Journal officiel
de l'Union européenne

FR
Série L

2026/179

28.1.2026

DÉCISION D'EXÉCUTION (UE) 2026/179 DE LA COMMISSION

du 26 janvier 2026

constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Brésil

[notifiée sous le numéro C(2026) 373]

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ([1]), et notamment son article 45, paragraphe 3,

considérant ce qui suit:

1. INTRODUCTION

(1) Le règlement (UE) 2016/679 fixe les règles applicables au transfert de données à caractère personnel, par des responsables du traitement ou des sous-traitants au sein de l'Union, vers des pays tiers et à des organisations internationales, dans la mesure où ces transferts relèvent de son champ d'application. Le chapitre V (articles 44 à 50) de ce règlement définit les règles applicables aux transferts internationaux de données. Bien que les flux de données à caractère personnel en provenance et à destination de pays non membres de l'Union européenne soient nécessaires au développement des échanges commerciaux transfrontières et de la coopération internationale, le niveau de protection assuré aux données à caractère personnel au sein de l'Union ne doit pas être compromis par des transferts vers des pays tiers ([2]).

(2) En vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679, la Commission peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, assure un niveau de protection adéquat. Dans cette circonstance, les transferts de données à caractère personnel vers un pays tiers peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autre autorisation, comme prévu à l'article 45, paragraphe 1, et au considérant 103 dudit règlement.

(3) Comme précisé à l'article 45, paragraphe 2, du règlement (UE) 2016/679, l'adoption d'une décision d'adéquation doit reposer sur une analyse approfondie de l'ordre juridique du pays tiers, en ce qui concerne tant les règles applicables aux importateurs de données que les limitations et les garanties en matière d'accès des autorités publiques aux données à caractère personnel. Dans son évaluation, la Commission doit déterminer si le pays tiers en question assure un niveau de protection «essentiellement équivalent» à celui qui est garanti dans l'Union européenne ([3]). La norme au regard de laquelle l'«équivalence essentielle» est évaluée est celle fixée par la législation de l'Union européenne, notamment le règlement (UE) 2016/679, ainsi que la jurisprudence de la Cour de justice de l'Union européenne (CJUE) ([4]). Les «critères de référence pour l'adéquation» du comité européen de la protection des données sont également importants à cet égard pour préciser davantage ce principe et fournir des orientations ([5]).

([1]) JO L 119 du 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.
([2]) Considérant 101 du règlement (UE) 2016/679.
([3]) Considérant 104 du règlement (UE) 2016/679.
([4]) Voir l'arrêt de la Cour dans l'affaire C-311/18, Facebook Ireland et Schrems (ci-après l'«arrêt Schrems II»), ECLI:EU:C:2020:559.
([5]) Comité européen de la protection des données, Critères de référence pour l'adéquation, WP 254 rév. 01. Disponible à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

(4) Comme l'a précisé la Cour de justice de l'Union européenne, il ne saurait être exigé qu'un pays tiers assure un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union ([6]). En particulier, les moyens auxquels le pays tiers concerné a recours pour protéger les données à caractère personnel peuvent être différents de ceux mis en œuvre au sein de l'Union, pour autant qu'ils se révèlent, en pratique, effectifs afin d'assurer un niveau de protection adéquat ([7]). Le principe d'adéquation n'exige donc pas que l'on reproduise à l'identique les règles de l'Union. Il s'agit plutôt de déterminer si le système étranger offre, dans son ensemble, par l'essence de ses droits en matière de protection de la vie privée et de ses garanties en matière de protection des données (notamment leur mise en œuvre effective, leur opposabilité et le contrôle de leur application), ainsi que par les circonstances relatives à un transfert de données à caractère personnel, le niveau de protection requis ([8]).

(5) La Commission a analysé le droit et la pratique de la République fédérative du Brésil (ci-après le «Brésil»). Sur la base des constatations exposées aux considérants 7 à 223, elle conclut que le Brésil assure un niveau de protection adéquat des données à caractère personnel transférées de l'Union au Brésil dans le cadre du champ d'application du règlement (UE) 2016/679.

(6) La présente décision a pour effet de permettre aux transferts de responsables du traitement et de sous-traitants situés dans l'Union européenne à leurs homologues au Brésil d'avoir lieu sans qu'aucune autre autorisation ne doive être obtenue. Elle ne devrait avoir aucune incidence sur l'application directe du règlement (UE) 2016/679 à ces entités lorsque les conditions relatives au champ d'application territorial dudit règlement, définies à son article 3, sont remplies.

2. RÈGLES APPLICABLES AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

2.1. Le cadre constitutionnel du Brésil

(7) Le Brésil est une République fédérative composée de l'union de 26 États et d'un district fédéral, comme le prévoit sa Constitution fédérale (ci-après la «Constitution») ([9]). Les États brésiliens ont également leurs propres constitutions, qui ne doivent pas aller à l'encontre de la Constitution fédérale ([10]). Le Brésil dispose d'un système présidentiel dans lequel le président et les membres des chambres législatives (à savoir la Chambre des députés et le Sénat fédéral) sont élus au suffrage direct.

(8) La vie privée et la protection des données sont garanties par la Constitution en tant que droits fondamentaux. Plus précisément, l'article 5, point X, de la Constitution protège l'intimité et la vie privée des personnes, l'article 5, point XII, garantit le secret des correspondances, y compris les données, et l'article 5, point LXXIX, établit le droit à la protection des données à caractère personnel en ligne et hors ligne ([11]).

(9) Tous les droits prévus par la Constitution s'appliquent aux ressortissants brésiliens et étrangers résidant au Brésil en vertu de son article 5. Les lois fédérales ont précisé que toute personne présente sur le territoire brésilien, qu'elle y réside ou non, a droit à la protection des droits fondamentaux ([12]). La portée de la protection de ces droits a encore été étendue par la jurisprudence constitutionnelle afin d'englober les étrangers résidant à l'étranger, comme le souligne également la doctrine juridique pertinente ([13]). Par conséquent, tout étranger résidant ou non au Brésil peut se prévaloir de ces protections constitutionnelles ([14]).

([6]) Affaire C-362/14, Schrems (ci-après l'«arrêt Schrems I»), ECLI:EU:C:2015:650, point 73.
([7]) Arrêt Schrems I, point 74.
([8]) Arrêt Schrems I, point 75.
([9]) Constitution de la République fédérative du Brésil de 1988. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.
([10]) Article 25, Constitution de la République fédérative du Brésil de 1988.
([11]) Amendement constitutionnel n° 115 du 10 février 2022. Disponible à l'adresse suivante: http://www.planalto.gov.br/ccivil_03/Constituicao/Emendas/Emc/emc115.htm#art1.
([12]) Voir, par exemple, l'article 4, point XIII, de la loi n° 13.445 du 24 mai 2017, loi sur les migrations. Disponible à l'adresse suivante: 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]) Voir, par exemple, FERREIRA FILHO, Manoel Gonçalves. Direitos humanos fundamentais. 6. ed. São Paulo: Saraiva, 2004.
([14]) Arrêt du Tribunal Superior de Justiça, 4a Turma, 2016. Disponible à l'adresse suivante: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.

(10) Le Brésil a ratifié la convention américaine des droits de l'homme, connue sous le nom de «pacte de San José» en 1992 ([15]) (ci-après dénommée la «convention»). Entre autres, l'article 11 de la convention garantit le droit au respect de la vie privée et l'article 8 protège le droit à un procès équitable. En 1998, le Brésil a reconnu l'autorité contraignante de la Cour interaméricaine des droits de l'homme pour l'interprétation et l'application de la convention ([16]). La Cour peut rendre des décisions concernant l'application de droits dans le cadre d'activités menées par des autorités publiques au Brésil, y compris des autorités exerçant des missions à des fins de sécurité publique et de défense ([17]).

2.2. **Le cadre de protection des données au Brésil**

(11) Le Brésil a adopté en 2018 un acte législatif général en matière de protection des données qui fournit des garanties à chacun, quelle que soit sa nationalité: la loi générale sur la protection des données (Lei Geral de Proteção de Dados, ci-après la «LGPD») ([18]).

(12) Depuis sa promulgation, la LGPD a été renforcée et clarifiée par de nouvelles dispositions législatives. En particulier, la loi n° 13.853 de 2019 a créé l'autorité brésilienne chargée de la protection des données (Agência Nacional de Proteção de Dados, ci-après l'«ANPD») ([19]), qui est devenue une autorité indépendante en vertu de l'acte législatif adopté en 2022 ([20]). D'autres décrets contraignants ont complété ces actes législatifs, entre autres, afin de relever le statut de l'ANPD ([21]), et de mieux définir sa composition et la procédure de nomination de ses administrateurs ([22]).

(13) Comme décrit plus en détail aux considérants 125 à 141 de la présente décision, l'ANPD est l'autorité chargée de l'interprétation et de l'application de la LGPD. Dans ce contexte, elle émet régulièrement des règlements contraignants pour interpréter et appliquer la loi. Par exemple, elle a adopté plusieurs règlements visant à développer davantage le régime de sanctions et à préciser les règles relatives à la notification des violations de données ([23]). D'autres orientations sur l'application et l'interprétation de la LGPD sont fournies par l'ANPD au moyen de documents et de guides, tels que ceux adoptés concernant l'interprétation de la base juridique (par exemple, l'intérêt légitime) et des concepts clés de la LGPD (par exemple, les sanctions ou le délégué à la protection des données).

([15]) Liste des signataires et des ratifications de la convention américaine des droits de l'homme. Disponible à l'adresse suivante: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm.

([16]) Déclaration du Brésil concernant la convention. Disponible à l'adresse suivante: http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights_sign.htm#Brazil.

([17]) Voir, par exemple, l'arrêt du 6 juillet 2009 dans l'affaire Escher e.a./Brésil. Disponible à l'adresse suivante: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_ing.pdf.

([18]) Loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données. Disponible à l'adresse suivante: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm et en anglais à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf.

([19]) Loi n° 13.853 du 8 juillet 2019 modifiant la LGPD afin, entre autres, de créer l'autorité de protection des données — Autoridade Nacional de Proteção de Dados (ANPD). Disponible à l'adresse suivante: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2.

([20]) Loi n° 14.460 du 25 octobre 2022, loi transformant l'ANPD en une autorité à statut spécial. Disponible à l'adresse suivante: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Lei/L14460.htm#art7.

([21]) Décret n° 1.317 du 17 septembre 2025 modifiant la LGPD afin de transformer l'Agência Nacional de Proteção de Dados. Disponibles à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

([22]) Décret n° 10.474 du 26 août 2020 établissant l'ANPD et sa composition. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/decreto-n-10.474-de-26-de-agosto-de-2020-274389226. Décret n° 11.758 du 30 octobre 2023 modifiant la composition de l'ANPD. Disponible à l'adresse suivante: http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11758.htm. Décret du 5 novembre 2020 relatif à la nomination des directeurs de l'ANPD. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/decretos-de-5-de-novembro-de-2020-286734594.

([23]) Voir la liste des règlements de l'ANPD. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes et, notamment, le règlement n° 4 du 24 février 2024 concernant l'application de sanctions administratives. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077 et le règlement n° 15 du 24 avril 2024 sur la notification des violations de données. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

(14) Dans le cadre de son engagement international en faveur de la promotion et de la protection de la protection des données, l'ANPD brésilienne est devenue membre de l'Assemblée mondiale de la vie privée en 2023, aux côtés de toutes les autorités de protection des données de l'Union européenne ([24]). Le Brésil a également rejoint, en tant qu'observateur, le Comité du Conseil de l'Europe sur la convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ([25]). Le Brésil a également joué un rôle de premier plan dans plusieurs avancées réalisées par les Nations unies en matière de droit au respect de la vie privée. Avec l'Allemagne, le Brésil a introduit les résolutions des Nations unies sur le droit à la vie privée à l'ère numérique, adoptées par l'Assemblée générale des Nations unies en 2013 et 2014 ([26]). Parmi d'autres dispositions, cette résolution relève que «la surveillance illicite ou arbitraire ou l'interception des communications, ainsi que la collecte illicite ou arbitraire de données personnelles, qui sont des actes extrêmement envahissants, portent atteinte aux droits à la vie privée et à la liberté d'expression et pourraient aller à l'encontre des principes de toute société démocratique». Elle invite les États à revoir les règles relatives à la collecte de données afin de les aligner sur le droit international en matière de droits de l'homme et à «créer des mécanismes nationaux de contrôle indépendants efficaces qui puissent assurer la transparence de la surveillance et de l'interception des communications et de la collecte de données personnelles qu'ils effectuent, le cas échéant, et veiller à ce qu'ils en répondent, ou à les maintenir en place s'ils existent déjà» ([27]).

(15) Au niveau de sa structure et de ses principaux éléments, le cadre juridique du Brésil applicable aux données à caractère personnel transférées au titre de la présente décision est très semblable à celui qui s'applique dans l'Union européenne. Cela comprend le fait que ce cadre ne repose pas uniquement sur les obligations énoncées dans le droit national et les droits consacrés dans sa constitution, mais également sur les obligations consacrées dans le droit international, en particulier du fait de l'adhésion du Brésil à la convention américaine relative aux droits de l'homme et à son acceptation de la compétence de la Cour interaméricaine des droits de l'homme ([28]).

2.3. **Champ d'application matériel et territorial de la LGPD**

2.3.1. *Champ d'application territorial*

(16) La LGPD s'applique à tout traitement de données à caractère personnel au Brésil, quel que soit le moyen utilisé pour exercer cette activité ([29]).

(17) L'article 3 de la LGPD précise le champ d'application territorial de la loi en indiquant qu'elle s'applique: 1) aux activités de traitement effectuées sur le territoire national du Brésil (qui couvre l'Union, les États, le district fédéral et les municipalités), 2) aux activités de traitement ayant pour but d'offrir ou de fournir des biens ou des services ou le traitement de données de personnes physiques situées sur le territoire national du Brésil, et 3) lorsque les données à caractère personnel traitées ont été collectées sur le territoire national brésilien. Cette approche est comparable à celle adoptée à l'article 3 du règlement (UE) 2016/679.

(18) En outre, en vertu de l'article 3, point II, de la LGPD, tout traitement de données à caractère personnel de personnes physiques se trouvant sur le territoire national relève de la loi. Cela inclut le traitement effectué aux fins de la surveillance du comportement des personnes sur le territoire, quel que soit le lieu où les données sont traitées.

([24]) L'Assemblée mondiale de la vie privée (Global Privacy Assembly, GPA) est un forum de coordination des efforts déployés par plus de 130 autorités chargées de la protection des données et de la vie privée dans le monde entier. Voir l'annonce de l'ANPD lors de son adhésion à la GPA. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-aceita-como-membro-pleno-no-global-privacy-assembly.

([25]) Conseil de l'Europe, Observateurs du Comité de la convention 108. Disponible à l'adresse suivante: https://rm.coe.int/list-of-observers-december-2022-bilingual-2781-7012-1734-1/1680a962eb.

([26]) Voir, par exemple, Assemblée générale des Nations unies, résolution sur le droit à la vie privée à l'ère numérique, 18 décembre 2013. Disponible à l'adresse suivante: https://digitallibrary.un.org/record/764407?ln=en&v=pdf.

([27]) Assemblée générale des Nations unies, résolution sur le droit à la vie privée à l'ère numérique, 18 décembre 2013, p. 1-2.

([28]) Voir Cour interaméricaine des droits de l'homme. Q&R sur la compétence de la Cour. Disponible à l'adresse suivante: https://www.corteidh.or.cr/que_es_la_corte.cfm?lang=en.

([29]) Article 3, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

(19) Enfin, selon la jurisprudence de la Cour suprême fédérale (Supremo Tribunal Federal, ci-après «STF»), il s'ensuit que les protections des droits fondamentaux prévues par la Constitution, tel que le droit à la protection des données, s'appliquent à toute personne, indépendamment de la nationalité ou de la résidence de la personne concernée ([30]).

2.3.2. *Définition des données à caractère personnel*

(20) L'article 5, point I, de la LGPD définit les données à caractère personnel comme des informations relatives à une personne physique identifiée ou identifiable. La loi précise qu'une «personne concernée» est une «personne physique à laquelle se rapportent les données à caractère personnel traitées» ([31]).

(21) En outre, les informations pseudonymes, c'est-à-dire les informations qui ne permettent plus d'identifier une personne ou de lui être associées sans utiliser d'informations complémentaires ou sans les combiner avec des informations complémentaires afin d'en rétablir la forme initiale, sont considérées comme des données à caractère personnel au sens de la LGPD ([32]).

(22) À l'inverse, les informations qui sont pleinement «anonymisées» sont exclues du champ d'application de la LGPD ([33]). En vertu de l'article 5 de la LGPD, les données anonymisées sont définies comme des données qui, par l'utilisation de moyens raisonnables et techniques disponibles au moment du traitement, ne peuvent pas être directement ou indirectement associées à une personne. L'article 12 de la LGPD précise que les données anonymisées ne sont pas considérées comme des données à caractère personnel, sauf lorsque le processus d'anonymisation auquel les données ont été soumises a été inversé ou peut l'être au moyen d'«efforts raisonnables». L'article 12 de la LGPD souligne également que pour déterminer la notion d'«efforts raisonnables», il convient de tenir compte de facteurs objectifs tels que: 1) le coût et le temps nécessaires à l'inversion, 2) la technologie disponible, et 3) l'utilisation exclusive des moyens propres d'un responsable du traitement. L'approche de l'anonymisation et des garanties introduites dans la LGPD pour traiter la possibilité de réidentification est semblable à celle suivie dans l'UE.

(23) Cela correspond au champ d'application matériel du règlement (UE) 2016/679 et à ses notions de «données à caractère personnel», «pseudonymisation» et «informations rendues anonymes».

2.3.3. *La définition du traitement*

(24) Les définitions du «traitement» des systèmes de l'Union européenne et du Brésil font toutes deux référence à «toute opération» effectuée avec des données à caractère personnel ([34]). L'article 5, point X, de la LGPD prévoit la liste non exhaustive suivante d'activités constituant un traitement: «collecte, production, réception, classification, utilisation, accès, reproduction, transmission, distribution, traitement, archivage, stockage, suppression, évaluation ou contrôle de l'information, modification, communication, transfert, diffusion ou extraction».

2.3.4. *Responsable du traitement et sous-traitant*

(25) La notion de responsable du traitement est définie dans la LGPD comme étant la personne physique ou morale, publique ou privée, qui est responsable des décisions concernant le traitement des données à caractère personnel ([35]).

([30]) Décision du Tribunal Superior de Justiça, 4a Turma, 2016. Disponible à l'adresse suivante: https://www.jusbrasil.com.de/jurisprudencia/stj/863001318.

([31]) Article 5, point V, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([32]) Article 13, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([33]) Article 12, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([34]) Article 5, point X, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([35]) Article 5, point VI, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

(26) La notion de sous-traitant est définie dans la LGPD comme étant la personne physique ou morale, publique ou privée, qui effectue le traitement de données à caractère personnel pour le compte du responsable du traitement ([36]). Le sous-traitant doit effectuer le traitement conformément aux instructions fournies par le responsable du traitement, qui est chargé de contrôler la conformité ([37]).

(27) Le responsable du traitement et le sous-traitant doivent tenir un registre des opérations de traitement de données à caractère personnel qu'ils effectuent, en particulier lorsqu'elles sont fondées sur un intérêt légitime ([38]).

(28) En vertu de la LGPD, deux ou plusieurs responsables du traitement qui participent directement au traitement ayant causé un préjudice à la personne concernée sont solidairement responsables ([39]). Un sous-traitant est conjointement et solidairement responsable du préjudice causé par le traitement lorsqu'il ne respecte pas les obligations de la LGPD, telles que définies à l'article 44 de la LGPD, ou lorsqu'il n'a pas suivi les instructions légales du responsable du traitement ([40]).

(29) Par conséquent, les règles régissant la relation entre les responsables du traitement et les sous-traitants au titre de la LGPD sont semblables à celles du chapitre IV du règlement (UE) 2016/679.

2.3.5. *Exemptions à certaines dispositions de la LGPD*

(30) Comme dans le système de l'Union européenne, la LGPD ne s'applique pas aux données anonymisées ([41]), au traitement de données à caractère personnel à des fins purement domestiques ([42]) ou lorsque le traitement est effectué à des fins exclusives de sécurité publique, de défense nationale, de sûreté de l'État ou d'enquêtes et de poursuites en matière d'infractions pénales ([43]).

(31) L'exemption dans le domaine de la sécurité publique, de la défense nationale, de la sûreté de l'État ainsi que des enquêtes et des poursuites en matière d'infractions pénales est toutefois partielle. La Cour suprême fédérale a interprété l'applicabilité de la LGPD à la lumière de la protection constitutionnelle des données à caractère personnel et a établi que les grands principes, droits et objectifs de la LGPD s'appliquent à tout traitement de données à caractère personnel par les autorités publiques, y compris lorsqu'il est effectué à des fins de «renseignement» ([44]). En outre, les conditions applicables au traitement des données à caractère personnel à des fins de sécurité publique, de défense nationale, de sûreté de l'État ou d'enquêtes et de poursuites en matière d'infractions pénales sont fixées à l'article 4, paragraphes 2 à 4, de la LGPD, en particulier pour empêcher les entités privées de traiter des données à de telles fins, pour donner instruction à l'ANPD d'émettre des avis techniques et des

([36]) Article 5, point VII, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([37]) Article 39, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([38]) Article 37, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([39]) Article 42, paragraphe 1, point II, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([40]) Article 42, paragraphe 1, point I, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([41]) Article 12, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([42]) Article 4, point I, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([43]) Article 4, point III, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([44]) Cour suprême fédérale. Décision relative à l'ADI 6649, septembre 2022. Disponible à l'adresse suivante: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

recommandations en la matière et pour habiliter l'ANPD à demander une analyse d'impact relative à la protection des données en ce qui concerne ces activités ([45]). Sur cette base, l'ANPD a, par exemple, mené des enquêtes et publié des orientations, telles qu'une note technique adressée au ministère de la Justice et de la Sécurité publique concernant l'utilisation des technologies, y compris la reconnaissance faciale, dans les espaces publics ([46]). Dans cette note, l'ANPD a rappelé que le traitement à ces fins doit respecter les principes généraux et les droits prévus par la LGPD ([47]).

(32) L'article 4, point II, de la LGPD introduit en outre une exemption partielle à la loi pour le traitement de données à caractère personnel à des fins de recherche universitaire et à des fins journalistiques et artistiques.

(33) En ce qui concerne la recherche universitaire, l'exemption est limitée par plusieurs éléments. Premièrement, selon l'article 4, point II, de la LGPD, le traitement doit être effectué «exclusivement» à des fins de recherche universitaire. Deuxièmement, l'article 4, point II, sous b), de la LGPD dispose que les articles 7 (exigence de base juridique) et 11 (règles relatives au traitement des données sensibles) s'appliquent à ces types de traitement ([48]). Troisièmement, l'ANPD a élaboré un guide d'orientation pour préciser davantage les règles applicables au traitement des données à des fins académiques et de recherche, y compris en définissant strictement quelles entités peuvent être considérées comme un «organisme de recherche» au sens de l'article 5, point XVII, de la LGPD ([49]). Dans ce guide, l'ANPD confirme que le traitement de données à des fins de recherche universitaire n'est que partiellement exempté de l'application de la LGPD et que les principes généraux de la loi s'appliqueront ([50]).

(34) En ce qui concerne spécifiquement les données utilisées pour la recherche dans le domaine de la santé, la LGPD contient des limitations supplémentaires. D'une part, l'article 13 de la LGPD fixe des obligations de sécurité pour les bases de données utilisées et encourage le recours aux techniques d'anonymisation et de pseudonymisation. Elle prévoit également que les entités de recherche seraient tenues pour responsables de l'absence de mise en œuvre de mesures de sécurité visant à protéger les données à caractère personnel ([51]). En revanche, le transfert de données utilisées à des fins de recherche sur la santé à un tiers «est interdit, en toutes circonstances» ([52]).

(35) En ce qui concerne le traitement de données à caractère personnel à des fins journalistiques et artistiques, l'exonération de la LGPD est semblable à celle prévue à l'article 85, paragraphe 2, du règlement (UE) 2016/679. L'exonération au titre de la LGPD couvre les situations dans lesquelles le traitement serait effectué «exclusivement» à ces fins ([53]). Cela signifie que, lorsque les organismes de presse, les médias et les entités artistiques traitent des données à caractère personnel à d'autres fins, par exemple la gestion des ressources humaines ou leur organisation interne, la LGPD s'applique intégralement.

([45]) Article 4, paragraphes 2 à 4, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([46]) Note technique nº 175/2023 sur le projet d'accord de coopération entre le ministère de la Justice et de la Sécurité publique et la Fédération brésilienne de football pour le partage de données à caractère personnel en vue d'améliorer le projet «Safe Stadium». Disponible à l'adresse suivante: 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]) Note technique nº 175/2023, point 5.1.

([48]) Article 4, point II, sous b), loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([49]) Guide d'orientation de l'ANPD sur le traitement des données à caractère personnel à des fins académiques et de recherche, juin 2023. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf.

([50]) Voir notamment les pages 18 à 43 du guide d'orientation sur le traitement des données à caractère personnel à des fins académiques et de recherche.

([51]) Article 13, paragraphe 2, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([52]) Article 13, paragraphe 2, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données. Voir également le guide d'orientation de l'ANPD sur le traitement des données à caractère personnel à des fins académiques et de recherche, juin 2023, p. 15.

