Avis 32/2021 concernant le projet de décision d'exécution de la Commission européenne conformément au règlement (UE) 2016/679 sur le niveau de protection adéquat des données à caractère personnel en République de Corée

Version 1.0

Adopté le 24 septembre 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

TABLE DES MATIÈRES

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 (le «**RGPD**»),

vu l'accord sur l'Espace économique européen («**EEE**») et en particulier son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 12 et 22 de son règlement intérieur,

A ADOPTÉ LE PRÉSENT AVIS:

1. SYNTHÈSE

1. Le 16 juin 2021, la Commission européenne a lancé le processus officiel en vue de l'adoption de son projet de décision d'exécution (le «**projet de décision**») sur le niveau de protection adéquat des données à caractère personnel en République de Corée dans le cadre de la Loi sur la protection des informations à caractère personnel («la loi **PIPA**»), conformément au RGPD[2].

2. Le même jour, la Commission européenne a demandé l'avis du comité européen de la protection des données (l'«**EDPB**»)[3]. L'appréciation par l'EDPB de l'adéquation du niveau de protection accordé en République de Corée a été effectuée sur la base de l'examen du projet de décision lui-même ainsi que d'une analyse de la documentation mise à disposition[4] par la Commission européenne.

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

4. L'EDPB a utilisé comme référence principale pour ces travaux ses critères de référence pour l'adéquation avec le RGPD[5] («**les critères de référence**») adoptés en février 2018 et les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance[6].

1.1. Domaines de convergence

5. L'objectif principal de l'EDPB consiste à donner un avis à la Commission européenne sur l'adéquation du niveau de protection accordé aux personnes dont les données à caractère personnel sont

[1] Dans le présent avis, on entend par «**États membres**» les «États membres de l'EEE».
[2] Voir le communiqué de presse https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2964.
[3] Ibidem.
[4] L'EDPB a fondé son analyse sur des traductions officielles effectuées par le gouvernement coréen.
[5] WP 254, Critères de référence pour l'adéquation avec le RGPD, 6 février 2018 (approuvé par l'EDPB, voir https://edpb.europa.eu/our-work-tools/general-guidance/endorsed-wp29-guidelines).
[6] Voir les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance, adoptées le 10 novembre 2020, https://edpb.europa.eu/our-work-tools/our-documents/preporki/recommendations-022020-european-essential-guarantees_en.

transférées à la République de Corée. Il importe de reconnaître que l'EDPB ne s'attend pas à ce que le cadre coréen de protection des données reproduise la législation européenne en la matière.

6. Toutefois, l'EDPB rappelle que, pour que le niveau de protection soit considéré comme adéquat, l'article 45 du RGPD et la jurisprudence de la Cour de justice de l'Union européenne (ci-après la«**CJUE**») exigent que la législation du pays tiers soit alignée sur l'essence des principes fondamentaux inscrits dans le RGPD. Dans ce contexte, le cadre coréen en matière de protection des données présente de nombreuses similitudes avec son équivalent européen, étant donné que l'un de ses principaux textes législatifs couvre à la fois le secteur public et le secteur privé et qu'il est complété par des actes législatifs sectoriels.

7. En ce qui concerne le contenu, l'EDPB note des domaines d'harmonisation essentiels entre le cadre du RGPD et le cadre coréen de protection des données en ce qui concerne certaines dispositions fondamentales telles que, par exemple, les notions (par exemple, les «informations à caractère personnel», le «traitement», la «personne concernée»); les fondements du traitement loyal et licite pour des finalités légitimes; la limitation de la finalité; la qualité et la proportionnalité des données; la conservation, la sécurité et la confidentialité des données; la transparence; et les catégories particulières de données.

8. Outre ce qui précède, l'EDPB se félicite des efforts déployés par la Commission européenne et les autorités coréennes pour garantir que la République de Corée assure un niveau de protection adéquat à celui du RGPD grâce à l'adoption de notifications par l'autorité de contrôle coréenne (qui ne s'appliquent pas uniquement aux données à caractère personnel transférées de l'EEE vers la Corée) dans le but de combler les lacunes entre le RGPD et le cadre coréen de protection des données. Dans ce contexte, l'EDPB souhaite souligner la pertinence de ces notifications pour l'évaluation de l'adéquation de la République de Corée, en notant, par exemple, qu'elles apportent des précisions pertinentes sur certaines garanties importantes, notamment en ce qui concerne le champ d'application des exemptions de la loi PIPA pour le traitement des informations à caractère personnel pseudonymisées à des fins scientifiques, de recherche et de statistiques, les transferts ultérieurs et les règles applicables dans le contexte de l'accès des autorités publiques aux données.

1.2. Les difficultés

9. Si l'EDPB a identifié de nombreux aspects du cadre coréen en matière de protection des données qui sont essentiellement équivalents au cadre européen, il a également conclu que certains aspects pourraient nécessiter un examen et des éclaircissements plus détaillés. Plus précisément, l'EDPB estime que les éléments suivants devraient être évalués de manière plus approfondie afin de garantir que le niveau de protection essentiellement équivalent est atteint, et qu'ils devraient faire l'objet d'un suivi attentif de la part de la Commission européenne.

1.2.1. Généralités

10. L'EDPB note que la notification n° 2021-1 *a le statut de règle administrative juridiquement contraignante pour le responsable du traitement des informations à caractère personnel, en ce sens que toute violation de la notification peut être considérée comme une violation des dispositions pertinentes de la loi PIPA*[7]. Toutefois, étant donné que la notification ne contient pas en soi de règles supplémentaires, mais plutôt des éclaircissements sur la manière dont le texte légal de la loi PIPA devrait être compris, et compte tenu de son importance globale, en particulier en ce qui concerne les dispositions relatives à la pseudonymisation prévues par la loi PIPA qui, d'après ce que comprend l'EDPB, font l'objet d'affaires judiciaires en cours, l'EDPB invite la Commission européenne à fournir des informations supplémentaires sur le caractère contraignant, exécutoire et la validité de la notification n° 2021-1 et recommande un suivi attentif de la manière dont celle-ci est respectée dans

[7] Voir la section I de l'annexe I du projet de décision.

la pratique, non seulement par l'autorité de contrôle coréenne, mais également par les tribunaux, en particulier si le niveau de protection équivalent offert par le cadre juridique coréen est fondé sur les éclaircissements qui figurent dans ladite notification.

1.2.2. Aspects généraux liés à la protection des données

11. En ce qui concerne le champ d'application de la décision d'adéquation, l'EDPB note qu'il couvrira les transferts depuis le cadre juridique de l'EEE vers les «responsables du traitement des informations à caractère personnel» à la fois publics et privés relevant du champ d'application de la loi PIPA. L'EDPB croit comprendre que les entités agissant en tant que sous-traitants au sens du RGPD sont incluses dans ce terme. Toutefois, afin d'éviter tout malentendu, il invite la Commission européenne à préciser que la décision d'adéquation couvrira également les transferts vers des «sous-traitants» en Corée.

12. Un aspect important que l'EDPB souhaite souligner concerne la notion d'informations pseudonymisées dans le cadre coréen de la protection des données. En vertu de la législation coréenne, des exemptions à un certain nombre de dispositions pertinentes, y compris celles relatives aux droits des personnes concernées et à la conservation des données, s'appliquent au traitement d'informations à caractère personnel pseudonymisées. D'après la Commission européenne, c'est uniquement le cas lorsque des informations à caractère personnel pseudonymisées sont traitées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt public. Toutefois, cette affirmation est principalement étayée par la notification n° 2021-1, qui rend très pertinent, dans ce contexte, le besoin déjà mentionné d'informations supplémentaires sur cette notification et d'un contrôle de sa nature contraignante, de son caractère exécutoire et de sa validité. En outre, l'EDPB invite la Commission européenne à poursuivre l'évaluation de l'incidence de la pseudonymisation en vertu du droit coréen et, surtout, de la manière dont elle est susceptible d'affecter les libertés et droits fondamentaux des personnes concernées dont les données à caractère personnel sont transférées vers la République de Corée en vertu de la décision d'adéquation. En particulier, l'EDPB invite la Commission européenne à poursuivre l'évaluation des dérogations prévues à l'article 28, paragraphe 7, de la loi PIPA et à l'article 40, paragraphe 3, de la loi coréenne sur l'utilisation et la protection des renseignements en matière de crédit («CIA») et à surveiller attentivement leur application et la jurisprudence pertinente afin de veiller à ce que les droits des personnes concernées ne soient pas indûment restreints lorsque des données à caractère personnel transférées en vertu de la décision d'adéquation sont traitées à ces fins.

