



Avis 28/2025 relatif au projet de décision d'exécution de la Commission européenne constatant, conformément au règlement (UE) 2016/679, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Brésil

Version 1.0

Adopté le 4 novembre 2025

Translations proofread by EDPB Members.

This language version has not yet been proofread.

ADOPTÉ

Synthèse

Le 5 septembre 2025, la Commission européenne a entamé le processus d'adoption de son projet de décision d'exécution (ci-après le «projet de décision») constatant le caractère adéquat du niveau de protection des données à caractère personnel assuré par la République fédérative du Brésil (ci-après le «Brésil»).

Le 5 septembre 2025, la Commission européenne a demandé l'avis du comité européen de la protection des données (ci-après l'«EDPB»). Celui-ci a évalué le caractère adéquat du niveau de protection assuré par le Brésil sur la base de l'examen du projet de décision même ainsi que d'une analyse des documents accessibles au public sur les sites web officiels des autorités brésiliennes.

L'EDPB s'est concentré sur l'évaluation à la fois des aspects généraux du projet de décision liés au RGPD et de l'accès des autorités publiques aux données à caractère personnel transférées depuis l'EEE à des fins répressives et de sécurité nationale, y compris aux fins des voies de droit à la disposition des particuliers dans l'EEE. L'EDPB a également examiné si les garanties prévues par le cadre juridique au Brésil étaient en place et efficaces.

L'EDPB a utilisé comme principale référence pour ces travaux les critères de référence pour l'adéquation adoptés le 28 novembre 2017 par le groupe de travail «Article 29»², tels que révisés en dernier lieu et adoptés le 6 février 2018 par l'EDPB (ci-après les «critères de référence pour l'adéquation») ainsi que les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance.

L'EDPB constate avec satisfaction que le cadre de protection des données, en particulier la loi générale sur la protection des données au Brésil (ci-après la «LGPD»), ainsi que les décrets présidentiels et les règlements contraignants adoptés par l'autorité brésilienne de protection des données (l'Agencia Nacional de Proteção de Dados, ci-après l'«ANPD»), établissent des exigences (y compris en ce qui concerne les principes, les droits des personnes concernées, les transferts, le contrôle et les recours) qui sont étroitement alignées sur le RGPD et la jurisprudence de la Cour de justice de l'Union européenne (ci-après la «Cour»).

L'EDPB a également conclu que la Commission européenne devrait clarifier dans son projet de décision certains aspects du cadre juridique brésilien et suivre de près son évolution.

Pour ce qui est du principe de responsabilité et des exigences ayant trait à l'analyse d'impact relative à la protection des données (ci-après l'«AIPD»), l'EDPB estime qu'il est important qu'elle doive obligatoirement être menée dans les cas où le traitement pourrait entraîner un risque élevé pour les droits et libertés des personnes physiques et qu'elle

¹ 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.

² Groupe de travail «Article 29», WP 254 rev.01, adoptés le 28 novembre 2017 et tels que révisés en dernier lieu et adoptés le 6 février 2018, approuvés par le comité européen de la protection des données.

couvre l'évaluation de la nécessité et de la proportionnalité du traitement. Dès lors, l'EDPB invite la Commission européenne à surveiller la mise en œuvre pratique de ces exigences.

La LGPD prévoit une limitation de la fourniture d'informations aux personnes concernées ou à l'autorité de contrôle sur la base du «secret commercial et industriel» dans certains cas. Compte tenu de l'importance des obligations de transparence pour que les personnes concernées aient la possibilité de contrôler la manière dont leurs données sont traitées, ainsi que de l'importance des obligations de coopérer avec l'autorité de contrôle, en particulier pour fournir les informations nécessaires à ses missions de contrôle, l'EDPB invite la Commission européenne à surveiller la mise en œuvre de ces limitations dans la pratique afin de mieux comprendre leur incidence sur le droit à l'information et le droit d'accès, ainsi que, le cas échéant, sur les pouvoirs de l'ANPD.

Quant aux règles relatives au transfert ultérieur, l'EDPB invite la Commission européenne à préciser, dans le projet de décision, si les transferts ne peuvent être effectués dans des conditions équivalentes à celles de l'article 49 du RGPD que dans des circonstances exceptionnelles où d'autres instruments de transfert ne peuvent être utilisés. La Commission est également invitée à préciser si les personnes concernées sont informées des risques éventuels liés au transfert lorsque celui-ci repose sur leur consentement et des circonstances du transfert (durée et finalité du transfert, pays de destination, responsabilités des parties concernées, droits des personnes concernées et moyens de les exercer), quel que soit l'outil de transfert utilisé.

Par ailleurs, l'EDPB invite la Commission européenne à donner davantage d'informations sur les tâches du Conseil national pour la protection des données à caractère personnel et de la vie privée ainsi que sur son interaction avec l'ANPD.

En ce qui concerne l'accès des autorités publiques brésiliennes aux données à caractère personnel transférées aux responsables du traitement et aux sous-traitants au Brésil à des fins d'application du droit pénal et de sécurité nationale et l'utilisation de ces données par ces autorités (ci-après l'«accès des pouvoirs publics»), l'EDPB observe que la LGPD ne s'applique pas au traitement de données effectué aux fins *exclusives* de la sécurité publique, de la défense nationale, de la sûreté de l'État ou des enquêtes sur les infractions pénales et des poursuites en la matière. Dans le même temps, l'EDPB relève avec satisfaction que la Cour suprême fédérale du Brésil a, dans sa jurisprudence, interprété la LGPD d'une manière qui élargit son applicabilité partielle au traitement des données à caractère personnel à des fins d'enquêtes pénales et de maintien de l'ordre public.

À la lumière de ce qui précède, il invite la Commission à évaluer plus avant et à clarifier, dans le projet de décision, l'applicabilité de la LGPD en cas de traitement de données à caractère personnel à des fins d'application du droit pénal, y compris les pouvoirs d'enquête et d'adopter des mesures correctrices de l'ANPD à l'égard des autorités répressives, ainsi qu'à prendre soigneusement en considération toute évolution pertinente à cet égard dans le cadre de son obligation de surveillance.

Conscient du fait que les États disposent d'une large marge d'appréciation dans la définition des questions de sécurité nationale, qui permet ensuite des exemptions en matière de sécurité nationale concernant le traitement des données à caractère personnel, l'EDPB invite la Commission à décrire et à expliquer plus précisément, dans le projet de décision, les grandes lignes de la notion de sécurité nationale en droit brésilien. À cet égard, l'EDPB invite la Commission à préciser davantage la manière dont les exemptions de la LGPD à des fins de sécurité nationale sont liées à la collecte et au partage de données entre les entités publiques au sein du système de renseignement brésilien (SISBIN).

Table des matières

1. INTRODUCTION	5
2. ASPECTS GÉNÉRAUX DE LA PROTECTION DES DONNÉES.....	7
2.1 Responsabilité et gouvernance des données.....	7
2.2 Champ d'application et définitions.....	8
2.2.1 Champ d'application matériel et territorial de la LGPD.....	8
2.2.2 Définitions	9
2.3 Principes et bases juridiques en matière de protection des données	9
2.3.1 Principes du traitement	9
2.3.2 Mesures de sécurité et violations.....	11
2.3.3 Licéité du traitement.....	12
2.4 Droits individuels	13
2.5 Limitations concernant les transferts ultérieurs	13
2.6 Mécanismes en matière de procédure et d'application	16
2.6.1 Contrôle indépendant.....	16
2.6.2 Recours.....	17
2.6.3 Sanctions	18
3. ACCÈS ET UTILISATION PAR LES AUTORITÉS PUBLIQUES AU BRÉSIL DES DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES À PARTIR DE L'UNION EUROPÉENNE.....	19
3.1 Accès aux données et utilisation de celles-ci par les autorités publiques brésiliennes à des fins d'application du droit pénal	20
3.1.1 Cadre juridique dans les domaines de l'application du droit pénal	20
3.1.2 Nécessité et proportionnalité	21
3.1.3 Utilisation ultérieure des données et transferts ultérieurs	23
3.1.4 Contrôle et recours	24
3.2 Accès aux données et utilisation de celles-ci par les autorités publiques brésiliennes à des fins de sécurité nationale	26

3.2.1 Champ d'application de l'exemption prévue à l'article 4, point III, de la LGPD et applicabilité de celle-ci aux infractions pénales portant atteinte à la sûreté de l'État ²⁶	
3.2.2 Cadre juridique pour la sécurité nationale	27
3.2.3 Transferts ultérieurs et accords internationaux.....	29
3.2.4 Contrôle et recours	30
4. MISE EN ŒUVRE ET SUIVI DU PROJET DE DÉCISION	31

Le comité européen de la protection des données,

vu l'article 70, paragraphe 1, point s), du 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 (ci-après le «RGPD»),

vu l'accord sur l'Espace économique européen (EEE), et notamment son annexe XI et son protocole 37, tels que modifiés par la décision n° 154/2018 du Comité mixte de l'EEE du 6 juillet 2018³,

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTE L'AVIS SUIVANT:

³ Dans le présent avis, on entend par «États membres» les États membres de l'EEE.

1. INTRODUCTION

- (1) Le chapitre V du RGPD définit les conditions applicables aux transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale. Les transferts de données à caractère personnel peuvent être effectués sur le fondement d'une décision d'adéquation de la Commission européenne (article 45 du RGPD) ou, en l'absence d'une telle décision, lorsque le responsable du traitement ou le sous-traitant fournit des garanties appropriées, y compris des droits opposables et des voies de droit pour la personne concernée (article 46 du RGPD). En l'absence de décision d'adéquation ou de garanties appropriées, un transfert ou un ensemble de transferts vers un pays tiers ou à une organisation internationale n'a lieu que sous certaines conditions (article 49 du RGPD).
- (2) L'EDPB rappelle que les décisions d'adéquation reconnaissent la protection continue des données à caractère personnel transférées de l'EEE vers des pays tiers ou à des organisations internationales et constituent un outil de transfert solide pour garantir que les droits de la personne concernée sont protégés lorsque des données sont transférées en dehors de l'EEE. Selon les critères de référence pour l'adéquation⁴ et la jurisprudence pertinente de la Cour⁵, bien que le pays tiers ne soit pas tenu de garantir un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union, l'expression «niveau de protection adéquat» figurant à l'article 45, paragraphe 1, du RGPD doit être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et des droits fondamentaux essentiellement équivalent à celui garanti au sein de l'Union, à la lumière de la charte des droits fondamentaux.
- (3) 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»)⁶. Les États brésiliens ont également leur propre constitution, qui ne doit pas aller à l'encontre de la Constitution fédérale. Le respect de la vie privée et la protection des données sont protégés par la Constitution en tant que droits fondamentaux (article 5, points X, XII et LXXIX, de la Constitution)⁷ et reconnus par la Cour constitutionnelle à toute personne, y compris aux étrangers, que la personne réside ou non au Brésil⁸.
- (4) Le principal acte législatif régissant la protection des données est la loi générale sur la protection des données ou «Lei Geral de Proteção de Dados» (ci-après la «LGPD») (n° 13.709 du 14 août 2018, modifiée en dernier lieu par la loi n° 14.460 du 25 octobre 2022).