([53]) Article 4, point Ii, sous a), loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

(36) L'expression artistique et la liberté des médias font toutes deux partie de la liberté d'expression au titre de l'article 5, point IX, de la Constitution, qui garantit la liberté d'expression pour l'expression «intellectuelle, artistique, scientifique et de communication». En ce qui concerne l'exercice de mise en balance entre la liberté d'expression et d'autres droits (y compris les droits au respect de la vie privée et à la protection des données), il est régi par les critères énoncés dans la Constitution telle qu'interprétée par la Cour suprême fédérale. En particulier, l'exercice du droit à la liberté d'expression ne nécessite aucune autorisation préalable, mais reste soumis aux limites imposées pour la protection d'autres droits fondamentaux. En particulier, une personne peut demander réparation en cas de préjudice ou de violation du droit à la vie privée, conformément à l'article 5, point X, de la Constitution. En outre, ces garanties ont été intégrées dans le cadre civil pour l'internet, une loi adoptée en 2014 pour protéger les droits fondamentaux en ligne ([54]). En particulier, l'article 7, point I, du cadre civil pour l'internet garantit l'«inviolabilité de la vie privée» et établit un droit à réparation pour tout préjudice matériel ou moral résultant d'une violation. En outre, dans sa jurisprudence, la STF fait référence à la nécessité d'«établir un équilibre entre les droits, en conciliant le droit à la liberté d'expression et l'inviolabilité de la vie privée», soulignant l'importance du droit à réparation et à l'accès à un recours en cas de violation de la vie privée ([55]). Dans un autre cas, la STF a rappelé que «les libertés de la presse et de la communication sociale doivent être exercées en harmonie avec d'autres principes constitutionnels» tels que l'inviolabilité de la vie privée et le droit à la protection des données ([56]).

(37) Enfin, la LGPD exclut du champ d'application de la loi le traitement de données qui proviennent de l'extérieur du Brésil et qui sont soit 1) non partagées ou communiquées à des agents de traitement au Brésil, soit 2) issues d'un pays jugé adéquat en vertu de la LGPD, tant qu'elles ne sont pas transférées vers un autre pays ([57]). L'ANPD a fourni une interprétation contraignante pour clarifier les deux scénarios de manière stricte dans son règlement sur le transfert de données ([58]).

(38) Dans le premier scénario, le simple transit de données à caractère personnel par le Brésil, sans traitement supplémentaire dans le pays, serait exclu de la loi ([59]). Toutefois, dès que les données seront consultées, utilisées ou traitées de quelque manière que ce soit au Brésil, la LGPD s'appliquerait. Les règles nationales existantes en matière de cybersécurité et d'accès aux données par les autorités publiques continueraient également de s'appliquer à ce scénario limité, indépendamment du fait que les données soient traitées ou restent en simple transit.

(39) Dans le deuxième scénario, l'ANPD a précisé que seul le transfert de retour de données initialement transférées depuis un pays bénéficiant d'une décision d'adéquation au titre de la LGPD est exclu de la loi, pour autant que le droit national de ce pays adéquat s'applique à ce traitement. Dans ce cas également, les règles en matière de cybersécurité et d'accès aux données par les autorités publiques continueraient de s'appliquer. Dans le contexte du transfert de données à caractère personnel entre l'UE et le Brésil, si l'UE bénéficiait d'une décision d'adéquation de la part du Brésil, le transfert de données du Brésil vers l'UE ne relèverait pas toujours du champ d'application de l'article 3 du règlement (UE) 2016/679. Par conséquent, dans les cas où le traitement en question ne relèverait pas du champ d'application du règlement (UE) 2016/679, il ressort de l'article 8, point II, sous b), du règlement sur le transfert de données que la LGPD s'appliquerait au transfert de données du Brésil vers l'UE.

([54]) Loi nº 12.965 du 23 avril 2014, Marco Civil da Internet («Cadre civil pour l'internet»). Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([55]) Cour suprême fédérale, décision relative à l'ADI 4815. Disponible à l'adresse suivante: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4271057.

([56]) Cour suprême fédérale, décision relative à l'ADI 5418. Disponible à l'adresse suivante: https://www.jurisprudencia.stf.jus.br/pages/search/sjur446943/false.

([57]) Article 4, point IV, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([58]) Section III, annexe I, ANPD, règlement sur le transfert international de données à caractère personnel (ci-après le «règlement sur le transfert de données»). Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([59]) Article 8, point I, ANPD, règlement sur le transfert international de données à caractère personnel.

2.4. **Garanties, droits et obligations**

2.4.1. *Licéité et loyauté du traitement*

(40) Les données à caractère personnel devraient être traitées de manière licite et loyale.

(41) Les principes de licéité, de bonne foi et de transparence ainsi que les motifs de licéité du traitement sont garantis par les articles 6 et 7 de la LGPD, par des conditions semblables à celles des articles 5 et 6 du règlement (UE) 2016/679.

(42) Conformément aux articles 6 et 7 de la LGPD, les responsables du traitement et les sous-traitants traitent les informations à caractère personnel licitement et de bonne foi dans la mesure minimale nécessaire à la finalité spécifiée, en analysant les données qui sont pertinentes, proportionnées et non excessives au regard de la finalité ([60]).

(43) Ces principes généraux de traitement licite sont précisés plus en détail à l'article 7 de la LGPD, qui énonce les différentes bases juridiques pour le traitement, y compris les circonstances dans lesquelles un changement de finalité peut se produire.

(44) Conformément à l'article 7 de la LGPD, un responsable du traitement et un sous-traitant ne peuvent traiter des données à caractère personnel que pour un nombre limité de motifs juridiques. Ces motifs juridiques prévus par la LGPD sont les suivants: 1) le consentement de la personne concernée (point I), 2) la nécessité d'exécuter un contrat ou des procédures préliminaires liées à un contrat auquel la personne concernée est partie, à la demande de celle-ci (point V), 3) le respect d'une obligation légale ou réglementaire par le responsable du traitement ([61]) (point II), 4) la protection de la vie ou la sécurité physique de la personne concernée ou d'un tiers (point VII), 5) le traitement des données par une administration publique s'il est nécessaire à l'exécution des politiques publiques prévues par des dispositions législatives et réglementaires ou fondées sur des contrats, des accords ou des instruments similaires ([62]) (point III), et 6) lorsque cela est nécessaire à la réalisation des intérêts légitimes du responsable du traitement ou d'un tiers, sauf lorsque prévalent des libertés et des droits fondamentaux de la personne concernée qui exigent la protection des données à caractère personnel (point IX).

(45) L'article 7 de la LGPD prévoit quatre bases juridiques spécifiques supplémentaires pour le traitement des données, à savoir: 1) la réalisation d'études par des entités de recherche, en assurant, dans la mesure du possible, l'anonymisation des données à caractère personnel (point IV), 2) l'exercice régulier des droits dans les procédures judiciaires, administratives ou arbitrales ([63]) (point VI), 3) la protection de la santé, exclusivement dans le cadre d'une procédure effectuée par des professionnels de la santé, des services de santé ou des autorités sanitaires (point VIII), et 4) la protection du crédit (point X) ([64]).

([60]) Voir, en particulier, article 6, paragraphe principal, points III, I et V, et article 7, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([61]) Toute obligation légale ou réglementaire est définie par la loi et doit être nécessaire et proportionnée.

([62]) Les dispositions spécifiques relatives au traitement des données à caractère personnel par les autorités publiques prévues au chapitre IV de la loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), doivent être respectées.

([63]) Les procédures sont décrites dans la loi n° 9.307 du 23 septembre 1996, loi sur l'arbitrage.

([64]) En ce qui concerne la protection du crédit, l'ajout de cette base juridique dans la LGPD a augmenté le niveau de protection des personnes concernées, par exemple en veillant à ce que les entités de crédit ne traitent que les données à caractère personnel nécessaires à l'analyse et au recouvrement de crédit. Depuis l'adoption de la LGPD, les tribunaux brésiliens ont rendu plusieurs décisions visant, par exemple, à restreindre le traitement des données à des fins de protection du crédit en excluant, par exemple, le «numéro d'inscription au registre des électeurs, le nom de la mère, le mode de vie, la classe sociale, la scolarisation, la propension marginale à consommer et le géoréférencement», qui n'ont pas été jugés nécessaires. Les tribunaux ont également précisé qu'un accès plus poussé aux données à caractère personnel nécessiterait le consentement de la personne concernée, limitant ainsi la portée du traitement des données qui peut avoir lieu aux fins de la protection du crédit. Voir Opice Blum Advogados, Rapport Jurimetrics, 2022. Disponible à l'adresse suivante: https://opiceblum.com.br/wp-content/uploads/2019/07/09-relatorio-jurimetria-2022.pdf.

2.4.2. *Critères du consentement*

(46) Les exigences formelles relatives à l'obtention d'un consentement valable pour le traitement des données à caractère personnel au titre de la LGPD sont énoncées à l'article 8, suivant une approche comparable à celle de l'article 4, paragraphe 11, et de l'article 7 du règlement (UE) 2016/679. Premièrement, le consentement doit être donné soit par écrit, soit par d'autres moyens susceptibles de démontrer la «manifestation de la volonté» de la personne concernée ([65]). Dans ses guides, l'ANPD a précisé que «le consentement doit être univoque, ce qui nécessite l'obtention d'une manifestation de volonté claire et positive de la part de la personne concernée», ce qui signifie qu'il n'est pas permis d'obtenir le consentement «de manière tacite ou à la suite d'une omission de la personne concernée» ([66]). Deuxièmement, le consentement fait référence à des «finalités particulières» et les «autorisations génériques de traitement» de données à caractère personnel sont considérées comme nulles ([67]). Troisièmement, le consentement est éclairé par des informations «transparentes, claires et non équivoques» ([68]). Lorsqu'il est inclus dans un contrat plus large, le consentement doit figurer dans une clause distincte et spécifique qui se distingue clairement des autres dispositions contractuelles ([69]). En outre, le consentement est considéré comme nul si les informations fournies à la personne concernée contiennent des «contenus trompeurs ou abusifs» ([70]). Le responsable du traitement doit également informer la personne concernée de tout changement concernant: 1) les finalités du traitement, 2) le type ou la durée du traitement, 3) l'identité du responsable du traitement, ou 4) toute information concernant le traitement et l'éventuel partage de données ([71]). Quatrièmement, le consentement peut être «révoqué à tout moment» par la personne concernée au moyen d'une «procédure gratuite» ([72]).

(47) La LGPD établit une interdiction stricte du traitement des données à caractère personnel lorsque le consentement est défectueux ou invalide ([73]). La LGPD précise en outre que c'est au responsable du traitement qu'il incombe de démontrer que le consentement a été légalement obtenu conformément à la LGPD ([74]).

(48) Enfin, la LGPD établit que, dans le cas où le consentement constituerait la base juridique appropriée pour le traitement, si des données à caractère personnel ont été rendues «manifestement publiques par la personne concernée», l'exigence de consentement est réputée levée ([75]). La notion de «données manifestement publiques» figure également à l'article 9 du règlement (UE) 2016/679. Toutefois, même lorsque l'exigence de consentement est réputée levée, les responsables du traitement et les sous-traitants ne sont pas exemptés du respect de tous les autres droits et obligations énoncés dans la LGPD ([76]). En particulier, les données qui ont été manifestement rendues publiques par la personne concernée peuvent faire l'objet d'un traitement ultérieur, pour autant que ce traitement ait une finalité «légitime et spécifique» et que les droits des personnes concernées et les principes établis en vertu de la LGPD soient respectés ([77]).

([65]) Article 8, paragraphe principal, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([66]) ANPD, Guide sur les cookies et la protection des données, p. 18-19. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf.

([67]) Article 8, paragraphe 4, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données. En outre, lorsque des données à caractère personnel doivent être partagées entre les responsables du traitement, un consentement spécifique distinct est requis pour ce partage, à moins que les données n'aient été manifestement rendues publiques, comme le prévoit l'article 7, paragraphe 5, de la loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([68]) Article 9, paragraphe 1, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([69]) Article 8, paragraphe 1, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([70]) Article 9, paragraphe 1, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([71]) Article 8, paragraphe 6, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([72]) Article 8, paragraphe 5, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([73]) Article 8, paragraphe 3, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([74]) Article 8, paragraphe 2, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([75]) Article 7, paragraphe 4, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données. Le champ d'application de cette mesure est limité, car il ne couvre pas le traitement de données sensibles autorisé en vertu de l'article 9, paragraphe 2, point e), du règlement (UE) 2016/679.

([76]) Article 7, paragraphe 4, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([77]) Article 7, paragraphe 7, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

2.4.3. *Critères relatifs à l'intérêt légitime*

(49) L'article 7, point IX, de la LGPD dispose que le traitement de données à caractère personnel ne peut jamais être effectué pour des motifs d'intérêt légitime lorsque ce traitement serait contraire aux libertés et droits fondamentaux d'une personne concernée, en soulignant que la protection des données à caractère personnel prévaut. Cette approche est semblable à celle suivie dans l'UE et exposée à l'article 6, paragraphe 1, point f), du règlement (UE) 2016/679.

(50) L'article 10 de la LGPD énonce les conditions supplémentaires dans lesquelles les responsables du traitement peuvent se fonder sur l'«intérêt légitime» en tant que base juridique pour le traitement de données à caractère personnel. Premièrement, lorsque le traitement de données à caractère personnel est fondé sur un intérêt légitime, le responsable du traitement ne traite que les données à caractère personnel qui sont «strictement nécessaires» à la finalité prévue ([78]). Deuxièmement, les responsables du traitement doivent également mettre en œuvre des mesures visant à garantir la transparence de leurs activités de traitement ([79]). Troisièmement, l'intérêt légitime ne peut être invoqué que dans des «situations particulières» ([80]).

(51) En outre, l'ANPD a publié le «Guide des intérêts légitimes», qui détaille les conditions d'utilisation de l'intérêt légitime ([81]). Ce guide, par exemple, a précisé que l'intérêt légitime ne saurait être utilisé comme base juridique pour le traitement de données sensibles ([82]) et il prévoit également, dans son annexe, un modèle de test de mise en balance de la protection des droits fondamentaux et de la liberté que tous les responsables du traitement souhaitant se prévaloir de l'intérêt légitime peuvent utiliser ([83]). En outre, l'ANPD peut exiger du responsable du traitement qu'il réalise une analyse d'impact relative à la protection des données ([84]).

(52) Dans le guide, l'ANPD a précisé que pour qu'un intérêt soit considéré comme «légitime», trois conditions doivent être remplies: 1) compatibilité avec le système juridique brésilien, 2) référence à une situation spécifique, et 3) le traitement doit être lié à des finalités légitimes, spécifiques et explicites ([85]). La première condition, à savoir la «compatibilité avec le système juridique», présuppose que l'intérêt légitime invoqué par le responsable du traitement soit compatible avec les principes, les normes juridiques et les droits fondamentaux garantis au Brésil. Cela signifie, par exemple, que le traitement envisagé de données à caractère personnel ne devrait pas être interdit par la législation brésilienne et ne saurait, directement ou indirectement, être en contradiction avec les dispositions juridiques ou les principes du droit brésilien. Deuxièmement, l'intérêt légitime invoqué doit être fondé sur des situations «concrètes, claires et précises», qui visent des intérêts spécifiques et bien définis. L'intérêt légitime invoqué ne saurait être fondé sur des «situations abstraites ou purement spéculatives» ([86]). L'ANPD précise en outre que les intérêts qui ne sont pas associés aux «activités actuelles du responsable du traitement ne sont pas considérés comme légitimes» ([87]). La troisième condition concerne la nécessité de démontrer l'existence d'une finalité spécifique pour le traitement. L'ANPD relève que l'intérêt légitime du responsable du traitement (qui justifie le

([78]) Article 10, paragraphe 1, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([79]) Article 10, paragraphe 2, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([80]) L'article 10 de la LGPD fournit quelques exemples de situations particulières dans lesquelles un intérêt légitime peut être invoqué: 1) soutenir et promouvoir les activités du responsable du traitement (point I), 2) protéger l'exercice des droits de la personne concernée ou permettre la prestation de services au bénéfice de la personne concernée, à condition que ce traitement respecte les attentes légitimes, les droits fondamentaux et les libertés de la personne concernée (point II). Loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([81]) ANPD, Guide — Base juridique pour le traitement des données à caractère personnel — Intérêt légitime, février 2024 («Guide des intérêts légitimes»). Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf.

([82]) ANPD, Guide des intérêts légitimes, p. 8.

([83]) ANPD, Guide des intérêts légitimes, annexe 3.

([84]) Article 10, paragraphe 3, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([85]) ANPD, Guide des intérêts légitimes, p. 16-17.

([86]) ANPD, Guide des intérêts légitimes, p. 16, article 10, paragraphe principal, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([87]) ANPD, Guide des intérêts légitimes, p. 16.

traitement) ne doit pas être confondu avec la finalité du traitement (qui constitue la finalité spécifique qui doit être atteinte par la réalisation du traitement). L'existence d'un intérêt légitime n'élimine pas l'obligation pour le responsable du traitement de respecter le principe de limitation de la finalité et toutes les obligations découlant de la LGPD. La finalité doit être décrite de manière claire et précise, avec les informations nécessaires pour délimiter la portée du traitement et permettre la mise en balance des intérêts du responsable du traitement ou des tiers avec les droits et les attentes légitimes des personnes concernées ([88]). Cela signifie que, lorsqu'il invoque un intérêt légitime aux fins de soutenir ou de promouvoir son activité, le responsable du traitement définit clairement, entre autres, l'activité qu'il entend promouvoir/soutenir et le lien avec le traitement envisagé.

2.4.4. *Traitement portant sur des catégories particulières de données*

(53) Des garanties spécifiques devraient être prévues pour le traitement des «catégories particulières» de données.

(54) L'article 5, point II, de la LGPD définit les données à caractère personnel sensibles comme «les données à caractère personnel relatives à l'origine raciale ou ethnique, aux convictions religieuses, aux opinions politiques, à l'affiliation syndicale ou à l'organisation religieuse, philosophique ou politique, aux données relatives à la santé ou à la vie sexuelle, aux données génétiques ou biométriques, lorsqu'elles sont liées à une personne physique». Comme il ressort de la jurisprudence nationale, la notion de vie sexuelle devrait être interprétée comme couvrant également l'orientation ou les préférences sexuelles de la personne. En particulier, dans sa jurisprudence sur le mariage homosexuel, la STF a jugé que la discrimination fondée sur le «sexe» couvre les «préférences sexuelles» ([89]) et que la liberté d'exercer son «orientation sexuelle» est une «condition préalable au développement de sa personnalité», qui est protégé par la Constitution ([90]). Par conséquent, les catégories de données considérées comme des données sensibles en vertu du droit brésilien sont les mêmes que celles prévues par l'article 9, paragraphe 1, du règlement (UE) 2016/679.

(55) Les juridictions brésiliennes ont encore élargi la définition des données à caractère personnel sensibles dans le cadre de la LGPD afin d'englober d'autres types d'informations susceptibles d'être utilisées pour exercer une discrimination à l'encontre de certaines personnes ([91]). Cette interprétation découle du droit d'être protégé contre la discrimination en droit brésilien, comme reflété également à l'article 6, point IX, de la LGPD. En particulier, la jurisprudence brésilienne a précisé que les informations concernant le casier judiciaire doivent être considérées comme des données sensibles ([92]).

(56) Le traitement de données sensibles au titre de la LGPD n'est autorisé que lorsque la personne concernée ou son représentant légal a donné son consentement «spécifique et distinct» à des fins spécifiques ([93]). Les conditions de validité du consentement décrites aux considérants 46 à 48 de la présente décision s'appliquent.

(57) Conformément à l'article 11, point II, de la LGPD, sans le consentement explicite de la personne concernée, le traitement de données sensibles peut être effectué: 1) lorsqu'il est nécessaire au respect d'une obligation légale ou réglementaire du responsable du traitement [point a)], 2) lorsqu'il est nécessaire au traitement par l'administration publique aux fins de l'exécution des politiques publiques prévues par des dispositions législatives ou réglementaires [point b)], 3) pour protéger la vie ou la sécurité physique de la personne concernée ou d'un tiers [point e)], 4) pour l'exercice de droits, y compris dans le cadre de procédures contractuelles et judiciaires, administratives et d'arbitrage, conformément au droit brésilien [point d)], 5) pour protéger la santé des personnes concernées, exclusivement dans le cadre de procédures effectuées par des professionnels de la santé, des services de santé ou des autorités sanitaires [point f)], 6) par les entités de recherche pour mener des études, en veillant à ce que les données soient anonymisées, dans la mesure du possible [point c)], et 7) pour garantir la prévention de la fraude et la sécurité des personnes concernées dans le cadre des processus d'identification et d'authentification par l'enregistrement dans des systèmes électroniques. Par conséquent, les motifs de traitement des données sensibles au titre de la LGPD et du règlement (UE) 2016/679 sont similaires.

([88]) ANPD, Guide des intérêts légitimes, p. 17.

([89]) Voir l'arrêt de la Cour suprême fédérale brésilienne autorisant le mariage homosexuel, interprétant l'article 3, section IV, de la Constitution fédérale, qui interdit toute discrimination fondée sur le sexe, la race et la couleur. Cour suprême fédérale, décision relative à l'ADI 4277 du 5 mai 2011, points 2 et 6. Disponible à l'adresse suivante: https://portal.stf.jus.br/peticaoInicial/verPeticaoInicial.asp?base=ADI&numProcesso=4277.

([90]) Voir l'arrêt de la Cour suprême fédérale brésilienne autorisant le mariage homosexuel, p. 14: «En tant que condition préalable sine qua non du développement de la personnalité humaine, la plus haute valeur protégée par la Constitution fédérale, il est essentiel de supprimer tout obstacle juridique qui constitue une limitation, même potentielle, au plein exercice de la liberté de tout être humain dans le plein exercice de son *orientation sexuelle*» *(caractères italiques ajoutés)*.

([91]) Cour supérieure du travail, décision TST-E-RR-933-49.2012.5.10.0001, décembre 2021. Disponible à l'adresse suivante: https://www.jusbrasil.com.br/jurisprudencia/tst/713123452/inteiro-teor-713123472.

([92]) Cour supérieure du travail, décision TST-E-RR-933-49.2012.5.10.0001, décembre 2021.

([93]) Article 11, point I, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

2.4.5. *Limitation de la finalité*

(58) Les données à caractère personnel devraient être collectées dans un but précis et d'une manière qui n'est pas incompatible avec la finalité du traitement.

(59) L'article 6, point I, de la LGPD dispose que les données à caractère personnel doivent être traitées «pour une finalité légitime, spécifique et explicite dont la personne concernée est informée», sans possibilité de traitement ultérieur «incompatible» avec la finalité initiale. Ce principe, ainsi que son libellé, sont presque identiques à ceux correspondants à l'article 5, paragraphe 1, point c), du règlement (UE) 2016/679. L'article 6, point II, de la LGPD dispose en outre que toute activité de traitement doit être compatible avec les finalités communiquées à la personne concernée.

(60) Il ressort des guides publiés par l'ANPD que, pour déterminer si un traitement pour une autre finalité est compatible avec la finalité pour laquelle les données ont été initialement collectées, le responsable du traitement doit démontrer l'existence d'un lien entre les deux finalités du traitement et tenir compte des «attentes légitimes» des personnes concernées ([94]). En cas de traitement pour d'autres finalités compatibles, les principes et obligations de la LGPD s'appliquent, à savoir veiller à ce que la nouvelle finalité soit spécifique et garantir la protection des droits des personnes concernées. Cela s'applique également au traitement ultérieur de données rendues «manifestement publiques» par la personne concernée ou qui sont accessibles au public ([95]).

2.4.6. *Exactitude et minimisation des données*

(61) Les données à caractère personnel doivent être exactes et, si nécessaire, tenues à jour. Elles doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

(62) Ces principes sont garantis par les principes de «qualité des données» et de «nécessité» de l'article 6, points III et V, de la LGPD, respectivement. Conformément à l'article 6, point V, de la LGPD, le responsable du traitement et les sous-traitants veillent à ce que les données à caractère personnel soient exactes, claires, pertinentes et à jour eu égard aux finalités pour lesquelles ces données sont traitées. L'article 6, point III, de la LGPD établit la «limitation du traitement au minimum nécessaire» pour atteindre une ou plusieurs finalités spécifiques, «couvrant les données qui sont pertinentes, proportionnées et non excessives» par rapport à cette ou ces finalités. Ces principes sont semblables à ceux énoncés à l'article 5, paragraphe 1, points c) et d), du règlement (UE) 2016/679.

2.4.7. *Limitation de la conservation*

(63) Les données ne doivent en principe pas être conservées plus longtemps que nécessaire pour atteindre les finalités pour lesquelles les données à caractère personnel sont traitées.

(64) Les principes de «finalité», de «nécessité» et d'«accès» énoncés, respectivement, à l'article 6, points I, III et IV, de la LGPD prévoient des exigences en matière de limitation de la conservation. Celles-ci limitent la possibilité de conserver des données au minimum nécessaire au regard d'une finalité «légitime, spécifique et explicite» et exigent que les personnes concernées soient informées de la durée de conservation.

([94]) ANPD, Guide des intérêts légitimes, p. 26 et annexe 2.