13. En outre, l'EDPB note qu'en vertu du droit coréen, le droit de retirer son consentement n'existe que dans certaines circonstances particulières, et invite dès lors la Commission européenne à évaluer plus avant l'incidence de l'absence d'un droit général de retrait du consentement, et à fournir des assurances supplémentaires afin de s'assurer qu'un niveau essentiel de protection des données soit garanti à tout moment, notamment, le cas échéant, en clarifiant le rôle du droit de suspension au titre de la loi PIPA, en l'absence d'un droit général de retrait du consentement.

14. En ce qui concerne les transferts ultérieurs, l'EDPB reconnaît que le consentement éclairé de la personne concernée servira généralement de base aux transferts de données d'un responsable du traitement d'informations à caractère personnel établi en Corée vers un destinataire établi dans un pays tiers, et que la notification n° 2021-1 prévoit que les personnes doivent être informées du pays tiers auquel leurs données seront fournies. Toutefois, l'EDPB invite la Commission européenne à veiller à ce que les informations à fournir à la personne concernée comprennent également des renseignements sur les risques éventuels des transferts découlant du défaut de protection adéquate dans le pays tiers ainsi que de l'absence de garanties appropriées. En outre, l'EDPB souhaiterait obtenir l'assurance, dans la décision d'adéquation, que les données à caractère personnel ne seront pas transférées par les responsables coréens responsables du traitement des données à caractère personnel vers un pays tiers dans une situation où, en vertu du RGPD, le consentement valable ne pourrait pas être donné, par exemple en raison d'un déséquilibre des pouvoirs.

15. En ce qui concerne la désignation des membres de l'autorité de contrôle coréenne, bien que la procédure formelle soit conforme au RGPD et réponde donc au critère de l'équivalence avec le cadre juridique de l'EEE, l'EDPB souhaiterait que la Commission européenne surveille toute évolution susceptible d'affecter l'indépendance des membres de l'autorité de contrôle sud-coréenne.

16. En ce qui concerne le budget, toujours sur la base des informations fournies par la Commission européenne, aucune référence n'est faite aux spécificités du personnel affecté à la Commission coréenne de protection des informations à caractère personnel («PIPC») ni aux ressources financières mises à sa disposition. L'EDPB souhaiterait donc que des informations supplémentaires soient fournies dans le projet de décision sur ces deux sujets pertinents.

1.2.3. L'accès des autorités publiques aux données transférées vers la République de Corée

17. L'EDPB a également analysé le cadre juridique coréen en ce qui concerne l'accès du gouvernement, à des fins répressives et de sécurité nationale, aux données à caractère personnel transférées de l'EEE vers la Corée. Tout en prenant acte des déclarations et assurances fournies par le gouvernement coréen, telles qu'elles sont exposées à l'annexe II du projet de décision, l'EDPB a recensé un certain nombre d'aspects qui nécessitent des éclaircissements ou soulèvent des préoccupations.

18. L'EDPB note que les dispositions de la loi PIPA s'appliquent sans restriction dans le domaine répressif. L'EDPB note également que le traitement des données dans le domaine de la sécurité nationale est soumis à un ensemble plus limité de dispositions inscrites dans la loi PIPA.

19. En ce qui concerne la divulgation volontaire d'informations à caractère personnel par les fournisseurs de télécommunications aux autorités nationales de sécurité, l'EDPB craint que la relation entre la section 3 de l'annexe I du projet de décision, qui précise que les fournisseurs doivent en principe informer la personne concernée lorsqu'ils se conforment volontairement à une demande, et l'article 58, paragraphe 1, point 2 de la loi PIPA, c'est-à-dire l'exemption partielle à des fins de sécurité nationale, n'est pas claire. Ceci pourrait rendre les exigences d'information inefficaces, ce qui compliquerait considérablement la revendication des droits des personnes concernées en matière de protection des données, en particulier en ce qui concerne le recours juridictionnel.

20. Bien que le projet de décision ne le précise pas explicitement, l'EDPB comprend, à la lecture des explications fournies par la Commission européenne, que le cadre juridique coréen ne permet pas l'interception en masse de données de télécommunications. Par conséquent, la jurisprudence récente de la Cour européenne des droits de l'homme («**la Cour EDH**») sur les régimes d'interception de masse ne serait pas directement pertinente pour l'appréciation du niveau de protection des données en Corée.

21. Le projet de décision ne contient aucune information sur le cadre juridique des transferts ultérieurs dans le domaine de la sécurité nationale. Si l'EDPB a compris que, de l'avis de la Commission européenne, les transferts ultérieurs à des fins de sécurité nationale sont suffisamment réglementés par les garanties et principes généraux découlant du cadre constitutionnel et de la loi PIPA, l'EDPB s'inquiète de savoir si ce dispositif peut être considéré comme satisfaisant aux exigences de précision et de clarté de la loi et s'il prévoit des garanties effectives et exécutoires. Les garanties auxquelles la Commission européenne fait référence sont de nature très générale et n'abordent pas, dans une base légale, les circonstances et conditions spécifiques dans lesquelles des transferts ultérieurs à des fins de sécurité nationale peuvent avoir lieu. Dans ce contexte, l'EDPB note également que la Commission européenne n'a pas tenu compte de l'existence d'accords internationaux entre la République de Corée et des pays tiers ou des organisations internationales susceptibles de prévoir des dispositions spécifiques pour le transfert international de données à caractère personnel par les services répressifs et/ou de renseignement vers des pays tiers. L'EDPB estime que la conclusion d'accords bilatéraux ou multilatéraux avec des pays tiers à des fins de coopération en matière répressive ou de renseignement

est susceptible d'affecter le cadre juridique coréen en matière de protection des données tel qu'il a été évalué.

22. L'EDPB note que le contrôle de l'application du droit pénal et des autorités nationales de sécurité est assuré par une combinaison de différents organes internes et externes, en particulier la PIPC, qui est dotée de pouvoirs d'exécution suffisants.

23. Afin de disposer de voies de recours effectives, les personnes concernées doivent pouvoir s'adresser à un organisme compétent qui satisfait aux exigences de l'article 47 de la charte des droits fondamentaux de l'Union européenne (la «**Charte**»), c'est-à-dire qui possède la compétence requise pour constater qu'un traitement de données a lieu, pour en vérifier la licéité, et qui dispose de pouvoirs réparatoires exécutoires en cas de traitement illicite de données. Dans ce contexte, l'EDPB demande à la Commission européenne de préciser si une réclamation auprès de la PIPC ou toute action devant une juridiction est soumise à des exigences de fond et/ou de procédure, telles que la charge de la preuve, et si les particuliers dans l'EEE seraient en mesure de remplir cette condition préalable.

1.3. Conclusion

24. L'EDPB estime que cette décision d'adéquation revêt une importance capitale, compte tenu également du fait que, sous réserve des exceptions mises en évidence dans l'avis, elle couvrira les transferts tant dans le secteur public que dans le secteur privé.

25. L'EDPB salue les efforts déployés par la Commission européenne et les autorités coréennes pour harmoniser le cadre juridique coréen avec celui de l'Europe. Les améliorations envisagées par la notification n° 2021-1 pour remédier à certaines différences entre les deux cadres sont très importantes et bien accueillies. Toutefois, l'EDPB constate qu'un certain nombre de préoccupations subsistent, notamment en ce qui concerne la notification n° 2021-1, ainsi que la nécessité d'éclaircissements supplémentaires sur d'autres questions, et le comité recommande à la Commission européenne de répondre aux préoccupations et aux demandes de clarification qu'il a formulées et de fournir de plus amples informations et explications sur les questions soulevées dans le présent avis.