⁴ Groupe de travail «Article 29», WP 254 rev.01, adoptés le 28 novembre 2017 et tels que révisés en dernier lieu et adoptés le 6 février 2018, approuvés par l'EDPB, chapitre 3, point C.

⁵ Arrêts de la Cour du 6 octobre 2015 dans l'affaire C-362/14, Maximilian Schrems/Data Protection Commissioner (ci-après l'«arrêt Schrems»), et du Tribunal du 3 septembre 2025 dans l'affaire T-553/23, Philippe Latombe/Commission européenne (ci-après l'«arrêt Latombe»).

⁶ Voir considérant 7 du projet de décision.

⁷ Voir considérant 8 du projet de décision.

⁸ Voir considérant 9 du projet de décision.

La LGPD est complétée par les décrets contraignants (décret présidentiel n° 10.474 du 26 août 2020 et décret présidentiel n° 11.758 du 30 octobre 2023), qui sont juridiquement contraignants et exécutoires⁹.

- (5) Outre la LGPD, le cadre brésilien de protection des données comprend les règlements contraignants adoptés par l'autorité brésilienne de protection des données (l'Agencia Nacional de Proteção de Dados, ci-après l'«ANPD»)¹⁰. Ces règlements prévoient des règles supplémentaires relatives à l'interprétation et à l'application de la LGPD¹¹. Citons, par exemple, le règlement n° 4 du 24 février 2024 relatif à l'application de sanctions administratives, le règlement n° 15 du 24 avril 2024 sur la notification des incidents de sécurité (ci-après le «règlement sur les notifications des incidents de sécurité»), le règlement n° 19 du 23 août 2024 sur le transfert international de données à caractère personnel (ci-après le «règlement sur le transfert de données»), le règlement n° 2 du 27 janvier 2022 relatif à l'application de la LGPD aux petites et moyennes entreprises et le règlement n° 18 du 15 juillet 2024 sur le rôle du délégué à la protection des données (ci-après le «règlement sur le DPD»).
- (6) L'EDPB se félicite de la reconnaissance constitutionnelle des droits au respect de la vie privée et à la protection des données en tant que droits fondamentaux, qui sont ensuite mis en œuvre par le droit national. En outre, il constate avec satisfaction les engagements internationaux pris par le Brésil¹².
- (7) L'EDPB fait observer que, conformément aux articles 47 et 94 du règlement (UE) 2018/1725, les institutions, organes et organismes de l'Union européenne¹³ peuvent transférer des données à caractère personnel vers un pays tiers, un territoire, un secteur ou une organisation internationale reconnu par la Commission européenne en vertu de l'article 45, paragraphe 3, du règlement (UE) 2016/679 comme assurant un niveau de protection adéquat, pour autant que le transfert serve exclusivement à permettre des missions qui relèvent de la compétence du responsable du traitement, sans qu'aucune autre autorisation ne soit nécessaire. L'EDPB invite la Commission européenne à rappeler cette possibilité juridique dans les considérants du projet de décision.

⁹ Voir considérants 11 et 12 du projet de décision.

¹⁰ Tous les règlements contraignants adoptés par l'ANPD sont disponibles à l'adresse suivante: https://www.gov.br/anpd/pt-br/aceso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd.

¹¹ Voir considérant 13 du projet de décision.

¹² Voir considérants 8 à 10 du projet de décision.

¹³ Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE (RPDUE) (JO L 295 du 21.11.2018, p. 39).

2. ASPECTS GÉNÉRAUX DE LA PROTECTION DES DONNÉES

2.1 Responsabilité et gouvernance des données

- (8) Selon la LGPD, le principe de responsabilité est l'un des principes généraux applicables au traitement des données à caractère personnel. Elle prévoit que les responsables du traitement et les sous-traitants¹⁴ doivent adopter des mesures techniques et organisationnelles appropriées pour se conformer effectivement à leurs obligations en matière de protection des données et doivent être en mesure de démontrer cette conformité, notamment à l'autorité de contrôle compétente (article 46 de la LGPD). L'EDPB fait observer que ces mesures comprennent la désignation d'un délégué à la protection des données (article 41 de la LGPD), telle que détaillée plus avant dans le règlement sur le DPD de l'ANPD; l'analyse d'impact relative à la protection des données (article 38 de la LGPD), ainsi que la tenue de registres des activités de traitement des données (article 37 de la LGPD). Par ailleurs, la LGPD indique que les responsables du traitement et les sous-traitants peuvent formuler des règles internes concernant les bonnes pratiques et les modèles de gouvernance, y compris des plans pour des activités éducatives, un mécanisme de contrôle interne et l'atténuation des risques (article 50 de la LGPD). L'EDPB constate avec satisfaction que ces instruments sont semblables à ceux prévus dans le RGPD pour mettre en œuvre le principe de responsabilité et se félicite de cet étroit alignement.
- (9) L'EDPB relève qu'en ce qui concerne l'AIPD, la LGPD ne prévoit pas d'obligation claire de procéder à l'AIPD dans les cas où le traitement pourrait entraîner un risque élevé pour les droits et libertés des personnes physiques, pour lesquels elle ne mentionne que l'éventuelle demande de l'ANPD. À cet égard, l'EDPB relève que l'ANPD recommande dans la «foire aux questions»¹⁵ relative à l'AIPD de réaliser une AIPD lorsque l'opération de traitement est susceptible d'entraîner un risque élevé. De plus, la LGPD n'inclut pas expressément l'appréciation de la nécessité et de la proportionnalité dans le champ d'application de l'AIPD. Toutefois, dans la foire aux questions précitée, il est recommandé aux responsables du traitement et aux sous-traitants d'apprécier dans leurs AIPD la nécessité et la proportionnalité du traitement.
- (10) Dans ce contexte, l'EDPB invite la Commission européenne à surveiller la mise en œuvre pratique de ces exigences afin de vérifier qu'une AIPD est réalisée lorsque l'opération de traitement peut entraîner un risque élevé pour les droits et libertés des personnes physiques

¹⁴ Les agents responsables du traitement, selon l'article 5, point IX, de la LGPD.

¹⁵ https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

et qu'une appréciation de la nécessité et de la proportionnalité des opérations de traitement par rapport aux finalités est également incluse dans les AIPD.

2.2 Champ d'application et définitions

- (11) Le chapitre 3 des critères de référence pour l'adéquation est consacré aux «Principes touchant au contenu» et fait référence aux notions et principes fondamentaux en matière de protection des données. Le système d'un pays tiers ou d'une organisation internationale doit contenir ces notions et principes fondamentaux afin d'assurer un niveau de protection des données à caractère personnel essentiellement équivalent à celui garanti par le droit de l'Union. Ceux-ci ne doivent pas refléter la terminologie du RGPD, mais ils devraient refléter les notions consacrées par la législation de l'Union européenne en matière de protection des données et être cohérents avec ces notions. Les critères de référence pour l'adéquation font référence aux notions importantes suivantes: «données à caractère personnel», «traitement», «responsables du traitement», «sous-traitant», «destinataire» et «données sensibles». Cet aspect du droit brésilien sera commenté dans les paragraphes suivants.

2.2.1 Champ d'application matériel et territorial de la LGPD

- (12) L'EDPB se réjouit que le champ d'application, tant matériel que territorial, de la LGPD soit très semblable à celui prévu par le cadre de protection des données de l'Union européenne.
- (13) L'article 4 de la LGPD exclut de son champ d'application le traitement à des fins purement personnelles et non économiques, et des exceptions de ce type sont également envisagées dans le RGPD [article 2, paragraphe 2, point c), du RGPD]. En outre, certaines autres opérations de traitement ne relèvent en partie pas du champ d'application de la LGPD, notamment le traitement à des fins: de sécurité publique, de défense nationale, de sûreté de l'État ou d'enquêtes sur les infractions pénales et de poursuites en la matière; journalistiques et artistiques; de recherche universitaire; et de recherche dans le domaine de la santé (article 3, point III, de la LGPD). Ce point est expliqué plus en détail dans la section 3.1 du présent avis.
- (14) En ce qui concerne plus particulièrement l'application partielle de la LGPD au traitement de données à caractère personnel effectué à des fins journalistiques et artistiques, l'EDPB observe que la portée de l'exception est équivalente à celle prévue à l'article 85, paragraphe 2, du RGPD¹⁶, c'est-à-dire que cette exception ne s'applique que lorsque les données à caractère personnel sont traitées exclusivement à cette fin; tous les autres traitements effectués par la presse, les médias et les organismes artistiques relèvent du champ d'application de la LGPD. En outre, certaines exceptions envisagées pour le traitement des données à caractère personnel exclusivement à des fins universitaires, à savoir les articles 7 (exigences concernant la base juridique) et 11 (règles relatives au traitement des

¹⁶ Voir aussi considérant 35 du projet de décision.

données sensibles) de la LGPD, restent applicables¹⁷. Le champ d'application de ces exceptions est également conforme à celui défini à l'article 85, paragraphe 2, du RGPD.

2.2.2 Définitions

- (15) L'EDPB constate avec satisfaction l'alignement sur le cadre de protection des données de l'Union en ce qui concerne les définitions utilisées dans la LGPD, qui sont cohérentes avec celles envisagées dans le RGPD. En particulier, la LGPD définit les «données à caractère personnel», les «informations pseudonymes», les «données anonymes»¹⁸, le «traitement des données», le «responsable du traitement», le «sous-traitant» et les «données sensibles» (article 5 de la LGPD) de manière semblable aux définitions prévues par le RGPD, en son considérant 26, son article 4 et son article 9, paragraphe 1. D'autres définitions, par exemple celles de la «personne concernée», du «délégué à la protection des données», du «consentement», de l'«analyse d'impact relative à la protection des données» et de la notion de «responsabilité conjointe du traitement»¹⁹, sont, elles aussi, essentiellement équivalentes aux notions prévues dans le RGPD.