([95]) Article 7, paragraphe 7, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données. Voir également le considérant 48 de la présente décision. La notion de données «manifestement publiques» figure également dans le règlement (UE) 2016/679, tandis que les données «accessibles au public» renvoient aux informations disponibles dans les registres ou bases de données publics en vertu du droit brésilien conformément à la loi n° 12.527 du 18 novembre 2011, loi sur l'accès à l'information. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

(65) En outre, le chapitre II, section IV, de la LGPD est consacré à la «cessation du traitement des données». En vertu de cette section, l'article 16 de la LGPD exige que toutes les données à caractère personnel soient supprimées à la suite de la cessation du traitement pour une finalité définie. Ces exigences, lues en combinaison avec les principes de «finalité», de «nécessité» et d'«accès» de la LGPD, sont analogues aux obligations découlant de l'article 5, paragraphe 1, point e), du règlement (UE) 2016/679.

(66) En vertu des exceptions strictes prévues à l'article 16 de la LGPD, les données peuvent être conservées et stockées: 1) pour le respect des obligations légales ou réglementaires, 2) à des fins de recherche, en garantissant, dans la mesure du possible, l'anonymisation des données, 3) lorsqu'elles sont transférées à des tiers conformément aux exigences de la LGPD, ou 4) lorsqu'elles sont utilisées exclusivement par le responsable du traitement, pour autant que les données soient anonymisées et que l'accès à ces données par des tiers soit interdit.

(67) Les exigences en matière de sécurité des données énoncées dans la LGPD et décrites aux considérants 68 à 78 de la présente décision s'appliquent aux données conservées.

2.4.8. *Sécurité des données*

(68) Les données à caractère personnel devraient être traitées d'une manière garantissant leur sécurité, y compris leur protection contre tout traitement non autorisé ou illicite et contre toute perte, toute destruction ou tout dégât d'origine accidentelle. À cette fin, les opérateurs devraient prendre les mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre d'éventuelles menaces. Ces mesures devraient être appréciées en fonction de l'état des connaissances et des coûts correspondants.

(69) Ce principe est garanti par l'article 6, point VII, de la LGPD, qui impose l'utilisation de «mesures techniques et administratives» pour protéger les données à caractère personnel contre «les accès non autorisés et le traitement accidentel ou illicite», y compris «la destruction, la perte, l'altération, la communication ou la diffusion» des données. Afin de réduire ces risques pour la sécurité, l'article 6, point VIII, de la LGPD impose l'adoption de mesures visant à «prévenir la survenance de dommages/préjudices dus au traitement de données à caractère personnel».

(70) L'article 44 de la LGPD dispose que le traitement de données à caractère personnel est illicite lorsqu'il ne respecte pas les normes de sécurité qu'une personne concernée est en droit d'attendre. Le niveau de sécurité approprié doit être déterminé, entre autres: 1) compte tenu des circonstances particulières entourant le traitement effectué, 2) le niveau raisonnable de risque attendu, et 3) les techniques de traitement disponibles au moment où il a été réalisé ([96]).

(71) Afin de mettre en œuvre le principe de sécurité des données, la LGPD a énoncé une série d'exigences au chapitre VII, section I, «Sécurité et confidentialité des données». En vertu de cette section, l'article 46 de la LGPD impose aux responsables du traitement et aux sous-traitants d'adopter «des mesures de sécurité, techniques et administratives permettant de protéger les données à caractère personnel contre les accès non autorisés et les traitements accidentels ou illicites», tels que «la destruction, la perte, l'altération, la communication ou tout type de traitement inapproprié ou illicite». Ces mesures doivent être respectées «depuis la phase de conception du produit ou du service jusqu'à son exécution» ([97]). L'article 47 de la LGPD impose à toutes les parties concernées par toute phase du traitement une obligation générale de respecter les exigences de sécurité. Ces obligations sont semblables à celles prévues à l'article 32 du règlement (UE) 2016/679.

(72) L'article 44 de la LGPD dispose en outre que le responsable du traitement ou le sous-traitant qui omet d'adopter des mesures de sécurité est tenu pour responsable des dommages causés en cas de violation de la sécurité ([98]). L'ANPD peut également établir des normes techniques minimales de sécurité afin de garantir le respect des obligations en matière de sécurité des données ([99]).

([96]) Article 44, points I à III, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([97]) Article 46, paragraphe 2, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([98]) Article 44, paragraphe unique, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([99]) Article 46, paragraphe 1, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

(73) Conformément à l'article 48 de la LGPD, en cas d'incident de sécurité susceptible de présenter un risque ou de causer un préjudice important aux personnes concernées, le responsable du traitement est tenu d'en informer l'ANPD et les personnes concernées. Cette notification doit avoir lieu dans un délai raisonnable, tel que déterminé par l'ANPD, et doit comprendre, au minimum: 1) une description de la nature des données à caractère personnel concernées, 2) des informations permettant d'identifier les personnes concernées touchées, 3) une indication des mesures techniques et de sécurité mises en œuvre pour protéger les données, sous réserve de la préservation du secret commercial et industriel, 4) une évaluation des risques associés à l'incident, 5) une explication de tout retard éventuel de communication, et 6) une description des mesures prises ou à prendre pour atténuer ou réparer le dommage causé. L'approche suivie dans la LGPD est largement semblable à celle établie par les articles 33 et 34 du règlement (UE) 2016/679.

(74) L'ANPD a adopté des règles supplémentaires sur les incidents liés à la sécurité des données afin de clarifier, par exemple, la définition d'un «incident» et le délai de notification d'un incident ([100]).

(75) L'article 3, point XII, du règlement sur la notification des incidents de sécurité définit un incident de sécurité comme «tout événement indésirable confirmé lié à la violation de la confidentialité, de l'intégrité, de la disponibilité et de l'authenticité de la sécurité des données à caractère personnel». Conformément à l'article 48 de la LGPD, une violation de données et un incident de sécurité susceptible de créer des risques pour les personnes concernées doivent toujours être communiqués à l'autorité chargée de la protection des données (ANPD) et aux personnes concernées. L'article 5 du règlement sur la notification des incidents de sécurité précise qu'un incident de sécurité peut entraîner un risque pour les personnes concernées lorsqu'il est susceptible d'affecter leurs intérêts et leurs droits fondamentaux et s'il porte sur au moins un des types de données suivants: 1) données à caractère personnel sensibles, 2) données relatives aux enfants, aux adolescents ou aux personnes âgées, 3) données financières, 4) données d'authentification dans les systèmes, 5) données protégées par le secret juridique, judiciaire ou professionnel, ou 6) bases de données à grande échelle. En outre, un incident de sécurité sera considéré comme affectant de manière significative les intérêts et droits fondamentaux des personnes concernées lorsque: 1) il peut empêcher l'exercice de droits ou l'utilisation d'un service, ou 2) il peut causer des dommages matériels ou moraux aux personnes concernées, tels qu'une discrimination, une violation de l'intégrité physique, du droit à l'image et de la réputation, une fraude financière ou une usurpation d'identité ([101]).

(76) La notification d'un incident de sécurité à l'ANPD et aux personnes concernées a lieu dans un délai de trois jours ouvrables à compter du moment où le responsable du traitement en prend connaissance ([102]). Le règlement contraignant sur la notification des incidents de sécurité précise aux responsables du traitement les informations qui doivent être fournies à l'ANPD et aux personnes concernées. La notification adressée aux personnes concernées comprend notamment: 1) une description de la nature et de la catégorie des données à caractère personnel concernées, 2) les mesures techniques et de sécurité utilisées pour protéger les données, 3) les risques liés à l'incident, en identifiant les incidences possibles sur les personnes concernées, 4) les raisons du retard, dans le cas où la communication n'a pas été effectuée dans les 72 heures, 5) les mesures qui ont été ou seront adoptées pour inverser ou atténuer les effets de l'incident, le cas échéant, 6) la date à laquelle l'incident de sécurité a été découvert, et 7) les coordonnées permettant d'obtenir des informations et, le cas échéant, les coordonnées de la personne responsable ([103]). Lorsqu'ils communiquent l'incident aux personnes concernées, les responsables du traitement utilisent un «langage simple et facile à comprendre» ([104]). La notification est effectuée directement et individuellement, s'il est possible d'identifier les personnes concernées ([105]).

(77) En outre, l'ANPD peut, lorsque cela est nécessaire pour préserver les droits des personnes concernées, évaluer la gravité de l'incident et enjoindre au responsable du traitement d'adopter des mesures spécifiques ([106]). Il peut s'agir notamment de la divulgation publique de l'incident par les canaux médiatiques appropriés, ainsi que de la mise en œuvre de mesures correctives ou d'atténuation. Le responsable du traitement tient un registre des incidents de sécurité des données ([107]).

([100]) ANPD, règlement sur la notification des incidents de sécurité, avril 2024. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.
([101]) Article 5, paragraphe 1, ANPD, règlement sur la notification des incidents de sécurité, avril 2024.
([102]) Articles 6 et 9, ANPD, règlement sur la notification des incidents de sécurité, avril 2024.
([103]) Article 9, points I à VII, ANPD, règlement sur la notification des incidents de sécurité, avril 2024.
([104]) Article 9, paragraphe 1, point I, ANPD, règlement sur la notification des incidents de sécurité, avril 2024.
([105]) Article 9, paragraphe 1, point II, ANPD, règlement sur la notification des incidents de sécurité, avril 2024.
([106]) Article 48, paragraphe 2, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([107]) Article 10, ANPD, règlement sur la notification des incidents de sécurité, avril 2024.

(78) Enfin, la LGPD établit un lien entre ses normes de «bonnes pratiques et de gouvernance (des données)» et les exigences en matière de sécurité des données, afin, entre autres, d'atténuer les risques liés au traitement des données ([108]). Il s'agit notamment de promouvoir l'adoption de programmes internes de gouvernance en matière de protection de la vie privée afin d'évaluer et d'atténuer les risques ([109]).

2.4.9. *Transparence*

(79) Il convient d'informer les personnes concernées des principales caractéristiques du traitement des données à caractère personnel les concernant.

(80) Suivant une approche comparable à celle de l'article 12 du règlement (UE) 2016/679, l'article 6, point VI, de la LGPD dispose que les personnes concernées reçoivent des informations claires, précises et facilement accessibles sur la réalisation du traitement de leurs données et sur les agents de traitement respectifs, sous réserve du «secret commercial et industriel».

(81) L'article 9 de la LGPD établit une liste d'informations devant être fournies aux personnes concernées en ce qui concerne le traitement des données, qui couvre: 1) les finalités du traitement, 2) le type et la durée du traitement, 3) l'identification du responsable du traitement, 4) les coordonnées du responsable du traitement, 5) des informations concernant le traitement des données par le responsable du traitement et la finalité, 6) les responsabilités des entités procédant au traitement et 7) les droits des personnes concernées, y compris des informations concernant l'exercice de ces droits.

(82) La limitation relative au «secret commercial et industriel» visée à l'article 6, point VI, et à d'autres dispositions de la LGPD devrait être interprétée à la lumière de la loi brésilienne sur l'accès à l'information (LAI) ([110]). La LAI érige en règle la divulgation d'informations contenues dans des registres ou des documents détenus par des organismes publics ([111]). Toute exception, c'est-à-dire l'imposition de restrictions à l'accès aux documents et aux informations, doit être justifiée et prévue par la loi ([112]). Le secret commercial et industriel est l'une de ces exceptions, avec une disposition légale spécifique visant à assurer la protection des «informations relatives aux activités commerciales des personnes physiques ou morales de droit privé obtenues par d'autres organismes ou entités dans l'exercice de l'activité de contrôle, de réglementation et de surveillance de l'activité économique, dont la divulgation pourrait représenter un avantage concurrentiel pour d'autres agents économiques» ([113]). Les dispositions de la LGPD relatives au «secret commercial et industriel» doivent donc être interprétées de manière que le traitement et la divulgation d'informations ne révèlent pas de secret d'affaires ou ne créent pas d'avantage concurrentiel pour d'autres acteurs, tout en poursuivant les objectifs de protection des données à caractère personnel. Cela signifie qu'en ce qui concerne le principe de transparence, et tout au long du texte de la LGPD, la limitation relative au «secret commercial et industriel» ne doit pas être comprise comme un motif général de refus de respect de la loi, mais plutôt comme indiquant que des garanties spécifiques doivent être mises en place pour garantir la divulgation d'informations d'une manière qui protège ces intérêts.

2.4.10. *Droits individuels*

(83) Les personnes concernées devraient disposer de certains droits qu'elles peuvent opposer au responsable du traitement, en particulier le droit d'accéder aux données, le droit d'obtenir la rectification des données, le droit à l'effacement des données, le droit de s'opposer au traitement, le droit à la portabilité et des droits dans le cadre du traitement automatisé des données. De tels droits peuvent être soumis à des limitations, dans la mesure où celles-ci sont nécessaires et proportionnées pour garantir des objectifs spécifiques d'intérêt public.

([108]) Articles 49 et 50, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([109]) Article 50, paragraphe principal et paragraphe 1, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([110]) Loi n° 12.527 du 18 novembre 2011, loi sur l'accès à l'information. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

([111]) Articles 6 et 9, loi n° 12.527 du 18 novembre 2011, loi sur l'accès à l'information.

([112]) Article 22, loi n° 12.527 du 18 novembre 2011, loi sur l'accès à l'information.

([113]) Article 5, paragraphe 2, du décret n° 7.721 du 16 mai 2012, relatif à la loi n° 12.527 du 18 novembre 2011, loi sur l'accès à l'information.

(84) Le chapitre III de la LGPD établit les droits des personnes concernées de la même manière que le font les articles 15 à 22 du règlement (UE) 2016/679. L'exercice de tous les droits est gratuit et les personnes concernées doivent être informées de leurs droits ([114]). Conformément à l'article 21 de la LGPD, les données relatives à l'exercice de droits par une personne concernée ne peuvent pas être utilisées au détriment de celle-ci. Les personnes concernées peuvent former un recours en justice, individuellement ou collectivement, en ce qui concerne leurs intérêts et leurs droits ([115]).

(85) Les responsables du traitement informent «immédiatement» les sous-traitants avec lesquels les données ont pu être partagées des demandes de rectification, d'effacement, d'anonymisation, de limitation et d'objection formulées par les personnes concernées afin que toutes les parties concernées puissent donner suite à ces demandes ([116]).

(86) En vertu de l'article 9 et de l'article 18, point II, de la LGPD, les personnes concernées ont un droit d'information et d'accès afin d'obtenir «à tout moment» des informations concernant le traitement de leurs données ([117]). Cela comprend notamment: 1) l'identité du responsable du traitement (point III), 2) les coordonnées du responsable du traitement (point IV), 3) des informations sur la finalité spécifique du traitement (point I), 4) des informations sur un éventuel partage des données (point V), 5) le type et la durée du traitement (point II), 6) l'existence de droits des personnes concernées, y compris le droit d'introduire une réclamation auprès de l'autorité chargée de la protection des données, et 7) les responsabilités des sous-traitants. En outre, l'article 10, paragraphe 2, de la LGPD impose au responsable du traitement d'être transparent en ce qui concerne le traitement fondé sur l'intérêt légitime. De même, l'article 9 du règlement sur les transferts de données précise que les personnes concernées sont informées en cas de transfert de données à caractère personnel.

(87) L'article 19 de la LGPD précise plus en détail les modalités permettant aux personnes concernées d'accéder à leurs informations à caractère personnel. À la demande d'une personne concernée, l'accès aux données à caractère personnel est accordé: immédiatement, «dans un format simplifié», ou dans un délai de 15 jours, au moyen d'une déclaration claire et complète ([118]). En outre, l'article 19, paragraphe 1, de la LGPD dispose que les responsables du traitement conservent les données à caractère personnel dans un format qui facilite l'exercice du droit d'accès. La personne concernée peut décider de recevoir ses informations sous forme électronique ou au format papier ([119]).

(88) Les personnes concernées ont le droit de demander la rectification des données incomplètes, inexactes ou obsolètes, conformément à l'article 18, point III, de la LGPD (droit de rectification).

(89) L'article 18, points IV et VI, de la LGPD confère aux personnes physiques le droit de demander l'effacement de leurs données lorsque: 1) il s'agit de données inutiles ou excessives, 2) il s'agit de toute donnée traitée avec le consentement de la personne concernée, ou 3) les données font l'objet d'un traitement illicite. En outre, la section IV, chapitre II, de la LGPD sur la «Cessation du traitement des données» indique que le traitement des données s'arrête lorsqu'une personne concernée s'oppose au traitement ou retire son consentement au traitement ([120]). Par la suite, les données sont effacées après la fin du traitement ([121]). Ces dispositions, lues conjointement, élargissent donc indirectement le champ d'application du droit à l'effacement prévu par la LGPD.

([114]) Article 18, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([115]) Article 22, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([116]) Article 18, paragraphe 6, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([117]) Article 6, point VI, article 18 et article 19, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([118]) Article 19, points I et II, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([119]) Article 19, paragraphe 2, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([120]) Voir l'article 15, point III, de la loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), où la «communication par la personne concernée» fait référence, entre autres, à une révocation du consentement (comme indiqué dans l'article). La signification du terme «communication» ne se limite pas à ce scénario et permet aux personnes concernées de demander l'arrêt d'un traitement.

([121]) Article 16, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

(90) Les personnes physiques ont le droit de s'opposer au traitement des données fondé sur une base juridique autre que le consentement en cas de non-respect de la LGPD (droit d'opposition) ([122]). En outre, en vertu de l'article 15 et de l'article 18, point IV, de la LGPD, les personnes concernées ont le droit de limiter le traitement des données («verrouillage»). Ce droit peut être invoqué, en particulier, lorsque les données traitées sont inutiles ou excessives, ou lorsque les données sont traitées d'une manière non conforme à la LGPD ([123]). L'article 15, point II, de la LGPD dispose que les données ne sont plus traitées sur la base d'une «communication» adressée par la personne concernée au responsable du traitement. Bien que cette disposition soit soumise à la notion d'«intérêt général», interprétée au sens large, elle prévoit un large champ d'application pour un droit d'opposition indirect d'une manière équivalente au droit d'opposition prévu par le règlement (UE) 2016/679.

(91) Les personnes physiques ont le droit de demander «une copie électronique complète» de leurs données afin de permettre leur utilisation par d'autres entités (droit à la portabilité) ([124]). De même, comme dans l'UE, les personnes concernées ne peuvent demander cette copie que lorsque les données ont été traitées sur la base d'un consentement ou d'un contrat.

(92) Bien que toute décision fondée sur un traitement automatisé de données collectées dans l'UE soit généralement prise par un responsable du traitement [qui a une relation directe avec la personne concernée et relève donc directement du champ d'application du règlement (UE) 2016/679], il convient de noter que la LGPD régit ce type de traitement d'une manière semblable à celle de l'article 22 du règlement (UE) 2016/679. Premièrement, l'article 6, point IX, de la LGPD reconnaît le principe de non-discrimination comme un principe de protection des données selon lequel il est interdit de procéder à un traitement de données à des fins discriminatoires illicites ou abusives. Ce principe s'applique à tous les traitements et est particulièrement pertinent dans le contexte du traitement automatisé. Ensuite, conformément à l'article 20 de la LGPD, les personnes concernées ont le droit de demander le «réexamen des décisions prises sur la seule base d'un traitement automatisé de données affectant leurs intérêts, y compris les décisions visant à définir leur profil personnel, professionnel, de consommateur et de crédit, ou certains aspects de leur personnalité». Lorsqu'il répond à une demande d'une personne concernée, le responsable du traitement doit fournir des informations claires sur «les critères et la procédure utilisés pour la décision automatisée» ([125]). Si ces informations ne peuvent pas être fournies à la personne concernée pour des raisons de «secret commercial et industriel», l'ANPD a le pouvoir de procéder à un audit afin de vérifier les aspects discriminatoires du traitement automatisé des données à caractère personnel ([126]). Par conséquent, le «secret commercial et industriel» ne saurait être invoqué pour refuser de répondre à la demande de la personne concernée.

(93) L'article 23 de la LGPD dispose que des actes législatifs spécifiques s'appliquent à la procédure et au délai d'exercice des droits des personnes concernées lorsque la demande est traitée par les autorités publiques ([127]). Par exemple, la loi brésilienne «*Habeas Data*» réglemente le droit d'accès des personnes physiques aux informations relatives aux données détenues dans les registres ou bases de données du gouvernement ou d'une entité publique ([128]). La loi brésilienne *Habeas Data* établit des dispositions spécifiques pour le droit d'accès, qui est accordé dans un délai de 10 jours à compter de la demande d'une personne, et le droit de rectification, qui est accordé dans un délai de 15 jours à compter de la demande ([129]). De même, la loi brésilienne sur la procédure administrative fédérale établit un droit à l'information et à l'accès des particuliers dans le cadre des procédures administratives ([130]). La loi brésilienne sur l'accès à l'information prévoit également des obligations d'information et de transparence pour les

([122]) Article 18, paragraphe 2, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([123]) Article 18, point IV, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([124]) Article 19, paragraphe 3, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([125]) Article 20, paragraphe 1, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([126]) Article 20, paragraphe 2, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([127]) Article 23, paragraphe 3, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([128]) Loi n° 9.507 du 12 novembre 1997, loi brésilienne Habeas Data. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/l9507.htm.

([129]) Articles 7 et 8, loi n° 9.507 du 12 novembre 1997, loi brésilienne Habeas Data. La loi prévoit des voies de recours en cas de non-respect des demandes des particuliers.

([130]) Voir, en particulier, article 6, loi n° 9.784 du 29 janvier 1999, loi fédérale sur la procédure administrative. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/l9784.htm. La loi établit les procédures et les délais pour les communications avec les personnes concernées, ainsi que des voies de recours en cas de non-respect.

autorités publiques, les entreprises publiques et les trois branches du gouvernement brésilien (législatif, exécutif et judiciaire) ([131]). Les dispositions de ces lois renforcent le droit d'accès et d'information établi par la LGPD concernant le traitement des données par les autorités publiques. Lorsque ces actes législatifs ne prévoient pas des droits spécifiques établis en vertu de la LGPD (par exemple, les droits liés à la prise de décision automatisée), les personnes concernées peuvent exercer ces droits par l'intermédiaire de la LGPD.

(94) Toute violation des droits des personnes concernées sera traitée par l'ANPD comme une violation «moyenne» ou «grave» de la loi, en fonction du facteur pertinent, et pourra donc être frappée du niveau de sanctions et d'amendes le plus élevé. Il est important de noter que, sur la base du règlement de l'ANPD relatif aux sanctions, le simple fait qu'un droit de la personne concernée ait été affecté par une violation signifie qu'une telle violation ne saurait être considérée comme «légère» ([132]).

(95) Depuis l'entrée en application de la LGPD, l'ANPD a reçu un nombre stable de plaintes et de demandes de la part de particuliers concernant leurs droits en matière de protection des données ([133]). Ces chiffres ont considérablement augmenté depuis juillet 2024, avec l'introduction par l'ANPD d'une plateforme modernisée et facile à utiliser pour la soumission de demandes et de plaintes ([134]). Chaque mois depuis, l'ANPD reçoit environ 400 plaintes et 100 demandes adressées par des particuliers ([135]).

2.4.11. *Transferts ultérieurs*

(96) Le niveau de protection conféré aux données à caractère personnel qui sont transférées depuis l'Union vers des responsables du traitement et des sous-traitants au Brésil ne doit pas être compromis par le transfert ultérieur de ces mêmes données vers des destinataires se trouvant dans un pays tiers.

(97) De tels «transferts ultérieurs» constituent des transferts à partir du Brésil du point de vue du responsable du traitement brésilien.

(98) Le chapitre V de la LGPD établit un cadre pour les transferts internationaux de données à caractère personnel. Les dispositions de ce chapitre sont en outre complétées par un règlement contraignant sur les transferts internationaux de données (règlement sur le transfert de données) qui a été adopté par l'ANPD en août 2024 ([136]).

(99) Le règlement sur le transfert de données définit un «transfert» comme «une opération de traitement par laquelle un agent chargé du traitement transmet, partage ou donne accès à des données à caractère personnel à un autre agent de traitement» et un «transfert international de données» comme un «transfert de données à caractère personnel vers un pays étranger ou vers une organisation internationale dont le pays est membre» ([137]).

([131]) Article 1er, articles 6 et 9, loi nº 12.527 du 18 novembre 2011, loi sur l'accès à l'information.

([132]) Article 8, paragraphe 2, ANPD, règlement relatif au calcul et à l'application des sanctions administratives, février 2023 (ci-après le «règlement relatif aux sanctions»). Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-4-de-24-de-fevereiro-de-2023-466146077.

([133]) ANPD, Rapport sur la quatrième année de l'ANPD, novembre 2023, p. 24-25. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/balanco-de-4-anos-anpd-2024.pdf/view.

([134]) ANPD, Plateforme pour les particuliers. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados.

([135]) ANPD, Rapport sur la quatrième année de l'ANPD, novembre 2023, p. 25.

([136]) ANPD, règlement sur les transferts internationaux de données, août 2024. Disponible en portugais à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-19-de-23-de-agosto-de-2024-580095396 et en anglais à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/regulation-on-international-transfer-of-personal-data.pdf.

([137]) Article 3, points III et IV, ANPD, règlement sur les transferts internationaux de données, août 2024, ainsi que l'article 5, point XV, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

(100) Les règles relatives aux transferts internationaux établies en vertu de la LGPD et du règlement sur le transfert de données s'appliquent à tous les traitements relevant du champ d'application de la LGPD. L'article 7 du règlement sur le transfert de données précise expressément que l'applicabilité de la LGPD à un transfert international de données ne dépend pas des moyens techniques utilisés pour le traitement, de la localisation géographique des données ou de la présence physique du responsable du traitement ou du sous-traitant ([138]). Au contraire, ce qui détermine l'applicabilité, c'est l'existence d'un lien substantiel entre l'activité de traitement des données et le Brésil.