2. INTRODUCTION

2.1. Cadre coréen de protection des données

26. Le principal acte législatif régissant la protection des données en République de Corée est la loi sur la protection des informations à caractère personnel (loi n°10465 du 29 mars 2011, modifiée en dernier lieu par la loi n° 16930 du 4 février 2020, «la loi **PIPA**»). Elle est complété par un décret d'exécution (décret présidentiel n° 23169 du 29 septembre 2011, modifié en dernier lieu par le décret présidentiel n° 30892 du 4 août 2020, le «décret d'application de la loi PIPA»), qui est juridiquement contraignant et exécutoire.

27. Outre la loi PIPA, le cadre coréen de protection des données comprend des «notifications» réglementaires publiées par l'autorité de contrôle coréenne, la Commission de protection des informations à caractère personnel («**PIPC**»), qui prévoit d'autres règles relatives à l'interprétation et à l'application de la loi PIPA. Récemment, la PIPC a adopté la notification n° 2021-1 du 21 janvier 2021 (qui modifiait la précédente notification n° 2020-10 du 1er septembre 2020, ci-après la «**notification n°2021-1**») concernant l'interprétation, l'application et l'exécution de certaines dispositions de la loi PIPA. Plus précisément, cette notification est le résultat de discussions sur l'adéquation qui ont eu lieu entre les autorités coréennes et la Commission européenne. Elle contient des précisions sur l'application de dispositions spécifiques de la loi PIPA, notamment en ce qui concerne le traitement des données à caractère personnel transférées vers la Corée sur la base de la décision d'adéquation

envisagée[8], et elle *a le statut de règle administrative juridiquement contraignante pour le responsable du traitement des informations à caractère personnel, en ce sens que toute violation de la notification peut être considérée comme une violation des dispositions pertinentes de la loi PIPA*[9]. Dans ce contexte, l'EDPB souhaite faire observer que, bien qu'elle soit dénommée «règles complémentaires» dans le projet de décision, la notification ne contient pas de règles supplémentaires à proprement parler, mais plutôt des explications visant à clarifier la manière dont il convient d'interpréter le texte légal de la loi PIPA, en particulier en ce qui concerne les données transférées depuis l'EEE. Dans ce contexte, l'EDPB recommande un contrôle attentif du respect de la notification n° 2021-1 dans la pratique, en particulier en ce qui concerne son application non seulement par la PIPC, mais aussi par les tribunaux, notamment si le niveau de protection équivalent offert par le cadre juridique coréen est fondé sur les éclaircissements prévus dans ladite notification.

28. D'autres lois pertinentes en matière de protection des données dans le cadre législatif coréen fixent des règles pour le traitement des données à caractère personnel dans des secteurs d'activités spécifiques:

- la loi sur l'utilisation et la protection des renseignements en matière de crédit (la loi «**CIA**»), incluant son décret d'exécution (le «**décret d'application de la loi CIA**»), qui établit des règles spécifiques applicables aux opérateurs commerciaux et aux entités spécialisées (tels que les agences de notation de crédit, les établissements financiers) lorsque ceux-ci traitent des renseignements personnels en matière de crédit nécessaires pour déterminer la solvabilité des parties à des transactions financières ou commerciales;
- la loi sur la promotion de l'utilisation des réseaux d'information et de communication et la protection des données («la **loi sur les réseaux**»); et
- la loi sur la protection de la vie privée dans le secteur des communications («**CPPA**»)

29. Dans le domaine de l'accès du gouvernement, outre les dispositions pertinentes contenues dans les lois PIPA et CPPA, l'EDPB a examiné d'autres textes législatifs, à savoir la loi sur la procédure pénale («**CPA**»), la loi sur les activités de télécommunications («**TBA**»), la loi sur la déclaration et l'utilisation d'informations spécifiques sur les transactions financières («**ARUSFTI**») et la loi sur le service national de renseignement («**NISA»**).

2.2. Portée de l'évaluation de l'EDPB

30. Le projet de décision de la Commission européenne est le résultat d'une évaluation du cadre coréen en matière de protection des données, suivie de discussions avec le gouvernement coréen. Conformément à l'article 70, paragraphe 1, point s), du RGPD, l'EDPB doit rendre un avis indépendant sur les conclusions de la Commission européenne, recenser les insuffisances du cadre d'adéquation, le cas échéant, et s'efforcer de faire des propositions pour y remédier.

31. Afin d'éviter les répétitions et en vue de contribuer à l'évaluation du cadre juridique coréen, l'EDPB a choisi de se concentrer sur certains points spécifiques présentés dans le projet de décision et de fournir son analyse et son avis à leur sujet, en s'abstenant de reproduire la plupart des constatations et appréciations factuelles pour lesquelles le comité ne dispose d'aucun élément permettant de supposer que le droit de la République de Corée ne serait pas essentiellement équivalent au droit de l'EEE. En outre, conformément à la jurisprudence de la CJUE, une partie très importante de l'analyse porte sur le régime juridique de l'accès de la sécurité nationale aux données à caractère personnel transférées à la République de Corée, ainsi que sur la pratique de son service de sécurité nationale.

[8] Voir la section I de l'annexe I du projet de décision.
[9] Ibidem.

32. Dans son appréciation, l'EDPB a tenu compte du cadre européen applicable en matière de protection des données, notamment des articles 7, 8 et 47 de la Charte, qui protègent respectivement le droit à la vie privée et familiale, le droit à la protection des données à caractère personnel et le droit à un recours effectif et à accéder à un tribunal impartial, ainsi que de l'article 8 de la CEDH protégeant le droit à la vie privée et familiale. Outre ce qui précède, l'EDPB a pris en considération les exigences du RGPD ainsi que la jurisprudence pertinente.

33. L'objectif de cet démarche est de fournir à la Commission européenne un avis sur l'évaluation de l'adéquation du niveau de protection en République de Corée. Le concept de «niveau de protection adéquat», qui existait déjà dans le cadre de la directive 95/46/CE, a été renforcé par la CJUE. Il importe de rappeler la norme définie par la CJUE dans l'arrêt Schrems, à savoir que si le «niveau de protection» dans le pays tiers doit être «substantiellement équivalent» à celui qui est garanti dans l'Union, «*les moyens auxquels ce pays tiers a recours, à cet égard, pour assurer un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union*»[10]. Par conséquent, l'objectif n'est pas de refléter point par point la législation européenne, mais d'établir les exigences essentielles et fondamentales de la législation examinée. L'adéquation peut être obtenue en combinant les droits des personnes concernées et les obligations de ceux qui traitent les données à caractère personnel ou qui exercent un contrôle sur ce traitement et la supervision par des organes indépendants. Toutefois, les règles sur la protection des données ne sont effectives que si elles sont applicables et suivies en pratique. Il convient donc de tenir compte non seulement du contenu des règles applicables aux données personnelles transférées vers un pays tiers ou une organisation internationale, mais également du système mis en place afin de garantir l'effectivité de ces règles. Des mécanismes d'application efficaces sont essentiels pour assurer l'effectivité des règles sur la protection des données[11].

2.3. Commentaires généraux et inquiétudes

2.3.1. Engagements internationaux souscrits par la République de Corée

34. Conformément à l'article 45, paragraphe 2, point c), du RGPD et aux critères de référence pour l'adéquation avec le RGPD[12], lorsque la Commission européenne évalue le caractère adéquat du niveau de protection dans un pays tiers, elle doit tenir compte, entre autres, des engagements internationaux pris par le pays tiers, ou des autres obligations découlant de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations.

35. La Corée est signataire de plusieurs accords internationaux qui garantissent le droit au respect de la vie privée, tels que le Pacte international relatif aux droits civils et politiques (article 17), la Convention relative aux droits des personnes handicapées (article 22) et la Convention relative aux droits de l'enfant (article 16). En outre, la Corée, en tant que membre de l'OCDE, adhère au cadre de l'OCDE en matière de protection de la vie privée, en particulier aux lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel.

36. L'EDPB prend également acte de la participation de la Corée en tant qu'État observateur aux travaux du comité consultatif de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (+), bien qu'elle n'ait pas encore décidé d'y adhérer.

[10] C-362/14, *Maximilian Schrems contre Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, points 73-74.
[11] WP 254, p. 2.
[12] WP254, p. 2.