2.3 Principes et bases juridiques en matière de protection des données

2.3.1 Principes du traitement

- (16) Les critères de référence pour l'adéquation établissent, conformément au RGPD, que les données doivent être traitées de manière licite, loyale et légitime. Conformément à l'article 6 de la LGPD, les activités de traitement des données à caractère personnel doivent être effectuées de bonne foi et soumises aux principes suivants: finalité, adéquation, nécessité, libre accès²⁰, qualité des données, transparence, sécurité, prévention, non-discrimination et responsabilité.
- (17) Compte tenu des notions de ces principes, le système juridique brésilien consacre les mêmes principes de traitement des données que ceux énoncés à l'article 5 du RGPD. Par exemple, en ce qui concerne la limitation de la finalité, la LGPD prévoit, en son article 7, paragraphe 7, que «le traitement ultérieur des données à caractère personnel visées aux paragraphes 3 (données à caractère personnel accessibles au public) et 4 (données manifestement rendues publiques par la personne concernée) du présent article peut être effectué à de nouvelles fins,

¹⁷ Voir aussi considérants 32 et 33 du projet de décision.

¹⁸ L'article 12 de la LGPD précise que les données anonymisées ne sont pas considérées comme étant des données à caractère personnel, sauf lorsque l'anonymisation a été ou peut être annulée par des efforts raisonnables. Cet article explique que l'adjectif «raisonnable» doit être considéré en tenant compte de facteurs objectifs tels que: 1) le coût et le temps nécessaires à l'annulation, 2) la technologie disponible et 3) l'utilisation exclusive des moyens propres d'un responsable du traitement.

¹⁹ Voir article 42, paragraphe 1, point I, de la LGPD.

²⁰ «Libre accès: garantie aux personnes concernées d'une consultation facilitée et gratuite concernant la forme et la durée du traitement, ainsi que l'intégrité de leurs données à caractère personnel» (article 6, point IV, de la LGPD).

pour autant que les finalités légitimes et spécifiques du nouveau traitement et la préservation des droits de la personne concernée soient respectées, de même que les motifs et principes énoncés dans la présente loi».

- (18) Le RGPD exige clairement qu'un tel traitement ultérieur n'ait lieu que si cette nouvelle finalité est compatible avec la finalité initiale. L'exigence de garantir la compatibilité des finalités (ainsi que le respect des normes éthiques et des garanties techniques et juridiques applicables) est mise en évidence dans le guide pour le traitement des données à caractère personnel à des fins universitaires et pour la réalisation d'études et de recherches publié par l'ANPD, ainsi que dans les lignes directrices sur l'intérêt légitime. L'ANPD explique, dans ses lignes directrices sur l'intérêt légitime, comment le responsable du traitement doit démontrer l'existence d'un lien effectif entre les deux finalités du traitement et tenir compte de la «confiance légitime» de la personne concernée. Ces lignes directrices précisent en outre que «[l']analyse de la confiance légitime peut reposer sur plusieurs facteurs, dont: d) la finalité prévue de la collecte des données et sa compatibilité avec le traitement sur la base de l'intérêt légitime». L'EDPB se réjouit de cette clarification apportée par l'ANPD, qui contribue à mieux aligner les exigences relatives à la limitation de la finalité.
- (19) Le principe de limitation de la conservation prévu par le RGPD dispose que les données ne doivent être conservées que pendant la durée nécessaire au regard des finalités pour lesquelles elles sont traitées [article 5, paragraphe 1, point e), du RGPD]. Même si l'article 6 de la LGPD n'inclut pas expressément le principe de limitation de la conservation, cet article doit être lu conjointement avec l'article 15 de la LGPD, qui précise l'exigence en cas de cessation du traitement des données. Dans cet article, le principe de limitation de la conservation est clairement lié aux principes d'«adéquation» et de «nécessité», qui font partie des principes généraux énumérés à l'article 6 de la LGPD. Par souci de clarté, l'EDPB encourage la Commission européenne à clarifier, dans le projet de décision, l'interaction entre les articles 6 et 15 de la LGPD en ce qui concerne le principe de limitation de la conservation.
- (20) En outre, en ce qui concerne les exigences en matière de limitation de la conservation, l'article 16 de la LGPD fixe les conditions de conservation et d'effacement des données à caractère personnel après la fin du traitement. Cet article prévoit également quatre finalités pour lesquelles les données peuvent être conservées après la fin de leur traitement: 1) pour le respect d'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. L'EDPB indique que ces situations de traitement sont conformes au principe de limitation de la conservation inscrit dans le RGPD.
- (21) Le principe de transparence et d'équité vise à garantir que les personnes concernées ont le contrôle de leurs données à caractère personnel et, à cette fin, les informations doivent, en

règle générale, être fournies à la personne concernée de manière proactive²¹. Dans le même temps, la LGPD prévoit une limitation à ce principe en ce qui concerne le «secret commercial et industriel», ce qui peut avoir une incidence sur la réception par les personnes concernées des informations sur le traitement de leurs données afin de pouvoir exercer leur contrôle sur celui-ci (par exemple, par l'introduction d'une réclamation auprès de l'ANPD). Toutefois, dans son projet de décision, la Commission européenne explique que cette limitation doit être interprétée à la lumière de la loi brésilienne sur l'accès à l'information et du décret présidentiel n° 7.721 du 16 mai 2012 et «doit donc être interprétée de manière à ce que le traitement et toute autre divulgation d'informations ne révèlent pas de secret d'affaires ou ne créent pas d'avantage concurrentiel pour d'autres acteurs, tout en remplissant les objectifs de la 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 au titre du "secret commercial et industriel" ne doit pas être comprise comme un motif général de refus de respect de la loi, mais plutôt que des garanties spécifiques doivent être mises en place pour garantir la divulgation des informations d'une manière qui protège ces intérêts»²².

- (22) Compte tenu de l'importance du principe de transparence, l'EDPB invite la Commission européenne à surveiller la mise en œuvre de cette disposition dans la pratique afin de mieux comprendre son incidence sur le droit à l'information et le droit d'accès.

2.3.2 Mesures de sécurité et violations

- (23) La LGPD inclut les principes de sécurité et de prévention, qui exigent l'application de mesures de protection des données à caractère personnel et de prévention des dommages liés à leur traitement (article 6, points VII et VIII, de la LGPD). En outre, la LGPD indique expressément que lorsque les mesures de sécurité ne sont pas correctement mises en œuvre, le traitement des données est considéré comme étant illicite. La loi exige la mise en œuvre des mesures nécessaires pour démontrer le respect de ce principe par l'approche fondée sur les risques (articles 44, 46 et 47 de la LGPD) et le respect des exigences relatives à l'évaluation et à la notification des violations (articles 48 et 49 de la LGPD). L'EDPB constate avec satisfaction que ces principes et obligations sont étroitement alignés sur ceux énoncés dans le RGPD.
- (24) L'EDPB se félicite que l'ANPD ait adopté un règlement contraignant supplémentaire sur les notifications des incidents de sécurité, qui prévoit la notion d'incident et les modalités d'évaluation de sa gravité (par exemple, lorsque l'incident est considéré comme créant des risques pour les personnes concernées ou comme affectant de manière significative les intérêts et droits fondamentaux des personnes concernées et doit donc être communiqué à l'ANPD et à la personne concernée), ainsi que les exigences en matière de notification des incidents²³. À cet égard, l'EDPB fait observer que, conformément au règlement sur les notifications des incidents de sécurité, en règle générale, «la communication d'un incident de

²¹ Ce point est également souligné dans les critères de référence pour l'adéquation, voir chapitre 3, point A 7).

²² Voir considérant 81 du projet de décision.

²³ Voir considérants 73 à 77 du projet de décision.

sécurité à l'ANPD doit être effectuée par le responsable du traitement dans un délai de trois jours ouvrables»²⁴, et invite la Commission européenne à aligner son projet de décision (considérant 75) en conséquence²⁵.

- (25) Pour ce qui est de la notification des violations de données, l'EDPB relève que la LGPD indique que cette notification (tant à l'ANPD qu'à la personne concernée) doit inclure, entre autres, des informations sur les mesures techniques et de sécurité utilisées pour la protection des données à caractère personnel, adoptées avant et après l'incident, dans le respect des secrets commerciaux et industriels (article 6, point III, et article 9, point II, de la LGPD). L'EDPB comprend la nécessité de faire effectivement en sorte que le droit au respect de la vie privée et à la protection des données ne porte pas atteinte à la protection d'autres droits et invite la Commission à surveiller la mise en œuvre de cette limitation lorsque des informations sur l'incident ont été fournies partiellement (compte tenu des secrets commerciaux et industriels), et son incidence sur les pouvoirs de l'ANPD, le cas échéant.

2.3.3 Licéité du traitement

- (26) L'EDPB constate que le principe de légalité et sa mise en œuvre, tels que prévus dans la LGPD (articles 5, point XII, 7, 8 et 10), sont étroitement alignés sur le principe consacré dans le RGPD (article 4, point 11, et articles 6, 7 et 9), et se félicite de cet alignement.

2.3.3.1 Intérêt légitime

- (27) Les exigences relatives à l'intérêt légitime à utiliser comme base juridique du traitement prévues dans la LGPD (article 7, point IX) sont alignées sur le RGPD [article 6, paragraphe 1, point f)]. La LGPD souligne également que les libertés et les droits fondamentaux (qui comprennent le droit à la protection des données²⁶) doivent généralement prévaloir.
- (28) L'EDPB observe que l'article 10 de la LGPD énumère les finalités légitimes pour lesquelles cette base juridique pourrait être utilisée. L'une de ces finalités légitimes est de soutenir et de promouvoir l'activité du responsable du traitement (article 10, point I, de la LGPD).
- (29) Bien que cette expression semble large, l'EDPB fait remarquer que les conditions d'utilisation de l'«intérêt légitime» sont détaillées dans le guide «Base juridique pour le traitement des données à caractère personnel – Intérêt légitime» (ci-après le «guide sur l'intérêt légitime») adopté par l'ANPD. Ce guide précise que, pour qu'un intérêt soit considéré comme «légitime», trois conditions doivent être remplies: 1) la compatibilité avec le système juridique brésilien, 2) la référence à une situation spécifique et 3) le traitement doit être lié à des finalités légitimes,

²⁴ Voir articles 6 et 9 du règlement sur les notifications des incidents de sécurité.

²⁵ Voir considérant 75 du projet de décision, selon lequel «[l]a notification d'un incident de sécurité à l'ANPD et aux personnes concernées a lieu dans les trois jours (72 heures) à compter de la date à laquelle le responsable du traitement en a eu connaissance».

²⁶ Voir section 3 du présent avis.

spécifiques et explicites²⁷. Ces conditions sont semblables aux trois conditions cumulatives à remplir pour que le traitement des données à caractère personnel soit licite en vertu de cette base juridique, précisées par la Cour²⁸, et à leur explication complémentaire fournie par la Cour. Par ailleurs, les conditions de l'«intérêt légitime» précisées dans le guide sur l'intérêt légitime sont proches de celles prévues dans les lignes directrices adoptées par l'EDPB²⁹. L'EDPB se félicite de l'approche adoptée par l'ANPD en ce qui concerne l'intérêt légitime et son utilisation pour le traitement.

