praw człowieka oraz do „ustanowienia lub utrzymania istniejących niezależnych, skutecznych krajowych mechanizmów nadzoru zdolnych do zapewnienia, w stosownych przypadkach, przejrzystości i odpowiedzialności za państwowy nadzór nad komunikacją, przechwytywanie wiadomości i gromadzenie danych osobowych" ([27]).

(15) Pod względem struktury i głównych elementów ramy prawne Brazylii mające zastosowanie do danych osobowych przekazywanych na podstawie niniejszej decyzji są podobne do ram obowiązujących w Unii Europejskiej. Jest to związane z faktem, że ramy takie opierają się nie tylko na zobowiązaniach ustanowionych w prawie krajowym i prawach gwarantowanych w konstytucji, ale również na zobowiązaniach zapisanych w prawie międzynarodowym, w szczególności w rezultacie przystąpienia przez Brazylię do Amerykańskiej Konwencji Praw Człowieka, a także poddania się jurysdykcji Międzyamerykańskiego Trybunału Praw Człowieka ([28]).

2.3. **Przedmiotowy i terytorialny zakres stosowania LGPD**

2.3.1. *Terytorialny zakres stosowania*

(16) LGPD ma zastosowanie do każdego przetwarzania danych osobowych w Brazylii, niezależnie od środków wykorzystywanych do dokonywania takich czynności ([29]).

(17) Art. 3 LGPD określa terytorialny zakres stosowania ustawy, wskazując, że ma ona zastosowanie do: 1) czynności przetwarzania dokonywanych na terytorium Brazylii (obejmującym federację, stany, Dystrykt Federalny i gminy); 2) czynności przetwarzania, których celem jest oferowanie lub dostarczanie towarów lub usług, lub przetwarzanie danych osób fizycznych znajdujących się na terytorium Brazylii; oraz 3) przypadków, w których przetwarzane dane osobowe zostały zgromadzone na terytorium Brazylii. Jest to podejście podobne do podejścia przyjętego w art. 3 rozporządzenia (UE) 2016/679.

(18) Ponadto zgodnie z art. 3 (II) LGPD wszystkie operacje przetwarzania danych osobowych osób fizycznych znajdujących się na terytorium Brazylii podlegają przepisom tej ustawy. Obejmuje to przetwarzanie prowadzone w celu monitorowania zachowania osób fizycznych na tym terytorium, niezależnie od miejsca, w którym odbywa się przetwarzanie danych.

([24]) Globalne Zgromadzenie ds. Prywatności jest forum łączącym wysiłki ponad 130 organów ochrony danych i prywatności z całego świata. Zob. ogłoszenie ANPD dotyczące członkostwa w Globalnym Zgromadzeniu ds. Prywatności. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-aceita-como-membro-pleno-no-global-privacy-assembly.

([25]) Rada Europy, obserwatorzy Komitetu ds. Konwencji nr 108. Dokument dostępny na stronie: https://rm.coe.int/list-of-observers-december-2022-bilingual-2781-7012-1734-1/1680a962eb.

([26]) Zob. np. Zgromadzenie Ogólne Narodów Zjednoczonych, rezolucja w sprawie prawa do prywatności w epoce cyfrowej z 18 grudnia 2013 r. Dokument dostępny na stronie: https://digitallibrary.un.org/record/764407?ln=en&v=pdf.

([27]) Zgromadzenie Ogólne Narodów Zjednoczonych, rezolucja w sprawie prawa do prywatności w epoce cyfrowej z 18 grudnia 2013 r., s. 1.

([28]) Zob. Międzyamerykański Trybunał Praw Człowieka, Pytania i odpowiedzi dotyczące właściwości Trybunału. Dokument dostępny na stronie: https://www.corteidh.or.cr/que_es_la_corte.cfm?lang=en.

([29]) Art. 3 ustawy nr 13.70914 z sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

(19) Co więcej, zgodnie z orzecznictwem Federalnego Sądu Najwyższego (Supremo Tribunal Federal – „STF") ochrona praw podstawowych przyznana na mocy konstytucji – jak prawo do ochrony danych – ma zastosowanie do każdej osoby, niezależnie od narodowości lub miejsca zamieszkania osoby, której dane dotyczą ([30]).

2.3.2. *Definicja danych osobowych*

(20) W art. 5 (I) LGPD zdefiniowano dane osobowe jako informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Ustawa stanowi, że „osoba, której dane dotyczą", to „osoba fizyczna, do której odnoszą się przetwarzane dane osobowe" ([31]).

(21) Ponadto informacje spseudonimizowane – tj. informacje, za pomocą których nie można zidentyfikować konkretnej osoby fizycznej bez wykorzystania dodatkowych informacji lub połączenia ich z dodatkowymi informacjami w celu przywrócenia ich do stanu pierwotnego – są uznawane za dane osobowe w rozumieniu LGPD ([32]).

(22) Z kolei informacje, które są całkowicie „zanonimizowane", są wyłączone z zakresu stosowania LGPD ([33]). Zgodnie z art. 5 LGPD dane zanonimizowane definiuje się jako dane, których nie można bezpośrednio lub pośrednio powiązać z osobą fizyczną przy użyciu racjonalnych i technicznych środków dostępnych w momencie przetwarzania. W art. 12 LGPD doprecyzowano, że danych zanonimizowanych nie uznaje się za dane osobowe, chyba że proces anonimizacji, któremu je poddano, został odwrócony lub może zostać odwrócony w drodze „racjonalnych starań". W art. 12 LGPD podkreślono również, że przy określaniu tego, co uznaje się za „racjonalne", uwzględnia się obiektywne czynniki, takie jak: 1) koszt i czas potrzebne do odwrócenia procesu; 2) dostępna technologia; oraz 3) wyłączne korzystanie z własnych środków administratora danych. Podejście do anonimizacji i zabezpieczenia wprowadzone w LGPD w celu uwzględnienia możliwości ponownej identyfikacji jest podobne do podejścia stosowanego w UE.

(23) Odpowiada to zakresowi przedmiotowemu rozporządzenia (UE) 2016/679 i używanym w nim pojęciom „danych osobowych", „pseudonimizacji" i „informacji zanonimizowanych".

2.3.3. *Definicja przetwarzania*

(24) Zarówno systemy Unii Europejskiej, jak i te obowiązujące w Brazylii definiują „przetwarzanie" jako „dowolną operację" wykonywaną w zakresie danych osobowych ([34]). Art. 5 (X) LGPD zawiera następujący niewyczerpujący wykaz czynności stanowiących przetwarzanie danych: „zbieranie, wytwarzanie, odbiór, klasyfikowanie, wykorzystywanie, dostęp, powielanie, przekazywanie, przesyłanie, przetwarzanie, archiwizowanie, przechowywanie, usuwanie, ocenianie lub kontrolowanie informacji, modyfikowanie, ujawnianie, transfer, rozpowszechnianie lub pobieranie".

2.3.4. *Administrator i podmiot przetwarzający*

(25) Pojęcie administratora danych zostało zdefiniowane w LGPD, zgodnie z którą jest to osoba fizyczna lub prawna, publiczna lub prywatna, odpowiedzialna za decyzje dotyczące przetwarzania danych osobowych ([35]).

([30]) Decyzja wydana przez Superior Tribunal de Justiça, izba czwarta, 2016 r. Dokument dostępny na stronie: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.

([31]) Art. 5 (V) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([32]) Art. 13 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([33]) Art. 12 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([34]) Art. 5 (X) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([35]) Art. 5 (VI) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

(26) Pojęcie podmiotu przetwarzającego dane zostało zdefiniowane w LGPD, zgodnie z którą jest to osoba fizyczna lub prawna, publiczna lub prywatna, która przetwarza dane osobowe w imieniu administratora ([36]). Podmiot przetwarzający musi prowadzić przetwarzanie zgodnie z instrukcjami przekazanymi przez administratora, który odpowiada za weryfikację zgodności ([37]).

(27) Administrator i podmiot przetwarzający mają obowiązek prowadzenia rejestru operacji przetwarzania danych, które wykonują, w szczególności gdy podstawą przetwarzania jest prawnie uzasadniony interes ([38]).

(28) Zgodnie z LGPD dwóch lub więcej administratorów, którzy są bezpośrednio zaangażowani w przetwarzanie danych, w wyniku którego osoba, której dane dotyczą, doznała szkody, ponosi odpowiedzialność solidarną ([39]). Podmiot przetwarzający ponosi odpowiedzialność solidarną za szkody spowodowane przetwarzaniem, jeżeli nie wypełnia obowiązków określonych w art. 44 LGPD lub gdy nie zastosował się do instrukcji prawnych administratora ([40]).

(29) W związku z tym przepisy LGPD regulujące stosunki między administratorami a podmiotami przetwarzającymi są podobne do przepisów rozdziału IV rozporządzenia (UE) 2016/679.

2.3.5. *Wyłączenie stosowania niektórych przepisów LGPD*

(30) Podobnie jak w systemie obowiązującym w Unii Europejskiej, LGPD nie ma zastosowania do danych zanonimizowanych ([41]), do przetwarzania danych osobowych do użytku domowego ([42]) ani do celów związanych wyłącznie z bezpieczeństwem publicznym, obroną narodową, bezpieczeństwem państwa lub śledzeniem i ściganiem przestępstw ([43]).

(31) Wyłączenie w obszarach bezpieczeństwa publicznego, obrony narodowej, bezpieczeństwa państwa oraz śledzenia i ścigania przestępstw jest jednak częściowe. Federalny Sąd Najwyższy dokonał wykładni stosowania LGPD w świetle konstytucyjnej ochrony danych osobowych i ustalił, że główne zasady, prawa i cele LGPD mają zastosowanie do wszelkiego przetwarzania danych osobowych przez organy publiczne, w tym do celów wywiadowczych ([44]). Ponadto warunki przetwarzania danych osobowych do celów bezpieczeństwa publicznego, obrony narodowej, bezpieczeństwa państwa lub prowadzenia postępowań przygotowawczych i ścigania przestępstw określono w art. 4 ust. 2–4 LGPD, w szczególności aby uniemożliwić podmiotom prywatnym przetwarzanie danych do takich celów, nakazać ANPD wydanie opinii technicznych i zaleceń w tej sprawie oraz

([36]) Art. 5 (VII) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([37]) Art. 39 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([38]) Art. 37 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([39]) Art. 42 ust. 1 (II) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([40]) Art. 42 ust. 1 (I) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([41]) Art. 12 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([42]) Art. 4 (I) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([43]) Art. 4 (III) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([44]) Federalny Sąd Najwyższy. Orzeczenie w sprawie ADI 6649, wrzesień 2022 r. Dokument dostępny na stronie: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

upoważnić ANPD do zwracania się o ocenę skutków dla ochrony danych w odniesieniu do takich działań ([45]). Na tej podstawie ANPD prowadził np. postępowania i wydał wytyczne, takie jak nota techniczna skierowana do Ministerstwa Sprawiedliwości i Bezpieczeństwa Publicznego, dotycząca stosowania technologii, w tym rozpoznawania twarzy, w przestrzeni publicznej ([46]). W nocie tej ANPD przypomniał, że przetwarzanie danych do tych celów musi odbywać się zgodnie z ogólnymi zasadami i prawami przewidzianymi w LGPD ([47]).

(32) W art. 4 (II) LGPD wprowadzono ponadto częściowe wyłączenie stosowania przepisów ustawy w odniesieniu do przetwarzania danych osobowych do celów badań naukowych oraz w celach dziennikarskich i na potrzeby wyrazu artystycznego.

(33) W odniesieniu do badań naukowych istnieje kilka elementów ograniczających przedmiotowe wyłączenie. Po pierwsze, zgodnie z art. 4 (II) LGPD przetwarzanie musi odbywać się „wyłącznie" do celów badań naukowych. Po drugie, art. 4 (II) lit. b) LGPD stanowi, że do tego rodzaju przetwarzania mają zastosowanie art. 7 (wymóg dotyczący wskazania podstawy prawnej) i art. 11 (przepisy dotyczące przetwarzania danych wrażliwych) ([48]). Po trzecie, ANPD opracował przewodnik wprowadzający, aby doprecyzować zasady mające zastosowanie do przetwarzania danych do celów badań naukowych, w tym poprzez ścisłe określenie, które podmioty można uznać za „jednostkę badawczą" w rozumieniu art. 5 (XVII) LGPD ([49]). W przewodniku tym ANPD potwierdza, że przetwarzanie danych do celów badań naukowych podlega jedynie częściowemu wyłączeniu stosowania przepisów LGPD, a ogólne zasady przewidziane w ustawie nadal mają zastosowanie ([50]).

(34) W odniesieniu do danych wykorzystywanych do badań naukowych w dziedzinie zdrowia LGPD przewiduje dodatkowe ograniczenia. Z jednej strony art. 13 LGPD określa obowiązki w zakresie bezpieczeństwa w odniesieniu do wykorzystywanych baz danych i zachęca do stosowania technik anonimizacji i pseudonimizacji. Stanowi on również, że jednostki badawcze ponoszą odpowiedzialność za niewdrożenie środków bezpieczeństwa w celu ochrony danych osobowych ([51]). Z drugiej strony przekazywanie danych wykorzystywanych do badań naukowych w dziedzinie zdrowia osobie trzeciej „jest zabronione w każdych okolicznościach" ([52]).

(35) W odniesieniu do przetwarzania danych osobowych w celach dziennikarskich i na potrzeby wyrazu artystycznego wyłączenie przewidziane w LGPD jest podobne do wyłączenia przewidzianego w art. 85 ust. 2 rozporządzenia (UE) 2016/679. Wyłączenie na gruncie LGPD obejmuje sytuację, w której przetwarzanie odbywałoby się „wyłącznie" do tych celów ([53]). Oznacza to, że gdy prasa, media lub podmioty artystyczne przetwarzają dane osobowe do innych celów, takich jak zarządzanie zasobami ludzkimi lub administracja wewnętrzna, LGPD ma zastosowanie w pełnym zakresie.

([45]) Art. 4 ust. 2–4 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([46]) Nota techniczna nr 175/2023 w sprawie projektu umowy o współpracy między Ministerstwem Sprawiedliwości i Bezpieczeństwa Publicznego a brazylijską Federacją Piłki Nożnej w sprawie udostępniania danych osobowych w celu usprawnienia „Projektu Bezpieczny Stadion". Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

([47]) Nota techniczna nr 175/2023, pkt 5.1.

([48]) Art. 4 (II) lit. b) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([49]) Przewodnik wprowadzający opracowany przez ANPD na temat przetwarzania danych osobowych do celów badań naukowych z czerwca 2023 r. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf.

([50]) Zob. w szczególności s. 18–43 przewodnika wprowadzającego dotyczącego przetwarzania danych osobowych do celów akademickich i prowadzenia badań.

([51]) Art. 13 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([52]) Art. 13 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych. Zob. również Przewodnik wprowadzający opracowany przez ANPD na temat przetwarzania danych osobowych do celów badań naukowych z czerwca 2023 r., s. 15.

([53]) Art. 4 (II) lit. a) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

(36) Zarówno wyraz artystyczny, jak i wolność mediów stanowią część wolności wypowiedzi w myśl art. 5 (IX) konstytucji, który gwarantuje wolność wypowiedzi w sferach „intelektualnej, artystycznej, naukowej i komunikacyjnej". Jeżeli chodzi o wyważenie wolności wypowiedzi i innych praw (w tym prawa do prywatności i ochrony danych), kwestia ta podlega kryteriom określonym w konstytucji zgodnie z wykładnią Federalnego Sądu Najwyższego. W szczególności korzystanie z prawa do wolności wypowiedzi nie wymaga uprzedniej zgody, lecz podlega ograniczeniom ustanowionym w celu ochrony innych praw podstawowych. Osoba fizyczna może dochodzić odszkodowania w przypadku wystąpienia szkody lub naruszenia prawa do prywatności, zgodnie z art. 5 (X) konstytucji. Ponadto zabezpieczenia te uwzględniono w obywatelskich ramach prawnych w internecie – ustawie przyjętej w 2014 r. w celu ochrony praw podstawowych w internecie ([54]). W szczególności art. 7 (I) obywatelskich ram prawnych w internecie gwarantuje „nienaruszalność prywatności" i ustanawia prawo do odszkodowania za wszelkie szkody materialne lub niematerialne wynikające z naruszenia. Dodatkowo Federalny Sąd Najwyższy odnosi się w swoim orzecznictwie do potrzeby „ustanowienia równowagi między prawami, godząc prawo do wolności wypowiedzi z nienaruszalnością prywatności", podkreślając znaczenie praw do dochodzenia roszczeń i dostępu do środka odwoławczego w przypadku naruszenia prywatności ([55]). W innym przypadku Federalny Sąd Najwyższy przypomniał, że „korzystanie z wolności prasy i komunikacji społecznej musi odbywać się w zgodzie z innymi zasadami konstytucyjnymi", takimi jak nienaruszalność prywatności i prawo do ochrony danych ([56]).

(37) Ponadto LGPD wyłącza z zakresu stosowania przepisów ustawy przetwarzanie danych, które pochodzą spoza Brazylii i które 1) nie są udostępniane ani przekazywane podmiotom przetwarzającym w Brazylii albo 2) pochodzą z kraju, który został uznany za odpowiedni na gruncie LGPD, o ile nie są one przekazywane do innego państwa ([57]). ANPD przedstawił wiążącą interpretację w celu ścisłego doprecyzowania tych dwóch scenariuszy w rozporządzeniu w sprawie przekazywania danych ([58]).

(38) W pierwszym scenariuszu samo przesyłanie danych osobowych przez Brazylię, bez jakiegokolwiek dodatkowego przetwarzania w tym kraju, byłoby wyłączone z zakresu stosowania ustawy ([59]). Niemniej jednak LGPD miałaby zastosowanie od chwili, w której dane stałyby się dostępne, zostałyby wykorzystane lub w inny sposób przetworzone w Brazylii. Obowiązujące przepisy krajowe dotyczące cyberbezpieczeństwa i dostępu do danych przez organy publiczne nadal miałyby zastosowanie do tego ograniczonego scenariusza, niezależnie od tego, czy dane są przetwarzane, czy też są wyłącznie przesyłane.

(39) W drugim scenariuszu ANPD doprecyzował, że z zakresu stosowania ustawy wyłączone jest jedynie przekazywanie z powrotem danych, które pierwotnie przekazano z kraju korzystającego z decyzji stwierdzającej odpowiedni stopień ochrony na gruncie LGPD, o ile do tego przetwarzania stosuje się prawo krajowe tego kraju uznanego za odpowiedni. Również w tym przypadku nadal miałyby zastosowanie przepisy dotyczące cyberbezpieczeństwa i dostępu do danych przez organy publiczne. W kontekście przekazywania danych osobowych między UE a Brazylią, w przypadku gdyby UE korzystała z decyzji Brazylii stwierdzającej odpowiedni stopień ochrony, przekazywanie danych z Brazylii z powrotem do UE nie zawsze podlegałoby zakresowi stosowania art. 3 rozporządzenia (UE) 2016/679. W związku z tym w przypadkach, w których przetwarzanie nie wchodziłoby w zakres rozporządzenia (UE) 2016/679, z art. 8 (II) lit. b) rozporządzenia w sprawie przekazywania danych wynika, że LGPD miałaby zastosowanie do przekazywania danych z Brazylii z powrotem do UE.

([54]) Ustawa nr 12.965 z dnia 23 kwietnia 2014 r., Marco Civil da Internet (obywatelskie ramy prawne w internecie). Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([55]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 4815. Dokument dostępny na stronie: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057.

([56]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 5418. Dokument dostępny na stronie: https://www.jurisprudencia.stf.jus.br/pages/search/sjur446943/false.

([57]) Art. 4 (IV) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([58]) Sekcja III załącznika I, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych osobowych („rozporządzenie w sprawie przekazywania danych"). Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([59]) Art. 8 (I) ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych osobowych.

2.4. **Zabezpieczenia, prawa i obowiązki**

2.4.1. *Zgodność z prawem i rzetelność przetwarzania*

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

(41) Zasady zgodności z prawem, dobrej wiary i przejrzystości oraz podstawy zgodności przetwarzania z prawem są zagwarantowane w art. 6 i 7 LGPD poprzez warunki podobne do tych przewidzianych w art. 5 i 6 rozporządzenia (UE) 2016/679.

(42) Zgodnie z art. 6 i 7 LGPD administratorzy i podmioty przetwarzające przetwarzają dane osobowe zgodnie z prawem i w dobrej wierze w minimalnym zakresie niezbędnym do osiągnięcia określonego celu, obejmującym dane, które są istotne, proporcjonalne i nienadmierne w stosunku do celu przetwarzania ([60]).

(43) Te ogólne zasady zgodnego z prawem przetwarzania danych rozwinięto w art. 7 LGPD, w którym określono poszczególne podstawy prawne przetwarzania danych, w tym okoliczności, w których może się z nim wiązać zmiana celu.

(44) Zgodnie z art. 7 LGPD administrator i podmiot przetwarzający mogą przetwarzać dane osobowe wyłącznie w oparciu o ograniczoną liczbę podstaw prawnych. W LGPD przewidziano następujące podstawy prawne przetwarzania: 1) zgoda osoby, której dane dotyczą (pkt I); 2) konieczność wykonania umowy lub wstępnych procedur związanych z umową, której stroną jest osoba, której dane dotyczą, na wniosek osoby, której dane dotyczą (pkt V); 3) wypełnienie obowiązku prawnego lub regulacyjnego przez administratora ([61]) (pkt II); 4) ochrona życia lub bezpieczeństwa fizycznego osoby, której dane dotyczą, lub osoby trzeciej (pkt VII); 5) przetwarzanie danych przez administrację publiczną, które jest niezbędne do realizacji polityk publicznych przewidzianych w przepisach ustawowych i wykonawczych, lub w oparciu o umowy, porozumienia czy podobne instrumenty ([62]) (pkt III), oraz 6) gdy jest to konieczne do realizacji prawnie uzasadnionych interesów administratora lub osoby trzeciej, z wyjątkiem sytuacji, w których charakter nadrzędny mają podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych (pkt IX).

(45) W art. 7 LGPD przewidziano następujące cztery dodatkowe szczególne podstawy prawne przetwarzania danych: 1) prowadzenie badań przez jednostki badawcze, z zapewnieniem, w miarę możliwości, anonimizacji danych osobowych (pkt IV); 2) wykonywanie praw w postępowaniach sądowych, administracyjnych lub arbitrażowych ([63]) (pkt VI); 3) wyłącznie w celu ochrony zdrowia w procedurach prowadzonych przez pracowników służby zdrowia, podmioty opieki zdrowotnej, organy ds. ochrony zdrowia lub organy sanitarne (pkt VIII); oraz 4) w celu ochrony kredytowej (pkt X) ([64]).

([60]) Zob. w szczególności główny akapit art. 6 (III), (I) i (V) oraz art. 7 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([61]) Każdy obowiązek prawny lub regulacyjny musi być określony ustawą oraz musi być konieczny i proporcjonalny.

([62]) Należy przestrzegać przepisów szczegółowych dotyczących przetwarzania danych osobowych przez organy publiczne, przewidzianych w rozdziale IV ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([63]) Procedury te opisano w ustawie nr 9.307 z dnia 23 września 1996 r. – prawo arbitrażowe.

([64]) Jeżeli chodzi o ochronę kredytową, włączenie tej podstawy prawnej do LGPD zwiększyło poziom ochrony osób, których dane dotyczą, zapewniając m.in., że instytucje kredytowe mogą przetwarzać wyłącznie dane osobowe niezbędne do analizy kredytowej i dochodzenia należności. Od czasu przyjęcia LGPD sądy w Brazylii wydały szereg orzeczeń, w których ograniczyły na przykład przetwarzanie danych do celów ochrony kredytowej poprzez wyłączenie danych takich jak „numer w rejestrze wyborców, imię matki, styl życia, klasa społeczna, wykształcenie, krańcowa skłonność do konsumpcji i georeferencje", które nie zostały uznane za niezbędne. Sądy doprecyzowały również, że dalszy dostęp do danych osobowych wymaga zgody osoby, której dane dotyczą, ograniczając tym samym zakres przetwarzania danych do celów ochrony kredytowej. Zob. Opice Blum Advogados, Jurimetrics Report, 2022 r. Dokument dostępny na stronie: https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf.

2.4.2. *Kryteria ważności zgody*

(46) Wymogi formalne dotyczące uzyskania ważnej zgody na przetwarzanie danych osobowych na podstawie LGPD określono w art. 8, przyjmując podejście podobne do zastosowanego w art. 4 ust. 11 i art. 7 rozporządzenia (UE) 2016/679. Po pierwsze, zgoda musi być wyrażona na piśmie lub za pomocą innych środków pozwalających wykazać „przejaw woli" osoby, której dane dotyczą ([65]). W swoich wytycznych ANPD doprecyzował, że „zgoda musi być jednoznaczna, co wymaga uzyskania jasnego i pozytywnego wyrażenia woli przez osobę, której dane dotyczą", i oznacza, że nie jest dozwolone uzyskanie zgody „w sposób dorozumiany ani w wyniku zaniechania osoby, której dane dotyczą" ([66]). Po drugie, zgoda musi odnosić się do „określonych celów", a „ogólne zezwolenia na przetwarzanie" danych osobowych należy uznać za nieważne ([67]). Po trzecie, zgodę wyraża się za pomocą informacji przekazywanych w „przejrzysty, jasny i niebudzący wątpliwości" sposób ([68]). W przypadku zawarcia zgody w treści umowy należy ją umieścić w oddzielnej i wyraźnie wyodrębnionej klauzuli, wyróżniającej się spośród innych postanowień umownych ([69]). Ponadto zgodę uznaje się za nieważną, jeżeli informacje przekazane osobie, której dane dotyczą, zawierają „treści wprowadzające w błąd lub stanowiące nadużycie" ([70]). Administrator musi również poinformować osobę, której dane dotyczą, o wszelkich zmianach dotyczących: 1) określonego celu przetwarzania; 2) rodzaju lub czasu trwania przetwarzania; 3) tożsamości administratora danych; lub 4) wszelkich informacji dotyczących przetwarzania i ewentualnego udostępniania danych ([71]). Po czwarte, zgoda może zostać „odwołana w dowolnym momencie" przez osobę, której dane dotyczą, w drodze „bezpłatnej procedury" ([72]).