2.3.2. Champ d'application de la décision d'adéquation

37. Conformément au considérant 5 du projet de décision, la Commission européenne conclut que la République de Corée assure un niveau adéquat de protection des données à caractère personnel transférées par un responsable du traitement ou un sous-traitant dans l'Union à des responsables du traitement des informations à caractère personnel (par exemple, des personnes physiques ou morales, des organisations, des institutions publiques) relevant du champ d'application de la loi PIPA, à l'exception du traitement des données à caractère personnel pour des activités de missionnaires par des organisations religieuses et pour la désignation de candidats par des partis politiques[13], ou du traitement de renseignements personnels en matière de crédit conformément à la loi CIA par des responsables du traitement qui sont soumis à la surveillance de la Commission des services financiers.

38. L'EDPB note que la décision d'adéquation couvrira les transferts du cadre juridique de l'EEE vers les «responsables du traitement des informations à caractère personnel» publics et privés relevant du champ d'application de la loi PIPA. L'EDPB comprend que les entités agissant en tant que sous-traitants au sens du RGPD sont également couvertes par le terme «responsable du traitement des informations à caractère personnel», étant donné que la loi PIPA leur sera également applicable et que des obligations spécifiques s'appliquent lorsqu'un responsable du traitement des informations à caractère personnel («le donneur d'ordre») engage un tiers pour le traitement de ces informations («le prestataire extérieur»). Toutefois, afin d'éviter tout malentendu, l'EDPB invite la Commission européenne à préciser que la décision d'adéquation couvrira également les transferts à des «sous-traitants» en Corée et que le niveau de protection des données à caractère personnel transférées depuis l'EEE ne sera pas compromis, même dans de tels cas.

39. En outre, compte tenu du fait que la décision d'adéquation couvre également les transferts de données à caractère personnel entre organismes publics, l'EDPB croit savoir qu'il s'agira également des transferts entre autorités de contrôle de la protection des données et, par souci de clarté, invite la Commission européenne à se pencher particulièrement sur cette question.

40. En outre, en ce qui concerne les entités exclues du champ d'application de la décision d'adéquation, l'EDPB tient à souligner que ladite décision gagnerait à une identification plus claire des «organisations commerciales» qui sont soumises au contrôle de la PIPC (article 45, paragraphe 3, de la loi CIA) afin que les responsables du traitement et les sous-traitants établis dans l'EEE puissent facilement évaluer si l'importateur relève également du champ d'application de la décision d'adéquation avant de transférer des données à des entités relevant du champ d'application de la loi CIA ,ou à tout le moins, être alertés sur la nécessité d'évaluer cet aspect.

41. En ce qui concerne le champ d'application de la décision d'adéquation, l'EDPB a compris, à la lecture des explications complémentaires de la Commission européenne, que la Cellule de renseignements financiers de la Corée (ci-après la «**KOFIU**»), qui est instituée par la Commission des services financiers et supervise la prévention du blanchiment de capitaux et du financement du terrorisme en vertu de la loi ARUSFTI[14], est également exclue du champ d'application, étant donné qu'elle n'est compétente que pour les établissements financiers qui ne sont pas eux-mêmes couverts par le projet de décision. Toutefois, l'article 1, paragraphe 2, point c), du projet de décision exclut de son champ d'application uniquement les responsables du traitement des informations à caractère personnel qui sont soumis à la surveillance de la Commission des services financiers et qui traitent des renseignements personnels en matière de crédit dans le cadre de la loi CIA. Dans ce contexte, l'EDPB demande à la Commission européenne de préciser si la KOFIU et les activités de traitement de données menées par cette cellule elle-même relèvent du projet de décision.

[13] Pour plus de contexte, voir ci-dessous la section 3.1.2 du présent avis.
[14] Voir l'annexe II, section 2.2.3.1.

3. ASPECTS GÉNÉRAUX LIÉS À LA PROTECTION DES DONNÉES

3.1. Principes touchant au contenu

42. Le chapitre 3 des critères de référence pour l'adéquation avec le RGPD est consacré aux «principes touchant au contenu». Le système d'un pays tiers doit comporter ces principes pour que le niveau de protection assuré puisse être considéré comme substantiellement équivalent à celui garanti par la législation européenne.

43. Bien que le droit à la protection des données à caractère personnel ne soit pas expressément consacré par la Constitution coréenne à proprement parler, il est reconnu comme un droit fondamental, dérivé des droits constitutionnels à la dignité humaine et à la recherche du bonheur (article 10), à la vie privée (article 17) et au respect de la vie privée dans les communications (article 18). Ceci a été confirmé à la fois par la Cour suprême et la Cour constitutionnelle, comme indiqué dans le projet de décision de la Commission européenne[15]. L'EDPB prend acte de cette reconnaissance puisqu'il en déduit que la protection des données en tant que droit fondamental, conformément à l'article 37 de la Constitution coréenne,«*ne peut être limitée que par la loi et lorsque cela est nécessaire à la sécurité nationale, au maintien de l'ordre public ou au salut public*» et que,«*même lorsque de telles restrictions sont imposées, elles ne peuvent affecter l'essence de la liberté ou du droit*».

44. Selon la Commission européenne[16], la Cour constitutionnelle a jugé que les ressortissants étrangers sont également bénéficiaires de droits fondamentaux. Selon les déclarations officielles du gouvernement coréen[17], bien que la jurisprudence n'ait pas, jusqu'à présent, abordé spécifiquement le droit au respect de la vie privée des ressortissants non coréens, il est largement admis par les spécialistes que les articles 12 à 22 de la Constitution énoncent les «droits des êtres humains». En outre, la République de Corée a adopté une série de lois dans le domaine de la protection des données, telles que la loi PIPA, qui prévoient des garanties pour toutes les personnes, quelle que soit leur nationalité. À cet égard, l'EDPB note que l'article 6, paragraphe 2, de la Constitution prévoit que le statut des ressortissants étrangers est garanti par le droit international et les traités internationaux, ainsi que par la jurisprudence mentionnée dans le projet de décision, selon laquelle un «étranger» peut être titulaire de «droits fondamentaux». Compte tenu de la pertinence de la reconnaissance du droit à la protection des données pour les «ressortissants étrangers», l'EDPB attire l'attention de la Commission européenne sur la nécessité de continuer à surveiller la jurisprudence relative à la protection des données en tant que droit fondamental reconnu non seulement aux citoyens coréens, mais également à toutes les personnes concernées, afin de veiller à ce que le niveau de protection des personnes physiques garanti par le RGPD ne soit pas compromis lorsque des données à caractère personnel sont transférées vers la Corée en vertu de la décision d'adéquation.

3.1.1. Notions

45. Sur la base des critères de référence pour l'adéquation avec le RGPD, des notions et/ou principes fondamentaux en matière de protection des données devraient exister dans le cadre juridique du pays tiers. Ils ne doivent pas nécessairement reprendre la terminologie du RGPD, mais devraient refléter les notions ancrées dans la législation européenne relative à la protection des données et être en cohérence avec ces concepts. À titre d'exemple, le RGPD inclut les notions importantes suivantes:

[15] Voir le considérant 8 du projet de décision et la jurisprudence pertinente mentionnée dans la note de bas de page n° 10 du projet de décision, dont seuls des résumés en anglais sont disponibles.
[16] Voir le considérant 9 du projet de décision.
[17] Section 1.1 de l'annexe II du projet de décision.

«données à caractère personnel», «traitement de données à caractère personnel», «responsable du traitement», «sous-traitant», «destinataire» et «données sensibles»[18].

46. La loi PIPA contient un certain nombre de définitions telles que celles des «informations à caractère personnel», du «traitement» et de la «personne concernée», qui ressemblent étroitement aux termes correspondants du RGPD.

3.1.1.1. *Notion de données pseudonymisées*

47. Parmi les définitions formulées dans la loi PIPA, l'article 2, paragraphe 1 définit, en particulier, les informations à caractère personnel comme l'une des types d'informations suivantes relatives à une personne vivante: a) les informations qui identifient une personne par son nom complet, son numéro d'enregistrement de résident, son image, etc. et b) les informations qui, même si elles ne permettent pas en soi d'identifier une personne donnée, peuvent aisément être combinées avec d'autres informations permettant d'identifier une personne particulière. Dans ces derniers cas, il convient de déterminer s'il existe ou non cette facilité de combinaison en prenant raisonnablement en considération le temps, le coût, la technologie, etc. utilisés pour identifier la personne, et la probabilité que les autres informations puissent être obtenues.