2.4 Droits individuels

- (30) L'EDPB accueille favorablement le fait que la LGPD confère aux personnes des droits semblables à ceux énoncés dans le RGPD (tous deux dans le chapitre III). En particulier, la LGPD prévoit le droit d'accès, le droit de rectification, le droit à la portabilité des données, le droit à la limitation du traitement, le droit à l'effacement, le droit à l'information, le droit de refuser ou de retirer le consentement, le droit de s'opposer au traitement et le droit de pétition (articles 9 et 18 de la LGPD).
- (31) La LGPD accorde également aux personnes concernées le droit de demander le réexamen des décisions fondées exclusivement sur un traitement automatisé de données à caractère personnel qui affectent leurs intérêts (article 20 de la LGPD). Le contenu de l'article 20 de la LGPD reflète, en substance, l'article 22 du RGPD.
- (32) L'EDPB relève qu'en ce qui concerne les droits des personnes concernées, la loi brésilienne sur l'habeas data établit des dispositions spécifiques pour accorder le droit d'accès et le droit de rectification dans un bref délai (respectivement 10 et 15 jours) à compter de la demande d'une personne, et se réjouit de cet aspect.
- (33) L'EDPB considère que la LGPD fixe pour les droits des personnes concernées des exigences essentiellement équivalentes à celles qui sont garanties par le RGPD.

2.5 Limitations concernant les transferts ultérieurs

- (34) Les critères de référence pour l'adéquation précisent que le niveau de protection des personnes physiques dont les données à caractère personnel sont transférées en vertu d'une décision d'adéquation ne doit pas être compromis par le transfert ultérieur et que, par conséquent, tout transfert ultérieur «ne devrai[t] être autoris[é] que si le nouveau destinataire (c'est-à-dire le destinataire du transfert ultérieur) est également soumis à des règles (y compris des règles contractuelles) assurant un niveau de protection adéquat et suivant les

²⁷ Voir considérant 52 du projet de décision.

²⁸ Par exemple, arrêt de la Cour du 7 décembre 2023 dans les affaires jointes C-26/22 et C-64/22, SCHUFA Holding AG, points 75 à 80.

²⁹ Lignes directrices 1/2024 sur le traitement des données à caractère personnel sur la base de l'article 6, paragraphe 1, point f), du RGPD (version 1.0), adoptées le 8 octobre 2024.

instructions pertinentes lors du traitement des données pour le compte du responsable du traitement».

- (35) En ce qui concerne l'appréciation du caractère adéquat du cadre juridique et de la pratique brésiliens, on entend par «transfert ultérieur» le transfert de données à caractère personnel de l'entité, agissant en qualité de responsable du traitement, située dans le champ d'application territorial de la LGPD, à savoir le Brésil, vers l'entité ne relevant pas de ce champ d'application.
- (36) Les exigences relatives au transfert ultérieur sont énoncées au chapitre V de la LGPD et complétées par l'ANPD, par l'adoption du «règlement sur le transfert de données», qui définit les notions de «transfert», de «transfert international de données», d'«importateur» et d'«exportateur» et comprend des exigences détaillées pour les transferts.
- (37) L'EDPB constate avec satisfaction que les définitions du «transfert» et du «transfert international de données» sont alignées sur celles de ses lignes directrices 05/2021³⁰.
- (38) Conformément à la LGPD et au règlement sur le transfert de données, les transferts ultérieurs ne peuvent avoir lieu qu'à des fins légitimes, spécifiques et explicites et lorsque des instruments ou conditions spécifiques sont en place (article 33 de la LGPD et articles 9 à 33 du règlement sur le transfert de données)³¹. L'EDPB apprécie le fait que ces instruments soient proches des outils de transfert prévus au chapitre V du RGPD. Cependant, il invite la Commission européenne à préciser dans le projet de décision si les transferts ne peuvent être effectués conformément à l'article 33, points III à IX, de la LGPD que dans des circonstances exceptionnelles, lorsque les conditions prévues à l'article 33, points I à II, de la LGPD ne sont pas remplies³².
- (39) Toutefois, le règlement sur le transfert de données précise que les transferts internationaux de données à caractère personnel sont autorisés «lorsque la personne concernée a donné son consentement spécifique et distinct à ce transfert, après avoir reçu des informations sur la nature internationale de l'opération envisagée, la distinguant clairement des autres finalités». Il n'est pas indiqué clairement si cette exigence suppose l'obligation d'informer les personnes concernées des risques que les transferts internationaux peuvent comporter en raison de l'absence de protection adéquate dans le pays tiers et de l'absence de garanties appropriées (par exemple, l'information selon laquelle il pourrait ne pas y avoir d'autorité de contrôle et/ou de principes de traitement des données et/ou de droits des personnes concernées dans le pays tiers), qui est une exigence au titre de l'article 49, paragraphe 1, point a), du RGPD. Pour l'EDPB, et en vertu du RGPD, la fourniture de ces informations est essentielle afin de permettre à la personne concernée de donner son consentement éclairé

³⁰ Lignes directrices 05/2021 sur l'interaction entre l'application de l'article 3 et des dispositions relatives aux transferts internationaux du chapitre V du RGPD, adoptées le 14 février 2023, point 9.

³¹ Voir aussi considérants 101 à 109 du projet de décision.

³² L'article 49 du RGPD précise que les dérogations envisagées dans cet article ne peuvent être utilisées qu'en l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, du RGPD ou de garanties appropriées en vertu de l'article 46 du RGPD.

en pleine connaissance de ces faits spécifiques du transfert. Dès lors, l'EDPB invite la Commission européenne à préciser dans le projet de décision si la personne concernée est informée des risques qu'un tel transfert peut comporter en raison de l'absence de protection adéquate dans le pays tiers et de garanties appropriées.

- (40) En outre, le règlement sur le transfert de données prévoit que «[t]ant le responsable du traitement que le sous-traitant adoptent des mesures efficaces de nature à démontrer le respect des règles en matière de protection des données à caractère personnel et la conformité à celles-ci, ainsi que l'efficacité de ces mesures, d'une manière compatible avec le niveau de risque du traitement et avec la modalité de transfert international utilisée» (article 4, paragraphe 2, du règlement sur le transfert de données). L'EDPB se réjouit de l'inclusion de cette obligation. Dans le même temps, il serait utile de préciser que l'efficacité de ces mesures devrait être évaluée de manière à garantir également que la législation locale du pays tiers concerné ne compromet pas la continuité de la protection des personnes concernées dont les données sont transférées³³. L'EDPB invite la Commission européenne à préciser que cet élément sera également pris en considération dans les scénarios de transfert.
- (41) L'EDPB accueille favorablement l'inclusion d'une obligation de transparence explicite à l'égard de la personne concernée, c'est-à-dire que les personnes concernées ont le droit de recevoir l'instrument contractuel utilisé pour le transfert ultérieur ainsi que la description de ce transfert, par exemple la durée et la finalité du transfert, les pays de destination, les responsabilités des parties concernées, les droits des personnes concernées et les moyens de les exercer (article 16 du règlement sur le transfert de données).
- (42) Cependant, il semble que cette portée de l'obligation de transparence ne soit pertinente que lorsque les transferts sont effectués sur la base de clauses contractuelles types et non lorsque d'autres outils sont utilisés³⁴. L'EDPB invite donc la Commission européenne à préciser que les mêmes obligations de transparence s'appliquent quel que soit l'outil de transfert utilisé.
- (43) L'EDPB observe également que les exigences relatives au contenu des règles d'entreprise contraignantes ne sont pas pleinement conformes à celles du RGPD, en particulier à son article 47, paragraphe 2, points f) et l). Afin de garantir que le niveau de protection assuré par le RGPD ne soit pas compromis, l'EDPB invite la Commission européenne à préciser dans le projet de décision que ces éléments³⁵ seront également pris en considération lorsque cet outil de transfert doit être utilisé pour les transferts ultérieurs de données à caractère personnel vers le Brésil en vertu de la décision d'adéquation.

³³ Voir arrêt Latombe. Voir aussi arrêt de la Cour du 16 juillet 2020 dans l'affaire C-311/18 («arrêt Schrems II»).

³⁴ Par exemple, le règlement sur le transfert de données comprend des obligations générales de transparence lorsque les règles d'entreprise contraignantes sont censées être utilisées, en particulier «l'établissement et la mise en œuvre d'un programme de gouvernance de la protection de la vie privée qui vise à instaurer une relation de confiance avec la personne concernée, au moyen d'actions transparentes garantissant des mécanismes de participation de la personne concernée» (article 25, point V, du règlement sur le transfert de données) et la transparence en ce qui concerne l'exercice des droits et du droit de réclamation de la personne concernée (article 26, point VI, du règlement sur le transfert de données).

³⁵ Responsabilité et coopération avec l'autorité de contrôle [article 47, paragraphe 2, points f) et l), du RGPD].

2.6 Mécanismes en matière de procédure et d'application

- (44) Selon les critères de référence pour l'adéquation³⁶ et la jurisprudence pertinente de la Cour³⁷, un système de protection des données essentiellement équivalent au modèle de l'Union européenne doit prévoir: i) une autorité indépendante, qui devrait contrôler et faire respecter la législation en matière de protection des données, ayant le pouvoir d'enquêter et de prendre des mesures sans influence extérieure. Les systèmes de protection des données doivent garantir ii) que les responsables du traitement et les sous-traitants sont responsables et conscients de leurs responsabilités, tandis que les personnes concernées sont informées de leurs droits. Des sanctions et des procédures de vérification efficaces devraient être mises en place pour garantir le respect des règles; et iii) que les responsables du traitement et les sous-traitants démontrent la conformité, au moyen de mesures telles que des analyses d'impact relatives à la protection des données, des registres des activités de traitement et la désignation de délégués à la protection des données. En outre, iv) le système de protection des données doit fournir un soutien et une aide aux différentes personnes concernées dans l'exercice de leurs droits et des mécanismes de recours appropriés.
- (45) Dans cette section, l'EDPB a axé son évaluation sur l'existence d'une autorité indépendante, d'un mécanisme de recours approprié et de sanctions efficaces.