(47) LGPD ustanawia ścisły zakaz przetwarzania danych osobowych, w przypadku gdy zgoda jest wadliwa lub nieważna ([73]). W LGPD doprecyzowano ponadto, że na administratorze spoczywa ciężar dowodu w celu wykazania, że zgodę uzyskano zgodnie z prawem i z LGPD ([74]).

(48) Wreszcie, LGPD stanowi, że w sytuacji, gdy zgoda byłaby właściwą podstawą prawną przetwarzania, jeżeli dane osobowe zostały „w sposób oczywisty upublicznione przez osobę, której dane dotyczą", wymóg uzyskania zgody uznaje się za zniesiony ([75]). Pojęcie „w sposób oczywisty upublicznionych danych" występuje również w art. 9 rozporządzenia (UE) 2016/679. Jednakże nawet w sytuacji, gdy wymóg zgody uznaje się za zniesiony, administratorzy i podmioty przetwarzające nie są zwolnieni z przestrzegania wszystkich pozostałych praw i obowiązków określonych w LGPD ([76]). W szczególności dane, które zostały w sposób oczywisty upublicznione przez osobę, której dane dotyczą, mogą być dalej przetwarzane, pod warunkiem że odbywa się to w „uzasadnionym i konkretnym" celu oraz z poszanowaniem praw osób, których dane dotyczą, a także zasad ustanowionych w LGPD ([77]).

([65]) Główny akapit art. 8 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([66]) ANPD, Przewodnik dotyczący plików cookie i ochrony danych, s. 18. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.

([67]) Art. 8 ust. 4 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych. Ponadto, gdy dane osobowe mają być udostępniane pomiędzy administratorami, wymagana jest odrębna, szczególna zgoda na takie udostępnienie, chyba że dane te zostały w sposób oczywisty upublicznione, zgodnie z art. 7 ust. 5 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([68]) Art. 9 ust. 1 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([69]) Art. 8 ust. 1 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([70]) Art. 9 ust. 1 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([71]) Art. 8 ust. 6 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([72]) Art. 8 ust. 5 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([73]) Art. 8 ust. 3 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([74]) Art. 8 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([75]) Art. 7 ust. 4 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych. Zakres tego środka jest ograniczony, ponieważ nie obejmuje on przetwarzania danych wrażliwych dozwolonego na mocy art. 9 ust. 2 lit. e) rozporządzenia (UE) 2016/679.

([76]) Art. 7 ust. 4 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([77]) Art. 7 ust. 7 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

2.4.3. *Kryteria prawnie uzasadnionego interesu*

(49) Art. 7 (IX) LGPD stanowi, że przetwarzanie danych osobowych nigdy nie może odbywać się na podstawie prawnie uzasadnionego interesu, jeżeli takie przetwarzanie byłoby sprzeczne z prawami podstawowymi i wolnościami osób, których dane dotyczą, podkreślając, że ochrona danych osobowych ma charakter nadrzędny. Podejście to jest podobne do podejścia stosowanego w UE i określonego w art. 6 ust. 1 lit. f) rozporządzenia (UE) 2016/679.

(50) W art. 10 LGPD określono dodatkowe warunki, jakie muszą spełnić administratorzy, aby móc powołać się na „prawnie uzasadniony interes" jako podstawę prawną przetwarzania danych osobowych. Po pierwsze, gdy przetwarzanie danych osobowych opiera się na prawnie uzasadnionym interesie, administrator przetwarza wyłącznie dane osobowe, które są „ściśle niezbędne" do osiągnięcia zamierzonego celu ([78]). Po drugie, administratorzy muszą również wdrożyć środki zapewniające przejrzystość wykonywanych czynności przetwarzania ([79]). Po trzecie, na prawnie uzasadniony interes można powoływać się wyłącznie w „konkretnych sytuacjach" ([80]).

(51) Ponadto ANPD opublikował „Przewodnik dotyczący prawnie uzasadnionego interesu", w którym wyszczególniono warunki stosowania tej podstawy prawnej ([81]). W przewodniku tym wyjaśniono na przykład, że prawnie uzasadniony interes nie może być wykorzystywany jako podstawa prawna do przetwarzania danych wrażliwych ([82]), a w załączniku zawarto również model testu wyważenia ochrony praw podstawowych i wolności, z którego może skorzystać każdy administrator pragnący powołać się na prawnie uzasadniony interes jako podstawę przetwarzania danych ([83]). Dodatkowo ANPD może zażądać od administratora przeprowadzenia oceny skutków dla ochrony danych ([84]).

(52) W przewodniku ANPD wyjaśnił, że aby dany interes można było uznać za „prawnie uzasadniony", muszą zostać spełnione trzy warunki: 1) zgodność z brazylijskim systemem prawnym; 2) odniesienie do konkretnej sytuacji; oraz 3) powiązanie przetwarzania z celami, które są zgodne z prawem, konkretne i wyraźnie określone ([85]). Pierwszy warunek – zgodność z systemem prawnym – zakłada, że interes, na który powołuje się administrator, musi być zgodny z zasadami, normami prawnymi i prawami podstawowymi gwarantowanymi w Brazylii. Oznacza to na przykład, że planowane przetwarzanie danych osobowych nie może być zakazane przez prawo brazylijskie ani nie może, wprost ani pośrednio, być sprzeczne z przepisami prawnymi lub zasadami prawa Brazylii. Drugi warunek – konkretna sytuacja – oznacza, że prawnie uzasadniony interes, na który można się powołać, musi opierać się na „konkretnych, jasnych i precyzyjnych" sytuacjach, które służą realizacji jasno określonych interesów. Prawnie uzasadniony interes nie może opierać się na „sytuacjach abstrakcyjnych lub czysto spekulacyjnych" ([86]). ANPD precyzuje ponadto, że interesy, które nie są związane z „bieżącą działalnością administratora danych, nie są uznawane za prawnie uzasadnione" ([87]). Trzeci warunek – cel przetwarzania – odnosi się do konieczności wykazania konkretnego celu przetwarzania. ANPD zaznacza, że prawnie uzasadnionego

([78]) Art. 10 ust. 1 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([79]) Art. 10 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([80]) Art. 10 LGPD zawiera przykłady konkretnych sytuacji, w których można powoływać się na prawnie uzasadniony interes: 1) wspieranie i promowanie działań administratora danych (pkt I); 2) ochrona korzystania przez osobę, której dane dotyczą, z przysługujących jej praw lub umożliwienie świadczenia usług korzystnych dla osoby, której dane dotyczą, pod warunkiem że takie przetwarzanie odbywa się z poszanowaniem uzasadnionych oczekiwań, praw podstawowych i wolności osoby, której dane dotyczą (pkt II). Ustawa nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([81]) ANPD, Przewodnik – Podstawy prawne przetwarzania danych osobowych – prawnie uzasadniony interes, luty 2024 r. („Przewodnik dotyczący prawnie uzasadnionego interesu"). Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf.

([82]) ANPD, Przewodnik dotyczący prawnie uzasadnionego interesu, s. 8.

([83]) ANPD, Przewodnik dotyczący prawnie uzasadnionego interesu, załącznik 3.

([84]) Art. 10 ust. 3 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([85]) ANPD, Przewodnik dotyczący prawnie uzasadnionego interesu, s. 16.

([86]) ANPD, Przewodnik dotyczący prawnie uzasadnionego interesu, s. 16, interpretacja akapitu głównego art. 10 ustawy nr 13.709 z 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([87]) ANPD, Przewodnik dotyczący prawnie uzasadnionego interesu, s. 16.

interesu administratora (który uzasadnia przetwarzanie) nie należy utożsamiać z celem przetwarzania (który stanowi konkretny, zamierzony rezultat, jaki ma zostać osiągnięty poprzez przetwarzanie). Istnienie prawnie uzasadnionego interesu nie znosi obowiązku przestrzegania przez administratora zasady ograniczenia celu ani innych obowiązków wynikających z LGPD. Cel musi być jasno i precyzyjnie opisany, z podaniem informacji niezbędnych do określenia zakresu przetwarzania i umożliwienia wyważenia interesów administratora lub osób trzecich z prawami i uzasadnionymi oczekiwaniami osób, których dane dotyczą ([88]). Oznacza to, że administrator, opierając się na prawnie uzasadnionym interesie w celu wspierania lub promowania swojej działalności, musi m.in. jasno określić, które działania zamierza promować lub wspierać, oraz określić ich związek z planowanym przetwarzaniem danych.

2.4.4. *Przetwarzanie szczególnych kategorii danych osobowych*

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

(54) W art. 5 (II) LGPD wrażliwe dane osobowe zdefiniowano jako „dane osobowe dotyczące pochodzenia rasowego lub etnicznego, przekonań religijnych, poglądów politycznych, przynależności do związków zawodowych lub organizacji religijnej, światopoglądowej lub politycznej, dane dotyczące zdrowia lub życia seksualnego, dane genetyczne lub biometryczne, gdy są one powiązane z osobą fizyczną". Jak wynika z orzecznictwa krajowego, pojęcie życia seksualnego należy interpretować jako obejmujące również orientację lub preferencje seksualne danej osoby fizycznej. W szczególności w swoim orzecznictwie dotyczącym małżeństw osób tej samej płci Federalny Sąd Najwyższy orzekł, że dyskryminacja ze względu na płeć obejmuje również „preferencje seksualne" ([89]) oraz że swoboda wyrażania swojej „orientacji seksualnej" jest „warunkiem niezbędnym do rozwoju osobowości", który jest chroniony na mocy konstytucji ([90]). W związku z tym kategorie danych uznawanych za dane wrażliwe na mocy prawa brazylijskiego są takie same jak w art. 9 ust. 1 rozporządzenia (UE) 2016/679.

(55) Sądy w Brazylii rozszerzyły definicję wrażliwych danych osobowych na podstawie LGPD na inne rodzaje informacji, które mogłyby być wykorzystywane do dyskryminacji osób fizycznych ([91]). Wykładnia ta wynika z prawa do ochrony przed dyskryminacją przewidzianego w brazylijskim prawie, co znajduje również odzwierciedlenie w art. 6 (IX) LGPD. W szczególności w brazylijskim orzecznictwie doprecyzowano, że informacje z rejestru karnego uznaje się za dane wrażliwe ([92]).

(56) Przetwarzanie danych wrażliwych jest dozwolone na podstawie LGPD tylko wtedy, gdy osoba, której dane dotyczą, lub jej przedstawiciel prawny wyrazili „konkretną i odrębną" zgodę w odniesieniu do określonych celów ([93]). Zastosowanie mają kryteria ważności zgody opisane w motywach 46–48 niniejszej decyzji.

(57) Zgodnie z art. 11 (II) LGPD bez wyraźnej zgody osoby, której dane dotyczą, przetwarzanie danych wrażliwych może mieć miejsce w następujących przypadkach: 1) gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego lub regulacyjnego administratora (lit. a)); 2) gdy jest to niezbędne do przetwarzania przez administrację publiczną w celu realizacji polityk publicznych przewidzianych w przepisach ustawowych lub wykonawczych (lit. b)); 3) w celu ochrony życia lub bezpieczeństwa fizycznego osoby, której dane dotyczą, lub osoby trzeciej (lit. e)); 4) w celu wykonywania praw, w tym wynikających z umów oraz postępowań sądowych, administracyjnych lub arbitrażowych, zgodnie z brazylijskim prawem (lit. d)); 5) w celu ochrony zdrowia osób, których dane dotyczą, wyłącznie w ramach procedur prowadzonych przez pracowników służby zdrowia, podmioty opieki zdrowotnej lub organy sanitarne (lit. f)); 6) przez jednostki badawcze w celu przeprowadzania badań, z zapewnieniem anonimizacji danych, gdy tylko jest to możliwe (lit. c)); oraz 7) w celu zapobiegania oszustwom i zapewnienia bezpieczeństwa osób, których dane dotyczą, w procesach identyfikacji i uwierzytelniania poprzez rejestrację w systemach elektronicznych. W związku z tym podstawy przetwarzania danych wrażliwych na mocy LGPD i rozporządzenia (UE) 2016/679 są podobne.

([88]) ANPD, Przewodnik dotyczący prawnie uzasadnionego interesu, s. 17.

([89]) Zob. orzeczenie Federalnego Sądu Najwyższego Brazylii zezwalające na małżeństwa osób tej samej płci, dotyczące wykładni art. 3 sekcja IV konstytucji federalnej, który zakazuje wszelkiej dyskryminacji ze względu na płeć, rasę i kolor skóry. Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 4277 z dnia 5 maja 2011 r., pkt 2 i 6. Dokument dostępny na stronie: https://portal.stf.jus.br/peticaoInicial/verPeticaoInicial.asp?base=ADI&numProcesso=4277.

([90]) Zob. orzeczenie Federalnego Sądu Najwyższego Brazylii zezwalające na małżeństwa osób tej samej płci, s. 14: „[j]ako niepodważalny warunek rozwoju ludzkiej osobowości – najwyższej wartości chronionej przez konstytucję federalną – konieczne jest usunięcie wszelkich przeszkód prawnych, które stanowią ograniczenie – nawet potencjalne – w pełnym korzystaniu z wolności przysługującej każdemu człowiekowi w zakresie pełnego wyrażania swojej *orientacji seksualnej*" [wyróżnienie dodane].

([91]) Sąd pracy wyższej instancji, orzeczenie nr TST-E-RR-933-49.2012.5.10.0001 z grudnia 2021 r. Dokument dostępny pod adresem: https://www.jusbrasil.com.br/jurisprudencia/tst/713123452/inteiro-teor-713123472.

([92]) Sąd pracy wyższej instancji, orzeczenie nr TST-E-RR-933-49.2012.5.10.0001 z grudnia 2021 r.

([93]) Art. 11 (I) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

2.4.5. *Ograniczenie celów*

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

(59) Art. 6 (I) LGPD stanowi, że dane osobowe należy przetwarzać „w prawnie uzasadnionym, konkretnym i wyraźnie określonym celu, o którym informuje się osobę, której dane dotyczą", bez możliwości dalszego przetwarzania, które byłoby „niezgodne" z pierwotnym celem. Zasada ta i jej brzmienie są niemal identyczne z odpowiadającą jej zasadą określoną w art. 5 ust. 1 lit. c) rozporządzenia (UE) 2016/679. Art. 6 (II) LGPD stanowi ponadto, że każda czynność przetwarzania musi być zgodna z celami przekazanymi osobie, której dane dotyczą.

(60) Z wytycznych wydanych przez ANPD wynika, że aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym pierwotnie zgromadzono dane, administrator musi wykazać związek między tymi dwoma celami przetwarzania i uwzględnić „uzasadnione oczekiwania" osób, których dane dotyczą ([94]). W przypadku przetwarzania danych do dalszych zgodnych celów zastosowanie mają zasady i obowiązki określone w LGPD, w szczególności obowiązek zapewnienia, że nowy cel jest konkretny, oraz zagwarantowania ochrony praw osób, których dane dotyczą. Dotyczy to również dalszego przetwarzania danych, które zostały „w sposób oczywisty udostępnione" przez osobę, której dane dotyczą, lub są publicznie dostępne ([95]).

2.4.6. *Prawidłowość i minimalizacja danych*

(61) Dane powinny być prawidłowe i w stosownych przypadkach uaktualniane. Powinny być one również adekwatne, stosowne i nienadmierne w stosunku do celów, w których są przetwarzane.

(62) Zasady te są zagwarantowane w ramach zasad „jakości danych" i „konieczności" określonych odpowiednio w art. 6 (III) i (V) LGPD. Zgodnie z art. 6 (V) LGPD administrator i podmioty przetwarzające dane zapewniają, aby dane osobowe były dokładne, przejrzyste, istotne i aktualne, z uwzględnieniem celów ich przetwarzania. W art. 6 (III) LGPD ustanowiono „ograniczenie zakresu przetwarzania do minimum niezbędnego" do osiągnięcia konkretnego celu lub konkretnych celów, „obejmującego dane, które są istotne, proporcjonalne i nienadmierne" w odniesieniu do tego celu lub tych celów. Zasady te są podobne do zasad określonych w art. 5 ust. 1 lit. c) i d) rozporządzenia (UE) 2016/679.

2.4.7. *Ograniczenie przechowywania danych*

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

(64) Zasady „celu", „konieczności" i „dostępu" określone odpowiednio w art. 6 (I), (III) i (IV) LGPD przewidują wymogi dotyczące ograniczenia przechowywania. Ograniczają one możliwość przechowywania danych do niezbędnego minimum w związku z „uzasadnionym, konkretnym i wyraźnym" celem i wymagają, by osoby, których dane dotyczą, były informowane o okresie przechowywania danych.

([94]) ANPD, Przewodnik dotyczący prawnie uzasadnionego interesu, s. 26 i załącznik 2.

([95]) Art. 7 ust. 7 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych. Zob. również motyw 48 niniejszej decyzji. Pojęcie danych, które zostały „w sposób oczywisty udostępnione" występuje również w rozporządzeniu (UE) 2016/679, natomiast dane „publiczne dostępne" odnoszą się do informacji dostępnych w publicznych rejestrach lub bazach danych na mocy prawa brazylijskiego zgodnie z ustawą nr 12.527 z dnia 18 listopada 2011 r. – ustawa o dostępie do informacji. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

(65) Ponadto sekcja IV rozdziału II LGPD dotyczy „zakończenia przetwarzania danych". Zgodnie z tą sekcją art. 16 LGPD nakłada obowiązek usunięcia wszystkich danych osobowych po zakończeniu przetwarzania w określonym celu. Wymogi te, odczytywane w związku z zasadami LGPD dotyczącymi „celu", „konieczności" i „dostępu", są podobne do obowiązków wynikających z art. 5 ust. 1 lit. e) rozporządzenia (UE) 2016/679.

(66) Z zastrzeżeniem ściśle określonych wyjątków zawartych w art. 16 ustawy LGPD dane można w dalszym ciągu zatrzymać i przechowywać: 1) w celu wypełnienia obowiązków prawnych lub regulacyjnych; 2) do celów badawczych, zapewniając, w miarę możliwości, anonimizację danych; 3) w przypadku przekazania osobom trzecim zgodnie z wymogami LGPD; lub 4) jeżeli są one wykorzystywane wyłącznie przez administratora, pod warunkiem że dane są zanonimizowane, a dostęp do nich przez osoby trzecie jest zabroniony.

(67) Wymogi dotyczące bezpieczeństwa danych określone w LGPD i opisane w motywach 68–78 niniejszej decyzji mają zastosowanie do danych przechowywanych.

2.4.8. *Bezpieczeństwo danych*

(68) 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.

(69) Zasada ta jest zagwarantowana w art. 6 (VII) LGPD, który nakazuje stosowanie „środków technicznych i administracyjnych" w celu ochrony danych osobowych przed „nieuprawnionym dostępem oraz przypadkowym lub niezgodnym z prawem" przetwarzaniem, w tym „zniszczeniem, utratą, modyfikacją, przekazywaniem lub rozpowszechnianiem" danych. Aby ograniczyć te zagrożenia dla bezpieczeństwa, art. 6 (VIII) LGPD nakazuje wprowadzenie środków mających na celu „zapobieganie szkodom majątkowym lub niemajątkowym spowodowanym przetwarzaniem danych osobowych".

(70) Art. 44 LGPD stanowi, że przetwarzanie danych osobowych jest niezgodne z prawem, jeżeli nie spełnia norm bezpieczeństwa, których osoba, której dane dotyczą, ma prawo oczekiwać. Odpowiedni poziom bezpieczeństwa należy określić między innymi: 1) w świetle konkretnych okoliczności towarzyszących przetwarzaniu; 2) z uwzględnieniem rozsądnego oczekiwanego poziomu ryzyka; oraz 3) z uwzględnieniem technik przetwarzania dostępnych w czasie jego przeprowadzania ([96]).

(71) Aby wdrożyć zasadę bezpieczeństwa danych, w LGPD ustanowiono szereg wymogów określonych w rozdziale VII sekcja I „Bezpieczeństwo i poufność danych". Zgodnie z tą sekcją art. 46 LGPD wymaga, aby administratorzy danych i podmioty przetwarzające dane stosowali „środki bezpieczeństwa oraz środki techniczne i administracyjne umożliwiające ochronę danych osobowych przed nieuprawnionym dostępem oraz przypadkowym lub niezgodnym z prawem przetwarzaniem", takim jak „zniszczenie, utrata, zmiana, przekazanie lub wszelkiego rodzaju niewłaściwe lub niezgodne z prawem przetwarzanie". Środki te należy stosować „od fazy projektowania produktu lub usługi aż do ich wykonania" ([97]). Art. 47 LGPD nakłada na wszystkie podmioty zaangażowane w jakikolwiek etap przetwarzania danych ogólny obowiązek przestrzegania wymogów bezpieczeństwa. Obowiązki te są podobne do obowiązków określonych w art. 32 rozporządzenia (UE) 2016/679.

(72) Art. 44 LGPD stanowi ponadto, że administrator lub podmiot przetwarzający, który nie wprowadził środków bezpieczeństwa, ponosi odpowiedzialność za szkody powstałe w przypadku naruszenia bezpieczeństwa ([98]). ANPD może również ustanowić minimalne techniczne normy bezpieczeństwa w celu zapewnienia zgodności z obowiązkami w zakresie ochrony bezpieczeństwa danych ([99]).

([96]) Art. 44 (I)–(III) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([97]) Art. 46 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([98]) Jedyny akapit art. 44 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([99]) Art. 46 ust. 1 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

(73) Zgodnie z art. 48 LGPD w przypadku incydentu bezpieczeństwa, który może stwarzać ryzyko lub spowodować poważne szkody dla osób, których dane dotyczą, administrator danych jest zobowiązany do powiadomienia zarówno ANPD, jak i osób, których dane dotyczą. Takie powiadomienie musi nastąpić w rozsądnym terminie określonym przez ANPD i musi zawierać co najmniej: 1) opis charakteru danych osobowych, których dotyczy incydent; 2) informacje umożliwiające identyfikację osób, których dane dotyczą; 3) wskazanie środków technicznych i środków bezpieczeństwa stosowanych w celu ochrony danych, z zastrzeżeniem zachowania tajemnicy handlowej i przemysłowej; 4) ocenę ryzyka związanego z incydentem; 5) uzasadnienie ewentualnych opóźnień w komunikacji; oraz 6) opis środków, które wprowadzono lub zamierza się wprowadzić w celu złagodzenia lub naprawienia wyrządzonej szkody. Podejście przyjęte w LGPD jest w dużej mierze podobne do podejścia ustanowionego w art. 33 i 34 rozporządzenia (UE) 2016/679.

(74) ANPD przyjął dodatkowe przepisy dotyczące incydentów bezpieczeństwa danych, aby doprecyzować między innymi definicję „incydentu" oraz ramy czasowe powiadamiania o wystąpieniu incydentu ([100]).

(75) W art. 3 (XII) rozporządzenia w sprawie powiadamiania o incydentach bezpieczeństwa zdefiniowano incydent bezpieczeństwa jako „każde potwierdzone zdarzenie niepożądane związane z naruszeniem poufności, integralności, dostępności i autentyczności bezpieczeństwa danych osobowych". Zgodnie z art. 48 LGPD naruszenie ochrony danych i incydent bezpieczeństwa, które mogą stwarzać ryzyko dla osób, których dane dotyczą, zawsze należy zgłosić organowi ds. ochrony danych (ANPD) i osobom, których dane dotyczą. W art. 5 rozporządzenia w sprawie powiadamiania o incydentach bezpieczeństwa doprecyzowano, że incydent bezpieczeństwa może wiązać się z ryzykiem dla osób, których dane dotyczą, jeżeli może mieć wpływ na ich interesy i prawa podstawowe oraz jeżeli dotyczy co najmniej jednego z następujących rodzajów danych: 1) wrażliwe dane osobowe; 2) dane dzieci, nastolatków lub osób starszych; 3) dane finansowe; 4) dane uwierzytelniające w systemach; 5) dane chronione tajemnicą prawną, sądową lub zawodową; lub 6) wielkoskalowe bazy danych. Ponadto incydent bezpieczeństwa zostanie uznany za mający istotny wpływ na podstawowe interesy i prawa osób, których dane dotyczą, jeżeli: 1) może uniemożliwić korzystanie z przysługujących praw lub z usługi; lub 2) może wyrządzić osobom, których dane dotyczą, szkody materialne lub niematerialne obejmujące np. dyskryminację, naruszenie integralności cielesnej lub prawa do wizerunku i reputacji, nadużycie finansowe lub kradzież tożsamości ([101]).

(76) Powiadomienie ANPD i osób, których dane dotyczą, o incydencie bezpieczeństwa powinno nastąpić w ciągu trzech dni roboczych od stwierdzenia incydentu przez administratora ([102]). W wiążącym rozporządzeniu w sprawie powiadamiania o incydentach bezpieczeństwa doprecyzowano, jakie informacje administratorzy powinni przekazać ANPD oraz osobom, których dane dotyczą. Powiadomienie skierowane do osób, których dane dotyczą, musi zawierać w szczególności: 1) opis charakteru i kategorię danych osobowych, których dotyczy incydent; 2) informację o środkach technicznych i środkach bezpieczeństwa zastosowanych do ochrony danych; 3) informację o rodzajach ryzyka związanych z incydentem, ze wskazaniem możliwych skutków dla osób, których dane dotyczą; 4) informację o przyczynach opóźnienia, w przypadku gdy powiadomienie nie zostało przekazane w ciągu 72 godzin; 5) informację o środkach, które wprowadzono lub zamierza się wprowadzić w celu odwrócenia lub złagodzenia skutków incydentu, w stosownych przypadkach; 6) datę wykrycia incydentu bezpieczeństwa; oraz 7) dane kontaktowe służące do uzyskiwania informacji oraz, w stosownych przypadkach, dane kontaktowe osoby wyznaczonej do kontaktów ([103]). Informując o incydencie osoby, których dane dotyczą, administratorzy posługują się „prostym i łatwym do zrozumienia językiem" ([104]). Powiadomienia dokonuje się bezpośrednio i indywidualnie, jeżeli możliwe jest zidentyfikowanie osób, których dane dotyczą ([105]).