(101) À l'instar des articles 44 à 49 du règlement (UE) 2016/679, l'article 33 de la LGPD établit les circonstances dans lesquelles un transfert international de données peut «uniquement» être autorisé. Ces circonstances sont décrites plus en détail à l'article 9 du règlement sur le transfert de données.

(102) Un transfert international de données peut avoir lieu si les trois circonstances cumulatives suivantes sont réunies: premièrement, un transfert international de données ne peut «être effectué que pour des finalités légitimes, spécifiques et explicites indiquées à la personne concernée, sans possibilité de traitement ultérieur incompatible avec cette finalité» ([139]). Deuxièmement, le transfert international de données doit se fonder sur une base juridique valable énoncée à l'article 7 de la LGPD (ou à l'article 11 dans le cas de données sensibles) ([140]). Troisièmement, un mécanisme de transfert de données «valide» doit être utilisé ([141]).

(103) L'article 33 de la LGPD prévoit plusieurs mécanismes de transfert de données.

(104) Premièrement, une décision d'adéquation peut être adoptée à l'égard d'un pays tiers ou d'une organisation internationale (article 33, point I). Pour déterminer si un pays tiers ou une organisation internationale garantit un niveau adéquat de protection des données à caractère personnel, l'ANPD tient compte de plusieurs critères définis dans la LGPD et le règlement sur le transfert de données ([142]), qui sont semblables à ceux correspondants en vertu du droit de l'Union. Cela inclut: 1) la législation générale et sectorielle en vigueur dans le pays de destination ou applicable à l'organisation internationale, qui a une incidence directe sur la protection des données à caractère personnel ([143]), 2) la nature des données ([144]), 3) veiller à ce que le pays tiers ou l'organisation internationale assure un niveau de protection des données à caractère personnel et garantisse les droits des personnes concernées d'une manière compatible avec la LGPD ([145]), 4) l'adoption de mesures techniques et organisationnelles appropriées pour garantir la sécurité des données et atténuer les risques d'incidences négatives sur la vie privée et d'autres droits fondamentaux ([146]), 5) l'existence de mécanismes judiciaires et institutionnels pour garantir les droits en matière de protection des données, notamment par l'existence d'une autorité de contrôle indépendante dotée de pouvoirs et de ressources suffisants pour contrôler et faire respecter les dispositions en matière de protection des données ([147]), et 6) toute autre circonstance spécifique pertinente pour le contexte du transfert international de données ([148]).

([138]) Article 7, ANPD, règlement sur les transferts internationaux de données, août 2024.
([139]) Article 9, ANPD, règlement sur les transferts internationaux de données, août 2024.
([140]) Article 9, point I, ANPD, règlement sur les transferts internationaux de données, août 2024.
([141]) Article 9, point II, ANPD, règlement sur les transferts internationaux de données, août 2024.
([142]) Article 34, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) et chapitre V, ANPD, règlement sur les transferts internationaux de données, août 2024.
([143]) Article 34, point I, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) et article 11, point I, ANPD, règlement sur les transferts internationaux de données, août 2024.
([144]) Article 34, point II, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) et article 11, point II, ANPD, règlement sur les transferts internationaux de données, août 2024.
([145]) Article 34, point III, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) et article 11, point III, ANPD, règlement sur les transferts internationaux de données, août 2024.
([146]) Article 34, point IV, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) et article 11, point IV, ANPD, règlement sur les transferts internationaux de données, août 2024.
([147]) Article 11, paragraphe 3, ANPD, règlement sur les transferts internationaux de données, août 2024.
([148]) Article 34, point VI, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) et article 11, point VI, ANPD, règlement sur les transferts internationaux de données, août 2024.

(105) Aux fins de l'évaluation du niveau de protection des données à caractère personnel dans le cadre d'une décision d'adéquation, l'ANPD s'intéressera également: 1) aux risques et avantages découlant d'une décision d'adéquation spécifique, compte tenu, entre autres, de la garantie des principes, des droits de la personne concernée et du régime de protection des données prévu pour la LGPD, ainsi que 2) aux incidences de la décision sur le flux international de données, les relations diplomatiques, le commerce international et la coopération internationale du Brésil avec d'autres pays et organisations internationales ([149]). L'évaluation et l'adoption d'une décision d'adéquation relèvent de la responsabilité de l'ANPD ([150]). À l'heure actuelle, l'ANPD travaille uniquement sur une décision d'adéquation avec l'Union européenne.

(106) Deuxièmement, l'article 33, point II, dispose que les transferts de données peuvent avoir lieu lorsque les responsables du traitement assurent «les garanties du respect des principes et des droits des personnes concernées et du régime de protection des données» prévus par la LGPD. Cela peut être garanti par 1) des clauses contractuelles spécifiques [point II, sous a)], 2) des clauses contractuelles types [point II, sous b)], 3) des règles d'entreprise contraignantes [point II, sous c)], ou 4) des labels, des certificats et des codes de conduite approuvés [point II, sous d)].

(107) Les responsables du traitement peuvent s'appuyer sur des dispositions contractuelles spécifiques pour les transferts internationaux ainsi que sur des clauses contractuelles types approuvées par l'ANPD ([151]). En vertu du règlement sur les transferts de données, l'ANPD a adopté un ensemble de clauses contractuelles types qui couvrent toutes les exigences pertinentes en matière de protection des données (c'est-à-dire les droits des personnes concernées, le contrôle et la surveillance indépendants, les mesures de sécurité des données, les garanties relatives aux transferts ultérieurs, etc.) ([152]). Ces clauses comprennent des dispositions qui ne peuvent pas être modifiées par les parties au contrat ([153]). Les clauses sont modulaires pour s'adapter aux différents scénarios de transfert de données (par exemple, de responsable du traitement à sous-traitant, de sous-traitant à sous-traitant) ([154]).

(108) En ce qui concerne les règles d'entreprise contraignantes (REC), l'ANPD précise, au chapitre VI du règlement sur le transfert de données, la manière dont ce mécanisme peut être utilisé, ainsi que les exigences relatives à leur validité. L'ANPD rappelle, en particulier, la «nature contraignante» de l'instrument pour tous les «membres du groupe ou conglomérat» qui s'en prévalent, les exigences relatives aux droits des personnes concernées et leur exercice, le régime de responsabilité applicable ([155]), ainsi que toutes les informations obligatoires que des REC doivent inclure ([156]). Les REC sont soumises à l'approbation préalable de l'ANPD conformément à un processus défini au chapitre VIII du règlement sur le transfert de données, qui impose aux entreprises de soumettre une documentation complète à l'ANPD et implique un processus d'examen de l'ANPD ([157]). Les entreprises sont également tenues de communiquer à l'ANPD tout problème susceptible d'avoir une incidence sur le respect de la LGPD, y compris lorsque les membres du groupe sont soumis à des obligations étrangères ([158]). Toutes les REC approuvées seront publiées sur la page web de l'ANPD, et les entreprises ont l'obligation de fournir des informations transparentes sur le transfert international effectué ([159]).

([149]) Article 12, ANPD, règlement sur les transferts internationaux de données, août 2024.

([150]) La procédure de délivrance d'une décision d'adéquation est décrite à la section III du règlement sur les transferts internationaux de données, août 2024.

([151]) Article 35, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([152]) Annexe II, ANPD, règlement sur les transferts internationaux de données, août 2024.

([153]) Annexe II, section II, ANPD, règlement sur les transferts internationaux de données, août 2024.

([154]) Annexe II, clause 4, ANPD, règlement sur les transferts internationaux de données, août 2024. Les responsables du traitement et les sous-traitants peuvent choisir l'«option» appropriée correspondant à leur situation en vertu de cette clause.

([155]) Article 3, point VIII, ANPD, règlement sur les transferts internationaux de données, août 2024. La définition de l'«entité responsable» établit qu'une «entreprise ayant son siège au Brésil est responsable de toute violation d'une règle d'entreprise contraignante, même si elle résulte d'un acte d'un membre du groupe économique ayant son siège dans un autre pays», suivant une approche similaire à celle de l'article 47, paragraphe 1, point f), du règlement (UE) 2016/679.

([156]) Article 27, ANPD, règlement sur les transferts internationaux de données, août 2024.

([157]) Articles 27 et 28 et chapitre VIII, ANPD, règlement sur les transferts internationaux de données, août 2024.

([158]) Article 25, point VIII, ANPD, règlement sur les transferts internationaux de données, août 2024.

([159]) Article 32, ANPD, règlement sur les transferts internationaux de données, août 2024. Cet article indique en outre que les entreprises ont l'obligation de mettre les REC à la disposition des personnes concernées sur demande.

(109) L'ANPD peut également désigner des entités de certification pour élaborer des labels, des certifications ou des codes de conduite pour les transferts de données ([160]). Les décisions et les activités menées par les entités de ces certifications peuvent être contrôlées par l'ANPD, qui peut réexaminer et révoquer les décisions en cas de non-respect de la LGPD ([161]).

(110) Enfin, la LGPD fournit une liste de «situations spécifiques» dans lesquelles un transfert international peut être effectué quand: 1) il est nécessaire à la coopération juridique internationale entre des organismes publics, conformément au droit international, 2) il est nécessaire à la protection de la vie ou de la sécurité physique de la personne concernée ou d'un tiers, 3) il est autorisé par l'ANPD, 4) il est lié à un engagement dans le cadre de la coopération internationale, 5) il est nécessaire à l'exécution d'une politique ou d'une obligation légale d'une autorité publique, 6) les personnes concernées ont consenti au transfert spécifique de données, après avoir reçu des informations préalables sur la nature du traitement, ou 7) il est nécessaire au respect d'une obligation légale ou réglementaire, liée à la fourniture d'un contrat, ou à l'exercice de droits dans le cadre de procédures judiciaires, administratives ou d'arbitrage ([162]). Comme l'indique le règlement sur le transfert de données, les transferts internationaux ne peuvent être effectués dans le cadre de ces scénarios que si «les particularités du cas d'espèce et les exigences légales applicables sont respectées» ([163]).

(111) En ce qui concerne la situation spécifique dans laquelle le transfert de données peut être effectué sur la base du consentement des personnes concernées, il est exigé 1) que les critères formels pour obtenir un consentement valable soient remplis (c'est-à-dire qu'ils soient spécifiques, donnés librement, explicites et informés); 2) que les personnes concernées soient informées de la nature du transfert *avant* qu'il ne soit effectué (par exemple, qu'elles reçoivent des informations sur la juridiction compétente pour le transfert envisagé et sur le niveau de protection assuré; des informations sur l'absence de décision d'adéquation ou d'autres mécanismes de transfert de données; des informations sur la durée des transferts); et 3) que le consentement soit obtenu pour chaque transfert spécifiquement et séparément de tout autre traitement. Comme indiqué au considérant 46, un accord tacite ne peut être considéré comme un consentement valable et les personnes concernées ont le droit de retirer leur consentement à tout moment.

(112) Le règlement sur le transfert de données encadre strictement l'utilisation de tous ces mécanismes sur la base de plusieurs conditions. Il s'agit notamment de fournir des «informations claires, exactes et facilement accessibles sur le transfert» à la personne concernée, ainsi que de garantir et de pouvoir démontrer que les transferts internationaux sont effectués de manière à garantir le respect des principes et des droits de la personne concernée, et qu'ils ne modifient pas le niveau de protection prévu par la LGPD, «quel que soit le pays où se trouvent les données à caractère personnel faisant l'objet du transfert, même après la fin du traitement et en cas de transferts ultérieurs» ([164]). Ces exigences s'appliquent également aux transferts effectués sur la base de «situations spécifiques», afin d'assurer la continuité de la protection indépendamment de l'instrument utilisé pour effectuer un transfert international.

(113) Les règles mentionnées aux considérants 96 à 112 de la présente décision assurent donc la continuité de la protection lorsque les données à caractère personnel font l'objet d'un transfert ultérieur depuis le Brésil d'une manière essentiellement équivalente à celle prévue par le règlement (UE) 2016/679.

2.4.12. *Responsabilité*

(114) Selon le principe de responsabilité, les entités traitant des données sont tenues de mettre en place les mesures techniques et organisationnelles appropriées pour s'acquitter effectivement de leurs obligations en matière de protection des données et doivent être en mesure de démontrer le respect de ces obligations, en particulier à l'autorité de contrôle compétente.

([160]) Article 35, paragraphe 3, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([161]) Article 35, paragraphe 4, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([162]) Article 33, points III à IX, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([163]) Article 1er (paragraphe unique), ANPD, règlement sur les transferts internationaux de données, août 2024.

([164]) Article 2, points III et IV, et article 4, ANPD, règlement sur les transferts internationaux de données, août 2024. Comme tous les transferts internationaux, tout transfert effectué dans le cadre de ces scénarios doit avoir «des finalités légitimes, spécifiques et explicites, communiquées à la personne concernée, sans possibilité de traitement ultérieur incompatible avec ces finalités», comme le prévoit l'article 9, paragraphe principal, ANPD, règlement sur les transferts internationaux de données, août 2024.

(115) L'article 6, point IX, de la LGPD établit le principe de responsabilité selon lequel le responsable du traitement et le sous-traitant adoptent des mesures «efficaces et à même» de démontrer la conformité à la LGPD.

(116) Afin de garantir la responsabilité, l'article 50 de la LGPD prévoit que les responsables du traitement et les sous-traitants peuvent adopter des règles internes et des modèles de gouvernance, en particulier pour garantir les bonnes pratiques en matière de traitement des plaintes et des demandes des personnes concernées, dans le respect des obligations en matière de sécurité et de toutes les autres obligations au titre de la LGPD («Bonnes pratiques et gouvernance»). Ces programmes devraient également comprendre des plans pour les activités éducatives, le mécanisme de supervision interne et l'atténuation des risques.

(117) La LGPD prévoit également l'obligation de désigner un délégué à la protection des données (DPD) qui joue un rôle important dans la conception et la mise en œuvre de ces programmes internes. Conformément à l'article 5, point VIII, le DPD joue le rôle de lien entre le responsable du traitement, les personnes concernées et l'ANPD. L'article 41 de la LGPD prévoit que tous les responsables du traitement désignent un DPD, dont l'identité est rendue publique.

(118) La LGPD a habilité l'ANPD à introduire une dérogation à l'obligation pour les responsables du traitement et les sous-traitants de désigner un DPD ([165]). Dans son règlement relatif à l'application de la LGPD aux petites et moyennes entreprises (PME), l'ANPD a établi que certaines petites entreprises, PME, jeunes pousses et organisations à but non lucratif peuvent bénéficier de cette dérogation ([166]). Plus précisément, le champ d'application de la dérogation couvre les entités suivantes: «microentreprises, petites entreprises, jeunes pousses, entités juridiques de droit privé, y compris les organisations à but non lucratif, conformément à la législation en vigueur, ainsi que les personnes physiques et les entités privées dépersonnalisées qui traitent des données à caractère personnel» ([167]). En vertu de la législation brésilienne, les microentreprises ([168]), les petites entreprises ([169]) ou les jeunes pousses ([170]) désignent les entreprises employant un seul ou peu de salariés ([171]) et dont le chiffre d'affaires annuel brut est inférieur à un certain seuil ([172]).

(119) La dérogation à l'obligation de désigner un DPD ne s'appliquerait à aucune de ces sociétés et entités, indépendamment de leur taille ou de leurs revenus, si elles effectuent un traitement «à haut risque» de données à caractère personnel ([173]). Un traitement sera considéré comme à haut risque si, cumulativement, il présente au moins une de ces caractéristiques générales: 1) traitement de données à caractère personnel à grande échelle, et 2) traitement de données susceptibles d'avoir une incidence significative sur les droits fondamentaux et les intérêts des personnes concernées, et au moins l'une de ces caractéristiques spécifiques: 1) utilisation de technologies émergentes ou innovantes, 2) surveillance ou contrôle des zones accessibles au public, 3) processus décisionnels exclusivement automatisés, et 4) le traitement de données sensibles ou de données appartenant à des enfants ou à des personnes âgées ([174]). Un traitement à «grande échelle» de données à caractère personnel est défini

([165]) Article 41, paragraphe 3, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([166]) ANPD, règlement relatif à l'application de la LGPD aux petites et moyennes entreprises (ci-après le «règlement sur les PME»), avril 2024. Disponible à l'adresse suivante: 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]) Article 2, point I, ANPD, règlement sur les PME, avril 2024.

([168]) Une «microentreprise» est définie comme une entreprise dont le chiffre d'affaires brut annuel est égal ou inférieur à 360 000 réaux brésiliens (R$). Voir article 3, point I, loi complémentaire n° 123 du 14 décembre 2006, loi sur le statut national des micro-, petites et moyennes entreprises. 360 000 R$ correspondent à 56 500 EUR.

([169]) Une «petite entreprise» ou «PME» est définie comme une entreprise dont le chiffre d'affaires brut annuel est compris entre 360 000 R$ et 4 800 000 R$. Voir article 3, point II, loi complémentaire n° 123 du 14 décembre 2006, loi sur le statut national des micro-, petites et moyennes entreprises. 4 800 000 R$ correspondent à 753 000 EUR.

([170]) Une «jeune pousse» est définie comme une «entreprise ou organisation d'entreprise, naissante ou récente, dont les activités se caractérisent par l'innovation appliquée au modèle d'entreprise ou aux produits ou services proposés». Voir article 2, point III, ANPD, règlement sur les PME, avril 2024.
Une jeune pousse ne peut être enregistrée en tant que telle que pour une durée maximale de 10 ans et avec un revenu brut annuel limité à 16 000 000 R$. Voir article 4, point I, loi complémentaire n° 182 du 1er juin 2021, loi sur les jeunes pousses. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp182.htm. 16 000 000 R$ correspondent à 2 500 000 EUR.

([171]) Voir, en particulier, article 2, point II, ANPD, règlement sur les PME, avril 2024, et article 41, loi n° 14.195 du 26 août 2021, loi sur l'ouverture des sociétés. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14195.htm.

([172]) Loi complémentaire n° 123 du 14 décembre 2006, loi sur le statut national des micro-, petites et moyennes entreprises. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm.

([173]) Article 4, ANPD, règlement sur les PME, avril 2024.

([174]) Article 4, points I et II, ANPD, règlement sur les PME, avril 2024.

comme un traitement qui «porte sur un nombre important de personnes concernées, compte tenu également du volume de données concernées, ainsi que de la durée, de la fréquence et de l'étendue géographique du traitement effectué» ([175]). Un «traitement de données susceptible d'avoir une incidence significative sur les droits et intérêts fondamentaux des personnes concernées» est défini «notamment, comme une situation dans laquelle l'activité de traitement peut entraver l'exercice de droits ou l'utilisation d'un service, ainsi que causer des dommages matériels ou moraux aux personnes concernées, tels que la discrimination, la violation de l'intégrité physique, le droit à l'image et à la réputation, la fraude financière ou l'usurpation d'identité» ([176]).

(120) L'ANPD a adopté un règlement contraignant sur le rôle du DPD, qui clarifie davantage ses obligations ([177]). Dans ce règlement, l'ANPD rappelle les obligations qui incombent aux entités privées et aux autorités publiques de publier des informations sur l'identité de leur DPD ([178]). L'article 10 du règlement DPD rappelle l'obligation, pour les responsables du traitement et les sous-traitants, de veiller, entre autres, à ce que le DPD puisse s'acquitter de ses tâches en toute indépendance, «protégé contre toute ingérence indue, en particulier lorsqu'il fournit des orientations sur les pratiques à adopter en matière de protection des données à caractère personnel» et à ce que le DPD ait un accès direct au plus haut niveau de l'encadrement supérieur et à tous les employés participant aux décisions stratégiques relatives au traitement des données au sein d'une entité. De même, le DPD s'acquitte de ses fonctions et de ses tâches avec «éthique, intégrité et indépendance technique, en évitant les situations susceptibles de constituer un conflit d'intérêts» ([179]).

(121) Le rôle du DPD a été une priorité de l'action répressive de l'ANPD. Par exemple, les premières sanctions prononcées par l'ANPD concernaient une entreprise qui s'est vu infliger une amende et a reçu un avertissement spécifique pour n'avoir pas été en mesure de démontrer qu'elle avait nommé un DPD ([180]). L'entité a décidé de désigner un DPD au cours de la procédure administrative pour se conformer à l'ordre de l'ANPD. Depuis lors, l'ANPD a continué d'infliger des sanctions à des entités publiques et privées en ce qui concerne les dispositions du DPD établies en vertu de la LGPD ([181]).

(122) L'analyse d'impact relative à la protection des données (AIPD) est un autre outil important pour garantir la responsabilité. L'AIPD permet d'évaluer et de déterminer l'incidence d'un traitement. Conformément à l'article 38 de la LGPD, l'ANPD peut demander à un responsable du traitement ou à un sous-traitant de réaliser une AIPD ([182]), qui doit comprendre une description du type de traitement des données à caractère personnel ainsi que des mesures, garanties et mécanismes visant à atténuer les risques. En outre, la section II de la LGPD établit des dispositions en matière de responsabilité qui autorisent l'ANPD à demander la publication d'une AIPD ou à recommander l'adoption de «bonnes pratiques» en matière de protection des données à caractère personnel par les autorités publiques ([183]).

(123) À la lumière des exigences et pratiques en matière de responsabilité décrites aux considérants 114 à 122 de la présente décision, le cadre brésilien met en œuvre le principe de responsabilité d'une manière semblable aux mesures prévues au chapitre 4, sections 3 et 4, du règlement (UE) 2016/679, y compris en prévoyant différents mécanismes pour garantir et démontrer la conformité à la LGPD.

2.5. **Surveillance et contrôle de l'application des règles**

(124) Pour garantir un niveau adéquat de protection des données dans la pratique, il convient de mettre en place une autorité de contrôle indépendante chargée de surveiller l'application des règles en matière de protection des données et de les faire respecter. Cette autorité devrait agir en toute indépendance et en toute impartialité dans l'exercice de ses fonctions et compétences.

([175]) Voir, par exemple, article 4, paragraphe 1, ANPD, règlement sur les PME, avril 2024.
([176]) Voir, par exemple, article 4, paragraphe 2, ANPD, règlement sur les PME, avril 2024.
([177]) ANPD, règlement relatif au rôle du DPD à l'égard du traitement des données à caractère personnel (ci-après le «règlement DPD»), juillet 2024. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074.
([178]) Articles 5 et 9, ANPD, règlement DPD, juillet 2024.
([179]) Article 18, ANPD, règlement DPD, juillet 2024.
([180]) Voir ANPD, Rapport d'instruction nº 1/2023 — Telekall Infoservice. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.
([181]) Voir, par exemple, ANPD, Rapport d'instruction nº 5/2024 — Ministério da Saúde. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.
([182]) Article 38, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.
([183]) Section II, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

2.5.1. *Surveillance indépendante*

(125) Au Brésil, l'autorité de contrôle indépendante chargée du contrôle et de l'application de la LGPD est l'Agência Nacional de Proteção de Dados — ANPD.

(126) L'ANPD a été créée par l'article 55-A de la LGPD et a été rendue indépendante au moyen, dans un premier temps, d'un décret provisoire, puis d'une loi en 2022 ([184]). L'adoption de la loi transformant la nature de l'ANPD a inclus des modifications apportées à la LGPD afin d'abroger les dispositions qui subordonnent le fonctionnement et les opérations financières de l'ANPD aux autorisations devant être accordées par l'exécutif en vertu de la loi budgétaire brésilienne ([185]). La disposition modifiée de la LGPD reconnaît que l'ANPD est une «autorité spéciale, disposant d'une autonomie technique et décisionnelle, dotée de ses propres actifs et ayant son siège dans le district fédéral» ([186]).

(127) En tant qu'«autorité à caractère spécial», l'ANPD dispose de l'autonomie nécessaire pour exercer pleinement ses fonctions et pouvoirs juridiques établis en vertu de la LGPD, y compris la gestion administrative de l'agence ([187]). Cela inclut l'autonomie dans la gestion de ses dépenses et de ses recrutements ([188]). Créée en tant qu'«autorité», l'ANPD est devenue une «agence» en septembre 2025, son nom étant ainsi aligné sur celui des 11 autres entités de régulation jouissant du même degré élevé d'indépendance au Brésil (par exemple, l'Agence nationale de l'électricité, l'Agence nationale des télécommunications, etc.) ([189]).

(128) Les ressources de l'ANPD proviennent en grande partie du budget général de l'État fédéral brésilien. En outre, le budget de l'ANPD peut inclure des dons, des subventions ou d'autres crédits conformément à l'article 55-L de la LGPD. Depuis sa création en 2021, l'ANPD connaît une croissance exponentielle. Les rapports annuels de l'ANPD indiquent que l'autorité comptait 141 employés/fonctionnaires à la fin de l'année 2023, après seulement quatre ans d'existence ([190]). Le budget annuel 2025 de l'ANPD s'élève à 18 millions de R$ ([191]). En septembre 2025, la création d'un nouveau parcours de carrière dans la fonction publique, relatif à la «protection des données», et doté de 200 postes, a été annoncée au Brésil, dans le cadre d'une augmentation, dans les années à venir, des effectifs de l'ANPD ([192]).