2.6.1 Contrôle indépendant

- (46) La LGPD institue l'Agencia Nacional de Proteção de Dados (ANPD) en tant qu'autorité nationale de contrôle chargée de la surveillance et de l'application de ses dispositions.
- (47) L'EDPB se réjouit du fait que l'ANPD s'est vu accorder le statut d'«autorité de nature spéciale», une désignation destinée à garantir l'autonomie nécessaire pour exercer pleinement les fonctions et pouvoirs juridiques qui lui sont conférés par la LGPD, notamment en révoquant les dispositions qui subordonnaient le fonctionnement et les opérations financières de l'ANPD à des autorisations devant être accordées par l'exécutif.
- (48) De même, l'EDPB se félicite des modifications apportées le 15 septembre 2025 au cadre juridique brésilien selon lesquelles l'ANPD est désormais reconnue en tant qu'**organisme de réglementation**³⁸. L'EDPB croit comprendre que, dès lors, l'un des principaux changements est que l'ANPD soumettra son budget directement au ministère de la planification et du budget au lieu de devoir le soumettre par l'intermédiaire du ministère de la justice. Le budget de l'ANPD reste une ligne distincte du budget de l'État fédéral. L'EDPB croit comprendre que l'ANPD disposait déjà d'une indépendance concernant également son budget et ses finances,

³⁶ Voir chapitre 3, point C, des critères de référence pour l'adéquation.

³⁷ Arrêt de la Cour du 6 octobre 2015 dans l'affaire C-362/14, Schrems.

³⁸ Mesure provisoire n° 1.317/2025 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>.

mais qu'en devenant un organisme de réglementation, sa procédure administrative est simplifiée.

- (49) L'EDPB se félicite également de la nouvelle compétence de l'ANPD, qui a récemment été désignée comme étant l'autorité responsable de la protection des enfants en ligne³⁹. L'EDPB prend acte du fait que, conformément au chapitre IX de la LGPD, l'ANPD est dotée des pouvoirs et missions nécessaires et disponibles pour garantir le respect des droits en matière de protection des données et promouvoir la sensibilisation, tels que des pouvoirs d'enquête et de sanction (article 55-J de la LGPD).
- (50) En ce qui concerne le personnel et le budget de l'ANPD, qui jouent un rôle dans son indépendance, l'EDPB prend acte avec satisfaction de la récente décision d'augmenter les effectifs grâce à la création de plus de 200 nouveaux postes⁴⁰.
- (51) L'EDPB observe que, conformément à l'article 55-C de la LGPD, l'(actuelle) ANPD se compose d'un certain nombre d'organes⁴¹, dont le Conseil national pour la protection des données à caractère personnel et de la vie privée (ci-après le «Conseil»). L'EDPB prend acte de sa composition, qui comprend également des représentants du pouvoir exécutif fédéral, du pouvoir législatif et du pouvoir judiciaire⁴². L'EDPB relève également que, conformément à l'article 58-B de la LGPD, le Conseil est chargé, entre autres, i) de «proposer des orientations stratégiques et fournir des informations générales pour l'élaboration de la politique nationale de protection des données à caractère personnel et de la vie privée et pour les activités de l'ANPD» et ii) de «recommander des actions à réaliser par l'ANPD».
- (52) En ce qui concerne tout particulièrement ces tâches, l'EDPB estime qu'il est important de mieux comprendre la manière dont elles sont exécutées et la mesure dans laquelle les propositions et recommandations du Conseil influencent les travaux de l'ANPD. Il invite donc la Commission européenne à fournir plus d'informations sur ces tâches et sur l'interaction entre le Conseil et l'ANPD, afin de mieux évaluer l'influence du Conseil sur les activités de l'ANPD.

2.6.2 Recours

- (53) L'EDPB se félicite du mécanisme de recours prévu par la LGPD, qui confère également aux personnes concernées le droit d'introduire une réclamation auprès de l'ANPD et de contester sa décision en formant un appel auprès de son conseil d'administration. Les particuliers peuvent ensuite faire appel des décisions du conseil d'administration devant un juge, ainsi

³⁹ Loi n° 15.211/2025 relative à la protection des enfants et des mineurs dans l'environnement numérique, disponible à l'adresse suivante: <https://www.in.gov.br/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619>.

⁴⁰ <https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314>.

⁴¹ Conformément à l'article 55-C de la LGPD, l'ANPD se compose: du conseil d'administration, la plus haute instance dirigeante; du Conseil national pour la protection des données à caractère personnel et de la vie privée; du conseil de discipline; IV – du bureau du Médiateur; V – du bureau des affaires juridiques, et VI – des unités administratives et unités spécialisées nécessaires à l'application des dispositions du LGPD. Voir aussi considérants 126 à 130 du projet de décision.

⁴² Voir aussi considérant 132 du projet de décision et article 55-C de la LGPD.

que former un recours contre l'ANPD pour non-respect des obligations qui lui incombent en vertu de la LGPD. Étant donné que la différence entre l'instrument d'appel et l'instrument de recours ne ressort pas clairement du projet de décision, l'EDPB invite la Commission à préciser davantage le fonctionnement de ces deux instruments, y compris la question de savoir si l'utilisation du recours se limite uniquement au refus de traiter une réclamation ou au rejet au fond d'une réclamation.

- (54) De même, l'EDPB se félicite du fait que la LGPD prévoie le droit à réparation des dommages matériels et moraux, ainsi que le recours collectif (article 22 de la LGPD).

2.6.3 Sanctions

- (55) L'EDPB rappelle que l'existence de sanctions efficaces et dissuasives peut jouer un rôle important pour garantir le respect des règles en matière de protection des données, étant donné qu'elle témoigne du degré élevé de responsabilité et de sensibilisation que le système assure. L'EDPB se réjouit des pouvoirs d'adopter des mesures correctrices conférés à l'ANPD, qui ont été exercés à plusieurs reprises⁴³ et comprennent une série de mesures telles que l'avertissement, des amendes pouvant aller jusqu'à deux pour cent (2 %) des recettes brutes de l'entité juridique privée concernée, des amendes journalières, le blocage des données à caractère personnel liées à l'infraction jusqu'à sa régularisation, la suspension temporaire des activités de traitement des données pertinentes et l'effacement des données à caractère personnel concernées (article 52 de la LGPD)⁴⁴. L'EDPB invite la Commission à surveiller leur application cohérente, en particulier en ce qui concerne les sanctions.
- (56) L'EDPB constate avec satisfaction que l'ANPD a publié un règlement (contraignant) sur les sanctions. Ce règlement classe les sanctions en différents niveaux en utilisant des facteurs objectifs tels que le type et le volume des données traitées ou l'incidence sur les droits des personnes concernées, et prévoit une méthode de calcul des amendes conforme aux exigences de l'article 83 du RGPD.

⁴³ Voir ANPD, registre des sanctions. https://www.gov.br/anpd/pt-br/centrais-de-conteudo/deciso-es-em-processos-sancionadores-1/deciso-es-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.

⁴⁴ «Ces sanctions peuvent être infligées à des entités publiques ou privées, à l'exception des amendes et des amendes journalières, qui ne peuvent être infligées à des entités publiques» (considérant 135 du projet de décision).

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

- (57) Conformément à l'article 45, paragraphe 2, du RGPD, l'évaluation des limitations et des garanties prévues par le droit brésilien en ce qui concerne l'accès des autorités publiques brésiliennes aux données à caractère personnel transférées aux responsables du traitement et aux sous-traitants au Brésil à des fins d'application du droit pénal et de sécurité nationale et l'utilisation ultérieure de ces données par ces autorités (ci-après l'«accès des pouvoirs publics») est un élément important du critère de l'«équivalence essentielle», tel qu'interprété par la Cour.
- (58) L'EDPB est satisfait de l'attention particulière accordée par la Commission et des informations factuelles qu'elle fournit au sujet de cet aspect dans le projet de décision⁴⁵. Il s'abstiendra donc de reproduire la plupart des constatations factuelles et des analyses dans le présent avis. En lieu et place, il évalue l'incidence du système brésilien d'accès des pouvoirs publics à des fins répressives et de sécurité nationale sur la base des quatre éléments recensés par l'EDPB dans les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020⁴⁶:
- garantie A - règles juridiques claires, précises et accessibles;
 - garantie B - nécessité et proportionnalité du traitement au regard des objectifs légitimes poursuivis;
 - garantie C - mécanisme de contrôle indépendant;
 - garantie D - voies de droit et mécanismes de recours efficaces à la disposition des particuliers.

⁴⁵ Voir considérants 152 à 217 du projet de décision.

⁴⁶ [Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance](#).

3.1 Accès aux données et utilisation de celles-ci par les autorités publiques brésiliennes à des fins d'application du droit pénal

3.1.1 Cadre juridique dans les domaines de l'application du droit pénal

- (59) L'EDPB relève que l'accès aux données à caractère personnel et leur utilisation ultérieure par les autorités répressives brésiliennes⁴⁷ sont régis par un système d'actes juridiques de nature juridique différente. La protection des données et de la vie privée, y compris le secret de la correspondance et des communications, est consacrée à l'article 5 de la Constitution en tant que droit fondamental. L'EDPB accueille en particulier favorablement le fait que, comme au sein de l'Union européenne, la portée de la protection de ces droits ne se limite pas aux seuls citoyens brésiliens, mais englobe également les étrangers résidant ou non au Brésil⁴⁸.
- (60) Ensuite, plusieurs lois sectorielles spécialisées régissent la possibilité d'accès aux données à caractère personnel à des fins répressives. En ce qui concerne l'accès aux données transférées au Brésil depuis l'Union européenne, le code pénal, la loi sur les écoutes téléphoniques, le cadre civil pour l'internet, la loi sur la confidentialité des établissements financiers et la loi relative aux organisations criminelles et aux enquêtes pénales, entre autres, sont particulièrement pertinents. L'EDPB observe que ces actes juridiques sont accessibles au public et pourraient être considérés comme suffisamment clairs pour donner aux personnes concernées une indication des circonstances et des conditions dans lesquelles les autorités publiques sont habilitées à accéder à leurs données⁴⁹.
- (61) Une autre source de droit importante au Brésil est la jurisprudence de la Cour suprême fédérale du Brésil, qui semble appliquer une interprétation large de la portée des droits au respect de la vie privée et à la protection des données⁵⁰, ainsi que la jurisprudence de la Cour interaméricaine des droits de l'homme, chargée de l'interprétation et de l'application de la convention américaine relative aux droits de l'homme, ratifiée par le Brésil en 1992⁵¹.
- (62) L'EDPB observe que le champ d'application de la LGPD en cas de traitement de données à caractère personnel à des fins d'application du droit pénal est partiel, ce qui peut entraîner une insécurité juridique.
- (63) Ainsi que la Commission l'a reconnu dans le projet de décision, la LGPD ne s'applique pas au traitement de données effectué aux fins *exclusives* de la sécurité publique, de la défense

⁴⁷ Voir liste des autorités au considérant 165 du projet de décision.

⁴⁸ Voir considérants 8 et 9 du projet de décision.

⁴⁹ Voir arrêt Zakharov de la Cour européenne des droits de l'homme, paragraphe 229.

⁵⁰ Voir décision de la Cour suprême fédérale dans l'affaire ADI 6649, septembre 2022.