(77) Ponadto ANPD może – jeśli jest to konieczne do ochrony praw osób, których dane dotyczą – ocenić wagę incydentu i nakazać administratorowi wprowadzenie określonych środków ([106]). Mogą one obejmować publiczne ujawnienie incydentu za pośrednictwem odpowiednich kanałów medialnych, a także wdrożenie działań naprawczych lub łagodzących. Administrator danych prowadzi rejestr incydentów bezpieczeństwa ([107]).

([100]) ANPD, rozporządzenie w sprawie powiadamiania o incydentach bezpieczeństwa z kwietnia 2024 r. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

([101]) Art. 5 ust. 1, ANPD, rozporządzenie w sprawie powiadamiania o incydentach bezpieczeństwa z kwietnia 2024 r.

([102]) Art. 6 i 9, ANPD, rozporządzenie w sprawie powiadamiania o incydentach bezpieczeństwa z kwietnia 2024 r.

([103]) Art. 9 (I)–(VII), ANPD, rozporządzenie w sprawie powiadamiania o incydentach bezpieczeństwa z kwietnia 2024 r.

([104]) Art. 9 ust. 1 (I), ANPD, rozporządzenie w sprawie powiadamiania o incydentach bezpieczeństwa z kwietnia 2024 r.

([105]) Art. 9 ust. 1 (II), ANPD, rozporządzenie w sprawie powiadamiania o incydentach bezpieczeństwa z kwietnia 2024 r.

([106]) Art. 48 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([107]) Art. 10, ANPD, rozporządzenie w sprawie powiadamiania o incydentach bezpieczeństwa z kwietnia 2024 r.

(78) Ponadto LGPD łączy swoje standardy „dobrych praktyk i zarządzania (danymi)" z wymogami dotyczącymi bezpieczeństwa danych, między innymi w celu ograniczenia ryzyka związanego z przetwarzaniem danych ([108]). Obejmuje to promowanie przyjmowania wewnętrznych programów zarządzania prywatnością w celu oceny i ograniczenia ryzyka ([109]).

2.4.9. *Przejrzystość*

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

(80) Zgodnie z podejściem porównywalnym do tego, które przyjęto w art. 12 rozporządzenia (UE) 2016/679, art. 6 (VI) LGPD stanowi, że osoby, których dane dotyczą, powinny otrzymywać jasne, precyzyjne i łatwo dostępne informacje zarówno na temat przetwarzania danych, które ich dotyczą, jak i odpowiednich podmiotów przetwarzających, z zastrzeżeniem „tajemnicy handlowej i przemysłowej".

(81) W art. 9 LGPD określono wykaz informacji, jakie należy przekazać osobom, których dane dotyczą, w związku z przetwarzaniem danych, obejmujący: 1) określony cel przetwarzania; 2) rodzaj i czas trwania przetwarzania; 3) tożsamość administratora danych; 4) dane kontaktowe administratora danych; 5) informacje dotyczące przetwarzania danych przez administratora i celu takiego przetwarzania; 6) obowiązki podmiotów przetwarzających oraz 7) prawa osób, których dane dotyczą, w tym informacje dotyczące korzystania z tych praw.

(82) Ograniczenie dotyczące „tajemnicy handlowej i przemysłowej", o którym mowa w art. 6 (VI), oraz inne przepisy LGPD należy interpretować w świetle brazylijskiej ustawy o dostępie do informacji (LAI) ([110]). LAI ustanawia zasadę ujawniania informacji zawartych w rejestrach lub dokumentach będących w posiadaniu organów publicznych ([111]). Wszelkie wyjątki – tj. ograniczenia dostępu do dokumentów i informacji – muszą być uzasadnione i przewidziane w ustawie ([112]). Jeden z takich wyjątków stanowi tajemnica handlowa i przemysłowa, przy czym istnieje szczególny przepis prawny zapewniający ochronę „informacji dotyczących działalności gospodarczej osób fizycznych lub prawnych prawa prywatnego, uzyskanych [...] przez inne organy lub podmioty w ramach wykonywania działalności kontrolnej, regulacyjnej i nadzorczej nad działalnością gospodarczą, których ujawnienie mogłoby stanowić przewagę konkurencyjną dla innych podmiotów gospodarczych" ([113]). Przepisy LGPD odnoszące się do „tajemnicy handlowej i przemysłowej" należy zatem interpretować w taki sposób, aby przetwarzanie i ujawnianie informacji nie prowadziło do ujawnienia tajemnicy przedsiębiorstwa ani nie tworzyło przewagi konkurencyjnej dla innych podmiotów, przy jednoczesnym realizowaniu celów ochrony danych osobowych. Oznacza to, że w odniesieniu do zasady przejrzystości i w całym tekście LGPD ograniczenia dotyczącego „tajemnicy handlowej i przemysłowej" nie należy uznawać za ogólną podstawę do odmowy wykonania obowiązków przewidzianych w ustawie, lecz raczej jako wymóg zastosowania szczególnych zabezpieczeń zapewniających ujawnianie informacji w sposób chroniący te interesy.

2.4.10. *Prawa indywidualne*

(83) Osobom, których dane dotyczą, powinny przysługiwać określone prawa, które można egzekwować wobec administratora, w szczególności prawo dostępu do danych, prawo do sprostowania danych, prawo do usunięcia danych, prawo do sprzeciwu wobec przetwarzania danych, prawo do przenoszenia danych oraz prawa związane z automatycznym przetwarzaniem danych. Prawa te mogą podlegać ograniczeniom w zakresie, w jakim ograniczenia te są niezbędne i proporcjonalne do ochrony szczególnych celów leżących w ogólnym interesie publicznym.

([108]) Art. 49 i 50 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([109]) Główny akapit art. 50 i ust. 1 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([110]) Ustawa nr 12.527 z dnia 18 listopada 2011 r. – ustawa o dostępie do informacji. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

([111]) Art. 6 i 9 ustawy nr 12.527 z dnia 18 listopada 2011 r. – ustawa o dostępie do informacji.

([112]) Art. 22 ustawy nr 12.527 z dnia 18 listopada 2011 r. – ustawa o dostępie do informacji.

([113]) Art. 5 ust. 2 dekretu nr 7.721 z dnia 16 maja 2012 r. dotyczącego ustawy nr 12.527 z dnia 18 listopada 2011 r. – ustawa o dostępie do informacji.

(84) W rozdziale III LGPD określono prawa osób, których dane dotyczą, w podobny sposób jak na mocy art. 15–22 rozporządzenia (UE) 2016/679. Korzystanie ze wszystkich praw jest bezpłatne, a osoby, których dane dotyczą, należy poinformować o przysługujących im prawach ([114]). Zgodnie z art. 21 LGPD dane dotyczące korzystania przez osobę, której dane dotyczą, z przysługujących jej praw nie mogą być wykorzystywane na jej niekorzyść. Osoby, których dane dotyczą, mogą dochodzić ochrony swoich interesów i praw przed sądem – indywidualnie lub zbiorowo ([115]).

(85) Administratorzy danych „niezwłocznie" informują podmioty przetwarzające dane, którym dane mogły zostać udostępnione, o wnioskach osób, których dane dotyczą, w sprawie sprostowania, usunięcia, anonimizacji, ograniczenia przetwarzania i wyrażenia sprzeciwu wobec przetwarzania, w celu zapewnienia, aby wszystkie zaangażowane podmioty mogły spełnić te żądania ([116]).

(86) Zgodnie z art. 9 i art. 18 (II) LGPD osoby, których dane dotyczą, mają prawo do informacji i dostępu, pozwalające im „w dowolnym momencie" uzyskać informacje dotyczące przetwarzania ich danych ([117]). Obejmuje to: 1) tożsamość administratora danych (pkt III); 2) dane kontaktowe administratora (pkt IV); 3) informacje o określonym celu przetwarzania (pkt I); 4) informacje o ewentualnym udostępnianiu danych (pkt V); 5) rodzaj i czas trwania przetwarzania (pkt II); 6) istnienie praw osób, których dane dotyczą, w tym prawa do wniesienia skargi do organu ds. ochrony danych; oraz 7) obowiązki podmiotów przetwarzających dane. Ponadto art. 10 ust. 2 LGPD nakłada na administratora obowiązek zachowania przejrzystości w odniesieniu do przetwarzania danych w oparciu o prawnie uzasadniony interes. Podobnie art. 9 rozporządzenia w sprawie przekazywania danych stanowi, że osoby, których dane dotyczą, powinny być informowane o przekazaniu danych osobowych.

(87) W art. 19 LGPD doprecyzowano sposób, w jaki osobom, których dane dotyczą, należy zapewnić dostęp do informacji o ich danych osobowych. Na wniosek osoby, której dane dotyczą, dostęp do danych osobowych zapewnia się: niezwłocznie „w formacie uproszczonym"; lub w terminie 15 dni – w formie jasnego i pełnego oświadczenia ([118]). Ponadto art. 19 ust. 1 LGPD stanowi, że administratorzy przechowują dane osobowe w formacie ułatwiającym korzystanie z prawa dostępu. Osoba, której dane dotyczą, może zdecydować, czy chce otrzymać informacje w formie elektronicznej, czy papierowej ([119]).

(88) Osoby, których dane dotyczą, mają prawo żądać sprostowania niekompletnych, niedokładnych lub nieaktualnych danych, zgodnie z art. 18 (III) LGPD (prawo do sprostowania).

(89) Art. 18 (IV) i (VI) LGPD przyznaje osobom fizycznym prawo do żądania usunięcia ich danych: 1) gdy dane są niepotrzebne lub nadmierne; 2) w odniesieniu do wszelkich danych przetwarzanych za zgodą osoby, której dane dotyczą; lub 3) gdy dane są przetwarzane niezgodnie z prawem. Ponadto sekcja IV rozdziału II LGPD dotycząca „zakończenia przetwarzania danych" wskazuje, że przetwarzania danych należy zaprzestać, gdy osoba, której dane dotyczą, wyrazi sprzeciw wobec przetwarzania lub cofnie zgodę na przetwarzanie danych ([120]). Następnie dane podlegają usunięciu po zakończeniu przetwarzania ([121]). Przepisy te, rozpatrywane łącznie, w sposób pośredni rozszerzają zatem zakres prawa do usunięcia danych przewidzianego w LGPD.

([114]) Art. 18 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([115]) Art. 22 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([116]) Art. 18 ust. 6 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([117]) Art. 6 (VI), art. 18 i 19 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([118]) Art. 19 (I) i (II) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([119]) Art. 19 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([120]) Zob. art. 15 (III) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych, w której „powiadomienie od osoby, której dane dotyczą", odnosi się między innymi do wycofania zgody (jak wskazano w tym artykule). Znaczenie terminu „powiadomienie" nie ogranicza się do tego scenariusza i umożliwia osobom, których dane dotyczą, zwrócenie się z wnioskiem o zaprzestanie przetwarzania.

([121]) Art. 16 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

(90) Osoby fizyczne mają prawo sprzeciwić się przetwarzaniu danych prowadzonemu w oparciu o podstawę prawną inną niż wyrażona zgoda, w przypadku gdy przetwarzanie odbywa się niezgodnie z LGPD (prawo do sprzeciwu) ([122]). Ponadto, zgodnie z art. 15 i art. 18 (IV) LGPD, osoby, których dane dotyczą, mają prawo ograniczyć przetwarzanie danych („ograniczenie przetwarzania"). Na prawo to można powołać się w szczególności, gdy przetwarzane dane są niepotrzebne lub nadmierne lub gdy dane są przetwarzane w sposób niezgodny z LGPD ([123]). W art. 15 (II) LGPD wskazano, że danych nie można już przetwarzać na podstawie „powiadomienia" przekazanego administratorowi przez osobę, której dane dotyczą. Choć przepis ten podlega wykładni w świetle szeroko interpretowanego „interesu publicznego", przewiduje on szeroki zakres pośredniego prawa do sprzeciwu w sposób równoważny prawu do sprzeciwu przewidzianemu w rozporządzeniu (UE) 2016/679.

(91) Osoby fizyczne mają prawo zażądać „pełnej kopii elektronicznej" swoich danych, aby umożliwić ich wykorzystanie przez inne podmioty (prawo do przenoszenia danych) ([124]). Podobnie jak w UE, osoby, których dane dotyczą, mogą wystąpić z wnioskiem o taką kopię tylko wtedy, gdy dane są przetwarzane na podstawie zgody lub umowy.

(92) Chociaż wszelkie decyzje oparte na zautomatyzowanym przetwarzaniu danych gromadzonych w UE są zazwyczaj podejmowane przez administratora (który ma bezpośredni kontakt z osobą, której dane dotyczą, i tym samym podlega bezpośrednio rozporządzeniu (UE) 2016/679), należy zauważyć, że LGPD reguluje tego rodzaju przetwarzanie w sposób podobny do art. 22 rozporządzenia (UE) 2016/679. Po pierwsze, art. 6 (IX) LGPD uznaje zasadę niedyskryminacji za zasadę ochrony danych, zgodnie z którą przetwarzanie danych w celach niezgodnych z prawem lub stanowiących nadużycie o charakterze dyskryminacyjnym jest zakazane. Zasada ta ma zastosowanie do każdego przetwarzania danych i jest szczególnie istotna w kontekście przetwarzania zautomatyzowanego. Następnie, zgodnie z art. 20 LGPD, osoby, których dane dotyczą, mają prawo żądać „przeglądu decyzji podejmowanych wyłącznie w oparciu o zautomatyzowane przetwarzanie danych mających wpływ na ich interesy, w tym decyzji mających na celu określenie ich profilu osobistego, zawodowego, konsumenckiego lub kredytowego albo aspektów ich osobowości". Odpowiadając na wniosek osoby, której dane dotyczą, administrator musi przedstawić jasne informacje na temat „kryteriów i procedur stosowanych przy podejmowaniu zautomatyzowanej decyzji" ([125]). W przypadku gdy takich informacji nie można przekazać osobie, której dane dotyczą, ze względu na istnienie „tajemnicy handlowej lub przemysłowej", ANPD jest uprawniony do przeprowadzenia audytu w celu zweryfikowania, czy w zautomatyzowanym przetwarzaniu danych osobowych nie występują elementy dyskryminacyjne ([126]). W związku z tym „tajemnica handlowa lub przemysłowa" nie może być wykorzystywana jako podstawa odmowy rozpatrzenia wniosku osoby, której dane dotyczą.

(93) Art. 23 LGPD stanowi, że do procedur i terminów wykonywania praw osób, których dane dotyczą, w przypadku przetwarzania danych przez organy publiczne, mają zastosowanie przepisy szczegółowe ([127]). Na przykład brazylijska ustawa *Habeas Data* reguluje prawo dostępu osób fizycznych do informacji dotyczących danych przechowywanych w rejestrach lub bazach danych rządu lub podmiotu publicznego ([128]). Brazylijska ustawa *Habeas Data* ustanawia przepisy szczegółowe dotyczące prawa dostępu, które należy zapewnić w terminie 10 dni od złożenia wniosku przez osobę fizyczną, oraz prawa do sprostowania danych, które należy zrealizować w terminie 15 dni od złożenia wniosku ([129]). Podobnie brazylijska federalna ustawa o postępowaniu administracyjnym ustanawia prawo do informacji i dostępu dla osób fizycznych w kontekście postępowań administracyjnych ([130]). Brazylijska ustawa o dostępie do informacji nakłada również obowiązki w zakresie udzielania informacji

([122]) Art. 18 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([123]) Art. 18 (IV) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([124]) Art. 19 ust. 3 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([125]) Art. 20 ust. 1 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([126]) Art. 20 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([127]) Art. 23 ust. 3 ustawy nr 13.709 14 z sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([128]) Ustawa nr 9.507 z dnia 12 listopada 1997 r. – brazylijska ustawa *Habeas Data*. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm.

([129]) Art. 7 i 8 ustawy nr 9.507 z dnia 12 listopada 1997 r. – brazylijska ustawa *Habeas Data*. Ustawa przewiduje sposoby dochodzenia roszczeń w przypadku nieprzestrzegania przepisów w odniesieniu do wniosku osoby fizycznej.

([130]) Zob. w szczególności art. 6 ustawy nr 9.784 z dnia 29 stycznia 1999 r. – federalna ustawa o postępowaniu administracyjnym. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. Ustawa określa procedury i terminy powiadamiania osób fizycznych, a także sposoby dochodzenia roszczeń w przypadku nieprzestrzegania przepisów.

i przejrzystości na organy publiczne, przedsiębiorstwa publiczne oraz trzy władze w Brazylii: ustawodawczą, wykonawczą i sądowniczą ([131]). Przepisy tych ustaw wzmacniają prawo dostępu oraz prawo do informacji ustanowione na mocy LGPD w odniesieniu do przetwarzania danych przez organy publiczne. Jeżeli jednak przepisy tych ustaw nie przewidują szczególnych praw ustanowionych na mocy LGPD (np. praw związanych ze zautomatyzowanym podejmowaniem decyzji), osoby, których dane dotyczą, mogą korzystać z tych praw na podstawie LGPD.

(94) Wszelkie naruszenia praw osób, których dane dotyczą, będą traktowane przez ANPD jako „średniej wagi" lub „poważne" naruszenie ustawy, w zależności od odpowiedniego czynnika, a zatem mogą podlegać najwyższym sankcjom i karom pieniężnym. Co ważne, zgodnie z rozporządzeniem ANPD w sprawie sankcji administracyjnych, sam fakt, że naruszenie wpłynęło na prawo osoby, której dane dotyczą, oznacza, że takiego naruszenia nie można uznać za „lekkiej wagi" ([132]).

(95) Od momentu wejścia w życie LGPD liczba otrzymywanych przez ANPD skarg i wniosków od osób fizycznych dotyczących ich praw w zakresie ochrony danych utrzymuje się na stałym poziomie ([133]). Liczba ta znacznie wzrosła od wprowadzenia przez ANPD zmodernizowanej i łatwej w użyciu platformy składania wniosków i skarg w lipcu 2024 r. ([134]) Od tego czasu ANPD co miesiąc otrzymuje około 400 skarg i 100 wniosków od osób fizycznych ([135]).

2.4.11. *Dalsze przekazywanie*

(96) Stopień ochrony zapewnianej danym osobowym przekazywanym z Unii administratorom i podmiotom przetwarzającym dane w Brazylii nie może zostać obniżony wskutek dalszego przekazywania takich danych odbiorcom z państw trzecich.

(97) Takie „dalsze przekazywanie danych" stanowi międzynarodowe przekazywanie danych z Brazylii z punktu widzenia brazylijskiego administratora.

(98) Rozdział V LGPD ustanawia ramy prawne międzynarodowego przekazywania danych osobowych. Przepisy zawarte w tym rozdziale zostały uzupełnione wiążącym rozporządzeniem w sprawie międzynarodowego przekazywania danych (rozporządzenie w sprawie przekazywania danych), które ANPD przyjął w sierpniu 2024 r. ([136])

(99) Rozporządzenie w sprawie przekazywania danych definiuje „przekazanie" jako „operację przetwarzania, w ramach której podmiot przetwarzający przekazuje lub udostępnia dane osobowe albo zapewnia do nich dostęp innemu podmiotowi przetwarzającemu", a „międzynarodowe przekazywanie danych" – jako „przekazywanie danych osobowych do innego państwa lub do organizacji międzynarodowej, której dane państwo jest członkiem" ([137]).

([131]) Art. 1, 6 i 9 ustawy nr 12.527 z dnia 18 listopada 2011 r. – ustawa o dostępie do informacji.

([132]) Art. 8 ust. 2, ANPD, rozporządzenie w sprawie obliczania i stosowania sankcji administracyjnych z lutego 2023 r. („rozporządzenie w sprawie sankcji administracyjnych"). Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077.

([133]) ANPD, Sprawozdanie z czwartego roku działalności ANPD z listopada 2023 r., s. 24. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([134]) ANPD, platforma dla osób fizycznych. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados.

([135]) ANPD, Sprawozdanie z czwartego roku działalności ANPD z listopada 2023 r., s. 25.

([136]) ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r. Dokument dostępny w języku portugalskim pod adresem: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396, a w języku angielskim pod adresem: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([137]) Art. 3 (III) i (IV), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r., a także art. 5 (XV) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

(100) Zasady dotyczące międzynarodowego przekazywania danych ustanowione na mocy LGPD i rozporządzenia w sprawie przekazywania danych mają zastosowanie do każdego przetwarzania objętego zakresem LGPD. W art. 7 rozporządzenia w sprawie przekazywania danych wyraźnie doprecyzowano, że zastosowanie LGPD do międzynarodowego przekazywania danych nie zależy od środków technicznych wykorzystywanych do przetwarzania, lokalizacji geograficznej danych ani fizycznej obecności administratora lub podmiotu przetwarzającego ([138]). O tym, czy LGPD ma zastosowanie, decyduje natomiast istnienie istotnego związku między przetwarzaniem danych a Brazylią.

(101) Podobnie jak w przypadku art. 44–49 rozporządzenia (UE) 2016/679, art. 33 LGPD określa zamknięty katalog okoliczności, w których międzynarodowe przekazywanie danych jest dopuszczalne. Okoliczności te zostały szczegółowo opisane w art. 9 rozporządzenia w sprawie przekazywania danych.

(102) Międzynarodowe przekazywanie danych może mieć miejsce, jeżeli spełnione są łącznie trzy następujące warunki: po pierwsze, międzynarodowe przekazywanie danych może być „dokonywane wyłącznie w prawnie uzasadnionych, konkretnych i wyraźnie określonych celach, o których poinformowano osobę, której dane dotyczą, bez możliwości dalszego przetwarzania niezgodnego z takim celem" ([139]). Po drugie, międzynarodowe przekazywanie danych musi opierać się na ważnej podstawie prawnej określonej w art. 7 LGPD (lub w art. 11 w przypadku danych wrażliwych) ([140]). Po trzecie, należy zastosować „uznany" mechanizm przekazywania danych ([141]).

(103) W art. 33 LGPD przewidziano szereg mechanizmów przekazywania danych.

(104) Po pierwsze, może zostać przyjęta decyzja stwierdzająca odpowiedni stopień ochrony w odniesieniu do państwa trzeciego lub organizacji międzynarodowej (art. 33 (I)). Przy ustalaniu, czy państwo trzecie lub organizacja międzynarodowa gwarantuje odpowiedni poziom ochrony danych osobowych, ANPD bierze pod uwagę kilka kryteriów określonych w LGPD i rozporządzeniu w sprawie przekazywania danych ([142]), które to kryteria są podobne do odpowiadających im kryteriów wynikających z prawa UE. Należą do nich: 1) obowiązujące w państwie przeznaczenia lub mające zastosowanie do organizacji międzynarodowej przepisy ogólne i sektorowe, które mają bezpośredni wpływ na ochronę danych osobowych ([143]); 2) charakter danych ([144]); 3) zapewnienie, że państwo trzecie lub organizacja międzynarodowa gwarantuje poziom ochrony danych osobowych oraz ochrony praw osób, których dane dotyczą, zgodny z LGPD ([145]); 4) wprowadzenie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa danych i ograniczenia ryzyka negatywnego wpływu na prywatność i inne prawa podstawowe ([146]); 5) istnienie mechanizmów sądowych i instytucjonalnych gwarantujących prawa ochrony danych, w szczególności poprzez istnienie niezależnego organu nadzorczego posiadającego odpowiednie uprawnienia i zasoby do monitorowania i egzekwowania przepisów o ochronie danych ([147]); oraz 6) wszelkie inne szczególne okoliczności istotne w kontekście międzynarodowego przekazywania danych ([148]).

([138]) Art. 7, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([139]) Art. 9, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([140]) Art. 9 (I), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([141]) Art. 9 (II), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([142]) Art. 34 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych i rozdział V, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([143]) Art. 34 (I) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych i art. 11 (I), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([144]) Art. 34 (II) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych i art. 11 (II), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([145]) Art. 34 (III) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych i art. 11 (III), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([146]) Art. 34 (IV) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych i art. 11 (IV), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([147]) Art. 11 ust. 3, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.
([148]) Art. 34 (VI) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych i art. 11 (VI), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

(105) Przy ocenie poziomu ochrony danych osobowych w kontekście decyzji stwierdzającej odpowiedni stopień ochrony ANPD ocenia również: 1) ryzyko i korzyści wynikające z konkretnej decyzji stwierdzającej odpowiedni stopień ochrony, biorąc pod uwagę między innymi gwarancję zasad, praw osoby, której dane dotyczą, oraz system ochrony danych przewidziany w LGPD; a także 2) wpływ decyzji na międzynarodowy przepływ danych, stosunki dyplomatyczne, handel międzynarodowy oraz współpracę międzynarodową Brazylii z innymi państwami i organizacjami międzynarodowymi ([149]). Ocena i wydanie decyzji stwierdzającej odpowiedni stopień ochrony należą do kompetencji ANPD ([150]). Obecnie ANPD pracuje wyłącznie nad decyzją stwierdzającą odpowiedni stopień ochrony dotyczącą Unii Europejskiej.

(106) Po drugie, art. 33 (II) stanowi, że przekazywanie danych może mieć miejsce, gdy administratorzy zapewniają „gwarancje zgodności z zasadami i prawami osób, których dane dotyczą, oraz systemem ochrony danych" przewidzianym w LGPD. Można to zagwarantować poprzez 1) szczególne klauzule umowne (pkt II lit. a)); 2) standardowe klauzule umowne (pkt II lit. b)); 3) wiążące reguły korporacyjne (pkt II lit. c)); lub 4) zatwierdzone znaki jakości, certyfikaty i kodeksy postępowania (pkt II lit. d)).

(107) Administratorzy mogą opierać się na szczególnych postanowieniach umownych dotyczących międzynarodowego przekazywania danych, jak i na standardowych klauzulach umownych zatwierdzonych przez ANPD ([151]). Na mocy rozporządzenia w sprawie przekazywania danych ANPD przyjął zestaw wzorcowych klauzul umownych, które obejmują wszystkie odpowiednie wymogi w zakresie ochrony danych (tj. prawa osób, których dane dotyczą, niezależny nadzór i kontrolę, środki w zakresie bezpieczeństwa danych, zabezpieczenia dotyczące dalszego przekazywania danych itp.) ([152]). Klauzule te zawierają postanowienia, których strony umowy nie mogą zmienić ([153]). Mają one charakter modułowy, aby można je było dostosować do różnych scenariuszy przekazywania danych (np. od administratora danych do podmiotu przetwarzającego, od podmiotu przetwarzającego do podmiotu przetwarzającego) ([154]).