48. En outre, conformément à l'article 2, paragraphe 1, point c) de la loi PIPA, les «informations pseudonymisées» sont également considérées comme des informations à caractère personnel. Les informations pseudonymisées sont définies comme les informations visées aux points a) ou b) ci-dessus qui sont pseudonymisées conformément aux paragraphes 1 et 2 et qui, de ce fait, ne permettent pas d'identifier une personne donnée sans l'utilisation ou la combinaison d'informations pour les restaurer dans leur état initial. Les informations totalement anonymisées sont exclues du champ d'application de la loi PIPA. Conformément à l'article 58, paragraphe 2, de la loi PIPA, cette dernière ne s'applique pas aux informations qui n'identifient plus un individu donné lorsqu'elles sont combinées à d'autres informations, en tenant compte raisonnablement du temps, du coût, de la technologie, etc.

49. Au considérant 17 de son projet de décision, la Commission européenne indique que cela correspond au champ d'application matériel du RGPD et à ses notions de «données à caractère personnel», de «pseudonymisation» et d'«informations anonymisées».

50. Toutefois, conformément à l'article 28, paragraphe 7, de la loi PIPA, les articles 20, 21, 27, 34 (paragraphe 1), 35 à 37, 39 (paragraphe 3, 4, 6 à 8), ne s'appliquent pas aux informations à caractère personnel pseudonymisées.

51. Dans son projet de décision, la Commission européenne indique que l'article 28, paragraphe 7, de la loi PIPA ne s'applique aux informations à caractère personnel pseudonymisées que lorsqu'elles sont traitées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt public[19]. Toutefois, cela ne découle pas directement de la lettre de la loi, mais des explications fournies dans la notification n° 2021-1[20]. Bien que l'EDPB reconnaisse qu'un argument peut être avancé sur la base de la structure et de la justification de la loi PIPA, selon laquelle le paragraphe 2 de l'article 28 de ladite loi devrait être compris et logiquement interprété comme s'appliquant également au paragraphe 7 du même article, compte tenu de l'importance de la notification n° 2021-1 dans l'évaluation, par la Commission européenne, de l'adéquation du niveau de protection des données à caractère personnel en République de Corée et afin d'éviter toute ambiguïté, le comité invite la Commission européenne

[18] WP254, p. 4.
[19] Voir, entre autres, le considérant 82 du projet de décision.
[20] Section 4 de l'annexe I du projet de décision.

à fournir des informations supplémentaires sur la nature contraignante, le caractère exécutoire et la validité de la notification n° 2021-1 et à contrôler son application dans ce contexte particulier.

52. Dans ce contexte, l'EDPB souhaite rappeler qu'en vertu du RGPD, la pseudonymisation est considérée comme une mesure de sécurité recommandée. En d'autres termes, en vertu du RGPD, les données pseudonymisées restent des données à caractère personnel auxquelles le RGPD s'applique pleinement. Sur la base de ce qui précède, l'EDPB craint que le niveau de protection du RGPD pour les données à caractère personnel pseudonymisées puisse être compromis lorsque des données à caractère personnel sont transférées vers la Corée. L'EDPB invite donc la Commission européenne à poursuivre l'évaluation de l'incidence de la pseudonymisation dans le cadre de la loi PIPA et, surtout, de la manière dont elle pourrait affecter les libertés et droits fondamentaux des personnes concernées dont les données à caractère personnel seraient transférées en République de Corée sur la base de la décision d'adéquation. Par conséquent, l'EDPB invite la Commission européenne à garantir que le niveau de protection des données à caractère personnel des personnes concernées dans l'EEE ne sera pas compromis après le transfert de ces données en République de Corée, même lorsque les données à caractère personnel transférées sont pseudonymisées.

3.1.1.2. *Notion de responsable du traitement des informations à caractère personnel*

53. L'article 2, paragraphe 5, de la loi PIPA contient une définition du «responsable du traitement des informations à caractère personnel» qui désigne une institution publique, une personne morale, une organisation ou une personne physique, etc. qui traite des informations à caractère personnel directement ou indirectement pour gérer des dossiers d'informations à caractère personnel «*dans le cadre de ses activités*». Or, dans les garanties supplémentaires énoncées dans la notification n° 2021-1, le terme «responsable du traitement des informations à caractère personnel» désigne une institution publique, une personne morale, une organisation, une personne physique, etc. qui traite des informations à caractère personnel directement ou indirectement pour gérer les dossiers d'informations à caractère personnel «*à des fins commerciales*». Au lieu de cela, la note de bas de page 272 du projet de décision indique ce qui suit, s'agissant de la notion de responsable du traitement des informations à caractère personnel: «*Conformément à la définition énoncée à l'article 2 de la loi PIPA, c'est-à-dire une institution publique, une personne morale, une organisation, une personne physique, etc. qui traite des informations à caractère personnel directement ou indirectement pour gérer des dossiers d'informations à caractère personnel "à des fins officielles ou commerciales"*».

54. L'EDPB reconnaît que ces incohérences peuvent être dues aux traductions du texte original fournies par les autorités coréennes et invite la Commission européenne à vérifier régulièrement la qualité et la fidélité des traductions. Toutefois, l'EDPB insiste sur le fait que pour pouvoir évaluer l'équivalence essentielle du niveau de protection des données du cadre juridique coréen, il est nécessaire de bien comprendre les finalités du traitement relevant du champ d'application matériel de la loi PIPA. En outre, dans ce contexte, l'EDPB observe que la loi PIPA n'utilise pas la même terminologie que le RGPD en ce qui concerne les notions de «responsable du traitement» et de «sous-traitant» et invite la Commission européenne à clarifier la définition et la portée correctes de la notion de «responsable du traitement des informations à caractère personnel», ainsi qu'à examiner particulièrement si ce terme couvre également les sous-traitants au sens du RGPD, étant donné que cela affecte directement le champ d'application de la décision d'adéquation[21].

[21] Voir également le point 38 ci-dessus.

3.1.2. Exemptions partielles prévues dans la loi PIPA

55. L'article 58, paragraphe 1, de la loi PIPA exclut l'application de certaines de ses parties (c'est-à-dire les articles 15 à 57) en ce qui concerne quatre catégories de traitement de données à caractère personnel décrites ci-dessous. Plus précisément, les exemptions concernent les dispositions de la loi PIPA pour des motifs spécifiques de traitement, certaines obligations en matière de protection des données, les modalités précises d'exercice des droits individuels ainsi que les règles régissant le règlement des litiges. Toutefois, l'EDPB note que certaines dispositions générales de la loi PIPA restent applicables, telles que celles relatives aux principes de protection des données (article 3 de la loi PIPA) et aux droits individuels (article 4 de la loi PIPA). En outre, l'article 58, paragraphe 4, de la loi PIPA prévoit des obligations spécifiques pour ces quatre catégories de traitement de données.

56. Premièrement, l'exemption partielle couvre les informations à caractère personnel collectées en vertu de la loi sur les statistiques pour le traitement par les institutions publiques. Au considérant 27 de son projet de décision, la Commission européenne déclare que, d'après les éclaircissements du gouvernement coréen, les données à caractère personnel traitées dans ce contexte concernent normalement des ressortissants coréens et ne peuvent inclure qu'exceptionnellement des informations sur les étrangers, notamment dans le cas de statistiques sur l'entrée et la sortie du territoire, ou sur les investissements étrangers. Toutefois, selon le projet de décision, même dans ces situations, ces données ne sont pas, normalement, transférées par les responsables du traitement/sous-traitants situés dans l'EEE, mais seraient plutôt collectées directement par les autorités publiques coréennes.