⁵¹ Voir considérant 10 du projet de décision.

nationale, de la sûreté de l'État ou des enquêtes sur les infractions pénales et des poursuites en la matière⁵². Conformément à l'article 4, points I et III, de la LGPD, le traitement des données dans ces domaines sera régi par une législation spécifique, qui doit englober les principes et les droits des personnes concernées énoncés dans la LGPD. D'après ce que sait l'EDPB, comme la Commission l'a confirmé, le Brésil n'a pas encore adopté de législation spécifique concernant le traitement des données à caractère personnel dans le domaine de la justice pénale et de la répression (par exemple, une législation semblable à la directive de l'Union en matière de protection des données dans le domaine répressif)⁵³.

- (64) L'EDPB relève avec satisfaction que la Cour suprême fédérale du Brésil a, dans sa jurisprudence⁵⁴, interprété la LGPD d'une manière qui élargit son applicabilité partielle au traitement des données à caractère personnel à des fins d'enquêtes pénales et de maintien de l'ordre public.
- (65) L'EDPB se réjouit du fait que l'autorité de contrôle brésilienne, l'ANPD, soutienne pleinement cette interprétation et considère que *«l'absence de législation spécifique n'accorde pas aux services de sécurité une autorisation large et illimitée de traiter les données à caractère personnel des citoyens aux fins exclusives de la sécurité publique ainsi que des enquêtes sur les infractions pénales et des poursuites en la matière sans aucune limite»*⁵⁵. Dans le même temps, l'EDPB relève que, conformément à l'article 4, point III, de la LGPD, pour certains traitements spécifiques de données effectués exclusivement à des fins répressives, l'ANPD semble avoir à l'heure actuelle principalement un rôle consultatif vis-à-vis des autorités répressives.
- (66) L'EDPB invite la Commission à évaluer plus avant et à clarifier, dans le projet de décision, l'applicabilité de la LGPD en cas de traitement de données à caractère personnel à des fins d'application du droit pénal, y compris les pouvoirs de l'ANPD, ainsi qu'à prendre soigneusement en considération toute évolution pertinente à cet égard dans le cadre de sa future surveillance (voir aussi section sur le contrôle et les recours).

3.1.2 Nécessité et proportionnalité

- (67) L'EDPB constate avec satisfaction qu'en règle générale, l'accès aux données de communication, tant au contenu qu'aux métadonnées, ainsi qu'à d'autres catégories d'informations confidentielles protégées telles que les données bancaires et fiscales, nécessite une autorisation judiciaire préalable.

⁵² Voir considérants 30 et 31 du projet de décision.

⁵³ Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

⁵⁴ Voir décision de la Cour suprême fédérale dans l'affaire ADI 6649, septembre 2022.

⁵⁵ Voir note technique n° 29/2024/FIS/CGF/ANPD de l'ANPD, adressée au ministère de la justice et de la sécurité publique, point 5.4.1.29, disponible à l'adresse suivante: [SEI/ANPD - 0132350 - Nota Técnica](#).

- (68) En ce qui concerne l'accès aux données de communication, l'EDPB se félicite que, conformément à la loi sur les écoutes téléphoniques et à la jurisprudence de la Cour suprême fédérale, cette mesure soit considérée comme exceptionnelle et soumise à des conditions strictes visant à garantir sa nécessité et sa proportionnalité⁵⁶. En outre, à titre de mesure de prévention d'éventuels abus, le droit brésilien prévoit que l'interception de communications 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 de prison⁵⁷.
- (69) La mise en œuvre stricte des garanties relatives à l'accès aux données de communication est particulièrement pertinente compte tenu de l'existence, au Brésil, d'une obligation générale pour les fournisseurs de services de connexion à l'internet et d'applications en ligne de conserver les journaux de connexion pendant un an⁵⁸. Bien que l'EDPB constate avec satisfaction que l'accès aux données conservées n'est possible que sous réserve d'une autorisation judiciaire⁵⁹, il rappelle l'approche stricte et les restrictions à la conservation générale et indifférenciée des métadonnées de communication dans l'Union européenne⁶⁰ et se réjouit de prendre acte des informations supplémentaires fournies par la Commission en ce qui concerne l'absence de conservation massive de données dans le pays. L'EDPB encourage donc la Commission à accorder une attention particulière au régime juridique et à la pratique au Brésil en ce qui concerne l'accès aux données de communication lors du suivi et de l'examen du projet de décision.
- (70) L'EDPB constate avec satisfaction que des garanties similaires s'appliquent également en ce qui concerne l'accès des autorités répressives aux données fiscales et bancaires, c'est-à-dire l'exigence d'une autorisation judiciaire préalable, accordée uniquement pour les crimes graves, l'existence de sanctions pénales en cas d'abus, etc.
- (71) Selon le projet de décision, il existe une exception à l'exigence générale d'autorisation judiciaire préalable pour l'accès des services répressifs à certaines catégories de données à caractère personnel⁶¹. En vertu des articles 15 et 16 de la loi relative aux organisations criminelles et aux enquêtes pénales, un chef de police et le ministère public peuvent accéder sans autorisation judiciaire aux données d'enregistrement d'une personne faisant l'objet d'une enquête concernant ses: «*qualification personnelle, affiliation et adresse conservées par le tribunal électoral, sociétés de téléphonie, établissements financiers, fournisseurs d'accès à l'internet et administrateurs de cartes de crédit*»⁶². Dans le même ordre d'idées, les entreprises de transport permettront, pendant une période de cinq ans, l'accès direct et permanent d'un

⁵⁶ Voir considérants 169 et 170 du projet de décision.

⁵⁷ Ibidem.

⁵⁸ Voir considérant 173 du projet de décision.

⁵⁹ Ibidem.

⁶⁰ Pour de plus amples informations sur la conservation des données, voir déclaration 5/2024 de l'EDPB sur les recommandations du groupe de haut niveau sur l'accès aux données aux fins d'une répression efficace, disponible à l'adresse suivante: https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf.

⁶¹ Voir considérant 164 du projet de décision.

⁶² Voir article 15 de la loi relative aux organisations criminelles et aux enquêtes pénales.

juge, du ministère public ou d'un chef de police aux bases de données des réservations et à l'historique des voyages⁶³.

- (72) L'EDPB remarque que le champ d'application de la loi relative aux organisations criminelles et aux enquêtes pénales se limite aux enquêtes et aux sanctions à l'encontre des groupes criminels organisés et des organisations terroristes, qui représentent un risque important pour les citoyens et la société et sont donc de nature à justifier une ingérence plus grave dans les droits fondamentaux au respect de la vie privée et à la protection des données⁶⁴. Dans le même temps, l'EDPB considère que les informations relatives à ces exceptions fournies au considérant 164 du projet de décision sont très générales et incomplètes. En particulier, il est difficile de savoir, sur la base des informations contenues dans le projet de décision si, dans ce cas, l'accès aux données à caractère personnel fait l'objet d'un contrôle juridictionnel ex post au regard de la nécessité et de la proportionnalité.
- (73) Compte tenu de ce qui précède, l'EDPB invite la Commission à préciser et à expliquer de manière plus détaillée, dans le projet de décision, la portée et la nature des cas dans lesquels l'accès aux données par les autorités répressives ne nécessite pas d'autorisation judiciaire, ainsi que les garanties applicables prévues par la législation brésilienne. L'EDPB estime également que la Commission devrait accorder une attention particulière à l'application de ces exceptions en vertu du droit brésilien lors de son suivi du projet de décision.

3.1.3 Utilisation ultérieure des données et transferts ultérieurs

- (74) L'EDPB rappelle que le niveau de protection accordé aux données à caractère personnel transférées de l'Union européenne/l'EEE vers le Brésil ne doit pas être compromis par l'utilisation ultérieure ou le partage des données avec des destinataires au Brésil ou dans un pays tiers, c'est-à-dire que les transferts ultérieurs ne devraient être autorisés que lorsqu'un niveau de protection continu essentiellement équivalent à celui prévu par le droit de l'Union est assuré.
- (75) À cet égard, l'EDPB constate avec satisfaction que la Cour suprême fédérale du Brésil a jugé que le partage de données à caractère personnel entre organismes publics (y compris lorsqu'elles sont partagées entre les services répressifs et les services de renseignement) présuppose: 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 public⁶⁵.

⁶³ Voir article 16 de la loi relative aux organisations criminelles et aux enquêtes pénales.

⁶⁴ Voir arrêts de la Cour du 6 octobre 2020 dans les affaires jointes C-511/18 et C-512/18, *La Quadrature du Net e.a.*, EU:C:2020:791, points 95 à 98; du 2 octobre 2018 dans l'affaire C-207/16, *Ministerio Fiscal*, EU:C:2018:788, points 54, 57 et 60; et du 2 mars 2021 dans l'affaire C-746/18, *Prokuratuur* (Conditions d'accès aux données relatives aux communications électroniques), EU:C:2021:152, point 35.

⁶⁵ Voir considérant 187 du projet de décision.

- (76) Nonobstant cette importante décision de la plus haute juridiction brésilienne, compte tenu de la complexité déjà mentionnée, du champ d'application exact et des modalités de l'application de la LGPD aux autorités répressives, l'EDPB invite la Commission à suivre de près l'évolution de la situation et la pratique dans ce domaine.
- (77) En ce qui concerne le transfert ultérieur de données à caractère personnel à des autorités chargées de l'application du droit pénal dans des pays tiers, le projet de décision fait référence à l'article 33, point III, de la LGPD, qui 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»⁶⁶. L'EDPB estime que cette explication est trop générale et invite la Commission à préciser davantage, dans le projet de décision, les conditions et les garanties régissant les transferts ultérieurs.

3.1.4 Contrôle et recours

- (78) L'EDPB rappelle que toute ingérence dans le droit au respect de la vie privée et à la protection des données devrait être soumise à un système de contrôle effectif, indépendant et impartial, qui doit être assuré par un juge ou par un autre organe indépendant (comme une autorité administrative ou un organe parlementaire)⁶⁷.
- (79) Il relève également que, dans le cadre brésilien, tel que décrit par la Commission, les activités des autorités chargées de l'application du droit pénal sont supervisées par différents organes: i) le pouvoir judiciaire, ii) l'ANPD et iii) le ministère public.
- (80) Le contrôle juridictionnel, comme expliqué ci-dessus dans la section relative à la nécessité et à la proportionnalité⁶⁸, s'applique à la collecte de données à caractère personnel et à l'accès à celles-ci, notamment sous la forme d'un examen et d'une autorisation ex ante.
- (81) Pour ce qui est du rôle de l'ANPD, comme cela a déjà été expliqué dans la section 3.1.1 du présent avis, le projet de décision d'adéquation rappelle que, conformément à l'article 4, point III, de la LGPD, cette loi ne s'applique pas au traitement des données à caractère personnel effectué *exclusivement* à des fins i) de sécurité publique, ii) de défense nationale, iii) de sûreté de l'État et iv) d'enquêtes sur les infractions pénales et de poursuites en la matière. Par ailleurs, l'article 4, point I, dispose que ce traitement sera régi par une législation spécifique qui, entre autres, doit englober les principes généraux de protection et les droits des personnes concernées tels qu'ils sont énoncés dans la LGPD. Le paragraphe 3 de l'article 4 reconnaît un rôle consultatif à l'ANPD en ce qui concerne les exceptions prévues au point III dudit article lorsque le traitement est effectué exclusivement à ces fins, notamment le

⁶⁶ Ibidem.