(108) Jeżeli chodzi o wiążące reguły korporacyjne, w rozdziale VI rozporządzenia w sprawie przekazywania danych ANPD wyjaśnił, w jaki sposób można stosować ten mechanizm oraz jakie wymogi regulują ważność reguł. ANPD przypomniał w szczególności o „wiążącym charakterze" tego instrumentu wobec wszystkich „członków grupy lub konglomeratu", którzy się na nim opierają, o wymogach dotyczących praw osób, których dane dotyczą, i sposobach ich realizacji, o zasadach dotyczących odpowiedzialności ([155]), a także o wszystkich obowiązkowych informacjach, jakie muszą zawierać wiążące reguły korporacyjne ([156]). Wiążące reguły korporacyjne podlegają uprzedniemu zatwierdzeniu przez ANPD zgodnie z procedurą określoną w rozdziale VIII rozporządzenia w sprawie przekazywania danych, która zobowiązuje przedsiębiorstwa do przedłożenia ANPD pełnej dokumentacji i obejmuje proces przeglądu przez ANPD ([157]). Przedsiębiorstwa są również zobowiązane do informowania ANPD o wszelkich kwestiach, które mogą mieć wpływ na zgodność z LGPD, w tym w przypadku gdy członkowie grupy podlegają zobowiązaniom zagranicznym ([158]). Wszystkie zatwierdzone wiążące reguły korporacyjne są publikowane na stronie internetowej ANPD, a przedsiębiorstwa mają obowiązek przejrzystego poinformowania o przeprowadzonym międzynarodowym przekazaniu danych ([159]).

([149]) Art. 12, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

([150]) Procedurę wydawania decyzji stwierdzającej odpowiedni stopień ochrony opisano w sekcji III rozporządzenia w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

([151]) Art. 35 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([152]) Załącznik II, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

([153]) Załącznik II sekcja II, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

([154]) Załącznik II ust. 4, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r. Administratorzy i podmioty przetwarzające mogą wybrać odpowiednią „opcję" odpowiadającą ich sytuacji na podstawie tej klauzuli.

([155]) Art. 3 (VIII), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r. Definicja „podmiotu odpowiedzialnego" stanowi, że „przedsiębiorstwo z siedzibą w Brazylii ponosi odpowiedzialność za każde naruszenie wiążącej reguły korporacyjnej, nawet jeżeli wynika ono z działania członka grupy gospodarczej mającego siedzibę w innym państwie", zgodnie z podejściem podobnym do podejścia przyjętego w art. 47 ust. 1 lit. f) rozporządzenia (UE) 2016/679.

([156]) Art. 27, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

([157]) Art. 27, 28 i rozdział VIII, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

([158]) Art. 25 (VIII), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

([159]) Art. 32, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r. W artykule tym wskazano ponadto, że przedsiębiorstwa mają obowiązek udostępnić wiążące reguły korporacyjne osobom, których dane dotyczą, na ich wniosek.

(109) ANPD może również wyznaczyć jednostki certyfikujące do opracowania znaków jakości, certyfikacji lub kodeksów postępowania dotyczących przekazywania danych ([160]). Decyzje i działania prowadzone przez te podmioty certyfikujące mogą być przedmiotem przeglądu ANPD, który może zmieniać i uchylać decyzje w przypadku niezgodności z LGPD ([161]).

(110) Ponadto LGPD zawiera wykaz „sytuacji szczególnych", w których można dokonać międzynarodowego przekazania, jeżeli: 1) jest to niezbędne do międzynarodowej współpracy prawnej między agencjami publicznymi, zgodnie z prawem międzynarodowym; 2) jest to niezbędne do ochrony życia lub bezpieczeństwa fizycznego osoby, której dane dotyczą, lub osoby trzeciej; 3) zostało to zatwierdzone przez ANPD; 4) jest to związane ze zobowiązaniem w ramach współpracy międzynarodowej; 5) jest to konieczne do celów porządku publicznego lub do wypełnienia obowiązku prawnego organu publicznego; 6) osoby, których dane dotyczą, wyraziły zgodę na konkretne przekazanie danych – po uprzednim poinformowaniu ich o charakterze przetwarzania danych; lub 7) gdy jest to konieczne do wypełnienia obowiązku prawnego lub regulacyjnego w związku z wykonaniem umowy lub dochodzeniem praw w postępowaniu sądowym, administracyjnym bądź arbitrażowym ([162]). Jak wskazano w rozporządzeniu w sprawie przekazywania danych, międzynarodowe przekazywanie danych może odbywać się w ramach tych scenariuszy wyłącznie wtedy, gdy „spełnione są szczególne warunki danego przypadku i mające zastosowanie wymogi prawne" ([163]).

(111) Jeżeli chodzi o sytuację szczególną, w której przekazywanie danych może odbywać się na podstawie zgody osób, których dane dotyczą, wymaga się, aby 1) spełnione zostały formalne kryteria uzyskania ważnej zgody (tj. konkretnej, dobrowolnej, wyraźnej, świadomej); 2) osoby, których dane dotyczą, były informowane o charakterze przekazania *przed* jego przeprowadzeniem (np. informacje na temat jurysdykcji planowanego przekazania i gwarantowanego przez nią poziomu ochrony; informacje o braku decyzji stwierdzającej odpowiedni stopień ochrony lub innych mechanizmów przekazywania danych; informacje na temat czasu trwania przekazań); oraz 3) zgodę uzyskano w odniesieniu do każdego przekazania w sposób szczególny i odrębny od jakiegokolwiek innego przetwarzania. Jak wskazano w motywie 46, zgody dorozumianej nie można uznać za zgodę ważną, a osoby, których dane dotyczą, mają prawo wycofać zgodę w dowolnym momencie.

(112) Rozporządzenie w sprawie przekazywania danych ściśle określa warunki korzystania ze wszystkich tych mechanizmów. Obejmuje to w szczególności zapewnienie osobom, których dane dotyczą, „jednoznacznych, dokładnych i łatwo dostępnych informacji na temat przekazywania danych" oraz zagwarantowanie i możliwość wykazania, że międzynarodowe przekazywanie danych odbywa się w sposób zapewniający przestrzeganie zasad oraz praw osób, których dane dotyczą, i nie zmienia poziomu ochrony przewidzianego w LGPD – niezależnie od kraju, w którym znajdują się przekazywane dane osobowe – także po zakończeniu przetwarzania i w przypadkach dalszego przekazywania danych ([164]). Wymogi te mają również zastosowanie w przypadku przekazywania danych na podstawie „sytuacji szczególnych", aby zapewnić ciągłość ochrony niezależnie od instrumentu wykorzystywanego do przeprowadzenia międzynarodowego przekazania danych.

(113) Przepisy opisane w motywach 96–112 niniejszej decyzji zapewniają zatem ciągłość ochrony w przypadku dalszego przekazywania danych osobowych z Brazylii w sposób zasadniczo odpowiadający temu, który przewidziano w rozporządzeniu (UE) 2016/679.

2.4.12. *Rozliczalność*

(114) 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.

([160]) Art. 35 ust. 3 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([161]) Art. 35 ust. 4 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([162]) Art. 33 (III)–(IX) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([163]) Art. 1 (jedyny akapit), ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

([164]) Art. 2 (I) i (IV) oraz art. 4, ANPD, rozporządzenie w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r. Podobnie jak we wszystkich przypadkach międzynarodowego przekazywania danych, każde przekazanie dokonywane w tych scenariuszach musi odbywać się w „prawnie uzasadnionych, konkretnych i wyraźnie określonych celach, o których poinformowano osobę, której dane dotyczą, bez możliwości dalszego przetwarzania niezgodnego z takimi celami", jak określono w głównym akapicie art. 9 rozporządzenia ANPD w sprawie międzynarodowego przekazywania danych z sierpnia 2024 r.

(115) W art. 6 (IX) LGPD ustanowiono zasadę rozliczalności, zgodnie z którą administrator i podmiot przetwarzający dane przyjmują środki, które są „skuteczne i zdolne" do wykazania zgodności z LGPD.

(116) W celu zapewnienia rozliczalności art. 50 LGPD stanowi, że administratorzy i podmioty przetwarzające dane mogą przyjmować przepisy wewnętrzne i modele zarządzania, w szczególności w celu zapewnienia dobrych praktyk w zakresie rozpatrywania skarg i wniosków osób, których dane dotyczą, przestrzegania obowiązków w dziedzinie bezpieczeństwa i wszystkich innych obowiązków wynikających z LGPD („dobre praktyki i zarządzanie"). Programy te powinny również obejmować plany działań edukacyjnych, wewnętrzny mechanizm kontroli i ograniczania ryzyka.

(117) LGPD przewiduje również wymóg wyznaczenia inspektora ochrony danych, który odgrywa istotną rolę w opracowywaniu i wdrażaniu tych wewnętrznych programów. Zgodnie z art. 5 (VIII) inspektor ochrony danych pełni funkcję łącznika między administratorem danych, osobami, których dane dotyczą, i ANPD. W art. 41 LGPD na wszystkich administratorów nałożono obowiązek wyznaczenia inspektora ochrony danych oraz podania jego tożsamości do wiadomości publicznej.

(118) LGPD upoważnia ANPD do wprowadzenia zwolnienia administratorów i podmiotów przetwarzających dane z obowiązku wyznaczenia inspektora ochrony danych ([165]). W rozporządzeniu w sprawie stosowania LGPD do małych i średnich przedsiębiorstw (MŚP) ANPD określił, że zwolnieniem tym można objąć niektóre małe przedsiębiorstwa, MŚP, przedsiębiorstwa typu start-up i organizacje nienastawione na zysk ([166]). W szczególności zakres tego zwolnienia obejmuje następujące podmioty: „mikroprzedsiębiorstwa, małe przedsiębiorstwa, przedsiębiorstwa typu start-up, osoby prawne prawa prywatnego, w tym organizacje nienastawione na zysk, zgodnie z obowiązującymi przepisami, a także osoby fizyczne i jednostki organizacyjne nieposiadające osobowości prawnej, które przetwarzają dane osobowe" ([167]). Zgodnie z brazylijskim prawem określenia „mikroprzedsiębiorstwa" ([168]), „małe przedsiębiorstwa" ([169]) lub „przedsiębiorstwa typu start-up" ([170]) oznaczają podmioty zatrudniające jednego pracownika lub niewielką liczbę pracowników ([171]) i nieosiągające określonego rocznego przychodu brutto ([172]).

(119) Zwolnienie z obowiązku wyznaczenia inspektora ochrony danych nie ma zastosowania do żadnego z tych przedsiębiorstw i podmiotów – niezależnie od ich wielkości i przychodów – jeśli dokonują one przetwarzania danych osobowych wiążącego się z „wysokim ryzykiem" ([173]). Przetwarzanie zostanie uznane za obarczone wysokim ryzykiem, jeżeli w ujęciu łącznym będzie miało co najmniej jedną z następujących cech ogólnych: 1) przetwarzanie danych osobowych na dużą skalę; oraz 2) przetwarzanie danych, które może mieć znaczący wpływ na prawa podstawowe i interesy osób, których dane dotyczą; oraz co najmniej jedną z następujących cech szczególnych: 1) wykorzystanie powstających lub innowacyjnych technologii; 2) nadzór lub kontrola w miejscach publicznych; 3) podejmowanie decyzji wyłącznie w sposób zautomatyzowany; oraz 4) przetwarzanie danych wrażliwych lub danych dotyczących dzieci lub osób starszych ([174]). Przetwarzanie danych osobowych na dużą skalę

([165]) Art. 41 ust. 3 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([166]) ANPD, rozporządzenie w sprawie stosowania LGPD do małych i średnich przedsiębiorstw z kwietnia 2024 r. („rozporządzenie w sprawie MŚP"). Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

([167]) Art. 2 (I), ANPD, rozporządzenie w sprawie MŚP z kwietnia 2024 r.

([168]) „Mikroprzedsiębiorstwo" definiuje się jako przedsiębiorstwo o rocznym przychodzie brutto równym lub niższym niż 360 000 reali brazylijskich (R$). Zob. art. 3 (I) ustawy uzupełniającej nr 123 z dnia 14 grudnia 2006 r., ustawa o krajowym statusie mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. 360 000 R$ stanowi równowartość 56 500 EUR.

([169]) „Małe przedsiębiorstwo" lub „MŚP" definiuje się jako przedsiębiorstwo o rocznym przychodzie brutto powyżej 360 000 R$, ale nieprzekraczającym 4 800 000 R$. Zob. art. 3 (II) ustawy uzupełniającej nr 123 z dnia 14 grudnia 2006 r. – ustawa o krajowym statusie mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. 4 800 000 R$ stanowi równowartość 753 000 EUR.

([170]) „Przedsiębiorstwa typu start-up" definiuje się jako „organizacje biznesowe lub korporacyjne – zarówno powstające, jak i prowadzące działalność od niedawna – których działalność charakteryzuje się innowacyjnością stosowaną do modelu biznesowego lub oferowanych produktów lub usług". Zob. art. 2 (III), ANPD, rozporządzenie w sprawie MŚP z kwietnia 2024 r.
Przedsiębiorstwo typu start-up może być zarejestrowane z takim statusem jedynie przez maksymalny okres 10 lat, a jego roczny przychód brutto nie może przekraczać 16 000 000 R$. Zob. art. 4 (I) ustawy uzupełniającej nr 182 z dnia 1 czerwca 2021 r. – ustawa o przedsiębiorstwach typu start-up. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp182.htm. 16 000 000 R$ stanowi równowartość 2 500 000 EUR.

([171]) Zob. w szczególności art. 2 (II), ANPD, rozporządzenie w sprawie MŚP z kwietnia 2024 r. i art. 41 ustawy nr 14.195 z dnia 26 sierpnia 2021 r. – ustawa o zakładaniu przedsiębiorstw. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm.

([172]) Ustawa uzupełniająca nr 123 z dnia 14 grudnia 2006 r. – ustawa o krajowym statusie mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm.

([173]) Art. 4, ANPD, rozporządzenie w sprawie MŚP z kwietnia 2024 r.

([174]) Art. 4 (I) i (II), ANPD, rozporządzenie w sprawie MŚP z kwietnia 2024 r.

definiuje się jako przetwarzanie, które „obejmuje znaczną liczbę osób, których dane dotyczą, przy jednoczesnym uwzględnieniu wolumenu przetwarzanych danych, a także czasu trwania, częstotliwości i zasięgu geograficznego przetwarzania” ([175]). „Przetwarzanie danych, które może mieć znaczący wpływ na podstawowe prawa i interesy osób, których dane dotyczą”, zdefiniowano jako „między innymi sytuacje, w których przetwarzanie może utrudnić korzystanie z przysługujących praw lub z usługi, a także wyrządzić osobom, których dane dotyczą, szkody materialne lub niematerialne obejmujące np. dyskryminację, naruszenie integralności cielesnej, prawo do wizerunku i reputacji, nadużycie finansowe lub kradzież tożsamości” ([176]).

(120) ANPD przyjął wiążące rozporządzenie w sprawie roli inspektora ochrony danych, w którym doprecyzowano jego obowiązki ([177]). W rozporządzeniu ANPD przypomina o obowiązku podmiotów prywatnych i organów publicznych do publikowania informacji na temat tożsamości swojego inspektora ochrony danych ([178]). W art. 10 rozporządzenia o inspektorach ochrony danych przypomniano o spoczywającym na administratorach i podmiotach przetwarzających dane obowiązku zapewnienia, między innymi, aby inspektor ochrony danych mógł wykonywać swoje zadania w sposób niezależny, „bez nadmiernej ingerencji, zwłaszcza w udzielanie wytycznych dotyczących praktyk, które należy przyjąć w odniesieniu do ochrony danych osobowych”, oraz aby inspektor ochrony danych miał bezpośredni dostęp do kadry kierowniczej najwyższego szczebla i wszystkich pracowników zaangażowanych w strategiczne decyzje dotyczące przetwarzania danych w ramach danego podmiotu. Podobnie inspektor ochrony danych wykonuje swoje obowiązki i zadania w sposób „etyczny, rzetelny i z zachowaniem niezależności technicznej, unikając sytuacji, które mogą stanowić konflikt interesów” ([179]).

(121) Rola inspektora ochrony danych stanowi jeden z priorytetów działań ANPD w zakresie egzekwowania przepisów. Na przykład pierwsze w historii sankcje nałożone przez ANPD dotyczyły przedsiębiorstwa, które zostało ukarane karą pieniężną i otrzymało specjalne ostrzeżenie, ponieważ nie wykazało, że powołało inspektora ochrony danych ([180]). Podmiot ten postanowił wyznaczyć inspektora ochrony danych w trakcie postępowania administracyjnego w celu zastosowania się do nakazu ANPD. Od tego czasu ANPD nadal nakłada sankcje na podmioty publiczne i prywatne w związku z naruszeniami przepisów LGPD dotyczących inspektora ochrony danych ([181]).

(122) Kolejnym ważnym narzędziem zapewniającym rozliczalność jest ocena skutków dla ochrony danych. Ocena skutków dla ochrony danych pozwala ocenić i określić wpływ przetwarzania danych. Zgodnie z art. 38 LGPD ANPD może zwrócić się do administratora lub podmiotu przetwarzającego dane o dokonanie oceny skutków dla ochrony danych ([182]), która musi zawierać opis rodzaju przetwarzania danych osobowych, a także środki, zabezpieczenia i mechanizmy ograniczania ryzyka. Ponadto w sekcji II LGPD ustanowiono przepisy dotyczące rozliczalności, które uprawniają ANPD do żądania opublikowania oceny skutków dla ochrony danych lub zalecenia przyjęcia przez organy publiczne „dobrych praktyk” w zakresie ochrony danych osobowych ([183]).

(123) W świetle wymogów i praktyk w zakresie rozliczalności opisanych w motywach 114–122 niniejszej decyzji brazylijskie ramy prawne wdrażają zasadę rozliczalności w sposób podobny do środków przewidzianych w rozdziale 4 sekcje 3 i 4 rozporządzenia (UE) 2016/679, w tym poprzez ustanowienie różnych mechanizmów służących zapewnieniu i wykazaniu zgodności z LGPD.

2.5. **Nadzór i egzekwowanie przepisów**

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

([175]) Zob. na przykład art. 4 ust. 1, ANPD, rozporządzenie w sprawie MŚP z kwietnia 2024 r.
([176]) Zob. na przykład art. 4 ust. 2, ANPD, rozporządzenie w sprawie MŚP z kwietnia 2024 r.
([177]) ANPD, rozporządzenie w sprawie roli inspektora ochrony danych w związku z przetwarzaniem danych osobowych z lipca 2024 r. („rozporządzenie o inspektorach ochrony danych”). Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074.
([178]) Art. 5 i 9, ANPD, rozporządzenie o inspektorach ochrony danych z lipca 2024 r.
([179]) Art. 18, ANPD, rozporządzenie o inspektorach ochrony danych z lipca 2024 r.
([180]) Zob. ANPD, raport z postępowania wyjaśniającego nr 1/2023 – Telekall Infoservice. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.
([181]) Zob. na przykład ANPD, raport z postępowania wyjaśniającego nr 5/2024 – Ministério da Saúde. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.
([182]) Art. 38 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([183]) Sekcja II ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

2.5.1. *Niezależny nadzór*

(125) W Brazylii niezależnym organem nadzorczym odpowiedzialnym za monitorowanie i egzekwowanie przepisów LGPD jest organ ochrony danych: Agência Nacional de Proteção de Dados – ANPD.

(126) ANPD został utworzony na mocy art. 55-A LGPD, a następnie uzyskał status organu niezależnego – początkowo na mocy dekretu tymczasowego, a następnie ustawy z 2022 r. ([184]) Przyjęcie ustawy przekształcającej ANPD obejmowało zmiany w LGPD polegające na uchyleniu przepisów, które uzależniały funkcjonowanie i operacje finansowe ANPD od zezwoleń udzielanych przez władzę wykonawczą na mocy brazylijskiej ustawy budżetowej ([185]). Zmieniony przepis LGPD stanowi, że ANPD jest „organem o statusie specjalnym, posiadającym autonomię techniczną i decyzyjną, własne aktywa oraz siedzibę w okręgu federalnym" ([186]).

(127) Jako „organ o statusie specjalnym" ANPD posiada autonomię w pełnym wykonywaniu swoich funkcji i uprawnień przewidzianych w LGPD, w tym we własnym zarządzaniu administracyjnym ([187]). Obejmuje to autonomię w zakresie dysponowania środkami finansowymi i zatrudniania pracowników ([188]). ANPD początkowo utworzono jako „organ", a następnie we wrześniu 2025 r. przekształcono w „agencję", dostosowując jej nazwę do nazw innych 11 podmiotów regulacyjnych korzystających w Brazylii z wysokiego stopnia niezależności (np. Krajowej Agencji Energii Elektrycznej, Krajowej Agencji Telekomunikacji itp.) ([189]).

(128) Zasoby ANPD pochodzą w dużej mierze z budżetu ogólnego brazylijskiego państwa federalnego. Dodatkowo budżet ANPD może obejmować darowizny, dotacje lub inne wpływy określone w art. 55-L LGPD. Od momentu powstania w 2021 r. ANPD rozwija się w szybkim tempie. Z rocznych sprawozdań ANPD wynika, że na koniec 2023 r., po zaledwie czterech latach istnienia, organ zatrudniał 141 pracowników lub urzędników służby cywilnej ([190]). Roczny budżet ANPD na 2025 r. wynosi 18 mln R$ ([191]). We wrześniu 2025 r. ogłoszono utworzenie w Brazylii nowej ścieżki kariery w służbie cywilnej w zakresie „ochrony danych", obejmującej 200 stanowisk, w ramach zwiększenia liczby pracowników ANPD w nadchodzących latach ([192]).

([184]) Art. 55-A ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych, w pierwotnym brzmieniu, zmieniony ustawą nr 14.460 z dnia 25 października 2022 r. – ustawa przekształcająca ANPD w organ o statusie specjalnym. W zakresie niezależności zob. środek tymczasowy nr 1.124 z dnia 13 czerwca 2022 r. przekształcający ANPD w organ o statusie specjalnym. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Mpv/mpv1124.htm oraz ustawa nr 14.460 z 25 października 2022 r. – ustawa przekształcająca ANPD w organ o statusie specjalnym. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14460.htm. Możliwość zmiany przez rząd statusu ANPD w celu zwiększenia jego niezależności została szczegółowo określona w (obecnie uchylonym) art. 55-A ust. 1 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([185]) Zob. art. 9 ustawy nr 14.460 z dnia 25 października 2022 r. – ustawa przekształcająca ANPD w organ o statusie specjalnym – uchylający i zastępujący art. 55-A ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([186]) Art. 7 ustawy nr 14.460 z dnia 25 października 2022 r. – ustawa przekształcająca ANPD w organ o statusie specjalnym.

([187]) Zob. ANPD, „ANPD staje się organem o statusie specjalnym" z czerwca 2022 r. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial.

([188]) Art. 55-L ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([189]) Art. 1, dekret nr 1.317 z dnia 17 września 2025 r. zmieniający LGPD w celu przekształcenia Agência Nacional de Proteção de Dados. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314 oraz art. 2 (XII), ustawa nr 13.848 z dnia 25 czerwca 2019 r. o organizacji agencji regulacyjnych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm.

([190]) ANPD, Sprawozdanie z czwartego roku działalności ANPD z listopada 2023 r., s. 8. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([191]) 18 225 566 R$ (2 857 768 EUR). Zob. roczna ustawa budżetowa, s. 190. Dokument dostępny na stronie: LEI15121-VOLUME I.pdf.

([192]) Art. 9 (I), dekret nr 1.317 z dnia 17 września 2025 r. zmieniający LGPD w celu przekształcenia Agência Nacional de Proteção de Dados. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

(129) ANPD składa się z Rady Dyrektorów (najwyższego organu zarządzającego), Krajowej Rady ds. Ochrony Danych Osobowych i Prywatności (posiadającej uprawnienia doradcze) oraz szeregu urzędów i jednostek administracyjnych ([193]). Strukturę tę ustanowiono w art. 55-C LGPD i szczegółowo opisano w dwóch dekretach przyjętych odpowiednio w 2020 i 2023 r. ([194])

(130) Rada Dyrektorów składa się z pięciu dyrektorów, w tym prezesa organu. Każdy członek Rady Dyrektorów ANPD jest powoływany na pięcioletnią kadencję przez prezydenta Brazylii, po zatwierdzeniu przez Senat Federalny ([195]).

(131) Dyrektorzy muszą być obywatelami Brazylii i posiadać wykształcenie odpowiednie do pełnionej funkcji ([196]). W celu zapewnienia niezależności wszyscy dyrektorzy muszą zaniechać prowadzenia działalności gospodarczej nastawionej na zysk i działalności politycznej oraz powstrzymać się od zajmowania, między innymi, stanowisk kierowniczych lub doradczych w przedsiębiorstwach ([197]). Ponadto brazylijskie przepisy regulujące zajmowanie wysokich stanowisk w federalnej administracji publicznej stanowią, że osoby zajmujące funkcje równoważne funkcjom dyrektorów ANPD są zobowiązane, między innymi, do powstrzymania się od działań niezgodnych z pełnionymi obowiązkami ([198]). Obejmuje to działalność w charakterze konsultantów lub pośredników na rzecz realizacji prywatnych interesów (także nieformalną) lub świadczenie usług na rzecz podmiotów podlegających nadzorowi lub regulacjom ANPD – nawet okazjonalnie. Ponadto po zakończeniu mandatu lub kadencji w ANPD i przez sześć miesięcy po tym okresie dyrektorom zabrania się wykonywania pewnych funkcji, które mogłyby stwarzać ryzyko konfliktu interesów ([199]).