57. L'EDPB admet le raisonnement de la Commission européenne sur l'exceptionnalité de l'application de la loi sur les statistiques au traitement des données à caractère personnel transférées en vertu de la décision d'adéquation; toutefois, le comité souhaiterait obtenir davantage d'informations et d'assurances quant aux garanties spécifiques qui seraient appliquées dans le cas où des données à caractère personnel transférées depuis l'EEE seraient ultérieurement collectées en vertu de la loi sur les statistiques en vue d'un traitement par des institutions publiques, notamment en ce qui concerne l'exercice des droits individuels des personnes concernées conformément à l'article 89, paragraphe 2, du RGPD, dans la mesure où ces droits ne risquent pas de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations ne sont pas nécessaires pour atteindre ces finalités.

58. De ce point de vue, l'application de l'article 4 de la loi PIPA à ce type de traitement semble également apporter des assurances complémentaires. Toutefois, l'EDPB souhaiterait que la décision d'adéquation contienne des informations et des éclaircissements supplémentaires sur les obligations spécifiques imposées à ces activités de traitement, conformément à l'article 58, paragraphe 4, de la loi PIPA,, notamment en ce qui concerne la minimisation des données, la limitation de leur conservation, les mesures de sécurité et le traitement des réclamations.

59. Deuxièmement, l'exemption partielle porte sur les informations à caractère personnel collectées ou demandées aux fins de l'analyse des informations liées à la sécurité nationale. L'EDPB est conscient du fait que, en matière de sécurité nationale, les États disposent d'une large marge d'appréciation reconnue par la Cour européenne des droits de l'homme. Le comité observe également que, conformément à l'article 37, paragraphe 2, de la Constitution coréenne, toute restriction aux libertés et aux droits, par exemple lorsque cela est nécessaire à la protection de la sécurité nationale, ne peut violer l'aspect essentiel de cette liberté ou de ce droit. En outre, l'EDPB prend note des garanties prévues à la section 6 de la notification n° 2021-1 en ce qui concerne le traitement des informations à caractère personnel à des fins de sécurité nationale, notamment les enquêtes sur les infractions et l'exécution. Toutefois, dans ce contexte, l'EDPB invite la Commission européenne à préciser davantage le champ d'application des exemptions, car il se demande si toutes les exemptions prévues à l'article 58, paragraphe 1, point 2 de la loi PIPA (chapitres III à VII) sont pertinentes pour le travail des

services de renseignement et si elles garantissent une équivalence avec les principes de nécessité et de proportionnalité. En particulier, l'EDPB invite la Commission européenne à fournir davantage de précisions sur les circonstances dans lesquelles un service de renseignement pourrait se prévaloir des exemptions. L'EDPB estime qu'il est nécessaire de surveiller de près l'incidence de ces limitations dans la pratique, en particulier sur l'exercice et l'application effectifs des droits des personnes concernées.

60. Troisièmement, l'exemption partielle s'applique aux «*informations à caractère personnel traitées temporairement lorsqu'elles sont urgentes pour des raisons de sûreté et de sécurité publiques, de santé publique, etc.*» Selon le considérant 29 du projet de décision de la Commission européenne, cette catégorie est interprétée strictement par la PIPC et ne s'applique qu'en cas d'urgence nécessitant une action immédiate, par exemple pour le suivi d'agents infectieux ou pour le sauvetage et l'aide aux victimes de catastrophes naturelles.

61. L'EDPB souligne également que toute dérogation au niveau de protection des données à caractère personnel devrait faire l'objet d'une interprétation stricte. Dans le même temps, l'EDPB observe que la disposition n'est pas strictement définie et ne fournit pas une liste exhaustive d'exemples de situations dans lesquelles le traitement d'informations à caractère personnel pourrait être considéré comme «*urgent*». Par exemple, l'EDPB s'interroge sur la question de savoir si les transferts internationaux de données sanitaires pendant la pandémie actuelle de COVID-19 relèvent également du champ d'application de cette exemption. À la lumière de ce qui précède, l'EDPB invite la Commission européenne à fournir des précisions supplémentaires sur le champ d'application de cette exemption et à surveiller pleinement son application et sa portée afin de s'assurer qu'elle n'entraîne pas une baisse du niveau de protection des données à caractère personnel en provenance de l'EEE après le transfert vers la Corée sur la base de la décision d'adéquation.

62. Enfin, l'exemption partielle s'applique aux informations à caractère personnel recueillies ou utilisées à des fins de compte rendu par la presse, d'activités de missionnaires menées par des organisations religieuses et de désignation de candidats par les partis politiques[22]. En ce qui concerne le traitement d'informations à caractère personnel par la presse pour des activités journalistiques, la Commission européenne indique au considérant 31 de son projet de décision que l'équilibre entre la liberté d'expression et d'autres droits, y compris le droit au respect de la vie privée, est assuré par la loi sur l'arbitrage et les recours, etc. pour les dommages causés par les articles de presse (ci-après la «**loi sur la presse**»), et présente des garanties spécifiques qui découlent de la loi sur la presse. L'EDPB invite toutefois la Commission européenne à surveiller pleinement cette exemption et la jurisprudence pertinente afin de garantir, dans la pratique du cadre juridique coréen, un niveau équivalent de protection des données.

3.1.3. Fondements du traitement loyal et licite pour des finalités légitimes

63. Selon les critères de référence pour l'adéquation avec le RGPD, conformément à ce règlement, les données doivent être traitées de manière licite, loyale et légitime. Les fondements juridiques au titre desquels des données à caractère personnel peuvent être traitées loyalement, licitement et légitimement doivent être définis de façon suffisamment claire. Le cadre européen reconnaît plusieurs de ces fondements juridiques, notamment des dispositions de la législation nationale, le consentement de la personne concernée, l'exécution d'un contrat ou les intérêts légitimes du responsable du traitement ou d'une tierce partie qui ne l'emporte pas sur les intérêts de la personne concernée.

[22] En conséquence, le traitement d'informations à caractère personnel par des organisations religieuses dans le cadre de leurs activités missionnaires et par les partis politiques dans le cadre de la désignation de candidats sont également exclus du champ d'application de la décision d'adéquation. Voir également le point 37 ci-dessus à la section 2.3.2.

64. Suivant une structure similaire à celle du RGPD, la loi PIPA introduit tout d'abord le principe de légalité, d'équité et de transparence au début de son texte (article 3, paragraphe 1 et 2, de la loi PIPA), en définissant ensuite, aux articles 15 à 19, les règles spécifiques régissant son application. Plus précisément, l'article 15 de la loi PIPA contient un inventaire des fondements juridiques sur lesquels les responsables du traitement des données peuvent s'appuyer pour collecter les informations à caractère personnel et les utiliser dans le cadre d'une collecte à visée spécifique. Ces fondements juridiques sont (1) le consentement éclairé de la personne concernée; (2) l'autorisation légale ou la nécessité du respect d'une obligation légale; (3) la nécessité de l'exercice des fonctions d'une institution publique; (4) la nécessité de la signature ou de l'exécution d'un contrat avec une personne concernée; (5) la nécessité de protéger les intérêts de la personne concernée ou d'un tiers à l'égard de la vie, de l'intégrité physique ou de la propriété contre un danger imminent (et le consentement préalable ne peut être obtenu); (6) la nécessité de satisfaire un intérêt justifiable d'un responsable du traitement des informations à caractère personnel, supérieur à celui d'une personne concernée.

65. En outre, l'article 17 de la loi PIPA énumère les fondements juridiques applicables au partage d'informations à caractère personnel avec un tiers, qui comprennent (1) le consentement éclairé de la personne concernée; (2) l'autorisation légale ou la nécessité du respect d'une obligation légale; (3) la nécessité de l'exercice des fonctions d'une institution publique; et (4) la nécessité de protéger les intérêts de la personne concernée ou d'un tiers à l'égard de la vie, de l'intégrité physique ou de la propriété contre un danger imminent (et le consentement préalable ne peut être obtenu). Même en l'absence de consentement de la personne concernée, le partage d'informations à caractère personnel est autorisé lorsque cela est raisonnablement lié aux finalités pour lesquelles les informations à caractère personnel ont été initialement collectées (article 17, paragraphe 4, de la loi PIPA).