⁶⁷ Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020, p. 12:

https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_fr.pdf.

⁶⁸ Voir section 3.1.2 ci-dessus.

pouvoir de l'ANPD d'émettre des recommandations et des avis techniques, ainsi que de demander des AIPD aux responsables du traitement concernés.

- (82) Dans son projet de décision⁶⁹, la Commission fait référence à une importante décision du 15 septembre 2022 de la Cour suprême fédérale, qui indique l'applicabilité des principes généraux de protection des données et des droits des personnes concernées au traitement des données à caractère personnel par l'État aux fins de la prestation de services publics. Cette décision porte sur le «partage de données à caractère personnel» entre les organes et entités de l'administration publique et dans le cadre des activités de renseignement, ainsi que sur l'«accès des agences et entités gouvernementales» au registre de citoyenneté de base. En ce qui concerne le rôle d'exécution de l'ANPD, l'EDPB croit comprendre, à la lecture d'informations supplémentaires fournies par la Commission, que l'ANPD a déjà exercé ce rôle à l'égard de la police ainsi que du ministère de la justice et de la sécurité publique, et ce sur la base de la jurisprudence qui, en étendant l'applicabilité partielle des principes généraux et des droits des personnes concernées au traitement effectué à des fins répressives, rend l'ANPD également responsable du contrôle et de l'application du droit dans ce domaine.
- (83) À la lumière de ce qui précède, l'EDPB invite la Commission à approfondir le rôle d'exécution de l'ANPD, notamment en ce qui concerne les bases juridiques pertinentes et ses pouvoirs d'enquête et d'adopter des mesures correctrices à l'égard des autorités répressives, et à suivre de près l'évolution de la situation dans ce domaine.
- (84) Enfin, l'EDPB observe que le ministère public dispose d'une compétence plus large que celle de contrôler les règles en matière de protection des données et de respect de la vie privée et d'infliger des sanctions en cas de violation des droits fondamentaux. Par exemple, comme déjà expliqué dans la section 3.1 du présent avis, en vertu de la loi relative aux organisations criminelles et aux enquêtes pénales, le ministère public est l'une des autorités qui peuvent accéder sans autorisation judiciaire aux données d'enregistrement d'une personne faisant l'objet d'une enquête. L'EDPB invite donc la Commission à préciser et à expliquer dans le projet de décision le rôle et les pouvoirs du ministère public en ce qui concerne le contrôle du traitement des données à caractère personnel par les autorités répressives brésiliennes.
- (85) Quant aux recours, l'EDPB constate avec satisfaction que les mécanismes juridiques décrits dans la première partie du présent avis, et en particulier les recours juridictionnels dont les personnes physiques disposent pour faire respecter leurs droits à la protection des données et au respect de la vie privée, s'appliquent également aux activités des organes chargés de l'application du droit pénal.

⁶⁹ Voir considérant 187 du projet de décision.

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

3.2.1 Champ d'application de l'exemption prévue à l'article 4, point III, de la LGPD et applicabilité de celle-ci aux infractions pénales portant atteinte à la sûreté de l'État

- (86) Comme indiqué par la Commission, l'article 4, point III, de la LGPD exempte la «sûreté de l'État» de l'application de la LGPD lors du traitement de données à caractère personnel, à l'instar de la sécurité publique, de la défense nationale et des activités d'enquêtes sur les infractions pénales et de poursuites en la matière.
- (87) L'EDPB fait observer que la législation brésilienne relative à la «*Seguranca Nacional*» (sécurité nationale), telle qu'elle figure dans la loi n° 14.197 du 1^{er} septembre 2021 modifiant le code pénal et abrogeant la loi de 1983 sur la sécurité nationale⁷⁰, exprime la notion brésilienne de sécurité nationale sur la base d'une liste exhaustive d'infractions pénales⁷¹, qui visent différentes menaces pour l'intégrité de l'État brésilien en tant qu'institution [souveraineté nationale, espionnage (article 350-K), crimes contre les institutions démocratiques (article 359-L), etc.]. Les normes de la loi n° 14.197 ont été établies en tant que partie intégrante du code pénal brésilien.
- (88) Cela dit, l'EDPB s'attendrait à ce que le traitement des données par les autorités brésiliennes aux fins de la poursuite des infractions prévues par la loi n° 14.197 soit régi par le régime applicable à l'accès aux données et à l'utilisation de celles-ci par les autorités brésiliennes à des fins d'application du droit pénal, comme décrit au chapitre 3.2 du projet de décision, et fasse donc l'objet des mêmes considérations en matière de protection des données que celles indiquées au chapitre 3.1 du présent avis. L'EDPB demande donc à la Commission de préciser dans le projet de décision si le traitement des données lié à la poursuite des infractions pénales énumérées dans la loi n° 14.197 est effectivement régi par le régime de protection des données applicable aux activités répressives, ou s'il est régi par un autre régime. Dans ce dernier cas, l'EDPB invite la Commission à expliquer plus en détail les règles en matière de protection des données applicables aux poursuites pénales pour ces infractions à des fins de sécurité nationale.

⁷⁰ Loi n° 14.197 du 1^{er} septembre 2021, disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm (2.10.2025).

⁷¹ Voir considérant 200 du projet de décision.

3.2.2 Cadre juridique pour la sécurité nationale

- (89) Le cadre juridique codifié sur lequel la Commission fonde ses conclusions dans son chapitre du projet de décision consacré à l'accès des pouvoirs publics à des «fins de sécurité nationale» se compose de la loi n° 14.197 de 2021, de la loi n° 9.883 du 7 décembre 1999 établissant le système de renseignement brésilien et du décret n° 4.376 de 2002 y afférent. Les deux derniers textes législatifs mentionnés ont mis en place le système de renseignement brésilien [Sistema Brasileiro de Inteligência (SISBIN)] et son fonctionnement. Ils ont été suivis par le décret présidentiel contraignant n° 8.793⁷² de 2016, qui définit la politique nationale en matière de renseignement [«*Política Nacional de Inteligência*» (PNI)], ainsi que par la LGPD en 2018.
- (90) Le décret présidentiel n° 8.793 de 2016 décrit l'objet, les objectifs et les limites de la PNI. Les activités relevant de ce décret visent à produire et à diffuser aux autorités compétentes des connaissances sur des faits et des situations qui se produisent à l'intérieur ou à l'extérieur du territoire national, et qui ont une influence immédiate ou potentielle sur le processus décisionnel, l'action gouvernementale et la sécurité de la société et du renseignement de l'État. Dans ces circonstances, le renseignement désigne l'ensemble des informations (et des données) requises et traitées pour soutenir le processus décisionnel du pouvoir exécutif dans ce domaine.
- (91) Conformément à la base juridique du SISBIN telle que présentée par la Commission, le SISBIN et ses entités ont été mis en place en tant que mécanisme central de mise en œuvre de la PNI et sont, à ce titre, chargés d'exercer des activités relevant du domaine de la sécurité nationale ainsi que de la sûreté et de la sécurité publiques et de la protection des institutions démocratiques. À cette fin, le SISBIN assure un échange de connaissances et une planification intégrée des activités⁷³. En conséquence, la notion de sécurité nationale au Brésil à la lumière des activités du SISBIN ne semble pas se limiter aux seules infractions pénales codifiées dans la loi n° 14.197, mais pourrait être considérée comme faisant partie intégrante d'une notion élargie du renseignement national.
- (92) Lors de sa création, le SISBIN se composait de 18 entités fédérales, dont 13 ministères, puis il a été étendu à 48 «agences» en vertu du décret n° 11.693 du 6 septembre 2023 relatif à l'organisation et au fonctionnement du SISBIN⁷⁴. L'EDPB relève que la coopération au sein du SISBIN intègre des entités en plus des institutions de sécurité classiques, telles que le ministère des sciences (article 4, point IV), de l'agriculture (article 4, point XV) et de l'énergie (article 4, point XVIII) et le procureur général fédéral (article 4, point XIX).

⁷² Voir considérant 199 du projet de décision.

⁷³ Le décret présidentiel n° 8.793, section 5, cite le SISBIN et les organes qui y sont intégrés, l'échange de connaissances au sein du SISBIN et la planification intégrée de la coopération entre les membres du SISBIN en tant qu'instruments de mise en œuvre de la PNI.

⁷⁴ Voir considérant 202 du projet de décision.

- (93) Alors que le décret n° 4.376 de 2002 a exigé du conseil consultatif du système de renseignement brésilien qu'il propose des normes et des procédures générales pour l'échange de «connaissances et de communications» au sein du SISBIN⁷⁵, le décret n° 11.693 de 2023 prévoit que l'organe central du SISBIN élabore des outils techniques⁷⁶ pour le partage d'informations et de connaissances et décrit le partage et l'utilisation des données obtenues par les entités du SISBIN. Le projet de décision de la Commission ne fournit toutefois aucune information supplémentaire sur ces règles ou normes juridiques émises par l'organe central, par exemple lorsque les entités du SISBIN partagent des données à caractère personnel entre elles.
- (94) En outre, il semble exister des différences entre les notions de sensibilité des informations, étant donné qu'en vertu du droit applicable régissant les activités du SISBIN, la sensibilité est liée au degré de confidentialité accordé à une information⁷⁷ et de limitation de la finalité par rapport aux principes généraux du RGPD⁷⁸.
- (95) Comme déjà expliqué ci-dessus, l'article 4, point III, points a) à c), de la LGPD, qui n'a été codifié qu'après l'établissement du SISBIN et la définition d'une politique nationale en matière de renseignement, exempte de l'application de la LGPD les activités de traitement de données effectuées exclusivement à des fins de sécurité publique, de défense nationale et de sûreté de l'État, à l'exception des principes généraux établis en matière de protection des données.
- (96) Comme la Commission l'a souligné dans le projet de décision, le cadre général de la Constitution brésilienne ainsi que la participation du Brésil à la Cour interaméricaine des droits de l'homme relèvent du cadre juridique qui régit l'accès des pouvoirs publics aux fins du renseignement national. L'EDPB reconnaît également que les décisions de la Cour suprême fédérale brésilienne ont aussi joué un rôle important dans la définition du paysage juridique⁷⁹. Les décisions de la Cour suprême ont jusqu'à présent constitué un soutien concis et pertinent à la poursuite du développement de la protection des données à caractère personnel conformément à la Constitution brésilienne. Dans le même temps, il est à noter que les décisions de la Cour suprême n'énoncent pas ou n'établissent pas de règles générales abstraites en matière de protection des données pour le traitement des données à caractère personnel, mais interprètent les dispositions et les principes de la Constitution et de la LGPD.
- (97) L'EDPB est conscient du fait que les États disposent d'une large marge d'appréciation dans la définition des questions de sécurité nationale, qui permet ensuite des exemptions en matière de sécurité nationale concernant le traitement des données à caractère personnel. Dans ce contexte, il rappelle la définition donnée par la Cour européenne des droits de l'homme, selon laquelle il doit être possible de distinguer, par leur nature, leur gravité et les

⁷⁵ Voir article 7, point II, du décret n° 4.376.