([184]) L'article 55-A de la loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), dans sa rédaction initiale, a été modifié par la loi nº 14.460 du 25 octobre 2022, loi transformant l'ANPD en autorité à statut spécial. En ce qui concerne l'indépendance, voir la mesure provisoire nº 1.124 du 13 juin 2022, transformant l'ANPD en une autorité à statut spécial. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Mpv/mpv1124.htm et la loi nº 14.460 du 25 octobre 2022, loi transformant l'ANPD en autorité à statut spécial. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14460.htm. La possibilité pour le gouvernement de modifier le statut de l'ANPD afin d'accroître son indépendance a été précisée dans l'article 55-A, paragraphe 1 (désormais abrogé), de la loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([185]) Voir l'article 9 de la loi nº 14.460 du 25 octobre 2022, loi transformant l'ANPD en autorité à statut spécial, abrogeant et remplaçant l'article 55-A de la loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([186]) Article 7, loi nº 14.460 du 25 octobre 2022, loi transformant l'ANPD en autorité à statut spécial.

([187]) Voir ANPD, L'ANPD devient une autorité à caractère spécial, juin 2022. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-torna-se-autarquia-de-natureza-especial.

([188]) Article 55-L, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([189]) Article 1er, Décret nº 1.317 du 17 septembre 2025 modifiant la LGPD afin de transformer l'Agência Nacional de Proteção de Dados. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314 et article 2, point XII, de la loi nº 13.848 du 25 juin 2019 relative à l'organisation des agences de régulation. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm.

([190]) ANPD, Rapport sur la quatrième année de l'ANPD, novembre 2023, p. 8. Disponible à l'adresse suivante: 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). Voir loi budgétaire annuelle, p. 190. Disponible à l'adresse suivante: LEI15121-VOLUME I.pdf.

([192]) Article 9, point I, Décret nº 1.317 du 17 septembre 2025 modifiant la LGPD afin de transformer l'Agência Nacional de Proteção de Dados. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

(129) L'ANPD est composée d'un conseil d'administration (qui est son organe directeur suprême), d'un Conseil national pour la protection des données à caractère personnel et de la vie privée (qui dispose de pouvoirs consultatifs) et de plusieurs unités et bureaux administratifs ([193]). Cette structure est établie à l'article 55-C de la LGPD et détaillée dans deux décrets adoptés respectivement en 2020 et 2023 ([194]).

(130) Le conseil d'administration se compose de cinq administrateurs, dont le président de l'Autorité. Chaque membre du conseil d'administration de l'ANPD est nommé pour cinq ans par le président de la République du Brésil, après approbation du Sénat fédéral ([195]).

(131) Les administrateurs sont brésiliens et possèdent un niveau d'éducation de haut niveau en rapport avec le poste ([196]). Afin de garantir leur indépendance, tous les administrateurs doivent notamment s'abstenir de toute activité commerciale ou politique lucrative et d'occuper des postes de direction ou de conseiller dans une société ([197]). En outre, la loi brésilienne réglementant l'exercice de hautes fonctions au sein de l'administration publique fédérale établit que les personnes exerçant des fonctions équivalentes à celles des directeurs de l'ANPD se voient interdire, entre autres restrictions, d'exercer des activités incompatibles avec leurs fonctions ([198]). Il s'agit notamment d'agir en tant que consultants ou intermédiaires d'intérêts privés (même de manière informelle) ou de fournir des services à des entités soumises à la surveillance ou à la réglementation de l'ANPD, même à titre occasionnel. En outre, à l'issue de leur mandat ou de leur poste à l'ANPD et pendant six mois à compter de cette date, les administrateurs ne peuvent pas exercer certaines fonctions susceptibles de créer un risque de conflit d'intérêts ([199]).

(132) Les administrateurs ne peuvent être révoqués que dans des circonstances spécifiques définies à l'article 55-E de la LGPD, à savoir «en cas de démission, de condamnation judiciaire définitive et non susceptible de recours ou de licenciement pour faute en raison d'une procédure administrative disciplinaire». La loi fédérale sur l'administration publique prévoit qu'une telle sanction doit être justifiée et ne peut être proposée qu'en cas d'infractions spécifiques avérées (faute grave, corruption, utilisation irrégulière de fonds publics) ([200]). Ces règles et procédures assurent aux administrateurs de l'ANPD une protection institutionnelle dans l'exercice de leurs fonctions. À ce jour, aucun administrateur de l'ANPD n'a jamais été révoqué ou n'a fait l'objet d'aucune procédure disciplinaire. Le conseil d'administration de l'ANPD était en place et est resté inchangé tout au long du changement d'administration au Brésil qui a eu lieu en 2023.

([193]) Article 55-C, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([194]) Décret nº 10.474 du 26 août 2020 relatif à la structure de l'ANPD. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10474.htm, modifié par le décret nº 11.758 du 30 octobre 2023 relatif à la structure modifiée de l'ANPD. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11758.htm#art1.

([195]) Article 55-D, paragraphes 1 et 3, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données et article 12, Décret nº 1.317 du 17 septembre 2025 modifiant la LGPD afin de transformer l'Agência Nacional de Proteção de Dados. Disponible à l'adresse suivante: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314. L'article 12 de ce décret étend la durée du mandat des directeurs de l'ANPD de quatre à cinq ans afin de l'aligner sur celui des directeurs de toutes les autres agences de régulation indépendantes du Brésil. Tous les directeurs de l'ANPD nommés avant l'adoption de ce' décret accompliront un mandat de quatre ans, comme le prévoyait initialement la loi au moment de leur nomination.

([196]) Article 55-D, paragraphe 2, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais, (LGPD) — loi générale sur la protection des données.

([197]) Article 11, décret nº 10.474 du 26 août 2020 relatif à la structure de l'ANPD.

([198]) Article 5, loi nº 12.813 du 16 mai 2013, loi sur les conflits d'intérêts pour les fonctionnaires et autres fonctions au sein des autorités publiques. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12813.htm.

([199]) Article 6, loi nº 12.813 du 16 mai 2013, loi sur les conflits d'intérêts pour les fonctionnaires et autres fonctions au sein des autorités publiques.

([200]) La liste exhaustive des infractions figure à l'article 132 de la loi nº 8112 du 11 décembre 1990, loi fédérale sur la fonction publique et les fonctionnaires. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm. Voir également le chapitre V de cette loi sur les conditions d'application d'une sanction.

(133) Les tâches et les pouvoirs de l'ANPD sont détaillés à l'article 55-J de la LGPD. Il s'agit notamment d'élaborer des politiques et des lignes directrices en matière de protection des données, de promouvoir l'adoption de normes facilitant le contrôle des personnes concernées sur leurs données à caractère personnel, d'enquêter sur les violations des droits individuels, de traiter les plaintes, de veiller au respect de la LGPD et d'infliger des sanctions, de garantir l'éducation et la promotion dans le domaine de la protection des données, ainsi que d'échanger et de coopérer avec les autorités des pays tiers chargées de la protection des données, entre autres ([201]).

(134) L'ANPD dispose d'un organe consultatif constitué par le Conseil national pour la protection des données à caractère personnel et de la vie privée, tel qu'établi par l'article 58-A de la LGPD. Cet organe est composé de représentants du pouvoir exécutif, législatif et judiciaire, ainsi que de représentants de la société civile, des syndicats et des entreprises ([202]). Il joue un rôle purement consultatif consistant à préparer des études ou des rapports annuels sur la protection des données, à organiser des débats publics et des auditions sur la protection des données à caractère personnel et la vie privée, à proposer des recommandations non contraignantes à l'ANPD et à diffuser des connaissances sur la protection des données à caractère personnel et de la vie privée ([203]). La coopération entre l'ANPD et le Conseil national est axée sur la promotion de la protection des données et de la vie privée au Brésil. Le Conseil national ne dispose d'aucun pouvoir en ce qui concerne le suivi et l'application de la LGPD, seule l'ANPD étant habilitée à superviser la mise en œuvre de cette loi et à la faire respecter, par exemple en adoptant des règlements, en menant des enquêtes et en appliquant des sanctions. En tant qu'autorité indépendante, l'ANPD n'est pas tenue de suivre les suggestions qui pourraient être présentées par le Conseil national dans le cadre de ses rapports ou recommandations non contraignantes.

2.5.2. *Contrôle de l'application des règles, y compris les sanctions*

(135) Afin de garantir la conformité, le législateur a accordé à l'ANPD des pouvoirs d'enquête et d'exécution, allant d'avertissements à des amendes administratives.

(136) En ce qui concerne les pouvoirs d'enquête, si une violation de la LGPD est soupçonnée ou a été signalée, ou lorsque cela est nécessaire à la protection des droits des personnes concernées qui ont été violés ou sont susceptibles de l'être, l'ANPD peut effectuer à tout moment des audits et des inspections sur place auprès des contrôleurs des secteurs public et privé et demander toute information nécessaire ([204]). En particulier, le règlement contraignant relatif aux pouvoirs de sanction de l'ANPD dispose que les responsables du traitement et les sous-traitants autorisent l'ANPD «à accéder aux bureaux/bâtiments, aux équipements, aux applications, aux installations, aux systèmes, aux outils et aux ressources technologiques, aux documents, aux données et aux informations de nature technique, opérationnelle et autre utiles pour l'évaluation des activités de traitement des données à caractère personnel, en leur possession ou en la possession de tiers» ([205]).

([201]) Article 55-J, points I à XXIV, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([202]) Pour de plus amples informations sur les membres et les activités du Conseil national, voir ANPD, Conseil national pour la protection des données à caractère personnel et de la vie privée. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/cnpd-2.

([203]) Article 58-B, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([204]) Article 55-J, point XVI, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), article 4, point I, décret nº 10.474 du 26 août 2020 sur la structure de l'ANPD et article 12, ANPD, règlement sur la notification des incidents de sécurité, avril 2024.

([205]) Article 5, ANPD, règlement relatif aux pouvoirs de sanction de l'ANPD, octobre 2021. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no1-2021.

(137) Dans le cadre de ses pouvoirs d'adoption de mesures correctrices, l'ANPD peut imposer des avertissements, des amendes ou d'autres sanctions telles que des injonctions de cesser temporairement le traitement de données ou d'effacer des données à caractère personnel ([206]). Ces sanctions peuvent être infligées à des entités publiques ou privées, à l'exception des amendes et des amendes journalières qui ne peuvent pas être infligées à des entités publiques ([207]). Plusieurs sanctions cumulatives peuvent être appliquées pour mettre une entité en conformité. Au moyen d'un avertissement, l'ANPD accorde à un responsable du traitement un délai spécifique pour adopter des mesures correctives afin de mettre un traitement en conformité avec la LGPD ([208]). Le non-respect de cette obligation entraînerait des sanctions supplémentaires. Par exemple, l'ANPD a adressé plusieurs avertissements au ministère de la santé pour défaut de fourniture d'une analyse d'impact relative à la protection des données et de notification d'une violation de données, entre autres ([209]). L'ANPD peut imposer plusieurs sanctions en lien avec la protection des droits des personnes concernées ou le respect de la LGPD. Par exemple, l'ANPD peut infliger une amende administrative pour violation de la LGPD ainsi qu'une injonction de supprimer des données liées à cette violation ([210]). L'ANPD peut également, en cas de sanctions non pécuniaires, décider d'infliger des «amendes journalières» «lorsque cela est nécessaire pour garantir la conformité (avec la LGPD) dans un certain délai» ([211]). L'amende journalière est appliquée de manière cumulative, compte tenu du temps écoulé entre l'application de l'amende et le respect de l'obligation, pour un montant pouvant aller jusqu'à 50 millions de R$ ([212]).

(138) En vertu de l'article 52, point II, de la LGPD, l'ANPD peut infliger des amendes administratives, en plus des amendes journalières, d'un montant allant jusqu'à 2 % des recettes d'une entité au Brésil, pour un montant maximal de 50 millions R$ ([213]). Les amendes peuvent être cumulées en cas de violations multiples. L'ANPD a infligé ses premières amendes, quelques mois après l'adoption de son règlement sur les sanctions, à une société de télécommunications qui n'a pas défini de base juridique pour le traitement et n'a pas désigné de délégué à la protection des données. L'entreprise a reçu un avertissement et deux amendes pour un montant total de 14 400 R$ ([214]). Dans le règlement contraignant sur les sanctions, l'ANPD a classé les sanctions selon trois niveaux de gravité: léger, moyen et grave ([215]) en fonction de facteurs établis tels que le type et le volume des données traitées, le type de traitement ou l'incidence sur les droits de la personne concernée. Par exemple, les violations concernant le traitement de données à caractère personnel sensibles relèvent du niveau de sanctions le plus élevé que l'ANPD peut imposer ([216]).

(139) Le règlement relatif aux sanctions prévoit une méthode de calcul des amendes, y compris pour tenir compte des circonstances aggravantes et/ou atténuantes ([217]). Par exemple, une amende peut être majorée de 10 % en cas de violations spécifiques répétées, voire de 90 % pour chaque mesure corrective non respectée dans un délai déterminé ([218]). De même, une amende peut être réduite de 50 % s'il est remédié à la violation juste après le lancement de la procédure administrative par l'ANPD ([219]).

([206]) Articles 55 et 55-J, point IV, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) et ANPD, règlement sur les sanctions, février 2023.

([207]) Article 52, paragraphe 3. Loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([208]) Article 52, point I, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([209]) Voir ANPD, décision nº 4/2024, disponible à l'adresse https://www.gov.br/anpd/pt-br/centrais-de-conteudo/relatorio_de_instrucao_no_4_2024_fis_cgf_anpd_v-publica.pdf, et ANPD, décision nº 5/2024, disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/relatorio_de_instrucao_5_publico_ocultado.pdf.

([210]) Article 52, point VI, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([211]) Article 16, ANPD, règlement relatif aux sanctions, février 2023.

([212]) Article 16, paragraphe 1, ANPD, règlement relatif aux sanctions, février 2023. 50 millions de réaux brésiliens représentent environ 7,8 millions d'euros.

([213]) 50 millions de réaux brésiliens représentent environ 7,8 millions d'euros.

([214]) ANPD, décision nº 1/2023, disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/assuntos/noticias/sei_00261-000489_2022_62_decisao_telekall_inforservice.pdf.

([215]) Article 8, ANPD, règlement relatif aux sanctions, février 2023.

([216]) Article 8, paragraphe 3, point I, sous d), ANPD, règlement relatif aux sanctions, février 2023.

([217]) Annexe I, articles 12-13, ANPD, règlement relatif aux sanctions, février 2023.

([218]) Article 12, points I à IV, ANPD, règlement relatif aux sanctions, février 2023.

([219]) Article 13, point I, ANPD, règlement relatif aux sanctions, février 2023.

(140) Le système brésilien combine donc différents types de sanctions, allant de mesures correctives à des amendes administratives. Immédiatement après l'entrée en vigueur de ses pouvoirs de sanction, l'ANPD a commencé à en faire usage ([220]). À ce jour, des sanctions et des recommandations ont été émises à l'encontre tant d'autorités publiques, y compris dans le domaine de la sécurité, que d'opérateurs privés ([221]). Les sanctions adoptées à ce jour par l'ANPD concernent un large éventail de questions, notamment l'absence de désignation d'un DPD, les incidents de sécurité, y compris les violations de données, ou le défaut de coopération avec l'ANPD. En plus d'infliger des amendes pécuniaires, l'ANPD s'est montrée particulièrement active dans l'utilisation de l'ensemble de ses pouvoirs en matière de mesures correctrices pour, par exemple, adresser des injonctions aux responsables du traitement de réaliser une AIPD ou de cesser le traitement de données à caractère personnel. Par exemple, en juillet 2024, l'ANPD a ordonné à une grande plateforme de médias sociaux de suspendre le traitement des données à caractère personnel pour l'entraînement des systèmes d'intelligence artificielle générative (IA) dans tous ses produits ([222]). L'ANPD a assorti cette mesure préventive, visant à protéger les droits fondamentaux des personnes concernées, d'une amende journalière de 50 000 R$ jusqu'à ce que le traitement soit mis en conformité avec la LGPD ([223]). Enfin, l'ANPD a annoncé l'ouverture d'enquêtes à l'encontre de plusieurs grandes plateformes technologiques multinationales, d'entreprises de médias sociaux et d'une banque, tout en poursuivant ses enquêtes à l'encontre d'entités du secteur public ([224]). Au cours de ses quelques années d'existence, l'ANPD a fait preuve d'un solide bilan en matière d'application de la législation, en faisant usage de l'ensemble de ses pouvoirs d'exécution.

(141) Enfin, les sanctions administratives instituées par la LGPD ne remplacent pas l'application d'autres sanctions administratives ou civiles et pénales, y compris celles prévues par le code brésilien de protection des consommateurs ([225]) et le cadre civil pour l'internet ([226]). En particulier, le code brésilien de protection des consommateurs impose aux entreprises de fournir aux consommateurs des informations sur leurs affaires et leurs activités ([227]). L'article 56 du code de protection des consommateurs énumère en outre les sanctions auxquelles font face les entreprises en cas de non-respect, qui vont des amendes à l'interdiction de vendre ou de produire un produit ou à l'obligation de suspendre un service. En outre, les articles 61 à 74 du code de protection des consommateurs énumèrent les infractions pénales pour lesquelles les entreprises peuvent se voir infliger de six mois à deux ans d'emprisonnement, y compris en cas d'allégations fausses ou trompeuses concernant un service ou la promotion d'un service susceptible de causer un préjudice au consommateur. Par exemple, en 2014, le département brésilien de la défense et de la protection des consommateurs a infligé à une entreprise de télécommunications une amende de 3,5 millions R$ pour une violation du code de protection des consommateurs et du cadre civil pour l'internet en raison de son utilisation du traçage à des fins de publicité comportementale en ligne et de vente de données de navigation ([228]).

(142) Il résulte de ce qui précède que le système brésilien garantit une application effective de ses règles en matière de protection des données dans la pratique.

2.5.3. *Voies de recours*

(143) En vue d'une protection adéquate et, en particulier, du respect de ses droits individuels, la personne concernée doit disposer de possibilités de recours administratif et juridictionnel effectif, y compris d'indemnisation.

([220]) ANPD, Registre des sanctions. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/decisoes-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

([221]) Voir, par exemple: Note technique n° 175/2023 sur le projet d'accord de coopération entre le ministère de la Justice et de la Sécurité publique et la Fédération brésilienne de football pour le partage de données à caractère personnel en vue d'améliorer le projet «Safe Stadium». Disponible à l'adresse suivante: 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, Mesure préventive, vote n° 11/2024. Disponible à l'adresse suivante: 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$ correspondent à 7 800 EUR.

([224]) La liste complète et actualisée des enquêtes et des affaires en cours ouvertes par l'ANPD est disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/composicao-1/coordenacao-geral-de-fiscalizacao/processos-de-fiscalizacao.

([225]) Loi n° 8.079 du 11 septembre 1990, loi sur la protection des consommateurs. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

([226]) Loi n° 12.965 du 23 avril 2014, Marco Civil da Internet («Cadre civil pour l'internet»). Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([227]) Article 6, loi n° 8.079 du 11 septembre 1990, loi sur la protection des consommateurs.

([228]) Le montant de 3,5 millions de R$ correspondait à environ 1,5 million d'euros, sur la base du taux de change de l'époque.

(144) Le système brésilien offre aux particuliers divers mécanismes leur permettant de faire valoir effectivement leurs droits et d'obtenir réparation.

(145) Dans un premier temps, les personnes qui considèrent que leurs droits ou intérêts en matière de protection des données ont été violés ou qui veulent exercer leurs droits à la protection des données peuvent s'adresser au responsable du traitement concerné. Conformément à l'article 9 de la LGPD, le responsable du traitement fournit, entre autres, les coordonnées pour permettre le dépôt des demandes et des plaintes des personnes concernées ([229]).

(146) En outre, en vertu de la LGPD et du système juridique brésilien, plusieurs voies de recours sont ouvertes aux personnes qui estiment que leurs droits ou intérêts en matière de protection des données ont été violés par le responsable du traitement ou le sous-traitant de données à caractère personnel.

(147) Premièrement, toute personne qui estime que ses droits ou intérêts en matière de protection des données ont été violés par le responsable du traitement ou le sous-traitant peut introduire une réclamation ou signaler cette violation à l'ANPD ([230]). L'ANPD dispose d'une page spécifique sur son site internet pour permettre aux personnes concernées de déposer une plainte en cas de violation de la LGPD ou une demande si elles ont des questions relatives à une demande adressée à un responsable du traitement concernant leurs droits en matière de protection des données ([231]). Comme expliqué au considérant 138 de la présente décision, en réponse à une plainte, l'ANPD peut imposer une sanction conformément à l'article 52 de la LGPD. Le règlement sur les pouvoirs de sanction de l'ANPD a établi la procédure administrative pour ses procédures, y compris les délais, les procédures régissant le droit d'être entendu et la publication de la décision ([232]).

(148) Les personnes concernées peuvent contester les décisions de l'ANPD en introduisant un recours devant le conseil d'administration de l'ANPD dans un délai de 10 jours à compter de la réception des décisions ([233]). Dans le cadre de leur droit à un recours effectif, les particuliers peuvent également former un recours juridictionnel contre les décisions du conseil d'administration et former un recours contre l'ANPD pour non-respect des obligations qui lui incombent en vertu de la LGPD (y compris un refus de traiter une plainte ou un rejet sur le fond d'une plainte) ([234]).

(149) Deuxièmement, l'ANPD peut encourager la «conciliation directe» (médiation) entre les personnes concernées et les responsables du traitement, afin de donner la priorité à la résolution des problèmes et à la «réparation des dommages par le responsable du traitement» ([235]). Ces processus n'empêchent pas les personnes concernées d'introduire une réclamation ou d'accéder à d'autres voies de recours.

(150) Troisièmement, en ce qui concerne les dommages et intérêts, l'article 42 de la LGPD établit l'obligation pour un responsable du traitement ou un sous-traitant de réparer «les dommages matériels, moraux, individuels ou collectifs causés à autrui» résultant du traitement de données à caractère personnel. Les personnes concernées peuvent intenter une action en justice, individuellement ou collectivement, pour demander réparation et indemnisation de ces dommages ([236]). La LGPD établit qu'un juge a le pouvoir discrétionnaire de «renverser la charge de la preuve en faveur de la personne concernée», en particulier dans les cas où «la production d'éléments de preuve par la personne concernée serait trop lourde» ([237]).

(151) Quatrièmement, lorsqu'une violation des droits des personnes concernées entre dans le champ d'application du droit des consommateurs et des relations avec les consommateurs, la protection accordée dans ce domaine s'applique et peut être invoquée en justice ([238]).

([229]) Article 9, lu en combinaison avec l'article 55-J, point V, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([230]) Article 55-J, point V, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([231]) Voir ANPD, Services pour les personnes concernées, dépôt d'une plainte ou d'une demande. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-peticao-de-titular.

([232]) Sections II et III, ANPD, règlement relatif aux pouvoirs de sanction de l'ANPD, octobre 2021.

([233]) Article 59, ANPD, règlement relatif aux pouvoirs de sanction de l'ANPD, octobre 2021.

([234]) Article 22, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([235]) Article 17, point VIII, ANPD, règlement relatif aux pouvoirs de sanction de l'ANPD, octobre 2021.

([236]) Article 42, paragraphe 3, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([237]) Article 42, paragraphe 2, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([238]) Article 45, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

(152) Cinquièmement, la Cour suprême fédérale brésilienne a reconnu que les particuliers ont le droit de réclamer une mesure injonctive en cas de violation de leurs droits découlant de la Constitution, y compris du droit à la protection des données à caractère personnel ([239]). Dans ce contexte, une juridiction peut, par exemple, ordonner à des responsables du traitement de suspendre ou de cesser toute activité illicite. En outre, les droits en matière de protection des données, notamment les droits protégés par la LGPD, peuvent être exercés au moyen d'actions civiles. L'article 22 de la LGPD permet explicitement que la défense des droits des personnes concernées puisse être exercée en justice et, plus généralement, que les personnes physiques puissent porter en justice des affaires relatives à la protection des données, que ce soit individuellement ou collectivement.

(153) Le système brésilien offre donc diverses voies de recours, allant d'options facilement accessibles et peu coûteuses (par exemple, des plaintes à l'ANPD) à des voies judiciaires, qui comprennent la possibilité d'obtenir réparation des dommages ou d'introduire un recours collectif.

3. ACCÈS ET UTILISATION PAR LES AUTORITÉS PUBLIQUES AU BRÉSIL DES DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES À PARTIR DE L'UNION EUROPÉENNE

(154) La Commission a également évalué les limitations et les garanties prévues, y compris les mécanismes de surveillance et de recours individuel prévus par le droit brésilien en ce qui concerne la collecte et l'utilisation ultérieure par les autorités publiques brésiliennes de données à caractère personnel transférées à des responsables du traitement et des sous-traitants au Brésil pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale (ci-après l'«accès des pouvoirs publics»).

(155) Lorsqu'elle a évalué si les conditions dans lesquelles les pouvoirs publics accèdent aux données transférées vers le Brésil en vertu de la présente décision remplissaient le critère de l'«équivalence essentielle» conformément à l'article 45, paragraphe 1, du règlement (UE) 2016/679, tel qu'il est interprété par la Cour de justice de l'Union européenne à la lumière de la Charte des droits fondamentaux, la Commission a notamment pris en considération les critères exposés ci-après.

(156) Premièrement, toute limitation du droit à la protection des données à caractère personnel doit être prévue par la loi et la base juridique qui permet l'ingérence dans ce droit doit définir elle-même la portée de la limitation de l'exercice du droit concerné ([240]).