(132) Dyrektorów można odwołać wyłącznie w szczególnych okolicznościach określonych w art. 55-E LGPD, a mianowicie „na skutek rezygnacji, prawomocnego i niepodlegającego zaskarżeniu wyroku skazującego lub kary polegającej na odwołaniu ze stanowiska nałożonej w wyniku administracyjnego postępowania dyscyplinarnego". Ustawa federalna o służbie publicznej stanowi, że taka kara musi być uzasadniona i można ją zastosować wyłącznie w przypadku udowodnionych konkretnych przestępstw (tj. poważnego uchybienia, korupcji, nieprawidłowego wykorzystania środków publicznych) ([200]). Te zasady i procedury zapewniają dyrektorom ANPD ochronę instytucjonalną w ramach wykonywania przez nich funkcji. Dotychczas nie odwołano żadnego dyrektora ANPD ani wobec żadnego dyrektora ANPD nie toczyło się postępowanie dyscyplinarne. Rada Dyrektorów ANPD funkcjonuje w niezmienionym składzie mimo zmiany administracji w Brazylii, która to zmiana miała miejsce w 2023 r.

([193]) Art. 55-C ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([194]) Dekret nr 10.474 z dnia 26 sierpnia 2020 r. w sprawie struktury ANPD. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm, zmieniony dekretem nr 11.758 z dnia 30 października 2023 r. w sprawie zmienionej struktury ANPD. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11758.htm#art1.

([195]) Art. 55-D ust. 1 i 3 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych oraz art. 12 dekretu nr 1.317 z dnia 17 września 2025 r. zmieniającego LGPD w celu przekształcenia Agência Nacional de Proteção de Dados. Dokument dostępny na stronie: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314. W art. 12 tego dekretu przedłużono kadencję dyrektorów ANPD z czterech do pięciu lat, aby dostosować ją do wszystkich innych istniejących niezależnych agencji regulacyjnych w Brazylii. Wszyscy dyrektorzy ANPD, którzy zostali mianowani przed przyjęciem tego dekretu, ukończą czteroletnią kadencję, jak pierwotnie przewidziano w prawie w momencie ich powołania.

([196]) Art. 55-D ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([197]) Art. 11 dekretu nr 10.474 z dnia 26 sierpnia 2020 r. w sprawie struktury ANPD.

([198]) Art. 5 ustawy nr 12.813 z dnia 16 maja 2013 r. – ustawa o konflikcie interesów urzędników publicznych i innych pełnionych funkcjach w organach publicznych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm.

([199]) Art. 6 ustawy nr 12.813 z dnia 16 maja 2013 r. – ustawa o konflikcie interesów urzędników publicznych i innych pełnionych funkcjach w organach publicznych.

([200]) Pełny i wyczerpujący wykaz przestępstw znajduje się w art. 132 ustawy nr 8112 z dnia 11 grudnia 1990 r. – ustawa federalna o służbie publicznej i urzędnikach służby cywilnej. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Zob. również rozdział V tej ustawy dotyczący warunków stosowania kar.

(133) Zadania i uprawnienia ANPD zostały wyszczególnione w art. 55-J LGPD. Obejmują one w szczególności opracowywanie polityk i wytycznych w zakresie ochrony danych, promowanie przyjmowania norm ułatwiających osobom, których dane dotyczą, kontrolę nad ich danymi osobowymi, prowadzenie postępowań wyjaśniających w sprawach naruszeń praw indywidualnych, rozpatrywanie skarg, egzekwowanie przestrzegania LGPD i nakładanie sankcji, zapewnianie edukacji i promocji w zakresie ochrony danych oraz wymianę informacji i współpracę z organami ochrony danych państw trzecich ([201]).

(134) ANPD posiada organ doradczy w postaci Krajowej Rady ds. Ochrony Danych Osobowych i Prywatności, ustanowionej na mocy art. 58-A LGPD. W skład tego organu wchodzą przedstawiciele władzy wykonawczej, ustawodawczej i sądowniczej, a także społeczeństwa obywatelskiego, związków zawodowych i sektora przedsiębiorstw ([202]). Pełni on wyłącznie funkcję doradczą, polegającą na przygotowywaniu badań lub rocznych sprawozdań na temat ochrony danych, organizowaniu debat publicznych i wysłuchań na temat ochrony danych osobowych i prywatności, proponowaniu niewiążących zaleceń dla ANPD oraz rozpowszechnianiu wiedzy na temat ochrony danych osobowych i prywatności ([203]). Współpraca między ANPD a Krajową Radą koncentruje się na promowaniu ochrony danych i prywatności w Brazylii. Krajowa Rada nie ma uprawnień w zakresie monitorowania i egzekwowania LGPD, ponieważ jedynie ANPD jest uprawniona do nadzorowania wdrażania tej ustawy i jej egzekwowania, na przykład poprzez wydawanie rozporządzeń, prowadzenie dochodzeń i stosowanie sankcji. Jako organ niezależny ANPD nie ma obowiązku stosowania się do sugestii przedstawianych przez Krajową Radę w jej sprawozdaniach lub niewiążących zaleceniach.

2.5.2. *Egzekwowanie prawa, w tym sankcje*

(135) W celu zapewnienia egzekwowania prawa prawodawca przyznał ANPD zarówno uprawnienia dochodzeniowe, jak i wykonawcze, od wydawania ostrzeżeń do nakładania administracyjnych kar pieniężnych.

(136) Jeśli chodzi o uprawnienia dochodzeniowe, w przypadku podejrzenia lub zgłoszenia naruszenia LGPD lub, w stosownych przypadkach, w celu ochrony praw osób, których dane dotyczą, które to prawa zostały lub mogły zostać naruszone, ANPD może w dowolnym czasie przeprowadzić kontrole na miejscu i zażądać od administratorów danych osobowych wszelkich niezbędnych informacji ([204]). W szczególności wiążące rozporządzenie w sprawie uprawnień ANPD do nakładania sankcji stanowi, że administratorzy i podmioty przetwarzające dane umożliwiają ANPD „dostęp do biur lub budynków, sprzętu, aplikacji, obiektów, systemów, narzędzi i zasobów technologicznych, dokumentów, danych i informacji o charakterze technicznym, operacyjnym i innym, mających znaczenie dla oceny czynności przetwarzania danych osobowych, będących w ich posiadaniu lub w posiadaniu osób trzecich” ([205]).

([201]) Art. 55-J (I)–(XXIV) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([202]) Więcej informacji na temat członków i działalności Krajowej Rady można znaleźć w: ANPD, Krajowa Rada ds. Ochrony Danych Osobowych i Prywatności. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/cnpd-2.

([203]) Art. 58-B ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([204]) Art. 55-J (XVI) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych, art. 4 (I) dekretu nr 10.474 z dnia 26 sierpnia 2020 r. w sprawie struktury ANPD oraz art. 12, ANPD, rozporządzenie w sprawie powiadamiania o incydentach bezpieczeństwa z kwietnia 2024 r.

([205]) Art. 5, ANPD, rozporządzenie w sprawie uprawnień ANPD do nakładania sankcji z października 2021 r. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021.

(137) W ramach swoich uprawnień naprawczych ANPD może wydawać ostrzeżenia, nakładać kary pieniężne lub inne sankcje, takie jak nakazy tymczasowego zaprzestania przetwarzania danych lub usunięcia danych osobowych ([206]). Sankcje te można nakładać na podmioty publiczne lub prywatne, z wyjątkiem kar pieniężnych i kar pieniężnych w stawkach dziennych, których nie można nakładać na podmioty publiczne ([207]). W celu doprowadzenia podmiotu do przestrzegania przepisów można zastosować kilka skumulowanych sankcji. W przypadku ostrzeżenia ANPD wyznacza administratorowi określony termin na podjęcie działań naprawczych w celu dostosowania przetwarzania danych do wymogów LGPD ([208]). Niepodjęcie tych działań skutkuje nałożeniem dodatkowych kar. Na przykład ANPD wystosował kilka ostrzeżeń do Ministerstwa Zdrowia w związku z niedostarczeniem oceny skutków dla ochrony danych i niedopełnieniem obowiązku powiadomienia o naruszeniu ochrony danych ([209]). ANPD może nałożyć kilka kar łącznie w celu ochrony praw osób, których dane dotyczą, lub zapewnienia zgodności z LGPD. Na przykład ANPD może nałożyć administracyjną karę pieniężną za naruszenie LGPD wraz z nakazem usunięcia danych związanych z tym naruszeniem ([210]). W przypadku sankcji niepieniężnych ANPD może również podjąć decyzję o nałożeniu „kar pieniężnych w stawkach dziennych, jeżeli jest to konieczne, aby zapewnić zgodność (z LGPD) w określonym terminie" ([211]). Karę pieniężną w stawkach dziennych stosuje się łącznie, z uwzględnieniem okresu pomiędzy nałożeniem kary a wykonaniem obowiązku, do maksymalnej kwoty 50 mln R$ ([212]).

(138) Zgodnie z art. 52 (II) LGPD ANPD może nakładać administracyjne kary pieniężne, oprócz kar pieniężnych w stawkach dziennych, w wysokości do 2 % przychodów danego podmiotu w Brazylii, do maksymalnej kwoty 50 mln R$ ([213]). Kary mogą być stosowane łącznie w przypadku wielu naruszeń. ANPD nałożył pierwsze kary pieniężne kilka miesięcy po przyjęciu rozporządzenia w sprawie sankcji administracyjnych – wobec przedsiębiorstwa telekomunikacyjnego, które nie określiło podstawy prawnej przetwarzania i nie wyznaczyło inspektora ochrony danych. Przedsiębiorstwo otrzymało ostrzeżenie oraz dwie kary pieniężne na łączną kwotę 14 400 R$ ([214]). W wiążącym rozporządzeniu w sprawie sankcji administracyjnych ANPD sklasyfikował sankcje według trzech poziomów wagi naruszenia: naruszenie lekkiej wagi, średniej wagi i poważne ([215]) – w zależności od ustalonego czynnika, takiego jak rodzaj i ilość przetwarzanych danych, rodzaj przetwarzania lub wpływ na prawa osób, których dane dotyczą. Na przykład naruszenia dotyczące przetwarzania wrażliwych danych osobowych podlegają najsurowszym sankcjom, jakie może nałożyć ANPD ([216]).

(139) Rozporządzenie w sprawie sankcji administracyjnych określa metodykę obliczania kar pieniężnych, w tym poprzez uwzględnienie czynników obciążających lub łagodzących ([217]). Na przykład kara pieniężna może zostać podwyższona o 10 % w przypadku powtarzających się naruszeń tego samego rodzaju lub nawet o 90 % za każde działanie naprawcze, którego nie wykonano w wyznaczonym terminie ([218]). Podobnie kara pieniężna może zostać zmniejszona o 50 %, jeżeli naruszenie zostanie usunięte tuż po wszczęciu postępowania administracyjnego przez ANPD ([219]).

([206]) Art. 55 i 55-J (IV) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych, i ANPD, rozporządzenie w sprawie sankcji administracyjnych z lutego 2023 r.

([207]) Art. 52 ust. 3. Ustawa nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([208]) Art. 52 (I) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([209]) Zob. decyzja ANPD nr 4/2024. Dokument dostępny pod adresem: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/relatorio_de_instrucao_no_4_2024_fis_cgf_anpd_v-publica.pdf oraz ANPD; oraz decyzja nr 5/2024. Dokument dostępny pod adresem: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.

([210]) Art. 52 (VI) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([211]) Art. 16, ANPD, rozporządzenie w sprawie sankcji administracyjnych z lutego 2023 r.

([212]) Art. 16 ust. 1, ANPD, rozporządzenie w sprawie sankcji administracyjnych z lutego 2023 r. 50 mln reali brazylijskich to około 7,8 mln EUR.

([213]) 50 mln reali brazylijskich to około 7,8 mln EUR.

([214]) ANPD, decyzja nr 1/2023. Dokument dostępny pod adresem: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.

([215]) Art. 8, ANPD, rozporządzenie w sprawie sankcji administracyjnych z lutego 2023 r.

([216]) Art. 8 ust. 3 (I) lit. d), ANPD, rozporządzenie w sprawie sankcji administracyjnych z lutego 2023 r.

([217]) Załącznik I, art. 12–13, ANPD, rozporządzenie w sprawie sankcji administracyjnych z lutego 2023 r.

([218]) Art. 12 (I)–(IV), ANPD, rozporządzenie w sprawie sankcji administracyjnych z lutego 2023 r.

([219]) Art. 13 (I), ANPD, rozporządzenie w sprawie sankcji administracyjnych z lutego 2023 r.

(140) Brazylijski system łączy zatem różne rodzaje sankcji, począwszy od działań naprawczych i administracyjnych kar pieniężnych. Niezwłocznie po wejściu w życie uprawnień ANPD do nakładania sankcji organ ten zaczął z tych uprawnień korzystać ([220]). Dotychczas nałożone sankcje i wydane zalecenia dotyczyły zarówno organów publicznych (w tym w dziedzinie bezpieczeństwa), jak i podmiotów prywatnych ([221]). Sankcje nałożone dotychczas przez ANPD dotyczyły szerokiego zakresu kwestii, w tym braku wyznaczenia inspektora ochrony danych, incydentów bezpieczeństwa, w tym naruszeń ochrony danych, lub braku współpracy z ANPD. Oprócz nakładania kar pieniężnych ANPD szczególnie aktywnie wykorzystuje pełen zakres swoich uprawnień naprawczych, np. do wydawania administratorom nakazów przeprowadzenia oceny skutków dla ochrony danych lub zaprzestania przetwarzania danych osobowych. Na przykład w lipcu 2024 r. ANPD wydał wobec dużej platformy mediów społecznościowych nakaz zawieszenia przetwarzania danych osobowych na potrzeby trenowania systemów generatywnej sztucznej inteligencji (AI) we wszystkich jej produktach ([222]). Wraz z tym środkiem zapobiegawczym, mającym na celu ochronę praw podstawowych osób, których dane dotyczą, ANPD nałożył karę pieniężną w stawkach dziennych w wysokości 50 000 R$ do czasu zapewnienia zgodności przetwarzania z LGPD ([223]). Wreszcie, ANPD ogłosił wszczęcie dochodzeń przeciwko kilku dużym międzynarodowym platformom technologicznym, przedsiębiorstwom z sektora mediów społecznościowych i jednemu bankowi, a jednocześnie kontynuował dochodzenia przeciwko podmiotom z sektora publicznego ([224]). W ciągu zaledwie kilku lat istnienia ANPD wykazał się dużą skutecznością w egzekwowaniu przepisów, wykorzystując pełen zakres swoich uprawnień kontrolnych.

(141) Wreszcie, sankcje administracyjne ustanowione na mocy LGPD nie zastępują stosowania innych sankcji administracyjnych lub innych sankcji cywilnych i karnych, w tym określonych w brazylijskim kodeksie ochrony konsumentów ([225]) i obywatelskich ramach prawnych w internecie ([226]). W szczególności brazylijski kodeks ochrony konsumentów nakłada na przedsiębiorstwa obowiązek udzielania konsumentom informacji o swojej działalności ([227]). W art. 56 kodeksu ochrony konsumentów wymieniono ponadto sankcje nakładane na przedsiębiorstwa w przypadku nieprzestrzegania przepisów, które to sankcje obejmują kary pieniężne, zakaz sprzedaży lub produkcji danego produktu oraz obowiązek zawieszenia świadczenia usługi. Ponadto w art. 61–74 kodeksu ochrony konsumentów wymieniono przestępstwa, za które przedsiębiorcy mogą podlegać karze pozbawienia wolności od sześciu miesięcy do dwóch lat, w tym w przypadku fałszywych lub wprowadzających w błąd oświadczeń dotyczących usługi lub promocji usługi, które mogą wyrządzić szkodę konsumentowi. Na przykład w 2014 r. brazylijski Departament Ochrony Konsumentów nałożył na przedsiębiorstwo telekomunikacyjne karę pieniężną w wysokości 3,5 mln R$ za naruszenia kodeksu ochrony konsumentów i obywatelskich ram prawnych w internecie w związku ze stosowaniem przez to przedsiębiorstwo technologii śledzenia internetowej reklamy behawioralnej i ze sprzedażą danych dotyczących przeszukiwania stron internetowych ([228]).

(142) Z powyższego wynika, że brazylijski system zapewnia skuteczne egzekwowanie przepisów o ochronie danych w praktyce.

2.5.3. *Dochodzenie roszczeń*

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

([220]) ANPD, rejestr sankcji. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/decisoes-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

([221]) Zob. na przykład nota techniczna nr 175/2023 w sprawie projektu umowy o współpracy między Ministerstwem Sprawiedliwości i Bezpieczeństwa Publicznego a brazylijską Federacją Piłki Nożnej w sprawie udostępniania danych osobowych w celu usprawnienia „Projektu Bezpieczny Stadion". Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf.

([222]) ANPD, środek zapobiegawczy, głosowanie nr 11/2024. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf.

([223]) 50 000 R$ stanowi równowartość 7 800 EUR.

([224]) Pełny i aktualny wykaz trwających dochodzeń i spraw wszczętych przez ANPD można znaleźć pod adresem: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao.

([225]) Ustawa nr 8.079 z dnia 11 września 1990 r. – ustawa o ochronie konsumentów. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

([226]) Ustawa nr 12.965 z dnia 23 kwietnia 2014 r., Marco Civil da Internet (obywatelskie ramy prawne w internecie). Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([227]) Art. 6 ustawy nr 8.079 z dnia 11 września 1990 r. – ustawa o ochronie konsumentów.

([228]) 3,50 mln R$ stanowiło równowartość ok. 1,5 mln EUR według ówczesnego kursu wymiany.

(144) Brazylijski system zapewnia osobom fizycznym różne mechanizmy skutecznego egzekwowania ich praw i dochodzenia roszczeń.

(145) W pierwszej kolejności osoby fizyczne, które uważają, że ich prawa lub interesy w zakresie ochrony danych zostały naruszone lub które chcą skorzystać z przysługujących im praw ochrony danych, mogą zwrócić się do właściwego administratora. Zgodnie z art. 9 LGPD administrator ma obowiązek m.in. udostępnić dane kontaktowe umożliwiające osobie, której dane dotyczą, złożenie wniosku lub skargi ([229]).

(146) Ponadto, zgodnie z LGPD i brazylijskim systemem prawnym, osoby fizyczne, które uważają, że ich prawa lub interesy w zakresie ochrony danych zostały naruszone przez administratora lub podmiot przetwarzający dane osobowe, mogą skorzystać z kilku możliwości dochodzenia roszczeń.

(147) Po pierwsze, każda osoba fizyczna, która uważa, że jej prawa lub interesy w zakresie ochrony danych zostały naruszone przez administratora lub podmiot przetwarzający, może złożyć skargę lub zgłosić takie naruszenie do ANPD ([230]). ANPD posiada na swojej stronie internetowej specjalną podstronę umożliwiającą osobom, których dane dotyczą, złożenie skargi w przypadku naruszenia LGPD lub wniosku w sprawie problemów związanych z realizacją żądań skierowanych do administratora danych w zakresie ich praw dotyczących ochrony danych ([231]). Jak wyjaśniono w motywie 138 niniejszej decyzji, w odpowiedzi na skargę ANPD może nałożyć sankcję wyszczególnioną w art. 52 LGPD. Rozporządzeniem w sprawie uprawnień ANPD do nakładania sankcji ustanowiono procedurę administracyjną dla postępowań ANPD, obejmującą terminy, procedury regulujące prawo do bycia wysłuchanym oraz publikację decyzji ([232]).

(148) Osoby, których dane dotyczą, mogą zaskarżyć decyzje ANPD, składając odwołanie do Rady Dyrektorów ANPD w terminie 10 dni od daty otrzymania decyzji ([233]). W ramach prawa do wniesienia skutecznego środka zaskarżenia osoby fizyczne mogą też odwołać się od decyzji Rady do sądu, a także wnieść skargę przeciwko ANPD z tytułu niewykonania obowiązków zgodnie z LGPD (w tym odmowy rozpatrzenia skargi lub oddalenia skargi co do istoty) ([234]).

(149) Po drugie, ANPD może zachęcać do „bezpośredniego pojednania" (w ramach mediacji) między osobami, których dane dotyczą, a administratorami danych w celu priorytetowego rozwiązania problemu i „naprawienia szkody przez administratora" ([235]). Procesy te nie wykluczają możliwości składania skarg przez osoby, których dane dotyczą, ani korzystania z innych środków ochrony prawnej.

(150) Po trzecie, w kwestii odszkodowań, art. 42 LGPD nakłada na administratora lub podmiot przetwarzający dane obowiązek naprawienia „szkód materialnych, niematerialnych, indywidualnych lub zbiorowych" wynikających z przetwarzania danych osobowych. Osoby, których dane dotyczą, mogą wytoczyć powództwo, indywidualnie lub zbiorowo, w celu ubiegania się o odszkodowanie za te szkody ([236]). LGPD stanowi, że sędzia może „odwrócić ciężar dowodu na korzyść osoby, której dane dotyczą", w szczególności w przypadkach, w których „przedstawienie dowodów przez osobę, której dane dotyczą, byłoby nadmiernie uciążliwe" ([237]).

(151) Po czwarte, gdy naruszenie praw osób, których dane dotyczą, mieści się w zakresie prawa konsumenckiego i relacji konsumenckich, stosuje się ochronę przewidzianą w tej dziedzinie, na którą można powołać się w sądzie ([238]).

([229]) Art. 9 w związku z art. 55-J (V) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([230]) Art. 55-J (V) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([231]) Zob. ANPD, usługi dla osób, których dane dotyczą – złożenie skargi lub wniosku. Dokument dostępny na stronie: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular.
([232]) Sekcje II i III, ANPD, rozporządzenie w sprawie uprawnień ANPD do nakładania sankcji z października 2021 r.
([233]) Art. 59, ANPD, rozporządzenie w sprawie uprawnień ANPD do nakładania sankcji z października 2021 r.
([234]) Art. 22 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([235]) Art. 17 (VIII), ANPD, rozporządzenie w sprawie uprawnień ANPD do nakładania sankcji z października 2021 r.
([236]) Art. 42 ust. 3 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([237]) Art. 42 ust. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.
([238]) Art. 45 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

(152) Po piąte, brazylijski Federalny Sąd Najwyższy stwierdził, że osoby fizyczne mają prawo do wystąpienia o nakaz sądowy z tytułu naruszenia ich praw wynikających z konstytucji, w tym prawa do ochrony danych osobowych ([239]). W tym kontekście sąd może na przykład nakazać administratorom zawieszenie lub zaprzestanie wszelkich bezprawnych działań. Ponadto prawa do ochrony danych, w tym prawa chronione przez LGPD, mogą być egzekwowane w drodze powództwa cywilnego. Art. 22 LGPD wyraźnie umożliwia obronę praw osób, których dane dotyczą, w sądzie, a także szersze dochodzenie spraw dotyczących ochrony danych osobowych w sądzie, zarówno indywidualnie, jak i zbiorowo.

(153) Brazylijski system oferuje zatem różne możliwości dochodzenia roszczeń – od łatwo dostępnych i tanich (np. skargi do ANPD) po drogi sądowe, które obejmują możliwość uzyskania odszkodowania lub zbiorowe dochodzenie roszczeń.

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

(154) Komisja oceniła również ograniczenia i zabezpieczenia, w tym mechanizmy nadzoru i indywidualne mechanizmy dochodzenia roszczeń dostępnych w prawie Brazylii, jeśli chodzi o zbieranie i późniejsze wykorzystanie przez brazylijskie organy publiczne danych osobowych przekazywanych w interesie publicznym administratorom i podmiotom przetwarzającym w Brazylii, szczególnie do celów ścigania przestępstw i bezpieczeństwa narodowego (zwane dalej „dostępem rządowym").

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

(156) Po pierwsze, każde ograniczenie prawa do ochrony danych osobowych musi być przewidziane ustawą, a podstawa prawna, która pozwala na ingerencję w te prawa, musi sama określać zakres ograniczenia wykonywania danego prawa ([240]).

(157) Po drugie, aby spełnić wymóg proporcjonalności, zgodnie z którym odstępstwa od ochrony danych osobowych i ograniczenia tej ochrony powinny mieć zastosowanie tylko w takim zakresie, w jakim jest to absolutnie niezbędne w społeczeństwie demokratycznym do osiągnięcia szczególnych celów interesu ogólnego, równoważnych z celami uznanymi przez Unię, ustawodawstwo danego państwa trzeciego, które zezwala na ingerencję, powinno określać jasne i precyzyjne zasady regulujące zakres i stosowanie środków oraz przewidywać wymagane zabezpieczenia, aby osoby, których dane zostały przekazane, miały wystarczające gwarancje skutecznej ochrony swoich danych osobowych przed ryzykiem nadużyć ([241]). Przepisy muszą w szczególności wskazywać, w jakich okolicznościach i na jakich warunkach można wprowadzić środek przewidujący przetwarzanie takich danych ([242]), a także poddawać spełnienie takich wymogów niezależnemu nadzorowi ([243]).

([239]) W 2020 r. Federalny Sąd Najwyższy Brazylii wydał orzeczenie, w którym wstrzymał wykonanie prezydenckiego dekretu wykonawczego nakazującego przedsiębiorstwom telekomunikacyjnym udostępnianie danych abonenta agencji ds. spisów powszechnych, uznając po raz pierwszy ochronę danych za prawo podstawowe i torując drogę do uwzględnienia go w konstytucji Brazylii. Zob. Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6387 z dnia 7 maja 2020 r. Dokument dostępny na stronie: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

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

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

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

([243]) Schrems II, pkt 179.

(158) Po trzecie, prawodawstwo i jego wymogi muszą być prawnie wiążące na mocy prawa krajowego. Dotyczy to przede wszystkim organów danego państwa trzeciego, ale te wymogi prawne muszą być również egzekwowalne wobec władz danego państwa trzeciego przed sądami ([244]). W szczególności osoby, których dane dotyczą, muszą mieć możliwość wytoczenia powództwa przed niezależnym i bezstronnym sądem, aby uzyskać dostęp do swoich danych osobowych lub uzyskać sprostowanie lub usunięcie takich danych ([245]).