⁷⁶ Voir article 10, point XI, disponible à l'adresse suivante: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm (26.9.2025).

⁷⁷ Voir décret n° 8.793 de 2016, décret n° 11.693 et considérant 204 du projet de décision.

⁷⁸ Voir article 6, point I, de la LGPD, qui mentionne des finalités légitimes et spécifiques, tandis que le RGPD exige des finalités licites et déterminées.

⁷⁹ Voir considérant 203 du projet de décision.

circonstances spécifiques, les menaces pour la sécurité nationale des risques généraux pour la sécurité publique ou des infractions pénales graves⁸⁰.

- (98) L'EDPB croit comprendre que les données traitées par les entités du SISBIN ne bénéficient de l'exemption prévue à l'article 4, point III, de la LGPD que lorsque le traitement est *exclusivement* effectué à des fins de sécurité publique, de défense nationale et de sûreté de l'État. Cela semble s'appliquer spécifiquement aux activités de l'organisme central du SISBIN, l'agence brésilienne de renseignement (ABIN). Par conséquent, à moins qu'une entité du SISBIN agisse pour le compte de l'ABIN à l'une de ces fins, la LGPD s'applique pleinement.
- (99) L'EDPB invite la Commission à confirmer cette interprétation et à décrire et expliquer plus précisément dans le projet de décision les grandes lignes de la notion de sécurité nationale en droit brésilien, en particulier en ce qui concerne la collecte et le partage de données entre et par les entités aux fins des activités du SISBIN, et pour ce qui est de la mise en œuvre de la PNI. À cet égard, l'EDPB invite également la Commission à préciser la manière dont les exemptions de la LGPD à des fins de sécurité nationale sont liées à l'exemption pour la sécurité nationale au titre du RGPD.

3.2.3 Transferts ultérieurs et accords internationaux

- (100) L'article 33 de la LGPD définit les conditions préalables au transfert international de données. L'article 33, points I et II, de la LGPD fixe des exigences semblables à celles d'une décision d'adéquation ou aux exigences en matière de garanties supplémentaires au titre du RGPD. Ces exigences sont levées à l'article 33, points III, VI et VII, de la LGPD, qui traite des cas de «coopération juridique entre les services de renseignement», de transferts répondant à un «engagement pris dans le cadre d'accords de coopération internationale» et de transferts «nécessaires à l'application d'une politique publique ou à une attribution légale d'un service public», c'est-à-dire de la sécurité nationale et du renseignement national. Cette décision semble être conforme à l'esprit de l'article 4, point III, de la LGPD, qui limite l'application de cette dernière à ses seuls principes en ce qui concerne les questions de sécurité publique, de défense nationale et de sûreté de l'État. On pourrait donc considérer que les transferts ultérieurs à des fins de renseignement national devraient être effectués dans le respect des principes généraux de protection des données de la LGPD, tout en étant soumis aux dispositions relatives à la coopération internationale prévues dans les actes juridiques établissant la PNI et le SISBIN.
- (101) Cela dit, l'EDPB reconnaît que le Brésil peut avoir besoin de transmettre et transmettre effectivement des données à caractère personnel à des services de renseignement étrangers aux fins de la coopération ou de la mise en œuvre de la PNI conformément à l'objectif de prévention et de détection des menaces fondé sur le concept intégré de sécurité susmentionné.

⁸⁰ Arrêt de la Cour européenne des droits de l'homme du 25 mai 2021 dans l'affaire Big Brother Watch et autres c. Royaume-Uni, paragraphe 350.

- (102) Comme indiqué précédemment, la Commission mentionne l'applicabilité du cadre général de la Constitution brésilienne et la garantie de l'habeas data pour la protection des données à caractère personnel au sein du SISBIN, qui s'appliquent également aux transferts ultérieurs à des fins de sécurité nationale. L'EDPB invite la Commission à mieux préciser la base juridique et les garanties et conditions en matière de protection des données que l'ABIN et les autres membres du SISBIN sont tenus de prendre en considération avant de divulguer des données à caractère personnel à des fins de renseignement national à des partenaires étrangers.
- (103) L'EDPB relève également que la Commission n'a pas intégré de considérations relatives à l'existence d'accords internationaux conclus entre le Brésil et des pays tiers ou des organisations internationales dans son appréciation du caractère adéquat du niveau de protection des données à caractère personnel assuré par le Brésil. Étant donné que la LGPD ne prévoit pas de législation contraignante outre les principes généraux de protection des données, de tels accords pourraient contenir des dispositions spécifiques pour le transfert international de données à caractère personnel détenues par l'ABIN ou les autres membres du SISBIN vers des pays tiers. L'EDPB considère que la conclusion d'accords bilatéraux ou multilatéraux avec des pays tiers aux fins du renseignement national est susceptible d'affecter le cadre juridique applicable en matière de protection des données.
- (104) L'EDPB invite donc la Commission à préciser s'il existe de tels accords internationaux à des fins de renseignement national et à évaluer leur incidence potentielle sur le niveau de protection accordé aux données à caractère personnel transférées de l'EEE vers le Brésil en ce qui concerne le cadre juridique principalement évalué pour le traitement des données à des fins de renseignement national.

3.2.4 Contrôle et recours

- (105) Le projet de décision d'adéquation présente différents organes chargés de contrôler les activités des autorités brésiliennes chargées de la sécurité nationale, notamment i) le pouvoir exécutif, ii) le pouvoir législatif, iii) l'ANPD et iv) le pouvoir judiciaire. En ce qui concerne l'ANPD, l'EDPB rappelle les considérations et conclusions formulées dans la section 3.1.4 du présent avis, qui restent valables ici également.
- (106) Selon le projet de décision, la chambre des relations extérieures et de la défense nationale du Conseil de gouvernement est chargée de contrôler la mise en œuvre de la police nationale du renseignement, et le bureau de sécurité institutionnelle est chargé de coordonner l'activité du renseignement fédéral. L'EDPB relève que ce contrôle porte uniquement sur les objectifs à réaliser par le système de renseignement et sur leur mise en œuvre, mais ne comprend aucun pouvoir d'enquête ou de sanction, et ne couvre pas le traitement effectif de données à caractère personnel.
- (107) C'est en effet à la commission mixte pour le contrôle des activités de renseignement (CCAI) (section législative) qu'il appartient d'exercer un contrôle sur les activités de renseignement, y compris leur légitimité et leur efficacité. L'EDPB se félicite du fait que la structure et les

pouvoirs de la CCAI ont été renforcés, ce qui a entraîné un accroissement de la transparence de ses activités et lui a permis d'exercer un contrôle approprié, par exemple en procédant à des examens a posteriori, à des audits et à des contrôles des opérations en cours. L'EDPB constate également avec satisfaction que la CCAI peut traiter les réclamations des personnes concernées dans le cadre de sa compétence d'enquête sur les réclamations relatives à des violations des garanties et droits fondamentaux.

(108) La compétence du pouvoir judiciaire consistant à connaître des affaires engagées par des citoyens contre des autorités publiques est un aspect positif, d'autant plus qu'elle permet un contrôle juridictionnel des activités menées au nom de la sécurité nationale, garantissant ainsi le respect, entre autres, des droits constitutionnels (y compris du droit à la protection des données) et de la LGPD. L'EDPB est satisfait de voir que la possibilité de faire appel est prévue par l'intermédiaire de la Cour suprême fédérale et, en dernier ressort, de la Cour interaméricaine des droits de l'homme.

(109) L'EDPB croit comprendre que, dans le contexte des activités de renseignement national, les personnes concernées se voient accorder i) les droits consacrés par la LGPD (en conséquence de la décision de la Cour suprême fédérale du 15 septembre 2022), ii) le droit d'obtenir l'accès aux données à caractère personnel et leur rectification par l'intermédiaire de la voie de recours constitutionnelle de l'habeas data, ainsi que iii) le droit à réparation des dommages matériels et moraux.

(110) L'EDPB se réjouit de l'existence de ces droits et du fait qu'ils peuvent être invoqués au moyen de mécanismes judiciaires et administratifs, en particulier la CCAI, ainsi que du fait que ces voies de recours sont accessibles à toutes les personnes, quelle que soit leur nationalité.

4. MISE EN ŒUVRE ET SUIVI DU PROJET DE DÉCISION

(111) En ce qui concerne le suivi et l'examen du projet de décision, l'EDPB indique que, selon la jurisprudence de la Cour, «au regard du fait que le niveau de protection assuré par un pays tiers est susceptible d'évoluer, il incombe à la Commission, après l'adoption d'une décision [d'adéquation (article 45 du RGPD)], de vérifier de manière périodique si la constatation relative au niveau de protection adéquat assuré par le pays tiers en cause est toujours justifiée en fait et en droit. Une telle vérification s'impose, en tout état de cause, lorsque des indices font naître un doute à cet égard»⁸¹.

(112) L'EDPB relève que le réexamen du constat d'adéquation aura lieu au moins tous les quatre ans, conformément à l'article 45, paragraphe 3, du RGPD⁸².

⁸¹ Arrêt Schrems I de la Cour, point 76. Voir aussi article 3, paragraphe 4, du projet de décision.

⁸² Voir considérant 229 et article 3, paragraphe 4, du projet de décision.

(113) L'EDPB se félicite que le projet de décision prévoie, en son considérant 230, la participation de l'EDPB à la réunion organisée entre la Commission et les autorités brésiliennes et consacrée à l'examen du fonctionnement de la décision d'adéquation. En ce qui concerne l'association concrète de l'EDPB et de ses représentants à la préparation et la réalisation des futurs examens périodiques, l'EDPB réaffirme que tout document pertinent, y compris la correspondance, devrait être communiqué par écrit au comité suffisamment longtemps avant les examens.

Pour le comité européen de la protection des données

La présidente

(Anu Talus)