66. L'article 18 de la loi PIPA établit des règles spécifiques pour l'utilisation et le partage d'informations à caractère personnel lorsque cela ne relève pas de l'objectif initial de la collecte ou de la fourniture. Entre autres, ici aussi, le consentement est l'une de ces règles d'autorisation.

67. Tout en reconnaissant la grande similitude entre le droit coréen et le RGPD en ce qui concerne le principe de légalité et l'existence d'un droit général à la suspension (article 37 de la loi PIPA), qui peut également être invoqué lorsque des données à caractère personnel sont traitées sur la base du consentement, l'EDPB souhaite souligner l'absence d'un droit général de retirer son consentement dans le cadre de la loi PIPA[23]. Compte tenu de l'importance du consentement en tant que fondement juridique dans tous les scénarios susmentionnés, et compte tenu du rôle des droits individuels dans un système juridique de protection des données aux fins de la sauvegarde des droits et libertés fondamentaux des personnes concernées, l'EDPB invite la Commission européenne à poursuivre l'évaluation de l'incidence de l'absence d'un droit général de retrait du consentement en vertu du droit coréen et à fournir des assurances supplémentaires pour garantir à tout moment un niveau essentiel de protection des données tel que celui prévu par le RGPD, y compris, lorsque cela est nécessaire, en précisant le rôle du droit à la suspension dans ce cadre particulier.

[23] Même si les personnes concernées peuvent refuser leur consentement dans certaines circonstances, voir par exemple l'article 18, paragraphe 3, point 5, de la loi PIPA. En revanche, le droit de retirer son consentement ne semble exister que dans des cas spécifiques; en vertu de l'article 27, paragraphe 1, point 2, de la loi PIPA, les personnes concernées ont le droit de retirer leur consentement lorsqu'elles ne souhaitent pas que leurs informations à caractère personnel soient transférées à un tiers en raison du transfert de tout ou partie des activités du responsable du traitement des données, d'une fusion, etc.; conformément à l'article 39, paragraphe 7, de la loi PIPA, les utilisateurs peuvent retirer à tout moment leur consentement à la collecte, à l'utilisation et à la fourniture d'informations à caractère personnel auprès du fournisseur de services d'information et de communication, etc.; et conformément à l'article 37 de la loi CIA, une personne concernée peut révoquer le consentement qui avait été donné à un fournisseur/utilisateur de renseignements en matière de crédit.

3.1.4. Le principe de la limitation de la finalité

68. Les critères de référence pour l'adéquation avec le RGPD, conformément à ce règlement, prévoit que les données à caractère personnel soient traitées pour une finalité spécifique et utilisées ultérieurement uniquement dans la mesure où cela n'est pas incompatible avec la finalité du traitement.

69. En vertu de l'article 3, paragraphes 1 et 2, de la loi PIPA, les responsables du traitement des informations à caractère personnel précisent et explicitent les finalités du traitement et veillent à ce que ce dernier soit compatible avec ces finalités. Bien que ce principe soit confirmé dans d'autres dispositions [à savoir les articles 15, paragraphe 1, 18, paragraphe 1, et 19, paragraphe 1, de la loi PIPA], le traitement à des fins «raisonnablement connexes» est autorisé dans certaines circonstances (voir l'article 17, paragraphe 4, de la loi PIPA)[24] ainsi que l'utilisation hors finalité et la fourniture d'informations à caractère personnel (voir les articles 18 et 19 de la loi PIPA)[25].

70. L'EDPB croit savoir que, dans le cas de transferts de données à caractère personnel de l'EEE vers la République de Corée sur la base de la décision d'adéquation, la finalité de la collecte par les responsables du traitement établis dans l'EEE constitue la finalité pour laquelle les données sont transférées, applicable au traitement effectué par le responsable du traitement des informations à caractère personnel destinataire établi en Corée. Un changement de finalité par le responsable du traitement établi en Corée ne serait autorisé que conformément à l'article 18, paragraphe 2, points 1 à 3 de la loi PIPA, «*à moins que cela ne soit de nature à porter injustement atteinte aux intérêts d'une personne concernée ou d'un tiers*»[26]. Dans ce contexte, l'EDPB prend acte de la déclaration de la Commission européenne au considérant 55 du projet de décision, selon laquelle, lorsque des changements de finalité sont autorisés par des lois, ces dernières doivent respecter le droit fondamental au respect de la vie privée et à la protection des données. Toutefois, l'EDPB observe qu'aucune information spécifique n'a été fournie à l'appui de cette déclaration particulière, par exemple, aucune référence n'a été faite à l'article 37 de la Constitution (coréenne). Par conséquent, l'EDPB invite la Commission européenne à fournir des assurances et des garanties supplémentaires dans le projet de décision afin de garantir que toutes les lois autorisant un changement de finalité de traitement sont nécessaires pour respecter les libertés et droits fondamentaux des personnes concernées à la vie privée et à la protection des données.

3.1.5. Le principe de qualité et de proportionnalité des données

71. Le règlement général sur la protection des données dispose que les données soient être exactes et, si nécessaire, tenues à jour. Les données à caractère personnel devraient être adéquates, pertinentes et non excessives au regard des finalités de leur traitement.

72. Dans le cadre de la loi PIPA, les responsables du traitement des données doivent veiller à ce que les informations à caractère personnel soient exactes, complètes et actualisées dans la mesure nécessaire au regard des finalités pour lesquelles elles sont traitées (article 3, paragraphe 3, de la loi PIPA). Les responsables du traitement des informations à caractère personnel sont tenus de recueillir une quantité d'informations à caractère personnel aussi réduite que nécessaire pour remplir une finalité donnée. La charge de la preuve leur incombe à cet égard (article 16, paragraphe 1, de la loi PIPA).

73. Dans ce contexte, l'EDPB partage l'appréciation de la Commission européenne en ce qui concerne l'équivalence essentielle du niveau de protection en vertu de la loi PIPA par rapport au RGPD à cet égard.

[24] La compatibilité de la finalité doit être vérifiée à l'avance sur la base des critères énoncés à l'article 14-2 du décret d'application de la loi PIPA.
[25] Voir également le point 66 ci-dessus.
[26] Article 18, paragraphe 2, de la loi PIPA.

3.1.6. Principe de conservation des données

74. Conformément aux critères de référence pour l'adéquation avec le RGPD, en règle générale, les données ne devraient pas être conservées plus longtemps que ce qui est nécessaire à la réalisation des finalités pour lesquelles elles sont traitées. Conformément à l'article 21, paragraphe 1, de la loi PIPA, ce principe existe également en droit coréen. Dans le cadre de la loi PIPA, les responsables du traitement sont tenus de détruire sans délai les informations à caractère personnel lorsque ces informations deviennent inutiles à l'expiration de la période de conservation ou après la réalisation de la finalité prévue du traitement, à moins que des périodes de conservation légales ne s'appliquent.

75. L'EDPB est toutefois préoccupé par le fait que l'article 21, paragraphe 1, de la loi PIPA ne s'applique pas aux informations à caractère personnel pseudonymisées. L'EDPB prend acte du fait que, conformément à la section 4, point iii), de la notification n° 2021-1, «[...] *lorsqu'un responsable du traitement des informations à caractère personnel traite des informations pseudonymisées aux fins de l'établissement de statistiques, de recherches scientifiques, de la conservation des archives publiques, etc., et que les informations pseudonymisées n'ont pas été détruites une fois que la finalité spécifique du traitement a été remplie, conformément à l'article 37 de la Constitution et à l'article 3 (Principes de protection des informations à caractère personnel) de la loi, il anonymise les informations en vue de garantir qu'elles n'identifient plus une personne particulière, seules ou combinées à d'autres informations, en tenant compte raisonnablement du temps, du coût, de la technologie, etc., conformément à l'article 58, paragraphe 2, de la loi PIPA*.» [27]Étant donné, ici aussi, l'importance de la notification n° 2021-1, et en vue d'obtenir des certitudes juridiques sur l'équivalence du niveau de protection des données à caractère personnel transférées en République de Corée en vertu de la décision d'adéquation, l'EDPB réitère son appel à la Commission européenne afin que cette dernière fournisse des informations supplémentaires notamment sur la manière dont la notification n°2021-1 est rendue contraignante, et dont sont garantis son caractère exécutoire et sa validité.