3.1. **Ogólne ramy prawne**

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

(160) Po pierwsze, dostęp brazylijskich organów publicznych do danych osobowych podlega ogólnej zasadzie legalności – z której wynikają zasady racjonalności, konieczności i proporcjonalności – zapisanej w konstytucji Brazylii ([246]). W szczególności, zgodnie z art. 5 konstytucji, ograniczenia w zakresie podstawowych praw i wolności (w tym prawa do prywatności i ochrony danych) można wprowadzić wyłącznie na podstawie ustawy i tylko wtedy, gdy jest to konieczne ze względu na wymogi bezpieczeństwa narodowego, bezpieczeństwa publicznego lub inny konkretny cel interesu publicznego określony w ustawie. Ograniczenia takie muszą być rozsądne i proporcjonalne ([247]). W szczególności ocena celu interesu publicznego ma zasadnicze znaczenie dla oceny proporcjonalności ingerencji w świetle zasady legalności. Art. 5 (LIV) konstytucji stanowi ponadto, że „nikt nie może być pozbawiony wolności lub mienia bez rzetelnego procesu sądowego".

(161) Po drugie, porządek prawny Brazylii gwarantuje *Habeas Data* jako konstytucyjną drogę dochodzenia roszczeń mającą na celu ochronę prawa dostępu do danych osobowych, a także do sprostowania i usunięcia danych osobowych, przechowywanych przez organy publiczne lub w publicznych zbiorach danych lub rejestrach ([248]). Ustawa ta służy jako zabezpieczenie przed niewłaściwym wykorzystaniem danych lub naruszeniem prywatności w związku z przetwarzaniem danych przez podmioty publiczne. Każda osoba fizyczna, niezależnie od swojej narodowości, może wnieść skargę lub wniosek w oparciu o *Habeas Data* ([249]).

(162) Po trzecie, ogólne zasady i prawa, które wymieniono w motywach 155–158, są również odzwierciedlone w ustawach szczególnych, które regulują uprawnienia organów ścigania i bezpieczeństwa narodowego. Na przykład w obywatelskich ramach prawnych w internecie przewidziano środki wymagające uprzedniego zezwolenia sądu na dostęp do danych i ograniczenie dostępu do danych internetowych ([250]). Podobnie w ustawie o przechwytywaniu komunikacji telefonicznej ustanowiono szczególne środki i zabezpieczenia dotyczące przetwarzania danych telekomunikacyjnych ([251]). W dziedzinie bezpieczeństwa narodowego ustawa ustanawiająca brazylijski system wywiadowczy przewiduje środki umożliwiające zgodny z prawem dostęp do danych do celów bezpieczeństwa narodowego ([252]).

([244]) Schrems II, pkt 181–182.

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

([246]) Art. 5 (II) konstytucji Federacyjnej Republiki Brazylii z 1988 r.

([247]) Brazylia podlega jurysdykcji Międzyamerykańskiego Trybunału Praw Człowieka, który, między innymi, uznał zasadę proporcjonalności za „niezbędną w społeczeństwie demokratycznym" oraz stwierdził, że ograniczanie praw podstawowych jest dopuszczalne tylko wtedy, gdy służy osiągnięciu nadrzędnego celu publicznego. Zob. np. MENDES, Gilmar Ferreira. Prawa podstawowe i kontrola sądowa. São Paulo: Saraiva, 2012 r., s. 78.

([248]) Art. 5 (LXXII) i (LXXVII) konstytucji Federacyjnej Republiki Brazylii z 1988 r.

([249]) Zob. też motywy 9 i 11 niniejszej decyzji.

([250]) Ustawa nr 12.965 z dnia 23 kwietnia 2014 r., Marco Civil da Internet (obywatelskie ramy prawne w internecie). Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([251]) Ustawa nr 9.296 z dnia 24 lipca 1996 r. – ustawa o przechwytywaniu komunikacji telefonicznej. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

([252]) Ustawa nr 9.883 z dnia 7 grudnia 1999 r. – ustawa ustanawiająca brazylijski system wywiadowczy.

(163) Po czwarte, przetwarzanie danych osobowych przez organy publiczne, w tym do celów ścigania przestępstw i bezpieczeństwa narodowego, podlega wymogom w zakresie ochronie danych zgodnie z LGPD. Jak opisano w motywie 31 niniejszej decyzji, wyłączenie dotyczące stosowania LGPD w obszarze bezpieczeństwa publicznego, obrony narodowej, bezpieczeństwa państwa oraz prowadzenia dochodzeń w sprawie przestępstw i ich ścigania, określone w LGPD, jest częściowe. Federalny Sąd Najwyższy dokonał wykładni stosowania LGPD w świetle konstytucyjnej ochrony danych osobowych i ustalił, że główne zasady, prawa i cele LGPD mają zastosowanie do wszelkiego przetwarzania danych osobowych przez organy publiczne, w tym do celów ścigania przestępstw lub do celów bezpieczeństwa narodowego ([253]). Na tej podstawie ANPD prowadził np. postępowania i wydał wytyczne, takie jak nota techniczna dla organów publicznych dotycząca działań związanych z bezpieczeństwem publicznym, w których przypomniał, że przetwarzanie do tych celów interesu publicznego musi być zgodne z ogólnymi zasadami i prawami przewidzianymi w LGPD ([254]).

(164) Wreszcie, osoby fizyczne mogą powołać się na swoje konstytucyjne prawa i wolności przed Federalnym Sądem Najwyższym, jeżeli uważają, że organy publiczne dopuściły się ich naruszenia podczas wykonywania swoich uprawnień. Osoby fizyczne mogą również ubiegać się o odszkodowanie w związku z przysługującymi im prawami ochrony danych przed niezależnymi organami nadzoru (np. ANPD) i sądami, jak wyszczególniono w motywach 143–153 niniejszej decyzji.

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

(165) W brazylijskim prawie ustanowiono szereg ograniczeń w zakresie dostępu do danych osobowych i ich wykorzystywania do celów ścigania przestępstw, a także zapewniono mechanizmy nadzoru i dochodzenia roszczeń zgodne z wymogami, o których mowa w motywach 155–158 niniejszej decyzji. Warunki uzyskania takiego dostępu oraz zabezpieczenia mające zastosowanie do wykonywania tych uprawnień poddano szczegółowej ocenie w kolejnych sekcjach.

3.2.1. *Podstawy prawne, ograniczenia i zabezpieczenia*

(166) Co do zasady dostęp organów publicznych do danych osobowych na potrzeby egzekwowania prawa karnego odbywa się na podstawie uprzedniego orzeczenia sądowego wydanego przez właściwy organ sądowy ([255]). W drodze wyjątku od tej zasady organy policji i prokuratury mogą, w przypadkach wyraźnie przewidzianych w ustawie, mieć dostęp do danych osób objętych dochodzeniem zawartych w rejestrze publicznym, tj. danych dotyczących kwalifikacji osobistych, przynależności i adresu ([256]). Przewidziany prawem wyczerpujący wykaz dostępnych rejestrów obejmuje informacje dotyczące Brazylijczyków lub osób zamieszkałych w Brazylii i nie obejmuje dostępu do danych przekazywanych z UE, a zatem nie wchodzi w zakres niniejszej decyzji ([257]). Dostęp do tych rejestrów podlega konstytucyjnej zasadzie legalizmu – z której wynikają zasady racjonalności, konieczności i proporcjonalności – i może podlegać kontroli sądowej *ex post*, jak wyjaśniono w motywach 159–161.

(167) Organami w Brazylii, które są uprawnione do dostępu do danych osobowych i ich gromadzenia do celów postępowań karnych na mocy uprzedniej zgody organu sądowego, są: 1) policja cywilna; 2) policja federalna; 3) prokuratura stanowa; 4) prokuratura federalna; 5) sędziowie i sądy; oraz 6) parlamentarne komisje śledcze.

([253]) Federalny Sąd Najwyższy. Orzeczenie w sprawie ADI 6649, wrzesień 2022 r. Dokument dostępny na stronie: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([254]) Nota techniczna nr 175/2023, pkt 5.1.

([255]) Zob. np. art. 5 (XII) konstytucji Federacyjnej Republiki Brazylii z 1988 r.

([256]) Art. 15 i 16 ustawy nr 12.850 z dnia 2 sierpnia 2013 r. – ustawa o organizacjach przestępczych i dochodzeniach w sprawach karnych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

([257]) Dostępne rejestry obejmują: rejestry zatrudnienia, rejestry wyborcze, rejestry telefoniczne, rejestry finansowe, rejestry dostawców usług internetowych, rejestry kart kredytowych. Informacje w tych rejestrach obejmują informacje o osobach nabywających te usługi lub korzystających z tych usług publicznych. Art. 15 i 16 ustawy nr 12.850 z dnia 2 sierpnia 2013 r. – ustawa o organizacjach przestępczych i dochodzeniach w sprawach karnych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

(168) Zgodnie z art. 3-B kodeksu karnego sędzia „odpowiedzialny za kontrolę zgodności z prawem dochodzenia lub postępowania przygotowawczego w sprawie karnej i za ochronę praw indywidualnych" może wydać postanowienie zezwalające na: 1) przechwytywanie komunikacji telefonicznej oraz komunikacji w systemach komputerowych i powiązanych lub innych form komunikacji; 2) uchylenie tajemnicy podatkowej, bankowej i telefonicznej lub zniesienie poufności danych; 3) dokonanie przeszukania i zajęcia w miejscu zamieszkania; oraz 4) dostęp do informacji niejawnych; a także 5) „inne środki pozyskania dowodów, które ograniczają prawa podstawowe osoby objętej dochodzeniem" ([258]).

3.2.1.1. Przechwytywanie komunikacji

(169) W brazylijskim systemie prawnym poufność korespondencji elektronicznej i telefonicznej jest uznawana za prawo podstawowe ([259]).

(170) Organy publiczne mogą uzyskać dostęp do tych danych wyłącznie w wyjątkowych przypadkach do celów dochodzenia, postępowania przygotowawczego lub ścigania w sprawach karnych. Zgodnie z orzecznictwem Federalnego Sądu Najwyższego, przechwytywanie komunikacji musi być zawsze środkiem pomocniczym i wyjątkowym, który jest dopuszczalny tylko wtedy, gdy nie ma innych sposobów rozwiązania konkretnej sprawy ([260]). Zasady przechwytywania połączeń internetowych i telefonicznych są uregulowane ustawą o przechwytywaniu komunikacji telefonicznej ([261]).

(171) W art. 2 ustawy o przechwytywaniu komunikacji telefonicznej określono rygorystyczne warunki umożliwienia dostępu do komunikacji. Każde przechwytywanie komunikacji wymaga uprzedniej zgody organu sądowego. Ważny wniosek o wydanie zgody na przechwytywanie musi zostać przedłożony sędziemu przez uprawnione organy publiczne, którymi mogą być: 1) odpowiedni organ policji w kontekście dochodzenia w sprawie karnej; lub 2) przedstawiciel prokuratury w kontekście postępowania przygotowawczego i postępowania karnego ([262]). Na przechwytywanie połączeń telefonicznych nie można uzyskać zgody w żadnej z następujących okoliczności, zgodnie z zasadami konieczności i proporcjonalności: 1) gdy nie istnieją racjonalne dowody wskazujące na udział w popełnieniu przestępstwa lub sprawstwo; 2) gdy dowody można uzyskać za pomocą innych dostępnych środków; 3) jeżeli czyn, którego dotyczy dochodzenie, stanowi przestępstwo zagrożone karą pozbawienia wolności ([263]).

(172) Ponadto ustawa o przechwytywaniu komunikacji telefonicznej wymaga, aby wniosek o wydanie zgody na przechwytywanie zawierał uzasadnienie konieczności zastosowania tego środka ([264]). Uprzednia zgoda organu sądowego musi być uzasadniona i uwzględniać proporcjonalność środków zastosowanych do przechwytywania ([265]). Sędzia może zezwolić na dostęp do treści komunikacji przez okres nie dłuższy niż 15 dni. Okres ten może zostać przedłużony nowym postanowieniem sądu po udowodnieniu niezbędności zastosowania tego środka ([266]). Przechwytywanie komunikacji, w tym podsłuch środowiskowy, prowadzone bez zgody organu sądowego lub w celu niedozwolonym przez prawo stanowi przestępstwo zagrożone karą do czterech lat pozbawienia wolności ([267]).

([258]) Dekret z mocą ustawy nr 3.689 z dnia 3 października 1941 r. – kodeks karny. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([259]) Art. 5 (XII) konstytucji Federacyjnej Republiki Brazylii z 1988 r.
([260]) Federalny Sąd Najwyższy, HC 108147/PR, 2012. Dokument dostępny na stronie: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
([261]) Art. 1 ustawy nr 9.296 z dnia 24 lipca 1996 r. o przechwytywaniu komunikacji telefonicznej.
([262]) Art. 2 (I) i (II) ustawy nr 9.296 z dnia 24 lipca 1996 r. – ustawa o przechwytywaniu komunikacji telefonicznej.
([263]) Art. 2 ustawy nr 9.296 z dnia 24 lipca 1996 r. o przechwytywaniu komunikacji telefonicznej.
([264]) Art. 4 ustawy nr 9.296 z dnia 24 lipca 1996 r. o przechwytywaniu komunikacji telefonicznej.
([265]) Art. 5 ustawy nr 9.296 z dnia 24 lipca 1996 r. o przechwytywaniu komunikacji telefonicznej.
([266]) Art. 5 ustawy nr 9.296 z dnia 24 lipca 1996 r. o przechwytywaniu komunikacji telefonicznej.
([267]) Art. 10 ustawy nr 9.296 z dnia 24 lipca 1996 r. o przechwytywaniu komunikacji telefonicznej.

(173) Co do zasady dane, do których uzyskano dostęp i które są gromadzone do celów postępowań karnych zgodnie z ustawą o przechwytywaniu komunikacji telefonicznej, będą przechowywane przez okres przetwarzania, a następnie zostaną usunięte, gdy nie będą już potrzebne w toku postępowania sądowego, zgodnie z wiążącymi wytycznymi wymiaru sprawiedliwości ([268]). Art. 9 ustawy o przechwytywaniu komunikacji telefonicznej stanowi ponadto, że jeżeli zgromadzone treści nie są związane z przedmiotem sprawy, dane te zostaną uznane za „nienadające się do wykorzystania" ([269]).

(174) Jeżeli chodzi o metadane telekomunikacyjne, w art. 17 ustawy o organizacjach przestępczych i dochodzeniach w sprawach karnych zobowiązano przedsiębiorstwa telefoniczne do przechowywania przez pięć lat informacji o koncie użytkownika dotyczących osób zamieszkałych w Brazylii oraz zapisów rozmów telefonicznych (wyłącznie numerów telefonów) ([270]). Dostęp do tego rejestru prowadzonego przez ANATEL (brazylijską agencję regulacyjną ds. telekomunikacji) jest ograniczony do określonych podmiotów publicznych i wymaga zgody organu sądowego, jak opisano powyżej.

(175) Jeżeli chodzi o informacje dostępne w internecie, art. 7 obywatelskich ram prawnych w internecie dodatkowo gwarantuje „nienaruszalność i poufność przepływu komunikacji w internecie", z wyjątkiem przypadków objętych nakazem sądowym, zgodnie z ustawą; oraz „nienaruszalność i poufność przechowywanej komunikacji prywatnej, z wyjątkiem przypadków objętych nakazem sądowym" ([271]).

(176) Zgodnie z art. 10 obywatelskich ram prawnych w internecie dostęp do treści komunikacji w internecie i do danych dotyczących połączeń (w tym metadanych) może mieć miejsce wyłącznie na podstawie uprzedniego nakazu sądowego. Zgodnie z art. 22 obywatelskich ram prawnych w internecie wniosek o wydanie nakazu sądowego musi zawierać: (i) oparte na mocnych przesłankach dowody, że popełniono przestępstwo; (ii) racjonalne uzasadnienie przydatności żądanych danych do celów dochodzenia lub do celów dowodowych; oraz (iii) określenie okresu, którego dotyczą żądane dane. Art. 13 wymaga ponadto, aby dostawcy usług internetowych lub aplikacji zatrzymywali dane z dzienników połączeń przez okres jednego roku „w kontrolowanym i zabezpieczonym środowisku" ([272]). Nie istnieje podobny obowiązek zatrzymywania danych w odniesieniu do treści komunikacji w internecie. Dostępu do zatrzymywanych danych z dzienników połączeń można udzielić właściwym organom jedynie za zgodą organu sądowego i na warunkach opisanych w niniejszym motywie ([273]).

(177) W art. 11 obywatelskich ram prawnych w internecie przypomniano, że każda czynność polegająca na gromadzeniu, przechowywaniu, zatrzymywaniu lub jakimkolwiek innym przetwarzaniu dzienników, danych osobowych lub komunikacji przez dostawców połączeń i aplikacji internetowych w Brazylii musi być zgodna z „brazylijskimi przepisami i prawem do prywatności, ochrony danych osobowych oraz poufności prywatnej komunikacji i rejestrów". Z zabezpieczeń odzwierciedlonych w motywach 175–177 wynika, że masowe gromadzenie i zatrzymywanie danych pochodzących z łączności internetowej zasadniczo w Brazylii nie jest dozwolone.

3.2.1.2. Zniesienie ochrony tajemnicy podatkowej, bankowej i telefonicznej, poufności danych i komunikacji

(178) W Brazylii poufność korespondencji elektronicznej (w tym danych) i telefonicznej podlega ochronie na mocy konstytucji ([274]). Ponadto LGPD chroni wykorzystanie danych i informacji komunikacyjnych ([275]), podczas gdy ustawa o poufności działalności instytucji finansowych chroni poufność informacji podatkowych i bankowych ([276]).

([268]) Art. 20 rezolucji nr 324 z dnia 20 czerwca 2020 r. Dokument dostępny na stronie: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/atos-do-poder-judiciario/resolucao-no-324-de-30-de-junho-de-2020.

([269]) Art. 9 ustawy nr 9.296 z dnia 24 lipca 1996 r. o przechwytywaniu komunikacji telefonicznej.

([270]) Art. 17 ustawy nr 12.850 z dnia 2 sierpnia 2013 r. – ustawa o organizacjach przestępczych i dochodzeniach w sprawach karnych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

([271]) Art. 7 ustawy nr 12.965 z dnia 23 kwietnia 2014 r., Marco Civil da Internet (obywatelskie ramy prawne w internecie).

([272]) Akapit główny art. 13 ustawy nr 12.965 z dnia 23 kwietnia 2014 r., Marco Civil da Internet (obywatelskie ramy prawne w internecie).

([273]) Art. 13 ust. 5 ustawy nr 12.965 z dnia 23 kwietnia 2014 r., Marco Civil da Internet (obywatelskie ramy prawne w internecie).

([274]) Art. 5 (XII) konstytucji Federacyjnej Republiki Brazylii z 1988 r.

([275]) Zob. art. 2 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([276]) Ustawa uzupełniająca nr 105 z dnia 10 stycznia 2001 r. – ustawa o poufności działalności instytucji finansowych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(179) Organy publiczne mogą uzyskać dostęp do tych informacji wyłącznie w wyjątkowych przypadkach do celów dochodzenia lub ścigania w sprawach karnych. Zgodnie z orzecznictwem Federalnego Sądu Najwyższego, przechwytywanie komunikacji musi być zawsze środkiem pomocniczym i wyjątkowym, który jest dopuszczalny tylko wtedy, gdy nie ma innych sposobów rozwiązania konkretnej sprawy ([277]).

(180) Kryteria i zabezpieczenia dotyczące dostępu do danych i komunikacji określono w obywatelskich ramach prawnych w internecie i w ustawie o przechwytywaniu komunikacji telefonicznej i opisano je szczegółowo w motywach 169–177 niniejszej decyzji.

(181) Jeżeli chodzi o dane podatkowe i bankowe, art. 1 ustawy o poufności działalności instytucji finansowych określa warunki zniesienia ogólnych obowiązków zagwarantowania poufności tych informacji. Po pierwsze, obowiązek zachowania poufności można znieść wyłącznie za zgodą organu sądowego ([278]). Po drugie, zgodę na zastosowanie tych środków można wydać wyłącznie w celach dochodzeń, postępowań przygotowawczych lub ścigania w sprawach następujących określonych przestępstw: 1) terroryzmu; 2) nielegalnego handlu substancjami narkotycznymi lub podobnymi środkami odurzającymi; 3) przemytu lub handlu bronią, amunicją albo materiałami przeznaczonymi do ich produkcji; 4) wymuszenia poprzez uprowadzenie; 5) przestępstw przeciwko krajowemu systemowi finansowemu; 6) przestępstw przeciwko administracji publicznej; 7) przestępstw przeciwko systemowi podatkowemu i zabezpieczeniu społecznemu; 8) prania pieniędzy lub ukrywania mienia; oraz 9) udziału w organizacji przestępczej ([279]). Art. 10 tej ustawy stanowi ponadto, że ochrony poufności danych podatkowych i bankowych nie można znieść w żadnym innym celu, a nieprzestrzeganie tego ograniczenia stanowi przestępstwo zagrożone karą do czterech lat pozbawienia wolności ([280]).

3.2.1.3. Przeszukanie i zajęcie

(182) Co do zasady konstytucja federalna przewiduje przeszukanie i zajęcie wyłącznie w ściśle określonych wyjątkowych okolicznościach lub zgodnie z przepisami prawa i na podstawie nakazu sądu wydanego przez właściwy organ sądowy oraz z poszanowaniem sprawiedliwości proceduralnej ([281]). Przeszukanie i zajęcie muszą odbywać się zgodnie z zasadą legalności i zostać przeprowadzone w niezbędnym zakresie.

(183) W następujących wyjątkowych okolicznościach przeszukanie i zajęcie może nastąpić bez nakazu sądu: 1) w przypadku ujęcia danej osoby na gorącym uczynku (*flagrante delicto*) (tj. jeżeli przestępstwo zostało popełnione w obecności organów ścigania); 2) w przypadku klęski żywiołowej (w celu ratowania życia lub mienia osób fizycznych); lub 3) w celu udzielenia pomocy osobie, która nie jest w stanie wyrazić zgody, a potrzebuje pomocy ([282]). W orzecznictwie Federalnego Sądu Najwyższego Brazylii doprecyzowano, że organy ścigania nie mogą powoływać się na „anonimowe doniesienia" i „podejrzane zachowanie" jako podstawę do dokonania przeszukania lub zajęcia bez nakazu, ponieważ nie spełnia to wymogu legalności i nie daje organom ważnego uzasadnienia naruszenia nienaruszalności miru domowego ([283]).

(184) Jeżeli chodzi o gwarancje proceduralne, zgodnie z zasadami konstytucyjnymi Brazylii przeszukania urządzenia elektronicznego nie można dokonać bez uzasadnionego podejrzenia, że znajdują się na nim dowody popełnienia przestępstwa, a co do zasady – bez nakazu sądu ([284]). Ponadto osoby fizycznej nie można zmusić do przekazania danych, jeżeli takie przekazanie mogłoby naruszyć jej konstytucyjne prawa, takie jak prawo do nieobciążania siebie winą ([285]). Składając do sądu wniosek o wydanie nakazu przeszukania, organ ścigania przedstawia istotne fakty

([277]) Federalny Sąd Najwyższy, HC 108147/PR, 2012. Dokument dostępny na stronie: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
([278]) Art. 3-B dekretu z mocą ustawy nr 3.689 z dnia 3 października 1941 r. – kodeks karny. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([279]) Art. 1 ust. 4 (I)–(IX) ustawy uzupełniającej nr 105 z dnia 10 stycznia 2001 r. – ustawa o poufności działalności instytucji finansowych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.
([280]) Art. 10 ustawy uzupełniającej nr 105 z dnia 10 stycznia 2001 r. – ustawa o poufności działalności instytucji finansowych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.
([281]) Art. 5 (XI) konstytucji Federacyjnej Republiki Brazylii z 1988 r.
([282]) Art. 5 (XI) konstytucji Federacyjnej Republiki Brazylii z 1988 r.
([283]) Federalny Sąd Najwyższy, 2020 r., sprawa J.S. Skarga nadzwyczajna nr 603616.
([284]) Art. 5 (XI) konstytucji Federacyjnej Republiki Brazylii z 1988 r.
([285]) Art. 5 (LXIII) konstytucji Federacyjnej Republiki Brazylii z 1988 r. Zob. również dekret z mocą ustawy nr 2.848 z dnia 7 grudnia 1940 r. – kodeks postępowania karnego. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

i dowody potwierdzające potrzebę uzyskania dostępu do systemu komputerowego i danych, z wykorzystaniem danych uwierzytelniających uzyskanych zgodnie z prawem ([286]). W przypadku gdy sąd wyda nakaz przeszukania, organy ścigania wykorzystują te dane uwierzytelniające, aby uzyskać dostęp do systemu komputerowego i zawartych w nim danych, zgodnie z warunkami określonymi w nakazie. Po zakończeniu przeszukania lub korzystania z dostępu właściwe organy muszą przedłożyć sądowi sprawozdanie opisujące wyniki przeszukania lub dostępu oraz zawierające wykaz uzyskanych danych lub informacji.

3.2.1.4. Dostęp do informacji poufnych

(185) Art. 4 ustawy o dostępie do informacji („LAI") definiuje „informacje poufne" jako informacje, które „tymczasowo podlegają ograniczeniu dostępu publicznego ze względu na ich zasadnicze znaczenie dla bezpieczeństwa społeczeństwa i państwa" ([287]). Dane osobowe mogą wchodzić w zakres informacji poufnych w rozumieniu powyższej definicji.

(186) Art. 6 LAI nakłada na podmioty publiczne obowiązek ochrony informacji poufnych i ograniczenia dostępu do nich. Jeżeli chodzi o dostęp do komunikacji, danych, bankowości i informacji podatkowych, dostęp do informacji poufnych na potrzeby dochodzeń, postępowań przygotowawczych i ścigania może nastąpić wyłącznie na podstawie zezwolenia organu sądowego, w wyjątkowych przypadkach, i jest dozwolony tylko wtedy, gdy nie ma innych środków umożliwiających rozstrzygnięcie konkretnej sprawy – zgodnie z orzecznictwem Federalnego Sądu Najwyższego i przepisami prawa ([288]).