(157) Deuxièmement, pour satisfaire à l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire dans une société démocratique pour répondre à des objectifs spécifiques d'intérêt général équivalents à ceux reconnus par l'Union, la réglementation du pays tiers en cause permettant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ([241]). Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise ([242]), ainsi que soumettre le respect de ces exigences à une surveillance indépendante ([243]).

([239]) En 2020, la Cour suprême fédérale brésilienne a rendu un arrêt qui a bloqué un décret présidentiel qui aurait contraint les entreprises de télécommunications à partager les données relatives aux abonnés avec l'agence de recensement, reconnaissant pour la première fois la protection des données comme un droit fondamental, ouvrant la voie à l'inscription de ce droit dans la Constitution brésilienne. Voir Cour suprême fédérale, décision relative à l'ADI 6387 du 7 mai 2020. Disponible à l'adresse suivante: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([240]) Arrêt Schrems II, points 174 et 175, et la jurisprudence citée. Voir également, en ce qui concerne l'accès aux données par les autorités publiques des États membres, arrêt dans l'affaire C-623/17, Privacy International, ECLI:EU:C:2020:790, point 65; et l'arrêt dans les affaires jointes C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a., ECLI:EU:C:2020:791, point 175.

([241]) Arrêt Schrems II, points 176 et 181, et la jurisprudence citée. Voir également, en ce qui concerne l'accès aux données par les autorités publiques des États membres, arrêt Privacy International, point 68; et arrêt La Quadrature du Net e.a., point 132.

([242]) Arrêt Schrems II, point 176. Voir également, en ce qui concerne l'accès aux données par les autorités publiques des États membres, arrêt Privacy International, point 68; et arrêt La Quadrature du Net e.a., point 132.

([243]) Arrêt Schrems II, point 179.

(158) Troisièmement, la législation et ses exigences doivent être juridiquement contraignantes en vertu du droit national. Cela concerne en premier lieu toutes les autorités du pays tiers en question, mais ces exigences légales doivent également être opposables à ces autorités devant les tribunaux ([244]). En particulier, les personnes concernées doivent disposer de la possibilité d'exercer des voies de droit devant un tribunal indépendant et impartial afin d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données ([245]).

3.1. **Cadre juridique général**

(159) Les limitations et les garanties applicables à la collecte et à l'utilisation ultérieure des données à caractère personnel par les autorités publiques brésiliennes découlent du cadre constitutionnel général, de lois spécifiques qui régissent leurs activités dans les domaines de la répression et de la sécurité nationale, ainsi que de règles qui s'appliquent spécifiquement au traitement des données à caractère personnel.

(160) Premièrement, l'accès des autorités publiques brésiliennes aux données à caractère personnel est régi par le principe général de légalité, dont découlent les principes de caractère raisonnable, de nécessité et de proportionnalité, consacré par la Constitution brésilienne ([246]). En particulier, conformément à l'article 5 de la Constitution, les libertés et droits fondamentaux (y compris le droit au respect de la vie privée et à la protection des données) ne peuvent être limités que par la loi et lorsque cela est nécessaire à des impératifs de sécurité nationale, de sécurité publique ou à d'autres fins spécifiques d'intérêt public spécifiées par la loi. Ces restrictions doivent être raisonnables et proportionnées ([247]). En particulier, l'évaluation de l'objectif d'intérêt général est essentielle pour apprécier la proportionnalité de l'ingérence, à la lumière du principe de légalité. L'article 5, point LIV, de la Constitution dispose en outre que «nul ne peut être privé de sa liberté ou de ses biens sans procédure régulière».

(161) Deuxièmement, l'ordonnance brésilienne garantit l'*Habeas Data* en tant que voie de recours constitutionnelle destinée à protéger le droit d'accès aux données à caractère personnel détenues par les autorités publiques ou figurant dans des bases de données ou registres publics, ainsi que le droit de rectification et d'effacement de ces données ([248]). Elle sert de garantie contre l'utilisation abusive ou la violation de la vie privée liée au traitement des données par des entités publiques. Toute personne peut introduire une réclamation ou une demande sur la base de l'*Habeas Data*, quelle que soit sa nationalité ([249]).

(162) Troisièmement, les principes généraux et les droits mentionnés aux considérants 155 à 158 sont également reflétés dans les lois spécifiques qui régissent les pouvoirs des autorités répressives et de sécurité nationale. Par exemple, le cadre civil pour l'internet prévoit des mesures exigeant une ordonnance judiciaire préalable pour l'accès aux données et une limitation de l'accès aux données en ligne ([250]). De même, la loi sur l'interception téléphonique prévoit des mesures et des garanties spécifiques pour le traitement des données de télécommunications ([251]). Dans le domaine de la sécurité nationale, la loi établissant le système de renseignement brésilien prévoit des mesures d'accès licite aux données à des fins de sécurité nationale ([252]).

([244]) Arrêt Schrems II, points 181 et 182.

([245]) Arrêts Schrems I, point 95, et Schrems II, point 194. À cet égard, la CJUE a notamment souligné que le respect de l'article 47 de la charte des droits fondamentaux, qui garantit le droit à un recours effectif devant un tribunal indépendant et impartial, «participe également du niveau de protection requis au sein de l'Union [et] dont la Commission doit constater le respect avant que celle-ci adopte une décision d'adéquation au titre de l'article 45, paragraphe 1, du RGPD» (arrêt Schrems II, point 186).

([246]) Article 5, point II, Constitution de la République fédérative du Brésil de 1988.

([247]) Le Brésil relève de la compétence de la Cour interaméricaine des droits de l'homme qui, entre autres, a reconnu le principe de proportionnalité comme «essentiel dans une société démocratique» et selon laquelle des limitations aux droits fondamentaux ne peuvent se produire que si elles sont destinées à répondre à un objectif public impératif. Voir, par exemple, MENDES, Gilmar Ferreira. Les droits fondamentaux et le contrôle juridictionnel. São Paulo; Saraiva, 2012, p. 78.

([248]) Article 5, points LXXII et LXXVII, Constitution de la République fédérative du Brésil de 1988.

([249]) Voir également les considérants 9 et 11 de la présente décision.

([250]) Loi n° 12.965 du 23 avril 2014, Marco Civil da Internet («Cadre civil pour l'internet»). Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

([251]) Loi n° 9.296 du 24 juillet 1996, Loi sur l'interception téléphonique. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

([252]) Loi n° 9.883 du 7 décembre 1999. Loi établissant le système de renseignement brésilien.

(163) Quatrièmement, le traitement des données à caractère personnel par les autorités publiques, y compris à des fins répressives et à des fins de sécurité nationale, est soumis aux exigences en matière de protection des données fixées par la LGPD. Comme décrit au considérant 31 de la présente décision, l'exemption concernant l'application de la LGPD dans le domaine de la sécurité publique, de la défense nationale, de la sûreté de l'État ainsi que des enquêtes et des poursuites en matière d'infractions pénales au titre de la LGPD est partielle. La Cour suprême fédérale a interprété l'applicabilité de la LGPD à la lumière de la protection constitutionnelle des données à caractère personnel et a établi que les grands principes, droits et objectifs de la LGPD s'appliquent à tout traitement de données à caractère personnel par les autorités publiques, y compris lorsqu'il est effectué à des fins répressives ou à des fins de sécurité nationale ([253]). Sur cette base, l'ANPD a, par exemple, mené des enquêtes et publié des orientations, telles qu'une note technique à l'intention des autorités publiques pour les activités liées à la sécurité publique, dans lesquelles elle a rappelé que le traitement à des fins d'intérêt public doit respecter les principes généraux et les droits prévus par la LGPD ([254]).

(164) Enfin, les particuliers peuvent faire valoir leurs droits et leurs libertés constitutionnels devant la Cour suprême fédérale s'ils estiment qu'ils ont été violés par des autorités publiques dans l'exercice de leurs pouvoirs. Les particuliers peuvent également demander réparation, en ce qui concerne leurs droits en matière de protection des données, devant des organes de contrôle indépendants (par exemple, l'ANPD) et des tribunaux, comme indiqué aux considérants 143 à 153 de la présente décision.

3.2. **Accès aux données et utilisation de celles-ci par les autorités publiques brésiliennes à des fins répressives**

(165) Le droit brésilien impose un certain nombre de limitations à l'accès aux données à caractère personnel et à l'utilisation de celles-ci à des fins répressives. Il prévoit également des mécanismes de surveillance et de recours dans ce domaine qui sont conformes aux exigences visées aux considérants 155 à 158 de la présente décision. Les conditions dans lesquelles un tel accès peut intervenir et les garanties applicables à l'utilisation de ces pouvoirs sont évaluées en détail dans les sections suivantes.

3.2.1. *Bases juridiques, limitation et garanties*

(166) En règle générale, l'accès aux données à caractère personnel par les autorités publiques à des fins répressives s'effectue sur la base d'une décision judiciaire préalable émise par une autorité judiciaire compétente ([255]). À titre d'exception à cette règle, il est possible pour les autorités de police et le ministère public, dans des cas spécifiquement prévus par la loi, d'avoir accès aux données des personnes faisant l'objet d'une enquête inscrites dans un registre public, c'est-à-dire aux données relatives à la qualification, à l'affiliation et à l'adresse personnelles ([256]). La liste exhaustive des registres accessibles, prévue par la loi, couvre les informations relatives aux Brésiliens ou aux particuliers résidant au Brésil, mais puisqu'elle ne couvre pas l'accès aux données transférées depuis l'UE, cette liste ne relève pas du champ d'application de la présente décision ([257]). L'accès à ces registres est régi par le principe constitutionnel de légalité — dont découlent les principes de caractère raisonnable, de nécessité et de proportionnalité — et peut faire l'objet d'un contrôle juridictionnel ex post, comme expliqué aux considérants 159 à 161.

(167) Les autorités brésiliennes qui ont le droit d'accéder aux données à caractère personnel et de les collecter à des fins criminelles, au moyen d'une décision judiciaire préalable, sont: 1) la police civile, 2) la police fédérale, 3) le Parquet général des États, 4) le Parquet général fédéral, 5) les juges et les tribunaux, et 6) les commissions d'enquête parlementaires.

([253]) Cour suprême fédérale. Décision relative à l'ADI 6649, septembre 2022. Disponible à l'adresse suivante: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([254]) Note technique n° 175/2023, point 5.1.

([255]) Voir, par exemple, l'article 5, point XII, de la Constitution de 1988 de la République fédérative du Brésil.

([256]) Articles 15 et 16, loi n° 12.850 du 2 août 2013, loi relative aux organisations criminelles et aux enquêtes pénales. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

([257]) Les registres accessibles couvrent les registres de l'emploi, les registres électoraux, les registres téléphoniques, les registres financiers, les registres des fournisseurs d'accès internet et les registres des cartes de crédit. Ces registres comprennent des informations sur les particuliers disposant d'un abonnement à ces services ou utilisant ces services publics. Articles 15 et 16, loi n° 12.850 du 2 août 2013, loi relative aux organisations criminelles et aux enquêtes pénales. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

(168) En vertu de l'article 3-B du code pénal, un juge «chargé du contrôle de la légalité de l'enquête pénale et de la sauvegarde des droits individuels» peut délivrer une ordonnance judiciaire autorisant: 1) l'interception téléphonique de communications par ordinateur et de systèmes connectés ou d'autres formes de communication, 2) la suppression de la confidentialité fiscale, bancaire, des données et des communications téléphoniques, 3) les perquisitions et saisies à domicile, 4) l'accès à des informations secrètes, et 5) «d'autres mesures visant à obtenir des éléments de preuve qui restreignent les droits fondamentaux de la personne faisant l'objet de l'enquête» ([258]).

3.2.1.1. Interception des communications

(169) La confidentialité de la correspondance des communications électroniques et téléphoniques est considérée comme un droit fondamental dans le cadre juridique brésilien ([259]).

(170) Les autorités publiques ne peuvent accéder à ces données que dans des cas exceptionnels à des fins d'enquêtes ou de poursuites pénales. L'interception de communications doit toujours être une mesure subsidiaire et exceptionnelle, qui n'est autorisée que lorsqu'il n'existe aucun autre moyen de résoudre une affaire spécifique, comme l'a établi le Tribunal fédéral ([260]). Les modalités de l'interception en ligne et des communications téléphoniques sont régies par la loi sur l'interception téléphonique ([261]).

(171) L'article 2 de la loi sur l'interception téléphonique fixe des conditions strictes permettant l'accès aux communications. Toute interception de communications nécessite une autorisation judiciaire préalable. Une demande valable d'interception est présentée à un juge par les autorités publiques autorisées, qui peuvent être soit 1) l'autorité de police compétente, dans le cadre d'une enquête pénale, soit 2) le représentant du ministère public, dans le cadre d'une enquête pénale et de poursuites pénales ([262]). L'interception de communications téléphoniques n'est autorisée dans aucune des circonstances suivantes, compte tenu des exigences de nécessité et de proportionnalité: 1) s'il n'existe aucune preuve raisonnable de la commission ou de la participation à une infraction pénale, 2) si les preuves peuvent être obtenues par d'autres moyens disponibles, 3) si le fait qui fait l'objet de l'enquête constitue une infraction pénale passible d'une peine de détention ([263]).

(172) En outre, la loi sur l'interception téléphonique exige que la demande d'interception clarifie la nécessité de la mesure ([264]). L'autorisation judiciaire préalable est justifiée et tient compte de la proportionnalité des moyens utilisés pour procéder à l'interception ([265]). Le juge peut autoriser l'accès au contenu des communications pendant une durée maximale de 15 jours. Cette durée peut être prolongée par une nouvelle décision judiciaire une fois que le caractère indispensable de la mesure est prouvé ([266]). Toute interception de communications, y compris la surveillance de l'environnement, effectuée sans autorisation judiciaire ou à des fins non autorisées par la loi constitue un crime passible d'une peine pouvant aller jusqu'à quatre ans d'emprisonnement ([267]).

([258]) Décret-loi n° 3.689 du 3 octobre 1941, Code pénal. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([259]) Article 5, point XII, Constitution de la République fédérative du Brésil de 1988.
([260]) Cour suprême fédérale, HC 108147/PR, 2012. Disponible à l'adresse suivante: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.
([261]) Article 1er, loi n° 9.296 du 24 juillet 1996, loi sur l'interception téléphonique.
([262]) Article 2, points I et II, Loi n° 9.296 du 24 juillet 1996, loi sur l'interception téléphonique.
([263]) Article 2, loi n° 9.296 du 24 juillet 1996, loi sur l'interception téléphonique.
([264]) Article 4, loi n° 9.296 du 24 juillet 1996, loi sur l'interception téléphonique.
([265]) Article 5, loi n° 9.296 du 24 juillet 1996, loi sur l'interception téléphonique.
([266]) Article 5, loi n° 9.296 du 24 juillet 1996, loi sur l'interception téléphonique.
([267]) Article 10, loi n° 9.296 du 24 juillet 1996, loi sur l'interception téléphonique.

(173) En règle générale, les données consultées et collectées à des fins pénales conformément à la loi sur l'interception téléphonique seront conservées pendant la durée du traitement puis supprimées une fois qu'elles ne sont plus nécessaires aux procédures judiciaires, conformément aux lignes directrices contraignantes du pouvoir judiciaire ([268]). L'article 9 de la loi sur l'interception téléphonique établit en outre que lorsque le contenu collecté n'est pas lié à l'affaire visée par l'enquête dans l'affaire en cause, les données sont rendues «inutilisables» ([269]).

(174) En ce qui concerne les métadonnées de télécommunication, l'article 17 de la loi relative aux organisations criminelles et aux enquêtes pénales impose aux entreprises de téléphonie de conserver pendant cinq ans les informations relatives aux comptes d'utilisateur des particuliers résidant au Brésil et les enregistrements des appels téléphoniques (numéros de téléphone exclusivement) ([270]). L'accès à ce registre géré par l'ANATEL (agence brésilienne de régulation des télécommunications) est limité à certaines entités publiques et nécessite une autorisation judiciaire, comme décrit ci-dessus.

(175) En ce qui concerne les informations disponibles en ligne, l'article 7 du cadre civil pour l'internet garantit en outre «l'inviolabilité et la confidentialité des flux de communications sur internet», sauf par décision judiciaire, conformément à la loi, et «l'inviolabilité et la confidentialité des communications privées stockées, sauf par décision judiciaire» ([271]).

(176) Conformément à l'article 10 du cadre civil pour l'internet, l'accès au contenu des communications en ligne et aux données de connexion (y compris les métadonnées) n'est possible qu'avec une décision judiciaire préalable. Conformément à l'article 22 du cadre civil pour l'internet, la demande de décision judiciaire doit comprendre: point i) des preuves étayées de la commission de l'infraction, point ii) une justification motivée de l'utilité des enregistrements demandés à des fins d'enquête ou d'établissement de la preuve, et point iii) une définition de la période à laquelle les enregistrements se rapportent. L'article 13 impose en outre aux fournisseurs de services internet ou d'applications de conserver les journaux de connexion pendant un an «dans un environnement contrôlé et sécurisé» ([272]). Il n'existe pas d'obligation similaire de conserver des données en ce qui concerne le contenu des communications en ligne. L'accès à l'enregistrement conservé des journaux de connexion ne peut être accordé à une autorité compétente que sur la base d'une autorisation judiciaire, dans les conditions décrites dans le présent considérant ([273]).

(177) L'article 11 du cadre civil pour l'internet rappelle que toute opération nécessitant la collecte, le stockage, la conservation ou tout autre traitement de journaux, de données à caractère personnel ou de communications par des fournisseurs de connexion et d'applications internet au Brésil doit respecter «la législation brésilienne et les droits au respect de la vie privée, à la protection des données à caractère personnel et à la confidentialité des communications et enregistrements privés». Il découle des garanties énoncées aux considérants 175 à 177 que la collecte et la conservation massives de données relatives aux communications internet ne sont généralement pas autorisées au Brésil.

3.2.1.2. Suppression de la protection de la confidentialité fiscale, bancaire, des données et des communications

(178) La confidentialité de la correspondance électronique (y compris les données) et des communications téléphoniques fait l'objet d'une protection constitutionnelle au Brésil ([274]). La LGPD protège en outre l'utilisation des données et des informations de communication ([275]), tandis que la loi sur la confidentialité des institutions financières protège la confidentialité des informations fiscales et bancaires ([276]).

([268]) Article 20, résolution n° 324 du 20 juin 2020. Disponible à l'adresse suivante: https://www.gov.br/conarq/pt-br/legislacao-arquivistica/atos-do-poder-judiciario/resolucao-no-324-de-30-de-junho-de-2020.

([269]) Article 9, loi n° 9.296 du 24 juillet 1996, loi sur l'interception téléphonique.

([270]) Article 17, loi n° 12.850 du 2 août 2013, loi relative aux organisations criminelles et aux enquêtes pénales. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm.

([271]) Article 7, loi n° 12.965 du 23 avril 2014, Marco Civil da Internet («Cadre civil pour l'internet»).

([272]) Article 13, paragraphe principal, loi n° 12.965 du 23 avril 2014, Marco Civil da Internet («Cadre civil pour l'internet»).

([273]) Article 13, paragraphe 5, loi n° 12.965 du 23 avril 2014, Marco Civil da Internet («Cadre civil pour l'internet»).

([274]) Article 5, point XII, Constitution de la République fédérative du Brésil de 1988.

([275]) Voir article 2, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([276]) Loi complémentaire n° 105 du 10 janvier 2001, loi sur la confidentialité des opérations des institutions financières. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(179) Les autorités publiques ne peuvent accéder à ces informations que dans des cas exceptionnels à des fins d'enquêtes ou de poursuites pénales. L'interception de communications doit toujours être une mesure subsidiaire et exceptionnelle, qui n'est autorisée que lorsqu'il n'existe aucun autre moyen de résoudre une affaire spécifique, comme l'a établi le Tribunal fédéral ([277]).

(180) Les critères et les garanties applicables à l'accès aux données et aux communications sont définis dans le cadre civil pour l'internet et la loi sur l'interception téléphonique et sont détaillés aux considérants 169 à 177 de la présente décision.

(181) En ce qui concerne les données fiscales et bancaires, l'article 1 de la loi sur la confidentialité des institutions financières fixe les conditions de la levée des obligations générales visant à garantir la confidentialité de ces informations. Premièrement, la confidentialité ne peut être levée qu'au moyen d'une autorisation judiciaire ([278]). Deuxièmement, les mesures ne peuvent être autorisées que pour des enquêtes ou des poursuites pénales portant sur des infractions ou des crimes identifiés dans les domaines suivants: 1) le terrorisme, 2) le trafic illicite de narcotiques ou de produits stupéfiants similaires, 3) la contrebande ou le trafic d'armes, de munitions ou de matériel destinés à leur production, 4) l'extorsion par enlèvement, 5) les infractions contre le système financier national, 6) les infractions contre l'administration publique, 7) les infractions contre le système fiscal et la sécurité sociale, 8) le blanchiment de capitaux ou dissimulation d'actifs, et 9) l'association avec une organisation criminelle ([279]). L'article 10 de la loi dispose en outre que la protection de la confidentialité des données fiscales et bancaires ne peut être levée à aucune autre fin et que le non-respect de cette limitation constitue un crime passible d'une peine pouvant aller jusqu'à quatre ans de prison ([280]).

3.2.1.3. Perquisitions et saisies

(182) En règle générale, la Constitution fédérale prévoit que les perquisitions et saisies ne peuvent avoir lieu que dans des circonstances exceptionnelles strictement définies ou dans les conditions prévues par la loi et sur la base d'une décision judiciaire rendue par une autorité judiciaire compétente et dans le respect d'une procédure régulière ([281]). Les perquisitions et saisies doivent respecter le principe de légalité et être effectuées dans la mesure nécessaire.

(183) Dans les circonstances exceptionnelles suivantes, des perquisitions et des saisies peuvent avoir lieu sans décision judiciaire: 1) en cas de flagrant délit (c'est-à-dire si un crime est commis en présence d'un agent des services répressifs), 2) en cas de catastrophe naturelle (afin de sauver des vies ou des biens), ou 3) pour fournir une assistance à une personne qui n'est pas en mesure de donner son consentement et qui a besoin d'aide ([282]). La jurisprudence de la Cour suprême fédérale brésilienne a précisé que les autorités répressives ne peuvent pas se fonder sur des «dénonciations anonymes» et sur des «comportements suspects» pour effectuer des perquisitions ou des saisies sans mandat, car cela ne respecterait pas l'exigence de légalité et ne fournirait pas aux autorités une justification valable pour enfreindre l'inviolabilité du domicile ([283]).

(184) En ce qui concerne les garanties procédurales, conformément aux principes constitutionnels brésiliens, aucune fouille d'un appareil électronique ne peut avoir lieu en l'absence d'un soupçon raisonnable qu'une infraction pénale y est enregistrée et, en règle générale, sans décision judiciaire ([284]). En outre, une personne ne saurait être contrainte de transmettre des données si une telle transmission risque de porter atteinte à ses droits constitutionnels, tels que le droit de ne pas s'incriminer soi-même ([285]). Lorsqu'elle soumet une demande de décision de perquisition à un

([277]) Cour suprême fédérale, HC 108147/PR, 2012. Disponible à l'adresse suivante: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401.

([278]) Article 3-B, décret-loi n° 3.689 du 3 octobre 1941, Code pénal. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

([279]) Article 1er, paragraphe 4, points I à IX, loi complémentaire n° 105 du 10 janvier 2001, loi sur la confidentialité des opérations des institutions financières. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

([280]) Article 10, loi complémentaire n° 105 du 10 janvier 2001, loi sur la confidentialité des opérations des institutions financières. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

([281]) Article 5, point XI, Constitution de la République fédérative du Brésil de 1988.

([282]) Article 5, point XI, Constitution de la République fédérative du Brésil de 1988.

([283]) Cour suprême fédérale, 2020, affaire J.S. Appel extraordinaire n° 603616.

([284]) Article 5, point XI, Constitution de la République fédérative du Brésil de 1988.

([285]) Article 5, point LXIII, Constitution de la République fédérative du Brésil de 1988. Voir également le décret-loi n° 2.848 du 7 décembre 1940, Code de procédure pénale. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.

tribunal, l'autorité répressive fournit les faits et éléments de preuve pertinents justifiant la nécessité d'accéder au système informatique et aux données, en utilisant les identifiants d'accès légalement acquis ([286]). Si la juridiction accorde la décision de perquisition, les autorités utilisent les identifiants d'accès pour accéder au système informatique et aux données qui y figurent, conformément aux modalités et conditions précisées dans la décision. Une fois la perquisition ou l'accès terminé, les autorités compétentes doivent soumettre à la juridiction un rapport décrivant les résultats de la perquisition ou de l'accès et fournissant une liste des données ou informations obtenues.

3.2.1.4. Accès aux informations confidentielles

(185) L'article 4 de la loi sur l'accès à l'information (LAI) définit les «informations confidentielles» comme des informations qui «font temporairement l'objet d'une restriction d'accès du public en raison de leur caractère essentiel pour la sécurité de la société et de l'État» ([287]). Des données à caractère personnel peuvent faire partie du champ d'application des informations confidentielles tel que défini dans la phrase précédente.

(186) L'article 6 de la LAI exige des entités publiques qu'elles protègent les informations confidentielles et limitent l'accès à celles-ci. En ce qui concerne l'accès aux informations relatives aux communications, aux données, aux banques et à la fiscalité, l'accès aux informations confidentielles aux fins d'enquêtes et de poursuites pénales ne peut avoir lieu que sur la base d'une autorisation judiciaire, dans des cas exceptionnels, et n'est autorisé que s'il n'existe aucun autre moyen de résoudre une affaire spécifique, comme l'ont établi la Cour suprême fédérale et la loi ([288]).