3.2.1.5. Inne środki ograniczające prawa podstawowe osoby objętej dochodzeniem, których celem jest uzyskanie dowodów

(187) „Inne środki ograniczające prawa podstawowe osoby objętej dochodzeniem, których celem jest uzyskanie dowodów" odnoszą się na przykład do możliwości wydania nakazu tymczasowego aresztowania lub objęcia danej osoby nadzorem fizycznym. Środki te co do zasady nie mają znaczenia w kontekście przekazywania danych na podstawie decyzji stwierdzającej odpowiedni stopień ochrony.

(188) Aby zapewnić kompletność informacji, należy wskazać, że takie środki, proponowane przez organ publiczny, mogą być zastosowane wyłącznie na podstawie zgody organu sądowego. Proponowane środki muszą być zgodne z zasadą legalności ustanowioną w konstytucji, a ich zastosowanie można zarządzić w wyjątkowych przypadkach i tylko wtedy, gdy nie można zastosować żadnej alternatywnej metody – zgodnie z orzecznictwem Federalnego Sądu Najwyższego.

3.2.2. *Dalsze wykorzystywanie informacji*

(189) Jeśli chodzi o późniejsze wykorzystanie danych osobowych przez organ publiczny w innym celu, art. 9 ustawy o przechwytywaniu komunikacji telefonicznej stanowi, że jeżeli zgromadzone treści nie są związane z przedmiotem badanej sprawy, dane te zostaną uznane za „nienadające się do wykorzystania". Ponadto art. 13 obywatelskich ram prawnych w internecie ogranicza okres zatrzymywania danych dotyczących połączeń w rejestrze do maksymalnie jednego roku. Art. 10 ustawy o poufności działalności instytucji finansowych ogranicza również cel, dla którego można znieść obowiązek zachowania poufności danych podatkowych i bankowych ([289]). Środki te w praktyce ograniczają możliwość jakiegokolwiek dalszego wykorzystywania tych informacji.

([286]) Art. 240 dekretu z mocą ustawy nr 2.848 z dnia 7 grudnia 1940 r. – kodeks postępowania karnego.
([287]) Art. 4 (III) ustawy nr 12.527 z dnia 18 listopada 2011 r. – ustawa o dostępie do informacji.
([288]) Federalny Sąd Najwyższy, HC 108147/PR, 2012. Dokument dostępny na stronie: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401 oraz art. 3-B dekretu z mocą ustawy nr 3.689 z dnia 3 października 1941 r. – kodeks karny. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([289]) Art. 10 ustawy uzupełniającej nr 105 z dnia 10 stycznia 2001 r. – ustawa o poufności działalności instytucji finansowych. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(190) Ponadto, co ważne, Federalny Sąd Najwyższy orzekł, że LGPD ma zastosowanie do udostępniania danych osobowych między organami publicznymi, w tym również między organami ścigania a agencjami wywiadowczymi ([290]). W szczególności Sąd przypomniał, że „udostępnianie danych osobowych między organami i podmiotami administracji publicznej zakłada: 1) wskazanie prawnie uzasadnionego, konkretnego i wyraźnie określonego celu przetwarzania danych; 2) zgodność przetwarzania ze wskazanym celem; 3) ograniczenie zakresu udostępniania do minimum niezbędnego do osiągnięcia wskazanego celu; jak również zachowanie pełnej zgodności z wymogami, zabezpieczeniami i procedurami określonymi w LGPD w zakresie, w jakim jest to zgodne z działalnością sektora publicznego". Sąd dodał, że „przetwarzanie danych osobowych przez organy publiczne w sposób sprzeczny z przepisami ustawowymi i konstytucyjnymi skutkuje odpowiedzialnością cywilną państwa za szkody wyrządzone osobom fizycznym" zgodnie z art. 42 LGPD.

(191) W odniesieniu do udostępniania danych osobowych między brazylijskimi organami ścigania a podobnymi organami w państwach trzecich, działania te są regulowane instrumentami prawa międzynarodowego, zgodnie z LGPD. W tym kontekście art. 33 (III) LGPD stanowi, że przekazywanie danych do państw trzecich może mieć miejsce, gdy jest to „niezbędne do międzynarodowej współpracy prawnej pomiędzy organami publicznymi zajmującymi się wywiadem, śledzeniem i ściganiem, zgodnie z międzynarodowymi instrumentami prawnymi". W Brazylii Ministerstwo Sprawiedliwości i Bezpieczeństwa Publicznego pełni funkcję organu centralnego w zakresie międzynarodowej współpracy prawnej w sprawach karnych. Ministerstwo odpowiada za przyjmowanie, analizowanie, przekazywanie i monitorowanie realizacji wniosków o współpracę międzynarodową z organami zagranicznymi, zgodnie z obowiązującymi przepisami prawa międzynarodowego i LGPD. Przetwarzanie danych osobowych niezbędnych do międzynarodowej współpracy prawnej podlega zasadom ograniczenia celu (art. 6 (I) LGPD), zgodności z prawem i rzetelności przetwarzania (art. 6 i 7 LGPD), minimalizacji i dokładności danych (art. 6 (III) i (V) LGPD), przejrzystości (art. 6 (VI) LGPD), bezpieczeństwa danych (art. 6 (VII) LGPD) oraz ograniczenia przechowywania (art. 6 (I), (III), (IV) i art. 16 LGPD). Ewentualne ujawnienie danych osobowych osobom trzecim (w tym państwom trzecim) może nastąpić wyłącznie zgodnie z tymi zasadami, po dokonaniu oceny zgodności z konstytucyjnymi zasadami konieczności i proporcjonalności oraz zapewnieniu ciągłości ochrony i przestrzegania praw osób, których dane dotyczą (art. 2 rozporządzenia w sprawie przekazywania danych).

(192) Uprawnienia organów ścigania w Brazylii w zakresie gromadzenia danych i dostępu do danych są zatem ograniczone jasnymi i precyzyjnymi zasadami przewidzianymi przepisami prawa i podlegają szeregowi zabezpieczeń. Zabezpieczenia te obejmują w szczególności gwarantowany nadzór nad stosowaniem takich środków, w tym za pomocą uprzedniej zgody organu sądowego i zabezpieczeń ograniczających czas dostępu do informacji i ich zatrzymywania, zgodnie z zasadami konieczności i proporcjonalności.

3.2.3. *Nadzór*

(193) W Brazylii działania organów ścigania są nadzorowane przez różne organy.

(194) Po pierwsze, jak potwierdził Federalny Sąd Najwyższy, ANPD jest uprawniony do nadzorowania przetwarzania danych osobowych prowadzonego przez organy ścigania w zakresie określonych wymogów LGPD ([291]). W tym kontekście ANPD może wykonywać uprawnienia dochodzeniowe i naprawcze przysługujące mu na mocy LGPD. Na przykład ANPD zbadała działania policji federalnej, Ministerstwa Sprawiedliwości i Bezpieczeństwa Publicznego oraz innych organów publicznych prowadzących działania w zakresie bezpieczeństwa na szczeblu federalnym, stanowym lub lokalnym lub mających obowiązki związane z egzekwowaniem prawa ([292]). Dochodzenia mogą być prowadzone z inicjatywy własnej ANPD lub na podstawie wniosków i skarg, które mogą być składane na przykład przez osoby fizyczne, organizacje społeczeństwa obywatelskiego i organy publiczne. ANPD przeprowadziła na przykład kilka dochodzeń w sprawie korzystania z kamer wideo w odpowiedzi na wnioski otrzymane od społeczeństwa obywatelskiego ([293]).

([290]) Federalny Sąd Najwyższy. Orzeczenie w sprawie ADI 6649, wrzesień 2022 r. Dokument dostępny na stronie: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([291]) Zob. motyw 163 niniejszej decyzji oraz orzeczenie Federalnego Sądu Najwyższego w sprawie ADI 6649 z dnia 15 września 2022 r. Dokument dostępny na stronie: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([292]) Zob. ANPD, Inspekcje, w tym sprawa 00261.000836/2021-76 i 00261.001028/2021-26. Dostępne pod adresem: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340.

([293]) Zob. ANPD, Inspekcje, sprawa 00261.002211/2022-20 dotycząca korzystania z kamery bezpieczeństwa przez organy w mieście Fortaleza. Wniosek skierowany do ANPD jest dostępny pod adresem: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos/arquivos-processos-de-fiscalizacao-concluidos/processosesec_pblico00261-002211_2022-20.pdf.

(195) Po drugie, działania organów ścigania są nadzorowane przez wymiar sprawiedliwości. Sądy są uprawnione do udzielania zgód na gromadzenie danych osobowych i dostęp do nich w okolicznościach, o których mowa powyżej w motywach 165–187. Ponadto sądy są uprawnione do nakładania sankcji cywilnych i karnych w przypadku nadużycia lub nieprzestrzegania obowiązujących przepisów – w tym kary pozbawienia wolności lub nakazu zaprzestania określonej działalności.

(196) Po trzecie, prokuratura, będąca niezależną i stałą instytucją w Brazylii odpowiedzialną za obronę porządku prawnego i systemu demokratycznego, posiada kompetencje do sprawowania kontroli zewnętrznej nad działalnością policji ([294]). Zgodnie z uchwałą w sprawie prokuratury celem kontroli zewnętrznej nad działalnością policji jest utrzymanie „prawidłowości i adekwatności procedur stosowanych przy wykonywaniu czynności policji", ze szczególnym uwzględnieniem „poszanowania praw podstawowych gwarantowanych przez konstytucję federalną i ustawy" ([295]). W ramach tych kompetencji prokuratura może m.in. przeprowadzać wizje lokalne – zarówno zapowiedziane, jak i niezapowiedziane – analizować dochodzenia, nadzorować zajęcie mienia oraz monitorować wykonanie nakazów sądowych ([296]). Wszelkie naruszenia prawa podlegają zgłoszeniu do sądu. W ramach swoich zadań prokuratura angażuje się w prowadzenie dochodzeń i ściganie przypadków przemocy ze strony policji, nadużyć władzy i naruszeń praw człowieka. Prokuratura odgrywa ponadto rolę w nadzorowaniu ochrony danych, inicjując działania prawne lub dołączając do działań prawnych na podstawie ochrony konstytucyjnej i propagując prawa do ochrony danych wraz z ANPD. Prokuratura przedstawiła na przykład swoje argumenty Federalnemu Sądowi Najwyższemu, popierając przełomową decyzję uznającą ochronę danych za prawo podstawowe w Brazylii ([297]). Rejestr czynności prokuratury dotyczących LGPD jest również dostępny na jej stronie internetowej ([298]).

3.2.4. *Dochodzenie roszczeń*

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

(198) Po pierwsze, osoby fizyczne mogą dochodzić roszczeń przed sądem, w tym odszkodowania. Konstytucja federalna i kodeks postępowania cywilnego stanowią podstawę prawną dochodzenia odszkodowania za szkodę niematerialną lub materialną spowodowaną przez organ publiczny, który niezgodnie z prawem zgromadził lub wykorzystał dane do celów postępowań karnych ([299]). W szczególności konstytucja wyraźnie wskazuje, że prawo do prywatności obejmuje „prawo do odszkodowania" za szkodę materialną lub niematerialną powstałą w wyniku z jego naruszenia ([300]). Od orzeczeń sądów można złożyć odwołanie do Federalnego Sądu Najwyższego oraz do Międzyamerykańskiego Trybunału Praw Człowieka. W 2009 r. Międzyamerykański Trybunał Praw Człowieka nakazał Brazylii wypłatę odszkodowania pracownikom spółdzielni rolniczych w związku z niewłaściwym przechwytywaniem komunikacji telefonicznej w stanie Paraná w 1999 r., przeprowadzonym z naruszeniem ustawy o przechwytywaniu komunikacji telefonicznej i Amerykańskiej Konwencji Praw Człowieka ([301]).

([294]) Art. 127 konstytucji Federacyjnej Republiki Brazylii z 1988 r.

([295]) Art. 20 rezolucji nr 20 z dnia 28 maja 2007 r. – zewnętrzna kontrola działalności policji. Dokument dostępny na stronie: https://www.cnmp.mp.br/portal/images/Comissoes/CSP/Resolu%C3%A7%C3%B5es_/Resolu%C3%A7%C3%A3o_20.pdf.

([296]) Art. 4 rezolucji nr 20 z dnia 28 maja 2007 r. – zewnętrzna kontrola działalności policji.

([297]) Zob. motyw 199 niniejszej decyzji oraz orzeczenie Federalnego Sądu Najwyższego w sprawie ADI 6.387 z maja 2020 r. Dokument dostępny na stronie: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([298]) Prokuratura, „LGPD w prokuraturze". Dokument dostępny na stronie: https://www.mpf.mp.br/servicos/lgpd/lgpd-no-mpf.

([299]) Zob. np. art. 43 ustawy nr 10.408 z dnia 10 stycznia 2002 r. Kodeks postępowania cywilnego. Dokument dostępny na stronie: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm.

([300]) Art. 5 (X) konstytucji Federacyjnej Republiki Brazylii z 1988 r.

([301]) Międzyamerykański Trybunał Praw Człowieka, sprawa Escher i in. przeciwko Brazylii: wstępne zarzuty, istota sprawy, odszkodowanie i koszty. Orzeczenie z dnia 6 lipca 2009 r., Dokument dostępny na stronie: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

(199) Po drugie, osoby fizyczne, niezależnie od ich narodowości, mogą powoływać się na ochronę ustanowioną przez instrument prawny *Habeas Data*, aby uzyskać dostęp do swoich danych przechowywanych przez organy publiczne oraz ich sprostowanie ([302]). Na tej podstawie osoby fizyczne mogą również wnosić sprawy do sądów, w tym „skargę bezpośrednią na niekonstytucyjność" (Ação Direta de Inconstitucionalidade – ADI) do Federalnego Sądu Najwyższego. Przełomowe orzeczenie Federalnego Sądu Najwyższego z 2020 r., które utorowało drogę do uznania ochrony danych osobowych za prawo podstawowe w Brazylii, wydano w wyniku skarg bezpośrednich na niekonstytucyjność wniesionych w oparciu o *Habeas Data* ([303]). W sprawę zaangażowana była również prokuratura, która poparła stanowisko osób fizycznych i społeczeństwa obywatelskiego, które wniosły sprawę. W sprawie tej zaskarżono dekret, który miał umożliwić udostępnienie danych osobowych ponad 200 milionów abonentów telefonii komórkowej Brazylijskiemu Instytutowi Geografii i Statystyki podczas pandemii COVID-19 ([304]). Federalny Sąd Najwyższy stwierdził, że dekret narusza podstawowe prawa do prywatności i poufności komunikacji chronione na mocy konstytucji ([305]). Obowiązywanie dekretu zostało zawieszone, a Federalny Sąd Najwyższy orzekł, że ochronę danych osobowych należy uznać za prawo podstawowe podlegające ochronie, podobnie jak prawo do prywatności ([306]). W chwili wydania orzeczenia LGPD nie była jeszcze w mocy. W związku z tym skład orzekający zastosował prawo porównawcze, w szczególności powołał się na orzecznictwo niemieckiego Federalnego Trybunału Konstytucyjnego i art. 8 Karty praw podstawowych Unii Europejskiej, aby uzasadnić niekonstytucyjność dekretu, a także dla celów wykładni praw podstawowych do godności i prywatności zagwarantowanych w konstytucji oraz uznania *Habeas Data* za narzędzie ochrony prawa do prywatności informacji ([307]).

(200) Po trzecie, osoby fizyczne mogą dochodzić roszczeń wobec ANPD w związku z naruszeniami LGPD zgodnie z jej art. 55-J (V) i na warunkach opisanych w motywach 146 i 149 niniejszej decyzji. Osoby fizyczne mogą również korzystać z przysługujących im praw ochrony danych ustanowionych na mocy LGPD w stosunku do organów publicznych ([308]).

(201) Mechanizmy dochodzenia roszczeń opisane w motywach 197–200 niniejszej decyzji zapewniają osobom, których dane dotyczą, skuteczne środki administracyjne i środki zaskarżenia umożliwiające im w szczególności egzekwowanie ich praw, w tym prawa do ochrony danych w odniesieniu do takich danych.

3.3. Dostęp brazylijskich organów publicznych do danych w celach związanych z bezpieczeństwem narodowym i korzystanie przez brazylijskie organy publiczne z tych danych w celach związanych z bezpieczeństwem narodowym

(202) W brazylijskim prawie ustanowiono szereg ograniczeń i zabezpieczeń w zakresie dostępu do danych osobowych i korzystania z nich do celów bezpieczeństwa narodowego, a także mechanizmy nadzoru i dochodzenia roszczeń, które są zgodne z wymogami określonymi w motywach 156–158 niniejszej decyzji. Warunki uzyskania takiego dostępu oraz zabezpieczenia mające zastosowanie do wykonywania tych uprawnień poddano szczegółowej ocenie w kolejnych sekcjach.

([302]) Zob. motywy 9 i 161 niniejszej decyzji.

([303]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6.387 z maja 2020 r. Dokument dostępny na stronie: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([304]) Zawieszony dekret nr 954 z dnia 17 kwietnia 2020 r. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm.

([305]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6.387 z maja 2020 r., pkt 12.

([306]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6.387 z maja 2020 r., pkt 8.

([307]) Zob. Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6.387 z maja 2020 r., s. 4 oraz Międzynarodowe Stowarzyszenie Prawników (International Bar Association), Wpływ pandemii COVID-19 na ochronę danych w Brazylii: perspektywa Sądu Najwyższego Brazylii (The impact of Covid-19 for data protection in Brazil: the perspective of Brazil's supreme court). Dokument dostępny na stronie: https://www.ibanet.org/article/82b25a81-7422-4f07-aaa8-9c2db19e22af#:~:text=On%206%20and%207%20May%202020%2C%20the,as%20an%20independent%20fundamental%20right%20in%20Brazil.&text=The%20processing%20of%20data%20is%20allowed%20only,legal%20principles%2C%20such%20as%20transparency%20and%20security.

([308]) Art. 23 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

3.3.1. *Podstawy prawne, ograniczenia i zabezpieczenia*

(203) W Brazylii dane osobowe mogą być udostępniane do celów bezpieczeństwa narodowego w ramach działań wywiadowczych na podstawie ustawy ustanawiającej brazylijski system wywiadowczy (Sistema Brasileiro de Inteligência – SISBIN) ([309]). Co do zasady art. 1 tej ustawy stanowi, że brazylijski system wywiadowczy „musi zapewniać przestrzeganie i zachowanie indywidualnych praw i gwarancji oraz innych postanowień konstytucji federalnej, traktatów, konwencji, umów i zobowiązań międzynarodowych, których Federacyjna Republika Brazylii jest stroną lub sygnatariuszem" ([310]). Obejmuje to zagwarantowanie zasad konieczności i proporcjonalności, a także prawa do ochrony danych ([311]). Działania, które mają być prowadzone przez brazylijski system wywiadowczy, opisano bardziej szczegółowo w wiążących dekretach ([312]).

(204) Zgodnie z art. 4 ustawy ustanawiającej brazylijski system wywiadowczy podmioty wchodzące w jego skład mogą pozyskiwać i analizować określone dane do celów bezpieczeństwa narodowego („Segurança Pública"). Pojęcie bezpieczeństwa narodowego reguluje ustawa z 2021 r., która zmieniła kodeks karny ([313]) i uchyliła brazylijską ustawę o bezpieczeństwie narodowym ([314]). W ustawie z 2021 r. ustanowiono wyczerpujący wykaz „przestępstw" przeciwko bezpieczeństwu narodowemu, który określa zakres tego pojęcia. Do przestępstw tych należą: 1) przestępstwa przeciwko „suwerenności narodowej" (obejmujące działania wojenne, inwazję na kraj, próbę zajęcia części terytorium kraju w celu utworzenia nowego państwa, udostępnianie informacji niejawnych obcym rządom lub zagranicznym organizacjom przestępczym, które mogłyby zagrozić porządkowi konstytucyjnemu lub suwerenności narodowej, oraz ułatwianie dostępu do systemów informatycznych osobom nieupoważnionym, w tym fałszowanie danych umożliwiających taki dostęp) ([315]); 2) przestępstwa przeciwko „instytucjom demokratycznym" (obejmujące próbę siłowego obalenia rządów prawa przez uniemożliwienie lub ograniczenie działania organów konstytucyjnych oraz zamach stanu) ([316]); 3) przestępstwa przeciwko „funkcjonowaniu instytucji demokratycznych w trakcie procesu wyborczego" (obejmujące zakłócenie procesu wyborczego i ograniczenie lub pozbawienie osób fizycznych, przy użyciu przemocy, możliwości korzystania z przysługujących im praw politycznych) ([317]); oraz 4) przestępstwa przeciwko funkcjonowaniu usług podstawowych (obejmujące sabotaż środków komunikacji publicznej lub obiektów obronnych w celu obalenia rządów prawa) ([318]). W art. 359-T ustawy doprecyzowano, że korzystania z wolności wypowiedzi, konstytucyjnych praw i uprawnień, prowadzenia działalności dziennikarskiej, w tym „poprzez marsze, spotkania, strajki, zgromadzenia lub jakiekolwiek inne formy demonstracji politycznych w celach społecznych", nie można uznać za przestępstwo ([319]). Brazylijska krajowa polityka wywiadowcza (PIN) wyznacza szereg kluczowych celów w zakresie wywiadu, które władze muszą brać pod uwagę, takich jak zapobieganie „sabotażowi" lub „szpiegostwu" ([320]). Jako „dokument orientacyjny wysokiego szczebla" PIN nie rozszerza jednak wykazu przestępstw związanych z pojęciem bezpieczeństwa narodowego ani nie zmienia jego definicji ([321]).

([309]) Ustawa nr 9.883 z dnia 7 grudnia 1999 r. – ustawa ustanawiająca brazylijski system wywiadowczy. Dokument dostępny na stronie: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

([310]) Art. 1 ust. 1 ustawy nr 9.883 z dnia 7 grudnia 1999 r. – ustawa ustanawiająca brazylijski system wywiadowczy.

([311]) Zob. motyw 160 niniejszej decyzji.

([312]) Dekret nr 8.793/2016 z dnia 29 czerwca 2016 r. w sprawie krajowej polityki wywiadowczej. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm oraz dekret nr 4.376/2002 z dnia 13 września 2002 r. w sprawie organizacji i funkcjonowania brazylijskiego systemu wywiadowczego. Dokument dostępny na stronie: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/decreto-no-4-376-de-13-de-setembro-de-2002-seopi_eng_rev-d.pdf.

([313]) Ustawa nr 14.197 z dnia 1 września 2021 r., ustawa zmieniająca kodeks karny i uchylająca ustawę z 1983 r. – ustawę o bezpieczeństwie narodowym. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm.

([314]) Uchylona ustawa nr 7.170 z dnia 14 grudnia 1983 r. – ustawa o bezpieczeństwie narodowym. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/LEIS/L7170.htm.

([315]) Rozdział I ustawy nr 14.197 z dnia 1 września 2021 r. – ustawa zmieniająca kodeks karny i uchylająca ustawę z 1983 r. o bezpieczeństwie narodowym.

([316]) Rozdział II ustawy nr 14.197 z dnia 1 września 2021 r. – ustawa zmieniająca kodeks karny i uchylająca ustawę z 1983 r. o bezpieczeństwie narodowym.

([317]) Rozdział III ustawy nr 14.197 z dnia 1 września 2021 r. – ustawa zmieniająca kodeks karny i uchylająca ustawę z 1983 r. o bezpieczeństwie narodowym.

([318]) Rozdział IV ustawy nr 14.197 z dnia 1 września 2021 r. – ustawa zmieniająca kodeks karny i uchylająca ustawę z 1983 r. o bezpieczeństwie narodowym.

([319]) Art. 359-T ustawy nr 14.197 z dnia 1 września 2021 r. – ustawa zmieniająca kodeks karny i uchylająca ustawę z 1983 r. o bezpieczeństwie narodowym.

([320]) Art. 3, dekret nr 8.793/2016 z dnia 29 czerwca 2016 r. w sprawie krajowej polityki wywiadowczej. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

([321]) Wprowadzenie, akapit pierwszy, dekret nr 8.793/2016 z dnia 29 czerwca 2016 r. w sprawie krajowej polityki wywiadowczej. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

(205) Dane, do których można uzyskać dostęp i które można analizować w celu zapobiegania wymienionym powyżej przestępstwom przeciwko bezpieczeństwu narodowemu, obejmują informacje, do których organy wchodzące w skład SISBIN mają dostęp w ramach swoich działań i zgodnie z warunkami opisanymi w motywach 165–187 niniejszej decyzji (tj. na podstawie zgody organu sądowego wydanej w odniesieniu do jasno określonego celu). Dane udostępniane SISBIN są przetwarzane za pomocą bezpiecznego zaszyfrowanego systemu elektronicznego z rejestrami dostępu w celu zapewnienia identyfikowalności i możliwości kontroli informacji ([322]). Jak wyjaśnił Federalny Sąd Najwyższy, udostępnianie danych SISBIN podlega zasadom LGPD, w tym zasadom ograniczenia celu (art. 6 (I) LGPD), minimalizacji i dokładności danych (art. 6 (III) i (V) LGPD), przejrzystości (art. 6 (VI) LGPD), bezpieczeństwa danych (art. 6 (VII) LGPD) oraz ograniczenia przechowywania (art. 6 (I), (III), (IV) i art. 16 LGPD) ([323]).

(206) W art. 2 ustawy ustanawiającej brazylijski system wywiadowczy wskazano, że w skład tego systemu wchodzą wyłącznie organy publiczne. SISBIN składa się z Brazylijskiej Agencji Wywiadowczej (Agência Brasileira de Inteligência – ABIN) oraz przedstawicieli ośrodków wywiadowczych, ministerstw, sekretariatów i agencji federalnej administracji publicznej. Wykaz organów wchodzących w skład SISBIN jest określony w dekrecie w sprawie organizacji i funkcjonowania brazylijskiego systemu wywiadowczego ([324]).