3.2.1.5. Autres mesures visant à obtenir des éléments de preuve qui restreignent les droits fondamentaux de la personne faisant l'objet de l'enquête

(187) Les «autres mesures visant à obtenir des éléments de preuve qui restreignent les droits fondamentaux de la personne faisant l'objet d'une enquête» renvoient, par exemple, à la possibilité d'ordonner une détention préventive ou de soumettre une personne à une surveillance physique. Ces mesures ne sont en principe pas pertinentes dans le contexte du transfert de données fondé sur une décision d'adéquation.

(188) Par souci d'exhaustivité, de telles mesures, proposées par une autorité publique, ne peuvent être mises en œuvre que sur la base d'une autorisation judiciaire. Les mesures proposées doivent respecter le principe de légalité consacré par la Constitution, être ordonnées dans des cas exceptionnels et lorsqu'aucune autre solution n'est possible, comme l'a établi la Cour suprême fédérale.

3.2.2. *Utilisation ultérieure des informations*

(189) En ce qui concerne l'utilisation ultérieure de données à caractère personnel à une autre fin par une autorité publique, l'article 9 de la loi sur l'interception téléphonique prévoit que lorsque le contenu collecté n'est pas lié à l'affaire examinée dans le cadre d'une enquête spécifique, les données seront rendues «inutilisables». L'article 13 du cadre civil pour l'internet limite également la conservation des données de connexion dans le registre à un maximum d'un an. L'article 10 de la loi sur la confidentialité des institutions financières limite également la finalité pour laquelle la confidentialité des données fiscales et bancaires peut être levée ([289]). Dans la pratique, ces mesures limitent la possibilité d'une utilisation ultérieure des informations.

([286]) Article 240, décret-loi n° 2.848 du 7 décembre 1940, Code de procédure pénale.
([287]) Article 4, point III, loi n° 12.527 du 18 novembre 2011, loi sur l'accès à l'information.
([288]) Cour suprême fédérale, HC 108147/PR, 2012. Disponible à l'adresse suivante: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4067401 et article 3-B, décret-loi n° 3.689 du 3 octobre 1941, Code pénal. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm.
([289]) Article 10, loi complémentaire n° 105 du 10 janvier 2001, loi sur la confidentialité des opérations des institutions financières. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp105.htm.

(190) En outre, et surtout, la Cour suprême fédérale a jugé que la LGPD s'applique au partage de données à caractère personnel entre organismes publics, y compris lorsqu'elles sont partagées entre les services répressifs et les services de renseignement ([290]). En particulier, la Cour a rappelé que «le partage de données à caractère personnel entre les organismes et entités de l'administration publique suppose: 1) la définition d'une finalité légitime, spécifique et explicite pour le traitement des données, 2) la compatibilité du traitement avec les finalités déclarées, 3) la limitation du partage au minimum nécessaire pour atteindre la finalité déclarée, ainsi que le plein respect des exigences, garanties et procédures prévues par la LGPD, dans la mesure où elle est compatible avec le secteur public». La Cour a ajouté que «le traitement de données à caractère personnel effectué par des organismes publics en violation des paramètres juridiques et constitutionnels entraînera la responsabilité civile de l'État pour les dommages subis par les particuliers», conformément à l'article 42 de la LGPD.

(191) En ce qui concerne le partage de données à caractère personnel entre les autorités répressives brésiliennes et les autorités similaires des pays tiers, ces activités sont régies par des instruments de droit international, conformément à la LGPD. À cet égard, l'article 33, point III, de la LGPD dispose que les transferts internationaux de données peuvent avoir lieu «lorsque cela est nécessaire à la coopération juridique internationale entre les organismes publics de renseignement, d'enquête et de poursuites, conformément aux instruments juridiques internationaux». Au Brésil, le ministère de la justice et de la sécurité publique joue le rôle d'autorité centrale pour la coopération judiciaire internationale en matière pénale. Le ministère est responsable de la réception, de l'analyse, de la transmission et du suivi de l'exécution des demandes de coopération internationale avec les autorités étrangères, dans le respect des règles applicables du droit international et de la LGPD. Le traitement des données à caractère personnel nécessaires à la coopération juridique internationale est soumis aux principes de limitation des finalités (article 6, point I, de la LGPD), de licéité et de loyauté du traitement (articles 6 et 7 de la LGPD), de minimisation et d'exactitude des données (article 6, points III et V, de la LGPD), de transparence (article 6, point VI, de la LGPD), de sécurité des données (article 6, point VII, de la LGPD) et de limitation de la conservation (article 6, points I, III et IV, et article 16 de la LGPD). La divulgation éventuelle de données à caractère personnel à des tiers (y compris des pays tiers) ne peut avoir lieu que conformément à ces principes, après avoir évalué le respect des principes constitutionnels de nécessité et de proportionnalité et assuré la continuité de la protection et du respect des droits des personnes concernées (article 2 du règlement sur le transfert de données).

(192) Les pouvoirs des autorités répressives brésiliennes en matière de collecte et d'accès aux données sont donc encadrés par des règles claires et précises prévues par la loi et sont soumis à un certain nombre de garanties. Ces garanties comprennent en particulier le contrôle garanti de l'exécution de ces mesures, y compris au moyen d'une approbation judiciaire préalable et de garanties limitant la durée d'accès et la conservation des informations conformément aux principes de nécessité et de proportionnalité.

3.2.3. *Surveillance*

(193) Au Brésil, les activités des autorités répressives sont supervisées par différents organismes.

(194) Premièrement, comme l'a confirmé la Cour suprême fédérale, l'ANPD est habilitée à surveiller le traitement des données à caractère personnel effectué par les autorités répressives au regard de certaines exigences de la LGPD ([291]). Dans ce contexte, l'ANPD peut exercer les pouvoirs d'enquête et d'adoption de mesures correctrices dont elle dispose en vertu de la LGPD. Par exemple, l'ANPD a enquêté sur les activités de la police fédérale, du ministère de la justice et de la sécurité publique, ainsi que d'autres organismes publics exerçant des activités de sécurité fédérale, étatique ou locale ou investis de responsabilités en matière pénale ([292]). Les enquêtes peuvent être menées à l'initiative même de l'ANPD à la suite de demandes et de plaintes, qui peuvent être déposées, par exemple, par des particuliers, des organisations de la société civile et des autorités publiques. L'ANPD a ainsi mené plusieurs enquêtes sur l'utilisation de caméras vidéo à la suite de demandes de la société civile ([293]).

([290]) Cour suprême fédérale. Décision relative à l'ADI 6649, septembre 2022. Disponible à l'adresse suivante: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([291]) Voir le considérant 163 de la présente décision et la décision de la Cour suprême fédérale sur l'ADI 6649 du 15 septembre 2022. Disponible à l'adresse suivante: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([292]) Voir ANPD, Inspections, dont affaires 00261.000836/2021-76 et 00261.001028/2021-26. Disponible à l'adresse suivante: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340.

([293]) Voir ANPD, Inspections, affaire 00261.002211/2022-20 relative à l'utilisation de caméras de sécurité par les autorités de la ville de Fortaleza. Demande adressée à l'ANPD disponible à l'adresse suivante: 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) Deuxièmement, les activités des autorités répressives sont supervisées par le pouvoir judiciaire. Les juridictions ont le pouvoir d'autoriser la collecte de données à caractère personnel et l'accès à celles-ci, dans les circonstances mentionnées ci-dessus aux considérants 165 à 187. Elles ont en outre le pouvoir d'infliger des sanctions civiles et pénales en cas d'abus ou de non-respect de la législation en vigueur, y compris la détention ou la cessation de certaines activités.

(196) Troisièmement, le ministère public, une institution indépendante et permanente au Brésil chargée de défendre l'ordre juridique et le système démocratique, a le pouvoir d'exercer un contrôle externe sur les activités de police ([294]). Comme indiqué dans la résolution relative au ministère public, le contrôle externe des activités de police a pour but de maintenir «la régularité et l'adéquation des procédures employées dans l'exercice des activités de police», notamment en ce qui concerne le «respect des droits fondamentaux garantis par la Constitution et les lois fédérales» ([295]). À ce titre, le ministère public peut, entre autres, effectuer une visite sur place, programmée ou à tout moment, examiner les enquêtes, superviser la saisie des marchandises et contrôler le respect des mandats d'arrêt ([296]). Toute violation de la loi est signalée aux juridictions. Dans le cadre de ses fonctions, le ministère public a participé à des enquêtes et à des poursuites dans des affaires de violence policière, d'abus de pouvoir et de violations des droits de l'homme. Le ministère public joue également un rôle dans la surveillance de la protection des données en engageant des actions en justice, ou en se joignant à ce type d'actions, sur la base des protections constitutionnelles, ainsi que dans la promotion des droits en matière de protection des données aux côtés de l'ANPD. Le ministère public a, par exemple, présenté à la Cour suprême fédérale sa thèse en faveur d'une décision historique reconnaissant la protection des données comme un droit fondamental au Brésil ([297]). Un registre des actions du ministère public concernant la LGPD est également disponible sur sa page web ([298]).

3.2.4. *Voies de recours*

(197) Le système brésilien offre différentes possibilités de recours juridictionnel et administratif, notamment d'indemnisation. Ces mécanismes mettent à la disposition des personnes concernées des moyens de recours administratif et judiciaire effectif, qui leur permettent notamment de protéger leurs droits, y compris le droit d'accéder aux données à caractère personnel les concernant ou d'obtenir la rectification ou l'effacement de telles données.

(198) Premièrement, les particuliers peuvent demander réparation en justice, y compris pour des dommages et intérêts. La Constitution fédérale et le Code de procédure civile fournissent les bases juridiques permettant de demander réparation du préjudice moral ou matériel causé par l'autorité publique qui a illégalement collecté ou utilisé des données à des fins criminelles ([299]). En particulier, la Constitution mentionne expressément que le droit au respect de la vie privée implique un «droit à réparation» du préjudice matériel ou moral résultant de sa violation ([300]). Les décisions des juridictions peuvent faire l'objet d'un recours devant la Cour suprême fédérale et devant la Cour interaméricaine des droits de l'homme. En 2009, la Cour interaméricaine des droits de l'homme a ordonné au Brésil d'indemniser les travailleurs des coopératives agricoles en raison d'opérations d'interception téléphonique inappropriées effectuées dans l'État du Paraná en 1999 en violation de la loi sur l'interception téléphonique et de la convention américaine des droits de l'homme ([301]).

([294]) Article 127, Constitution de la République fédérative du Brésil de 1988.

([295]) Article 20, résolution 20 du 28 mai 2007, Contrôle externe des activités de police. Disponible à l'adresse suivante: https://www.cnmp.mp.br/portal/images/Comissoes/CSP/Resolu%C3%A7%C3%B5es_/Resolu%C3%A7%C3%A3o_20.pdf.

([296]) Article 4, résolution 20 du 28 mai 2007, Contrôle externe des activités de police.

([297]) Voir le considérant 199 de la présente décision et la décision de la Cour suprême fédérale sur l'ADI 6.387, mai 2020. Disponible à l'adresse suivante: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([298]) Ministère public, «LGPD at the Public Prosecutor's Office» («LGPD au sein du ministère public»). Disponible à l'adresse suivante: https://www.mpf.mp.br/servicos/lgpd/lgpd-no-mpf.

([299]) Voir, par exemple, l'article 43 de la loi n° 10.408 du 10 janvier 2002. Code de procédure civile. Disponible à l'adresse suivante: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm.

([300]) Article 5, point X, Constitution de la République fédérative du Brésil de 1988.

([301]) Cour interaméricaine des droits de l'homme, affaire Escher et al./Brésil, objections préliminaires, motivation, réparations et coûts. Arrêt du 6 juillet 2009. Disponible à l'adresse suivante: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf.

(199) Deuxièmement, les personnes physiques, quelle que soit leur nationalité, peuvent se prévaloir de la protection prévue par la notion de *Habeas Data* pour obtenir davantage l'accès à leurs données détenues par les autorités publiques et leur rectification ([302]). Sur cette base, les particuliers peuvent également porter des affaires devant les juridictions, y compris devant la Cour suprême fédérale par une action directe en inconstitutionnalité (Ação Direta de Inconstitucionalidade, «ADI»). La décision historique de 2020 de la CSF, qui ouvre la voie à la reconnaissance de la protection des données en tant que droit fondamental par le Brésil, a été initiée par des ADI ouvertes sur la base du principe *Habeas Data* ([303]). Le ministère public est également intervenu dans cette affaire, en soutenant la position des particuliers et de la société civile qui avaient engagé l'action. L'affaire contestait un décret présidentiel qui visait à partager des données à caractère personnel de plus de 200 millions d'abonnés aux télécommunications avec l'Institut brésilien de géographie et de statistique pendant la pandémie de COVID-19 ([304]). La CSF a estimé que le décret présidentiel violait les droits fondamentaux au respect de la vie privée et à la confidentialité des communications protégés par la Constitution ([305]). Le décret présidentiel a été suspendu et la CSF a jugé que la protection des données devait être considérée et protégée comme un droit fondamental, à l'instar du droit au respect de la vie privée ([306]). Au moment de la décision, la LGPD n'était pas encore en vigueur. Par conséquent, les juges ont utilisé le droit comparé, notamment la jurisprudence de la Cour constitutionnelle fédérale allemande et l'article 8 de la charte des droits fondamentaux de l'Union européenne pour étayer leur compréhension de l'inconstitutionnalité du décret présidentiel, ainsi qu'une interprétation des droits fondamentaux à la dignité et à la vie privée garantis par la Constitution et la reconnaissance de l'*Habeas Data* en tant qu'outil de protection du droit à l'autodétermination informationnelle ([307]).

(200) Troisièmement, les personnes physiques peuvent demander réparation à l'ANPD en cas de violation de la LGPD en vertu de son article 55-J, point V, et dans les conditions détaillées aux considérants 146 et 149 de la présente décision. Les particuliers peuvent également exercer leurs droits en matière de protection des données établis au titre de la LGPD à l'égard des autorités publiques ([308]).

(201) Les mécanismes de recours décrits aux considérants 197 à 200 de la présente décision offrent aux personnes concernées des voies de recours administratif et juridictionnel efficaces, leur permettant notamment de faire valoir leurs droits, y compris leur droit à la protection des données à l'égard de ces données.

3.3. Accès aux données et utilisation de celles-ci par les autorités publiques brésiliennes à des fins de sécurité nationale

(202) Le droit du Brésil prévoit un certain nombre de limitations et de garanties en ce qui concerne l'accès aux données à caractère personnel et l'utilisation de celles-ci à des fins de sécurité nationale. Il prévoit également des mécanismes de surveillance et de recours qui sont conformes aux exigences visées aux considérants 156 à 158 de la présente décision. Les conditions dans lesquelles un tel accès peut intervenir et les garanties applicables à l'utilisation de ces pouvoirs sont évaluées en détail dans les sections suivantes.

([302]) Voir considérants 9 et 161 de la présente décision.

([303]) Cour suprême fédérale, décision relative à l'ADI 6.387, 2020. Disponible à l'adresse suivante: https://www.stf.jus.br/arquivo/cms/noticianoticiastf/anexo/adi6387mc.pdf.

([304]) Décret présidentiel suspendu n° 954 du 17 avril 2020. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm.

([305]) Cour suprême fédérale, décision relative à l'ADI 6.387, mai 2020, p. 12.

([306]) Cour suprême fédérale, décision relative à l'ADI 6.387, mai 2020, p. 8.

([307]) Voir Cour suprême fédérale, décision relative à l'ADI 6.387, mai 2020, p. 4, et Association internationale du barreau, The impact of Covid-19 for data protection in Brazil: the perspective of Brazil's supreme court (L'incidence du Covid-19 sur la protection des données au Brésil, le point de vue de la juridiction suprême brésilienne). Disponible à l'adresse suivante: 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]) Article 23, loi n° 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

3.3.1. *Bases juridiques, limitations et garanties*

(203) Au Brésil, les données à caractère personnel peuvent être consultées à des fins de sécurité nationale dans le cadre d'activités de renseignement sur la base de la loi établissant le système de renseignement brésilien (SISBIN) ([309]). De manière générale, l'article 1er de cette loi dispose que le système de renseignement brésilien «doit respecter et préserver les droits et garanties des personnes et les autres dispositions de la Constitution fédérale, des traités, conventions, accords et engagements internationaux auxquels la République fédérative du Brésil est partie ou signataire» ([310]). Il s'agit notamment de garantir les principes de nécessité et de proportionnalité, ainsi que le droit à la protection des données ([311]). Les activités à mener par le système de renseignement brésilien sont décrites plus en détail dans des décrets contraignants ([312]).

(204) En vertu de l'article 4 de la loi établissant le système de renseignement brésilien, les entités faisant partie du SISBIN peuvent obtenir et analyser des données spécifiques à des fins de sécurité nationale («Segurança Pública»). La notion de sécurité nationale est régie par une loi de 2021 qui a modifié le code pénal ([313]) et qui a abrogé la loi brésilienne sur la sécurité nationale ([314]). La loi de 2021 a établi une liste exhaustive des «crimes» contre la sécurité nationale qui encadre cette notion. Ces crimes sont 1) les crimes contre la «souveraineté nationale» (qui couvrent les actes de guerre, l'invasion du pays, la tentative de saisir une partie du territoire national pour former un nouveau pays, le partage d'informations classifiées avec des gouvernements étrangers ou des organisations criminelles étrangères qui pourraient mettre en péril l'ordre constitutionnel de souveraineté nationale, et le fait de donner accès ou un accès illicite à des systèmes d'information à des personnes non autorisées) ([315]), 2) les crimes contre les «institutions démocratiques» (qui couvrent la tentative violente de mettre un terme à l'état de droit en prévenant ou en limitant les pouvoirs constitutionnels et le coup d'État) ([316]), 3) les crimes contre le «fonctionnement des institutions démocratiques pendant le processus électoral» (qui couvre l'interruption du processus électoral et la limitation ou l'empêchement, par la violence, de la capacité des individus à exercer leurs droits politiques) ([317]), et 4) les infractions portant atteinte au fonctionnement des services essentiels (qui couvrent le sabotage des moyens de communication publique, les installations de défense, dans le but de mettre un terme à l'État de droit) ([318]). L'article 359-T de la loi précise que l'exercice de la liberté d'expression, des droits et pouvoirs constitutionnels, la conduite d'activités journalistiques, y compris «par le biais de marches, de réunions, de grèves, de rassemblements ou de toute autre forme de manifestation politique à des fins sociales» ne peuvent être considérés comme des infractions pénales ([319]). La politique nationale brésilienne en matière de renseignement a fixé une série d'objectifs clés en matière de renseignement que les autorités doivent prendre en considération, tels que la prévention du «sabotage» ou de l'«espionnage» ([320]). En tant que «document d'orientation de haut niveau», cette politique n'étend toutefois pas la liste des infractions liées à la notion de sécurité nationale ni ne modifie sa définition ([321]).

([309]) Loi 9.883 du 7 décembre 1999. Loi établissant le système de renseignement brésilien. Disponible à l'adresse suivante: 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]) Article 1er, paragraphe 1, loi no 9.883 du 7 décembre 1999. Loi établissant le système de renseignement brésilien.

([311]) Voir le considérant 160 de la présente décision.

([312]) Décret no 8.793/2016 du 29 juin 2016 relatif à la politique nationale en matière de renseignement. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm et décret no 4.376/2002 du 13 septembre 2002 relatif à l'organisation et au fonctionnement du système de renseignement brésilien. Disponible à l'adresse suivante: 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]) Loi no 14.197 du 1er septembre 2021, loi modifiant le code pénal et abrogeant la loi de 1983 sur la sécurité nationale. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm.

([314]) Loi abrogée no 7.170 du 14 décembre 1983, loi sur la sécurité nationale. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/LEIS/L7170.htm.

([315]) Chapitre I, loi no 14.197 du 1er septembre 2021, loi modifiant le code pénal et abrogeant la loi de 1983 sur la sécurité nationale.

([316]) Chapitre II, loi no 14.197 du 1er septembre 2021, loi modifiant le code pénal et abrogeant la loi de 1983 sur la sécurité nationale.

([317]) Chapitre III, loi no 14.197 du 1er septembre 2021, loi modifiant le code pénal et abrogeant la loi de 1983 sur la sécurité nationale.

([318]) Chapitre IV, loi no 14.197 du 1er septembre 2021, loi modifiant le code pénal et abrogeant la loi de 1983 sur la sécurité nationale.

([319]) Article 359-T, loi no 14.197 du 1er septembre 2021, loi modifiant le code pénal et abrogeant la loi de 1983 sur la sécurité nationale.

([320]) Article 3, Décret no 8.793/2016 du 29 juin 2016 relatif à la politique nationale en matière de renseignement. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

([321]) Introduction, premier paragraphe, Décret no 8.793/2016 du 29 juin 2016 relatif à la politique nationale en matière de renseignement. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8793.htm.

(205) Les données qui peuvent être analysées et auxquelles il est possible d'accéder afin de prévenir les crimes susmentionnés contre la sécurité nationale couvrent les informations auxquelles la partie des autorités du SISBIN a eu accès dans le cadre de ses opérations et conformément aux conditions décrites aux considérants 165 à 187 de la présente décision (c'est-à-dire sur la base d'une autorisation judiciaire délivrée dans un but clairement défini). Les données partagées avec le SISBIN sont traitées au moyen d'un système électronique chiffré sécurisé avec journaux d'accès afin de garantir la traçabilité et la vérifiabilité des informations ([322]). Comme l'a précisé la Cour suprême fédérale, le partage des données avec le SISBIN est soumis aux principes de la LGDP, et notamment ceux de limitation des finalités (article 6, point I, de la LGPD), de minimisation et d'exactitude des données (article 6, points III et V, de la LGPD), de transparence (article 6, point VI, de la LGPD), de sécurité des données (article 6, point VII, de la LGPD) et de limitation de la conservation (article 6, points I, III et IV, et article 16 de la LGPD) ([323]).

(206) L'article 2 de la loi établissant le système de renseignement brésilien indique que seules les autorités publiques font partie de ce système. Le SISBIN est composé de l'agence de renseignement brésilienne (ABIN) et de représentants des centres de renseignement, des ministères, des secrétariats et des agences de l'administration publique fédérale. La liste des autorités membres du SISBIN est prévue dans un décret relatif à l'organisation et au fonctionnement du système ([324]).

(207) L'ABIN est l'organe central du système de renseignement et est responsable de la planification, de l'exécution, de la coordination, de la surveillance et de la supervision des activités de renseignement. Ces activités doivent être menées à l'aide de moyens et de techniques confidentiels fondés sur des informations. Pour s'acquitter de ses missions, l'ABIN reçoit des informations et des données spécifiques des différentes autorités publiques qui font partie du SISBIN en ce qui concerne la sécurité nationale. Les autorités qui font partie du SISBIN sont tenues de fournir ces informations ([325]), étant donné que la loi n'autorise pas l'ABIN à collecter elle-même des informations. La licéité de l'obligation de partage des données incombant aux membres du SISBIN a été contestée devant la Cour suprême fédérale ([326]). Dans son arrêt rendu en 2021, la CSF a précisé que les données que les autorités publiques partagent avec l'ABIN doivent respecter les objectifs stricts d'intérêt public (par exemple, la défense des institutions publiques et de l'intérêt national) et a rappelé que la finalité spécifique et légitime de chaque activité de partage de données est définie au moyen d'une procédure formelle soumise à une autorisation judiciaire et définie dans celle-ci ([327]). Ces limitations s'appliquent également à tout partage ultérieur de données entre autorités publiques ([328]).

(208) Enfin, le traitement des données effectué par l'intermédiaire du SISBIN doit protéger les informations contre l'accès par des personnes ou des organismes non autorisés. L'article 5 du décret relatif au fonctionnement du SISBIN exige explicitement que la coordination et le partage des données entre les membres du système des autorités respectent «la législation relative au secret professionnel et à la sécurité, à la protection des données à caractère personnel et à

([322]) Voir brochure SISBIN, 2024, p. 18. Disponible à l'adresse suivante: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.

([323]) Cour suprême fédérale. Décision relative à l'ADI 6649, septembre 2022. Disponible à l'adresse suivante: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([324]) Article 7, décret nº 11.693 du 6 septembre 2023 relatif à l'organisation et au fonctionnement du SISBIN. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm. Parmi les exemples d'autorités membres du SISBIN, on compte: le centre de renseignement du ministère de la défense, la direction du renseignement pénitentiaire du secrétariat national du ministère de la justice et de la sécurité publique, le secrétariat général des relations extérieures du ministère des affaires étrangères et la direction du renseignement de la police fédérale.

([325]) Article 4, loi nº 9.883 du 7 décembre 1999. Loi établissant le système de renseignement brésilien. Disponible à l'adresse suivante: 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]) Cour suprême fédérale, décision relative à l'ADI 6529 du 15 octobre 2021. Disponible à l'adresse suivante: https://www.jusbrasil.com.br/jurisprudencia/stf/1303041724/inteiro-teor-1303041733.

([327]) Cour suprême fédérale, décision relative à l'ADI 6529 du 15 octobre 2021, p. 22.

([328]) Cour suprême fédérale, décision relative à l'ADI 6529 du 15 octobre 2021, p. 3.

la sécurité des informations et des connaissances» et fait de la LGPD la principale législation brésilienne en matière de protection des données à caractère personnel ([329]). L'article 6 du décret précise en outre que les informations échangées par les autorités dans le cadre du SISBIN respectent «les principes de sécurité juridique, de nécessité et d'intérêt public» et poursuivent un objectif légitime ([330]). Le SISBIN reconnaît également l'importance du respect de la LGPD dans ses documents publics et ses procédures internes ([331]).

(209) Les pouvoirs des autorités traitant des données à des fins de sécurité nationale au Brésil sont donc encadrés par des règles claires et précises prévues par la loi et sont soumis à un certain nombre de garanties. Ces garanties comprennent en particulier le contrôle garanti de l'exécution de ces mesures, y compris au moyen d'une approbation judiciaire préalable et des garanties limitant l'accès aux informations conformément aux principes de nécessité et de proportionnalité.

3.3.2. *Utilisation ultérieure des informations*

(210) Le traitement des données à caractère personnel recueillies par les autorités brésiliennes à des fins de sécurité nationale est soumis aux principes de limitation des finalités (article 6, point I, de la LGPD), de licéité et de loyauté du traitement (articles 6 et 7 de la LGPD), de minimisation et d'exactitude des données (article 6, points III et V, de la LGPD), de transparence (article 6, point VI, de la LGPD), de sécurité des données (article 6, point VII, de la LGPD) et de limitation de la conservation (article 6, points I, III et IV, et article 16 de la LGPD).

(211) La divulgation éventuelle de données à caractère personnel à des tiers (y compris à des pays tiers et dans le cadre d'accords internationaux) ne peut avoir lieu que conformément aux principes de la LGPD, après avoir évalué le respect des principes constitutionnels de nécessité et de proportionnalité et assuré la continuité de la protection et du respect des droits des personnes concernées (article 2 du règlement sur le transfert de données).

3.3.3. *Surveillance*

(212) Les activités des autorités nationales de sécurité brésiliennes sont supervisées par différents organismes. Le décret relatif à la stratégie nationale en matière de renseignement du Brésil souligne l'importance de disposer de plusieurs niveaux de mécanisme de surveillance pour protéger l'«état de droit démocratique» ([332]). La Cour suprême fédérale a rappelé l'importance de ce contrôle dans une affaire concernant le traitement des données dans le cadre du SISBIN, déclarant que «l'efficacité des activités de renseignement est souvent liée au secret du processus et des informations recueillies. Dans l'état de droit démocratique, cette fonction est soumise au contrôle externe du pouvoir législatif et du pouvoir judiciaire afin d'évaluer si le secret imposé est adapté aux objectifs publics stricts auxquels il est destiné» ([333]).

(213) Premièrement, le pouvoir exécutif exerce un contrôle, qui veille à ce que les objectifs à atteindre par le système de renseignement ainsi que les politiques à mettre en œuvre et les plans formulés répondent de manière adéquate aux demandes de la société. L'exécutif est également chargé de veiller à ce que les dépenses des services de renseignement soient effectuées de manière rationnelle et exclusive pour des actions légitimes, nécessaires et utiles pour l'État. Dans le cadre brésilien, ce contrôle est exercé par la Chambre des relations extérieures et de la défense nationale du Conseil de gouvernement, qui est chargée de superviser la mise en œuvre de la police nationale du renseignement, et par le Bureau de sécurité institutionnelle, qui est chargé de coordonner l'activité du renseignement fédéral ([334]).

([329]) Article 5, décret n° 11.693 du 6 septembre 2023 relatif à l'organisation et au fonctionnement du SISBIN.
([330]) Article 6, décret n° 11.693 du 6 septembre 2023 relatif à l'organisation et au fonctionnement du SISBIN.
([331]) Voir, par exemple, brochure SISBIN, p. 9: «L'un des objectifs de ce repositionnement est d'accroître les niveaux de traçabilité et de transparence des processus internes du SISBIN par l'adoption d'outils et de plateformes numériques spécialement conçus à ces fins. Ces outils doivent être alignés sur le cadre juridique établi par la loi sur l'accès à l'information et la loi générale sur la protection des données (LGPD), toutes deux adoptées en 2012». Disponible à l'adresse suivante: https://www.gov.br/abin/pt-br/institucional/sisbin/cart_ingles.pdf.
([332]) Article 2.4, paragraphe 4, décret du 15 décembre 2017 relatif à une stratégie nationale en matière de renseignement.
([333]) Cour suprême fédérale, décision du 15 octobre 2021, p. 2.
([334]) Section 2.4, décret du 15 décembre 2017 relatif à une stratégie nationale en matière de renseignement. Disponible à l'adresse suivante: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/dsn/Dsn14503.htm.

(214) Deuxièmement, la branche législative exerce un contrôle en ce qui concerne les activités de renseignement. L'objectif de ce contrôle est de vérifier à la fois la légitimité et l'efficacité de l'activité de renseignement. Les chefs des partis majoritaires et minoritaires au sein de la Chambre des députés et du Sénat fédéral, ainsi que les présidents des commissions des relations extérieures et de la défense nationale de la Chambre des députés et du Sénat fédéral, font partie de l'organe de contrôle externe des activités de renseignement, appelé Commission mixte pour le contrôle des activités de renseignement («Comissão mista de Controle da Atividade de Inteligência — CCAI») ([335]). Le contrôle exercé par la branche législative sur les activités de renseignement a été défini par la loi établissant le système de renseignement brésilien en 1999 et le rôle de surveillance et les pouvoirs de la CCAI ont été considérablement renforcés par l'adoption d'une résolution contraignante du Congrès en 2013 ([336]). Cette résolution remédiait aux lacunes constatées précédemment en ce qui concerne la poursuite de l'institutionnalisation de la CCAI en lui fournissant une structure et un secrétariat permanents, en clarifiant ses pouvoirs et en renforçant la transparence de ses activités. Le rôle, les activités et les pouvoirs de la CCAI sont détaillés dans ladite résolution et par la loi. La CCAI surveille et contrôle les activités de renseignement menées par les organes de l'administration publique fédérale, en particulier les organes faisant partie du SISBIN, en vue de s'assurer que les activités sont réalisées conformément à la Constitution et afin de protéger les droits et les garanties des individus, de la société et de l'État ([337]). La CCAI peut procéder à un examen a posteriori, mais aussi à des audits et contrôles des opérations en cours ([338]). Les membres de la CCAI disposent d'une habilitation maximale pour accéder aux documents. La CCAI établit des rapports annuels sur ses activités, sans inclure d'informations susceptibles de compromettre la sécurité nationale ([339]). Comme indiqué au considérant 222 de la présente décision, la CCAI peut également recevoir et examiner les plaintes de particuliers.

(215) Troisièmement, l'ANPD veille à ce que les autorités nationales de sécurité, en matière de traitement des données à caractère personnel, respectent les paramètres définis par la LGPD. La LGPD s'applique partiellement au traitement de données à caractère personnel effectué à des fins de sécurité publique, de défense nationale, de sûreté de l'État ou d'activités d'enquête et de poursuite d'infractions pénales ([340]). Dans ce contexte, l'ANPD peut exercer les pouvoirs d'enquête et d'adoption de mesures correctrices dont elle dispose en vertu de la LGPD. L'ANPD peut, par exemple, effectuer des audits à tout moment auprès de toutes les autorités publiques, y compris l'agence de renseignement ([341]).

(216) Enfin, le pouvoir judiciaire statuera sur les poursuites intentées par des citoyens contre des autorités publiques et, dans ce contexte, pourra superviser les activités menées à des fins de sécurité nationale afin de garantir le respect de tous les droits constitutionnels et du cadre législatif pertinent, y compris la LGPD. Les décisions des juridictions peuvent faire l'objet d'un recours devant la Cour suprême fédérale et devant la Cour interaméricaine des droits de l'homme.

3.3.4. *Voies de recours*

(217) Le système brésilien offre différentes possibilités de recours juridictionnel et administratif, notamment d'indemnisation. Ces mécanismes mettent à la disposition des personnes concernées des moyens de recours administratif et judiciaire effectif, qui leur permettent notamment de protéger leurs droits, y compris le droit d'accéder aux données à caractère personnel les concernant ou d'obtenir la rectification ou l'effacement de telles données.

([335]) Article 6, paragraphe 1, loi nº 9.883 du 7 décembre 1999. Loi établissant le système de renseignement brésilien.

([336]) Résolution nº 2 de 2021-CN sur la Comissão mista de Controle da Atividade de Inteligência (CCAI). Disponible à l'adresse suivante: https://www2.camara.leg.br/legin/fed/rescon/2013/resolucao-2-22-novembro-2013-777449-publicacaooriginal-141944-pl.html.

([337]) Section 2.4, décret du 15 décembre 2017 relatif à une stratégie nationale en matière de renseignement.

([338]) Voir notamment l'article 3 de la résolution nº 2 de 2021-CN sur la Comissão mista de Controle da Atividade de Inteligência (CCAI).

([339]) Article 13, résolution nº 2 de 2021-CN sur la Comissão mista de Controle da Atividade de Inteligência (CCAI).
Des informations sur les réunions et les documents préparés par la CCAI sont disponibles en ligne et régulièrement mises à jour, à l'adresse suivante: https://legis.senado.leg.br/atividade/comissoes/comissao/449/ et https://www.congressonacional.leg.br/legislacao-e-publicacoes/glossario-legislativo/-/legislativo/termo/comissao_mista_de_controle_das_atividades_de_inteligencia_ccai_cn.

([340]) Article 4, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

([341]) Article 55-J, point XI, loi nº 13.709 du 14 août 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) — loi générale sur la protection des données.

(218) Comme indiqué au considérant 9 de la présente décision, l'accès aux voies de recours est garanti pour les ressortissants brésiliens et les ressortissants de pays tiers, qu'ils se trouvent ou non sur le territoire national.

(219) Premièrement, les particuliers ont un droit «absolu» d'intenter une action en justice en ce qui concerne la protection de leurs droits. Conformément aux règles générales énoncées dans le code de procédure civile, pour intenter une action en justice, une personne n'est pas tenue de démontrer qu'elle a subi un préjudice (c'est-à-dire qu'elle n'est pas tenue de démontrer qu'elle peut faire l'objet d'une surveillance ou que ses données ont été traitées à des fins de sécurité nationale). La personne peut exercer ses droits au titre de *Habeas Data* en ce qui concerne les données traitées par les autorités de renseignement ([342]).

(220) Lorsqu'elles demandent réparation en justice, les personnes peuvent demander des dommages et intérêts. De la même manière qu'en ce qui concerne le traitement à des fins répressives, la Constitution fédérale et le Code de procédure civile fournissent les bases juridiques permettant de demander réparation du préjudice moral ou matériel causé par l'autorité publique qui a illégalement collecté ou utilisé des données, y compris au moyen d'actions collectives ([343]).

(221) Deuxièmement, la Cour suprême fédérale a confirmé l'application partielle de la LGPD aux finalités de sécurité nationale et, par extension, le pouvoir de l'ANPD de traiter les plaintes relatives au traitement de données à caractère personnel par les autorités publiques à des fins de sécurité nationale ([344]). Dans le même arrêt, la Cour a relevé que «le traitement de données à caractère personnel effectué par des organismes publics en violation des paramètres juridiques et constitutionnels entraînera la responsabilité civile de l'État pour les dommages subis par les particuliers», conformément à l'article 42 de la LGPD ([345]).

(222) Troisièmement, la CCAI peut recevoir et enquêter sur des plaintes concernant des violations des droits fondamentaux et des garanties fondamentales commises par des organismes et entités publics menant des activités de renseignement et de contre-espionnage par tout citoyen, parti politique ou association ([346]). Sur cette base, la CCAI peut mener des contrôles ou des enquêtes. La CCAI prévoit donc une voie de recours administratif supplémentaire en cas de violation des droits liés au traitement des données à des fins de sécurité nationale. Les plaintes reçues par la CCAI peuvent ensuite être transmises aux tribunaux.

(223) Les différents recours juridictionnels disponibles dans le cadre du régime brésilien permettent aux particuliers d'obtenir réparation. En particulier, les particuliers peuvent contester la légalité des actes des autorités publiques et des services de renseignement. En outre, ils peuvent obtenir réparation du préjudice subi.

4. **CONCLUSION**

(224) La Commission considère que la République fédérative du Brésil, grâce à la LGPD, assure un niveau de protection des données à caractère personnel transférées depuis l'Union européenne essentiellement équivalent à celui garanti par le règlement (UE) 2016/679.

(225) De plus, la Commission estime que, pris dans leur ensemble, les mécanismes de surveillance et les voies de recours prévus dans le droit brésilien permettent de repérer et de sanctionner en pratique les éventuelles infractions commises par des responsables du traitement et des sous-traitants au Brésil et offrent aux personnes concernées des voies de droit leur permettant d'avoir accès aux données à caractère personnel les concernant et, in fine, d'obtenir leur rectification ou leur effacement.

([342]) Voir le considérant 9 de la présente décision.

([343]) Voir, par exemple, l'article 43 de la loi n° 10.408 du 10 janvier 2002. Code de procédure civile. Disponible à l'adresse suivante: https://www.planalto.gov.br//ccivil_03/leis/2002/l10406compilada.htm et article 1er, loi n° 7.397 du 24 juillet 1985, loi sur la responsabilité civile. Disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/leis/l7347orig.htm.

([344]) Voir les considérants 31 et 162 de la présente décision et la décision de la Cour suprême fédérale sur l'ADI 6649 du 15 septembre 2022. Disponible à l'adresse suivante: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([345]) Cour suprême fédérale, décision sur l'ADI 6649 du 15 septembre 2022, point 8. Disponible à l'adresse suivante: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false.

([346]) Article 3, point XI, résolution n° 2 de 2021-CN sur la Comissão mista de Controle da Atividade de Inteligência (CCAI).

(226) Enfin, sur la base des informations disponibles concernant l'ordre juridique brésilien, la Commission considère que toute atteinte aux droits fondamentaux des particuliers dont les données à caractère personnel sont transférées de l'Union européenne vers le Brésil par des autorités publiques brésiliennes pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale, sera limitée à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridique effective contre les atteintes de cette nature.

(227) Par conséquent, à la lumière des constatations de la présente décision, il convient de décider que le Brésil assure un niveau de protection adéquat, au sens de l'article 45 du règlement (UE) 2016/679, interprété à la lumière de la Charte des droits fondamentaux de l'Union européenne, des données à caractère personnel transférées de l'Union européenne aux responsables du traitement et aux sous-traitants au Brésil soumis à la LGPD.

5. EFFETS DE LA PRÉSENTE DÉCISION ET ACTION DES AUTORITÉS CHARGÉES DE LA PROTECTION DES DONNÉES

(228) Les États membres et leurs organes sont tenus de prendre les mesures nécessaires pour se conformer aux actes des institutions de l'Union, car ces derniers jouissent d'une présomption de légalité et produisent, dès lors, des effets juridiques aussi longtemps qu'ils n'ont pas été retirés, annulés à la suite d'un recours en annulation ou déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité.

(229) En conséquence, une décision d'adéquation de la Commission adoptée en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 a un caractère contraignant pour tous les organes des États membres destinataires, y compris leurs autorités de surveillance indépendantes. En particulier, les transferts d'un responsable du traitement ou d'un sous-traitant situé dans l'Union européenne à des responsables du traitement ou des sous-traitants situés au Brésil peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autorisation supplémentaire.

(230) Il convient de rappeler que, comme prévu à l'article 58, paragraphe 5, du règlement (UE) 2016/679 et ainsi que la Cour de justice l'a expliqué dans l'arrêt Schrems I, lorsqu'une autorité nationale chargée de la protection des données met en cause, notamment après avoir été saisie d'une plainte, la compatibilité d'une décision d'adéquation de la Commission avec la protection des droits fondamentaux que constituent le respect de la vie privée et la protection des données, le droit national doit prévoir des voies de recours lui permettant de faire valoir ces griefs devant les juridictions nationales, qui, en cas de doute, doivent surseoir à statuer et procéder à un renvoi préjudiciel devant la Cour de justice ([347]).

6. SUIVI, SUSPENSION, ABROGATION OU MODIFICATION DE LA PRÉSENTE DÉCISION

(231) Conformément à la jurisprudence de la Cour de justice ([348]), et comme consacré par l'article 45, paragraphe 4, du règlement (UE) 2016/679, la Commission devrait suivre, de manière permanente, les évolutions dans le pays tiers après l'adoption d'une décision d'adéquation, afin de déterminer si le pays tiers continue de garantir un niveau de protection essentiellement équivalent. Une telle vérification s'impose, en tout état de cause, lorsque la Commission reçoit des informations faisant naître un doute justifié à cet égard.

(232) Par conséquent, la Commission devrait surveiller de manière permanente la situation au Brésil en ce qui concerne le cadre juridique et la pratique proprement dite de traitement des données à caractère personnel tels qu'évalués dans la présente décision. À cet égard, elle devrait accorder une attention particulière à l'application pratique des exigences en matière d'analyse d'impact relative à la protection des données; aux exigences de transparence et à leur éventuelle limitation en ce qui concerne les droits à l'information et à l'accès; aux règles relatives à la notification des violations de données; au régime de sanctions ainsi qu'au respect des limitations et garanties en ce qui concerne l'accès des pouvoirs publics, en tenant compte de toute évolution pertinente en la matière.

([347]) Arrêt Schrems I, point 65: «À cet égard, il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision.»

([348]) Arrêt Schrems I, point 76.

(233) Pour faciliter ce processus de suivi, il est attendu des autorités brésiliennes, dont l'ANPD, qu'elles informent la Commission de toute évolution importante en rapport avec la présente décision, concernant tant le traitement des données à caractère personnel par les opérateurs économiques et les autorités publiques que les limitations et garanties applicables à l'accès des autorités publiques aux données à caractère personnel.

(234) En outre, afin de permettre à la Commission d'accomplir efficacement sa mission de suivi, les États membres devraient l'informer de toute mesure pertinente prise par les autorités nationales chargées de la protection des données, en particulier en ce qui concerne les questions ou les plaintes des personnes concernées de l'UE au sujet du transfert de leurs données à caractère personnel de l'Union européenne vers des responsables du traitement et des sous-traitants au Brésil. La Commission devrait également être informée de tout élément indiquant que les actions des autorités brésiliennes responsables de la prévention, de la détection, des enquêtes et des poursuites en matière d'infractions pénales, ou de la sécurité nationale, y compris de tout organisme de surveillance, n'assurent pas le niveau de protection requis.

(235) En application de l'article 45, paragraphe 3, du règlement (UE) 2016/679 ([349]), et au regard du fait que le niveau de protection assuré par l'ordre juridique du Brésil est susceptible d'évoluer, la Commission, après l'adoption de la présente décision, devrait vérifier de manière périodique si les conclusions relatives au niveau adéquat de la protection assurée par le Brésil sont toujours justifiées en fait et en droit.

(236) À cette fin, la présente décision devrait faire l'objet d'un premier examen dans un délai de quatre ans après son entrée en vigueur. Des réexamens périodiques ultérieurs devraient avoir lieu au moins une fois tous les quatre ans ([350]). Les réexamens devraient porter sur tous les aspects du fonctionnement de la présente décision, y compris la coopération de l'ANPD avec les autorités de l'UE chargées de la protection des données concernant les plaintes émanant de particuliers. Il devrait également englober l'efficacité de la surveillance et du contrôle du respect des règles applicables et dans le domaine de la répression et de la sécurité nationale.

(237) En vue de la réalisation de cet examen, la Commission devrait rencontrer la ANPD, accompagnée, le cas échéant, d'autres autorités brésiliennes responsables de l'accès des pouvoirs publics aux données, y compris les organismes de surveillance concernés. La participation à cette réunion devrait être ouverte aux représentants des membres du comité européen de la protection des données. Dans le cadre de l'examen, la Commission devrait demander à la ANPD de fournir des informations exhaustives sur tous les aspects pertinents pour le constat d'adéquation, y compris sur les limitations et les garanties en ce qui concerne l'accès des pouvoirs publics aux données. La Commission devrait également demander des explications sur toute information reçue présentant de l'intérêt pour la présente décision, notamment des rapports publics établis par les autorités brésiliennes ou d'autres parties prenantes au Brésil, par le comité européen de la protection des données, par diverses autorités de protection des données, par des groupes de la société civile, ainsi que des informations relayées par les médias ou toute autre source d'informations disponible.

(238) Sur la base de l'examen, la Commission devrait élaborer un rapport public qui sera présenté au Parlement européen et au Conseil.

(239) Lorsque des informations disponibles, en particulier les informations résultant du suivi de la présente décision ou fournies par les autorités brésiliennes ou des États membres, révèlent que le niveau de protection assuré par le Brésil pourrait ne plus être adéquat, la Commission devrait en informer les autorités compétentes du Brésil et demander que des mesures appropriées soient prises dans un délai raisonnable bien défini.

(240) Si, à l'expiration de la période précisée, les autorités brésiliennes compétentes n'ont pas pris ces mesures ou échouent à démontrer de manière satisfaisante que la présente décision reste fondée sur un niveau de protection adéquat, la Commission lancera la procédure visée à l'article 93, paragraphe 2, du règlement (UE) 2016/679 en vue de la suspension partielle ou complète ou de l'abrogation de la présente décision.

(241) À défaut, la Commission lancera cette procédure visant à modifier la présente décision, notamment en soumettant les transferts de données à des conditions supplémentaires ou en limitant le constat d'adéquation aux seuls transferts de données pour lesquels un niveau de protection adéquat continue à être garanti.

([349]) Conformément à l'article 45, paragraphe 3, du règlement (UE) 2016/679, «[l]'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale».

([350]) L'article 45, paragraphe 3, du règlement (UE) 2016/679 dispose qu'un examen périodique doit avoir lieu «au moins tous les quatre ans». Voir également comité européen de la protection des données, Critères de référence pour l'adéquation, WP 254 rév. 01.

(242) La Commission devrait également envisager de lancer la procédure conduisant à la modification, à la suspension ou à l'abrogation de la présente décision si, dans le contexte ou non de l'examen, les autorités brésiliennes compétentes ne fournissent pas les informations ou les clarifications nécessaires pour apprécier le niveau de protection conféré aux données à caractère personnel transférées de l'Union européenne vers le Brésil, ou concernant le respect de la présente décision. À cet égard, la Commission devrait prendre en compte la mesure dans laquelle les informations concernées peuvent être obtenues auprès d'autres sources.

(243) Pour des raisons d'urgence impérieuse dûment justifiées, la Commission aura recours à la possibilité d'adopter, conformément à la procédure visée à l'article 93, paragraphe 3, du règlement (UE) 2016/679, des actes d'exécution immédiatement applicables suspendant, abrogeant ou modifiant la décision.

7. **CONSIDÉRATIONS FINALES**

(244) Le comité européen de la protection des données a publié son avis ([351]), dont il a été tenu compte dans l'élaboration de la présente décision.

(245) Les mesures prévues dans la présente décision sont conformes à l'avis du comité institué par l'article 93, paragraphe 1, du règlement (UE) 2016/679,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Aux fins de l'article 45 du règlement (UE) 2016/679, le Brésil garantit un niveau de protection adéquat des données à caractère personnel transférées depuis l'Union européenne vers les responsables du traitement et les sous-traitants au Brésil soumis à la loi générale sur la protection des données (LGPD).

Article 2

Lorsque, afin de protéger les personnes à l'égard du traitement de leurs données à caractère personnel, les autorités compétentes des États membres exercent les pouvoirs que leur confère l'article 58 du règlement (UE) 2016/679 concernant les transferts de données relevant du champ d'application défini à l'article 1er, l'État membre concerné en informe la Commission sans délai.

Article 3

1. La Commission suit de manière permanente l'application du cadre juridique sur lequel se fonde la présente décision dans le but de déterminer si le Brésil continue d'assurer un niveau de protection adéquat au sens de l'article 1er.

2. Les États membres et la Commission s'informent mutuellement des cas dans lesquels l'autorité brésilienne de protection des données (Agência Nacional de Proteção de Dados — ANPD), ou toute autre autorité brésilienne compétente, échoue à faire respecter le cadre juridique sur lequel se fonde la présente décision.

3. Les États membres et la Commission s'informent mutuellement de tout élément indiquant que les atteintes au droit des personnes à la protection de leurs données à caractère personnel commises par des autorités publiques brésiliennes vont au-delà de ce qui est strictement nécessaire ou qu'il n'existe pas de protection juridique effective contre les atteintes de cette nature.

4. Dans un délai de quatre ans à compter de la date de notification de la présente décision aux États membres, et ensuite au moins une fois tous les quatre ans, la Commission évalue le constat établi à l'article 1er, sur la base de toutes les informations disponibles, notamment les informations reçues dans le cadre de l'examen conjoint réalisé avec les autorités brésiliennes concernées.

([351]) Comité européen de la protection des données, avis sur une décision d'adéquation concernant le Brésil, novembre 2025. Disponible à l'adresse suivante: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-282025-regarding-european-commission-draft_en.

5. Lorsqu'elle est en possession d'éléments indiquant qu'un niveau de protection adéquat n'est plus assuré, la Commission en informe les autorités brésiliennes compétentes et peut suspendre, abroger ou modifier la présente décision.

6. La Commission peut également suspendre, abroger ou modifier la présente décision si le défaut de coopération de la part des autorités brésiliennes l'empêche de déterminer si le constat établi à l'article 1er de la présente décision est affecté.

Article 4

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 26 janvier 2026.

Par la Commission
Michael McGRATH
Membre de la Commission