(207) ABIN jest centralnym organem systemu wywiadowczego i odpowiada za planowanie, wykonywanie, koordynowanie, nadzorowanie i monitorowanie działań wywiadowczych. Działania te muszą być prowadzone z wykorzystaniem poufnych środków i technik opartych na informacjach. W celu realizacji swoich zadań ABIN otrzymuje określone informacje i dane związane z bezpieczeństwem narodowym od różnych organów publicznych będących częścią SISBIN. Organy wchodzące w skład SISBIN są zobowiązane do przekazania tych informacji ([325]), ponieważ prawo nie upoważnia ABIN do samodzielnego gromadzenia informacji. Zgodność z prawem obowiązku przekazywania danych przez organy należące do SISBIN była przedmiotem postępowania przed Federalnym Sądem Najwyższym ([326]). W orzeczeniu wydanym w 2021 r. Federalny Sąd Najwyższy wyjaśnił, że dane, które organy publiczne udostępniają ABIN, muszą być zgodne z rygorystycznymi celami interesu publicznego (np. obrona instytucji publicznych i interesu narodowego), i przypomniał, że konkretny i uzasadniony cel każdej operacji przekazywania danych jest określany w ramach formalnej procedury i wymaga zgody organu sądowego ([327]). Ograniczenia te mają również zastosowanie dalszego udostępniania danych między organami publicznymi ([328]).

(208) Przetwarzanie danych w ramach SISBIN musi również obejmować ochronę informacji przed dostępem osób lub podmiotów nieuprawnionych. Art. 5 dekretu w sprawie funkcjonowania brazylijskiego systemu wywiadowczego wyraźnie stanowi, że koordynacja i wymiana danych między organami wchodzącymi w skład systemu musi odbywać się z poszanowaniem „przepisów dotyczących tajemnicy zawodowej i bezpieczeństwa, ochrony danych

([322]) Zob. broszura SISBIN, 2024, s. 18. Dokument dostępny na stronie: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

([323]) Federalny Sąd Najwyższy. Orzeczenie w sprawie ADI 6649, wrzesień 2022 r. Dokument dostępny na stronie: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([324]) Art. 7 dekretu nr 11.693 z dnia 6 września 2023 r. w sprawie organizacji i funkcjonowania brazylijskiego systemu wywiadowczego (Sistema Brasileiro de Inteligência – SISBIN). Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Przykładami organów należących do SISBIN są: Centrum Wywiadowcze Ministerstwa Obrony, Dyrekcja ds. Wywiadu Penitencjarnego Sekretariatu Krajowego Ministerstwa Sprawiedliwości i Bezpieczeństwa Publicznego, Sekretariat Generalny ds. Stosunków Zewnętrznych Ministerstwa Spraw Zagranicznych oraz Dyrekcja ds. Wywiadu Policji Federalnej.

([325]) Art. 4 ustawy nr 9.883 z dnia 7 grudnia 1999 r. – ustawa ustanawiająca brazylijski system wywiadowczy. Dokument dostępny na stronie: https://www.gov.br/mj/pt-br/acesso-a-informacao/atuacao-internacional/legislacao-traduzida/lei-no-9-883-de-7-de-dezembro-de-1999_eng_rev-d.pdf.

([326]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6529 z dnia 15 października 2021 r. Dokument dostępny na stronie: https://www.jusbrasil.com.br/jurisprudencia/stf/1303041724/inteiro-teor-1303041733.

([327]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6529 z dnia 15 października 2021 r., pkt 22.

([328]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6529 z dnia 15 października 2021 r., pkt 3.

osobowych oraz bezpieczeństwa informacji i wiedzy", co obejmuje w szczególności LGPD jako główny akt ustawodawczy w Brazylii w zakresie ochrony danych osobowych ([329]). W art. 6 dekretu doprecyzowano ponadto, że wymiana informacji przez organy w ramach SISBIN musi odbywać się zgodnie z „zasadami pewności prawa, konieczności i interesu publicznego" oraz mieć prawnie uzasadniony cel ([330]). SISBIN uznaje również znaczenie przestrzegania LGPD w swoich ogólnodostępnych materiałach i procedurach wewnętrznych ([331]).

(209) Uprawnienia organów przetwarzających dane do celów bezpieczeństwa narodowego w Brazylii są zatem ograniczone jasnymi i precyzyjnymi zasadami przewidzianymi przepisami prawa i podlegają szeregowi zabezpieczeń. Zabezpieczenia te obejmują w szczególności gwarantowany nadzór nad stosowaniem takich środków, w tym za pomocą uprzedniej zgody organu sądowego i zabezpieczeń ograniczających dostęp do informacji zgodnie z zasadami konieczności i proporcjonalności.

3.3.2. *Dalsze wykorzystywanie informacji*

(210) Przetwarzanie danych osobowych gromadzonych przez brazylijskie organy do celów bezpieczeństwa narodowego podlega zasadom ograniczenia celu (art. 6 (I) LGPD), zgodności z prawem i rzetelności przetwarzania (art. 6 i 7 LGPD), minimalizacji i dokładności danych (art. 6 (III) i (V) LGPD), przejrzystości (art. 6 (VI) LGPD), bezpieczeństwa danych (art. 6 (VII) LGPD) oraz ograniczenia przechowywania (art. 6 (I), (III), (IV) i art. 16 LGPD).

(211) Ewentualne ujawnienie danych osobowych osobom trzecim (w tym państwom trzecim i za pośrednictwem umów międzynarodowych) może nastąpić wyłącznie zgodnie z zasadami LGPD, po dokonaniu oceny zgodności z konstytucyjnymi zasadami konieczności i proporcjonalności oraz zapewnieniu ciągłości ochrony i przestrzegania praw osób, których dane dotyczą (art. 2 rozporządzenia w sprawie przekazywania danych).

3.3.3. *Nadzór*

(212) Działania brazylijskich organów bezpieczeństwa narodowego są nadzorowane przez różne organy. W dekrecie w sprawie brazylijskiej krajowej strategii wywiadowczej zwrócono uwagę na znaczenie istnienia kilku poziomów mechanizmu nadzoru w celu ochrony „demokratycznego państwa prawa" ([332]). Federalny Sąd Najwyższy przypomniał o znaczeniu tego nadzoru w sprawie dotyczącej przetwarzania danych w ramach SISBIN, stwierdzając, że „skuteczność działań wywiadowczych jest często związana z poufnością procesu i gromadzonych informacji. W demokratycznym państwie prawa funkcja ta podlega zewnętrznej kontroli władzy ustawodawczej i sądowniczej w celu oceny, czy nałożona tajemnica jest odpowiednia do realizacji ściśle określonych celów publicznych, którym ma służyć" ([333]).

(213) Po pierwsze, kontrolę sprawuje władza wykonawcza, gwarantując, aby cele, które ma osiągnąć system wywiadowczy, a także wdrażana polityka oraz opracowywane plany odpowiadały potrzebom społecznym. Władza wykonawcza jest również odpowiedzialna za zapewnienie, aby wydatki służb wywiadowczych były racjonalne i służyły wyłącznie do pokrycia kosztów prawnie uzasadnionych, niezbędnych i użytecznych działań dla państwa. W brazylijskim systemie kontrolę tę sprawuje Izba ds. Stosunków Zewnętrznych i Obrony Narodowej Rady Rządowej, która jest odpowiedzialna za nadzór nad wdrażaniem krajowej polityki wywiadowczej, oraz Biuro Bezpieczeństwa Instytucjonalnego, które odpowiada za koordynację działalności federalnych służb wywiadowczych ([334]).

([329]) Art. 5 dekretu nr 11.693 z dnia 6 września 2023 r. w sprawie organizacji i funkcjonowania brazylijskiego systemu wywiadowczego (Sistema Brasileiro de Inteligência – SISBIN).

([330]) Art. 6 dekretu nr 11.693 z dnia 6 września 2023 r. w sprawie organizacji i funkcjonowania brazylijskiego systemu wywiadowczego (Sistema Brasileiro de Inteligência – SISBIN).

([331]) Zob. np. broszura SISBIN, s. 9: „[j]ednym z celów tej reformy jest zwiększenie poziomu identyfikowalności i przejrzystości wewnętrznych procesów SISBIN poprzez zastosowanie narzędzi i platform cyfrowych opracowanych specjalnie do tych celów. Narzędzia te muszą być dostosowane do ram prawnych ustanowionych ustawą o dostępie do informacji oraz ogólną ustawą o ochronie danych (LGPD), które to ustawy zostały przyjęte w 2012 r.". Dokument dostępny na stronie: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

([332]) Sekcja 2.4 akapit czwarty dekretu z dnia 15 grudnia 2017 r. w sprawie krajowej strategii wywiadowczej.

([333]) Federalny Sąd Najwyższy, orzeczenie z dnia 15 października 2021 r., s. 2.

([334]) Sekcja 2.4 dekretu z dnia 15 grudnia 2017 r. w sprawie krajowej strategii wywiadowczej. Dokument dostępny na stronie: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm.

(214) Po drugie, władza ustawodawcza sprawuje kontrolę nad działaniami wywiadowczymi. Celem tej kontroli jest weryfikacja zarówno legalności, jak i skuteczności działań wywiadowczych. Przewodniczący partii większościowych i mniejszościowych w Izbie Deputowanych i Senacie Federalnym, a także przewodniczący Komisji ds. Stosunków Zewnętrznych oraz Komisji Obrony Narodowej Izby Deputowanych i Senatu Federalnego wchodzą w skład organu nadzoru zewnętrznego nad działaniami wywiadowczymi – Wspólnej Komisji ds. Kontroli Działalności Wywiadowczej („Comissão mista de Controle da Atividade de Inteligência – CCAI") ([335]). Kontrola władzy ustawodawczej nad działalnością wywiadowczą została wprowadzona ustawą ustanawiającą brazylijski system wywiadowczy w 1999 r., a rola nadzorcza i uprawnienia CCAI zostały znacząco wzmocnione w wyniku przyjęcia wiążącej rezolucji Kongresu z 2013 r. ([336]) Rezolucja ta miała na celu wyeliminowanie wcześniej zidentyfikowanych niedociągnięć dalszej instytucjonalizacji CCAI poprzez zapewnienie jej stałej struktury i sekretariatu, doprecyzowanie jej uprawnień oraz zwiększenie przejrzystości działań. Rola, działalność i uprawnienia CCAI zostały szczegółowo opisane w tej rezolucji i w ustawie. CCAI monitoruje i kontroluje działalność wywiadowczą prowadzoną przez organy federalnej administracji publicznej, w szczególności przez organy wchodzące w skład SISBIN, w celu zapewnienia, że działania te są prowadzone zgodnie z konstytucją, oraz w celu ochrony praw i gwarancji osób fizycznych, społeczeństwa i państwa ([337]). CCAI może prowadzić kontrole następcze, a także audyty i kontrole operacji w toku ([338]). Członkowie CCAI mają najwyższy poziom uprawnień dostępu do dokumentów. CCAI sporządza coroczne sprawozdania ze swojej działalności, z wyłączeniem informacji, które mogłyby zagrozić bezpieczeństwu narodowemu ([339]). Jak wyszczególniono w motywie 222 niniejszej decyzji, CCAI może również przyjmować i rozpatrywać skargi od osób fizycznych.

(215) Po trzecie, ANPD nadzoruje przestrzeganie przepisów przez krajowe organy bezpieczeństwa w odniesieniu do przetwarzania danych osobowych zgodnie z warunkami określonymi w LGPD. LGPD ma częściowo zastosowanie do przetwarzania danych osobowych dokonywanego do celów bezpieczeństwa publicznego, obrony narodowej, bezpieczeństwa państwa lub w ramach działań w zakresie prowadzenia dochodzeń, postępowań przygotowawczych i ścigania w sprawach karnych ([340]). W tym kontekście ANPD może wykonywać uprawnienia dochodzeniowe i naprawcze przysługujące mu na mocy LGPD. ANPD może na przykład w dowolnym momencie przeprowadzać kontrole wszystkich organów publicznych, w tym agencji wywiadowczej ([341]).

(216) Ponadto wymiar sprawiedliwości rozpatruje pozwy obywateli przeciwko organom publicznym i w tym kontekście może sprawować nadzór nad działaniami prowadzonymi do celów bezpieczeństwa narodowego, aby zapewnić przestrzeganie wszystkich praw konstytucyjnych i odpowiednich ram prawnych, w tym LGPD. Od orzeczeń sądów można złożyć odwołanie do Federalnego Sądu Najwyższego oraz do Międzyamerykańskiego Trybunału Praw Człowieka.

3.3.4. *Dochodzenie roszczeń*

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

([335]) Art. 6 ust. 1 ustawy nr 9.883 z dnia 7 grudnia 1999 r. – ustawa ustanawiająca brazylijski system wywiadowczy.

([336]) Rezolucja nr 2 2021-CN w sprawie Wspólnej Komisji ds. Kontroli Działalności Wywiadowczej (Comissão mista de Controle da Atividade de Inteligência – CCAI). Dokument dostępny na stronie: https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html.

([337]) Sekcja 2.4 dekretu z dnia 15 grudnia 2017 r. w sprawie krajowej strategii wywiadowczej.

([338]) Zob. w szczególności art. 3 rezolucji nr 2 2021-CN w sprawie Wspólnej Komisji ds. Kontroli Działalności Wywiadowczej (Comissão mista de Controle da Atividade de Inteligência – CCAI).

([339]) Art. 13 rezolucji nr 2 z 2021-CN w sprawie Wspólnej Komisji ds. Kontroli Działalności Wywiadowczej (Comissão mista de Controle da Atividade de Inteligência – CCAI).
Informacje na temat posiedzeń i dokumentów przygotowanych przez CCAI są dostępne i regularnie aktualizowane pod adresem: https://legis.senado.leg.br/atividade/comissoes/comissao/449/ and https://www.congressonacional.leg.br/legislacao-e-publicacoes/glossario-legislativo/-/legislativo/termo/comissao_mista_de_controle_das_atividades_de_inteligencia_ccai_cn.

([340]) Art. 4 ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

([341]) Art. 55-J (XI) ustawy nr 13.709 z dnia 14 sierpnia 2018 r., Lei Geral de Proteção de Dados Pessoais (LGPD) – ogólna ustawa o ochronie danych.

(218) Jak wyszczególniono w motywie 9 niniejszej decyzji, dostęp do mechanizmów dochodzenia roszczeń jest zagwarantowany obywatelom Brazylii i państw trzecich, niezależnie od tego, czy przebywają oni na terytorium tego kraju, czy też nie.

(219) Po pierwsze, osoby fizyczne mają „bezwzględne" prawo do wniesienia powództwa w zakresie ochrony swoich praw. Zgodnie z ogólnymi zasadami określonymi w kodeksie postępowania cywilnego, aby wytoczyć powództwo przed sądem, osoba fizyczna nie musi wykazać szkody (tj. nie musi dowieść, że była lub mogła być poddana nadzorowi albo że jej dane były przetwarzane do celów bezpieczeństwa narodowego). Osoba fizyczna może korzystać ze swoich uprawnień wynikających z *Habeas Data* w odniesieniu do danych przetwarzanych przez organy wywiadowcze ([342]).

(220) Osoby fizyczne mogą dochodzić przed sądem rekompensaty. Podobnie jak w przypadku przetwarzania danych do celów egzekwowania prawa karnego, konstytucja federalna oraz kodeks postępowania cywilnego stanowią podstawę prawną do dochodzenia – w tym również w drodze powództw zbiorowych – odszkodowania za szkodę niemajątkową lub majątkową wyrządzoną przez organ publiczny, który niezgodnie z prawem gromadził lub wykorzystywał dane ([343]).

(221) Po drugie, Federalny Sąd Najwyższy potwierdził częściowe stosowanie LGPD do celów bezpieczeństwa narodowego, a tym samym uprawnienia ANPD do rozpatrywania skarg dotyczących przetwarzania danych osobowych przez organy publiczne w tych celach ([344]). W tym samym wyroku Sąd stwierdził, że „przetwarzanie danych osobowych przez organy publiczne, które jest sprzeczne z przepisami ustawowymi i konstytucyjnymi, skutkuje odpowiedzialnością cywilną państwa za szkody wyrządzone osobom fizycznym" zgodnie z art. 42 LGPD ([345]).

(222) Po trzecie, CCAI może przyjmować i rozpatrywać skargi dotyczące naruszeń praw i wolności podstawowych popełnionych przez organy i podmioty prowadzące działalność wywiadowczą lub kontrwywiadowczą, zgłaszane przez dowolnego obywatela, partię polityczną lub stowarzyszenie ([346]). Na tej podstawie CCAI może przeprowadzać kontrole lub dochodzenia. CCAI zapewnia zatem dodatkową administracyjną ścieżkę dochodzenia roszczeń w przypadku naruszenia praw związanych z przetwarzaniem danych do celów bezpieczeństwa narodowego. Skargi otrzymane przez CCAI mogą być następnie przekazywane do sądów.

(223) Różne środki ochrony sądowej dostępne w brazylijskim systemie prawnym umożliwiają osobom fizycznym dochodzenie roszczeń. W szczególności osoby fizyczne mogą kwestionować legalność działań organów publicznych i wywiadowczych. Ponadto mogą one uzyskać odszkodowanie za poniesione szkody.

4. **PODSUMOWANIE**

(224) Komisja uważa, że Federacyjna Republika Brazylii – poprzez LGPD – zapewnia stopień ochrony danych osobowych przekazywanych z Unii Europejskiej, który zasadniczo odpowiada stopniowi ochrony zagwarantowanemu w rozporządzeniu (UE) 2016/679.

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

([342]) Zob. motyw 9 niniejszej decyzji.

([343]) Zob. np. art. 43 ustawy nr 10.408 z dnia 10 stycznia 2002 r. Kodeks postępowania cywilnego. Dokument dostępny na stronie: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm oraz art. 1 ustawy nr 7.397 z dnia 24 lipca 1985 r. – ustawa o odpowiedzialności cywilnej. Dokument dostępny na stronie: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm.

([344]) Zob. motywy 31 i 162 niniejszej decyzji oraz orzeczenie Federalnego Sądu Najwyższego w sprawie ADI 6649 z dnia 15 września 2022 r. Dokument dostępny na stronie: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([345]) Federalny Sąd Najwyższy, orzeczenie w sprawie ADI 6649 z dnia 15 września 2022 r., pkt 8. Dokument dostępny na stronie: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([346]) Art. 3 (XI) rezolucji nr 2 z 2021-CN w sprawie Wspólnej Komisji ds. Kontroli Działalności Wywiadowczej (Comissão mista de Controle da Atividade de Inteligência – CCAI).

(226) Wreszcie, na podstawie dostępnych informacji na temat brazylijskiego porządku prawnego, Komisja uważa, że wszelkie naruszenia praw podstawowych osób fizycznych, których dane osobowe są przekazywane z Unii Europejskiej do Brazylii, jakich dopuszczają się brazylijskie organy publiczne do celów interesu publicznego, w szczególności do celów ścigania przestępstw i bezpieczeństwa narodowego, będą ograniczać się do tego, co jest absolutnie niezbędne do osiągnięcia tego uzasadnionego celu oraz że ustanowiono skuteczną ochronę prawną przed takimi naruszeniami.

(227) W świetle ustaleń niniejszej decyzji należy zatem uznać, że Brazylia zapewnia odpowiedni stopień ochrony w rozumieniu art. 45 rozporządzenia (UE) 2016/679, interpretowanego w świetle Karty praw podstawowych Unii Europejskiej, danych osobowych przekazywanych z Unii Europejskiej administratorom danych i podmiotom przetwarzającym w Brazylii podlegającym przepisom LGPD.

5. SKUTKI NINIEJSZEJ DECYZJI I DZIAŁANIA ORGANÓW OCHRONY DANYCH

(228) 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.

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

(230) Należy przypomnieć, że zgodnie z art. 58 ust. 5 rozporządzenia (UE) 2016/679 i jak wyjaśnił Trybunał Sprawiedliwości w wyroku w sprawie Schrems, jeżeli krajowy organ ochrony danych kwestionuje, w tym na podstawie skargi, zgodność wydanej przez Komisję decyzji stwierdzającej odpowiedni stopień ochrony z przysługującymi osobie fizycznej prawami podstawowymi do prywatności i ochrony danych, należy zapewnić w prawie krajowym drogę prawną umożliwiającą tej osobie podniesienie tych zarzutów przed sądem krajowym, który może być zobowiązany do wystąpienia z odesłaniem prejudycjalnym do Trybunału Sprawiedliwości ([347]).

6. MONITOROWANIE, ZAWIESZENIE, UCHYLENIE LUB ZMIANA NINIEJSZEJ DECYZJI

(231) Zgodnie z orzecznictwem Trybunału Sprawiedliwości ([348]), a także jak wskazano w art. 45 ust. 4 rozporządzenia (UE) 2016/679, Komisja powinna na stale monitorować istotne zmiany zachodzące w państwie trzecim po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony, aby ocenić, czy państwo trzecie nadal zapewnia stopień ochrony zasadniczo odpowiadający temu w Unii Europejskiej. Taka kontrola jest wymagana w każdym przypadku, gdy Komisja otrzyma informacje budzące uzasadnione wątpliwości w tym względzie.

(232) W związku z powyższym Komisja powinna na bieżąco monitorować sytuację w zakresie ram prawnych i rzeczywistej praktyki w Brazylii w odniesieniu do przetwarzania danych osobowych, podlegających ocenie w niniejszej decyzji. W związku z tym należy zwrócić szczególną uwagę na stosowanie w praktyce wymogów dotyczących oceny skutków dla ochrony danych, wymogów dotyczących przejrzystości i ich ewentualnego ograniczenia w odniesieniu do prawa do informacji i dostępu, zasad dotyczących powiadamiania o naruszeniach ochrony danych, systemu sankcji, a także przestrzegania ograniczeń i zabezpieczeń w odniesieniu do dostępu rządowego, z uwzględnieniem wszelkich istotnych zmian w tym zakresie.

([347]) Schrems I, 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".

([348]) Schrems I, pkt 76.

(233) W celu ułatwienia i monitorowania tego procesu zachęca się brazylijskie władze, w tym ANPD, do informowania Komisji o zmianach w prawie materialnym, które są istotne dla niniejszej decyzji w związku z przetwarzaniem danych osobowych przez podmioty gospodarcze i organy publiczne, jak również z ograniczeniami i zabezpieczeniami dotyczącymi dostępu organów publicznych do danych osobowych.

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

(235) W zastosowaniu art. 45 ust. 3 rozporządzenia (UE) 2016/679 ([349]) oraz w świetle tego, że stopień ochrony zapewniany w porządku prawnym Brazylii może ulec zmianie, Komisja po przyjęciu niniejszej decyzji powinna okresowo sprawdzać, czy ustalenia odnoszące się do adekwatności stopnia ochrony gwarantowanego przez Brazylię są nadal faktycznie i prawnie uzasadnione.

(236) W tym celu niniejsza decyzja powinna zostać poddana pierwszemu przeglądowi w ciągu czterech lat od jej wejścia w życie. Okresowe przeglądy następcze powinny odbywać się co najmniej raz na cztery lata ([350]). Przeglądy powinny obejmować wszystkie aspekty funkcjonowania niniejszej decyzji, w tym współpracę ANPD z organami ochrony danych państw członkowskich UE w zakresie skarg składanych przez osoby fizyczne. Powinny one również obejmować ocenę skuteczności mechanizmów nadzoru i egzekwowania przepisów w obszarach prawa karnego i bezpieczeństwa narodowego.

(237) W celu przeprowadzenia przeglądu Komisja powinna odbyć spotkanie z ANPD, któremu będą towarzyszyć, w stosownych przypadkach, inne brazylijskie organy odpowiedzialne za dostęp rządowy do informacji, w tym właściwe organy nadzorcze. Uczestnictwo w tym spotkaniu powinno być otwarte dla przedstawicieli członków Europejskiej Rady Ochrony Danych. W ramach przeglądu Komisja powinna wystąpić do ANPD 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. Komisja powinna również zwracać się o wyjaśnienia dotyczące wszelkich otrzymanych informacji istotnych dla niniejszej decyzji, w tym o wyjaśnienia dotyczące publicznych sprawozdań przygotowanych przez brazylijskie władze lub inne zainteresowane strony z Brazylii, informacji otrzymanych od Europejskiej Rady Ochrony Danych, poszczególnych organów ochrony danych, organizacji społeczeństwa obywatelskiego, a także doniesień medialnych i informacji pochodzących z innych dostępnych źródeł.

(238) Na podstawie tej oceny Komisja powinna przygotować ogólnodostępne sprawozdanie, które przedłoży Parlamentowi Europejskiemu i Radzie.

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

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

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

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

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

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

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

7. **UWAGI KOŃCOWE**

(244) Europejska Rada Ochrony Danych opublikowała swoją opinię ([351]), która została uwzględniona podczas przygotowywania niniejszej decyzji.

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

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Do celów art. 45 rozporządzenia (UE) 2016/679 Brazylia zapewnia odpowiedni poziom ochrony danych osobowych przekazywanych z Unii Europejskiej administratorom i podmiotom przetwarzającym w Brazylii podlegającym przepisom ogólnej ustawy o ochronie danych (LGPD).

Artykuł 2

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

Artykuł 3

1. Komisja stale monitoruje stosowanie ram prawnych, na których opiera się niniejsza decyzja, w celu oceny, czy Brazylia nadal zapewnia odpowiedni stopień ochrony w rozumieniu art. 1.

2. Państwa członkowskie oraz Komisja informują się nawzajem o przypadkach, w których brazylijski organ ochrony danych (Agência Nacional de Proteção de Dados – ANPD) lub jakikolwiek inny właściwy organ brazylijski 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 brazylijskich organów publicznych w prawo osób fizycznych do ochrony ich danych osobowych wykraczają poza to, co jest absolutnie niezbędne, lub że nie zapewniono skutecznej ochrony prawnej przed takimi ingerencjami.

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

([351]) Europejska Rada Ochrony Danych, opinia w sprawie decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Brazylii, listopad 2025 r. Dokument dostępny na stronie: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282025-regarding-european-commission-draft_en.

5. Jeżeli Komisja posiada dowody na to, że odpowiedni stopień ochrony nie jest już zapewniony, Komisja powiadamia o tym właściwe brazylijskie organy i może zawiesić, uchylić albo zmienić niniejszą decyzję.

6. Komisja może również zawiesić, uchylić albo zmienić niniejszą decyzję, jeżeli brak współpracy ze strony rządu Brazylii nie pozwala Komisji stwierdzić, czy istnieją przesłanki do podważenia ustalenia zawartego w art. 1.

Artykuł 4

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 26 stycznia 2026 r.

W imieniu Komisji
Michael McGRATH
Członek Komisji