3.1.7. Le principe de sécurité et de confidentialité

76. Comme il est décrit dans les critères de référence pour l'adéquation avec le RGPD, le principe de sécurité et de confidentialité exige des entités de traitement des données qu'elles veillent à ce que les données à caractère personnel soient traitées de façon à garantir la sécurité de ces données, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées. Le niveau de sécurité devrait tenir compte de l'état des connaissances et des coûts correspondants.

77. La Commission européenne a identifié un principe similaire de sécurité des données à l'article 3, paragraphe 4, de la loi PIPA, qui est précisé plus en détail à l'article 29 de cette dernière. En outre, les dispositions relatives à la sécurité des données s'appliquent lorsque le responsable du traitement des informations à caractère personnel a recours à un «prestataire extérieur». La sécurité du traitement doit être assurée au moyen de garanties techniques et de gestion, qui doivent également figurer dans l'accord contraignant sur le traitement des données (article 26 de la loi PIPA et article 28 de son décret d'application). En outre, en vertu de la loi PIPA, des obligations spécifiques s'appliquent en cas de violation de données, notamment l'obligation d'informer les personnes concernées et l'autorité de contrôle lorsque le nombre de personnes concernées dépasse le seuil applicable (article 34 de la loi PIPA en liaison avec l'article 39 du décret présidentiel sur la loi PIPA), sauf lorsque les données concernées sont des informations à caractère personnel pseudonymisées traitées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt public (article 28, paragraphe 7,

[27] Voir également le point 51 ci-dessus, à la section 3.1.1.1 du présent avis, ainsi que le point 52 pour les préoccupations générales de l'EDPB concernant l'incidence de la pseudonymisation en vertu du droit coréen.

de la loi PIPA). Ici aussi[28], l'EDPB s'inquiète des larges exemptions pour les informations pseudonymisées et demande une nouvelle fois à la Commission européenne de poursuivre l'évaluation de cet aspect afin de garantir qu'un niveau de protection essentiellement équivalent soit prévu par le droit coréen[29].

78. Néanmoins, somme toute, l'EDPB est satisfait de l'évaluation et de la conclusion de la Commission européenne concernant l'équivalence essentielle du droit coréen au regard des principes de sécurité et de confidentialité.

3.1.8. Le principe de transparence

79. Sur la base de l'article 5, paragraphe 1, point a), du RGPD, la transparence est un principe fondamental du système de protection des données de l'Union. Le considérant 39 du RGPD définit la fonction essentielle de ce principe en indiquant que *«[l]e fait que des données à caractère personnel concernant des personnes physiques sont collectées, utilisées, consultées ou traitées d'une autre manière et la mesure dans laquelle ces données sont ou seront traitées devraient être transparents à l'égard des personnes physiques concernées. [...] Les personnes physiques devraient être informées des risques, règles, garanties et droits liés au traitement des données à caractère personnel et des modalités d'exercice de leurs droits en ce qui concerne ce traitement.»*

80. Les critères de référence pour l'adéquation avec le RGPD considèrent la «transparence» comme l'un des principes touchant au contenu dont il convient de tenir compte lors de l'évaluation de l'équivalence essentielle du niveau de protection assuré par un pays tiers. Plus précisément, ils disposent que *«[c]haque personne devrait être informée de façon claire, aisément accessible, concise, transparente et compréhensible des principaux éléments du traitement des données à caractère personnel la concernant. Ces informations devraient comprendre la finalité du traitement, l'identité du responsable du traitement, les droits mis à sa disposition et d'autres informations dans la mesure où celles-ci sont nécessaires pour garantir un traitement loyal. Dans certaines conditions, il peut y avoir des exceptions à ce droit à l'information, notamment pour protéger des enquêtes criminelles, la sécurité nationale, l'indépendance de la justice et des procédures judiciaires ou d'autres objectifs importants d'intérêt public général, conformément à l'article 23 du RGPD.»*

81. De même, comme c'est le cas avec le RGPD, dans le cadre de la loi PIPA, un principe général de transparence exige que les responsables du traitement des informations à caractère personnel communiquent publiquement leur politique en matière de respect de la vie privée et d'autres questions liées au traitement des informations à caractère personnel (article 3, paragraphe 5, de la loi PIPA). Des obligations d'information spécifiques s'appliquent lorsque les responsables du traitement des informations à caractère personnel cherchent à obtenir le consentement des personnes concernées pour la collecte et le traitement d'informations à caractère personnel (article 15, paragraphe 2, de la loi PIPA), pour le partage d'informations à caractère personnel avec un tiers (article 17, paragraphe 2, de la loi PIPA) et pour un traitement hors finalité (article 18, paragraphe 3, de la loi PIPA). Il convient de noter que ces obligations d'information s'appliquent également *mutatis mutandis* au prestataire extérieur (article 26, paragraphe 7, de la loi PIPA).

82. L'EDPB prend acte et se félicite des garanties supplémentaires prévues à la section 3, points i) et ii), de la notification n° 2021-1[30] concernant les informations à fournir aux personnes concernées lorsque leurs données sont transférées par une entité de l'EEE, compte tenu du fait que, conformément à l'article 20, paragraphe 1, de la loi PIPA, lorsque les données n'ont pas été recueillies auprès des personnes concernées, ces dernières ne sont informées que sur demande, tandis qu'un droit général à être informé n'est reconnu en vertu de l'article 20, paragraphe 2, de la loi PIPA lorsque certaines

[28] Comme déjà indiqué aux points 51 à 52 ci-dessus et à la section 3.1.1.1 du présent avis.
[29] Voir également les sections 3.1.6 et 3.1.10 du présent avis.
[30] Annexe I du projet de décision.

opérations de traitement dépassent les seuils fixés dans le décret d'application de ladite loi (article 15, paragraphe 2).

83. Dans l'ensemble, l'EDPB est convaincu que le niveau de protection prévu par le droit coréen en ce qui concerne le principe de transparence est essentiellement équivalent à celui garanti par le RGPD.

3.1.9. Catégories particulières de données à caractère personnel

84. Pour que le système de protection des données d'un pays tiers soit reconnu comme offrant un niveau de protection des données à caractère personnel essentiellement équivalent à celui du RGPD, des garanties spécifiques devraient exister lorsque des catégories particulières de personnes au sens des articles 9 et 10 du RGPD sont concernées.

85. Dans le cadre de la loi PIPA, des dispositions spécifiques s'appliquent au traitement des informations dites sensibles, qui incluent les informations à caractère personnel révélant l'idéologie, les convictions, l'adhésion à un syndicat ou à un parti politique ou la radiation de ceux-ci, les opinions politiques, la santé, la vie sexuelle et d'autres informations à caractère personnel susceptibles de menacer sensiblement le respect de la vie privée de toute personne concernée, ainsi que, par référence au décret d'application de la loi PIPA, les informations d'ADN obtenues à partir de tests génétiques, les données qui constituent un casier judiciaire; les informations à caractère personnel résultant de techniques spécifiques de traitement des données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne, aux fins de son identification unique; et les informations à caractère personnel révélant l'origine raciale ou ethnique.

86. À l'instar du RGPD, le droit coréen en matière de protection des données interdit le traitement d'informations sensibles à moins que des exemptions spécifiques ne s'appliquent, à savoir (1) l'information de la personne concernée et l'obtention d'un consentement spécifique et (2) des dispositions juridiques autorisant le traitement (article 23, paragraphe 2, de la loi PIPA).

87. Sur cette base, l'EDPB souscrit en principe à la conclusion de la Commission européenne concernant l'équivalence essentielle du droit coréen en ce qui concerne le traitement de catégories particulières de données à caractère personnel. Toutefois, l'EDPB tient à faire observer que ni le manuel de la loi PIPA, ni les précisions fournies par la PIPC ne lui ont suggéré une interprétation de l'expression «vie sexuelle» comme recouvrant également l'orientation ou les préférences sexuelles de l'individu, qui n'ont pas été incluses dans la notification n° 2021-1. L'EDPB invite donc la Commission européenne à fournir ces informations afin de pouvoir les évaluer de manière indépendante. En outre, l'EDPB invite la Commission européenne à citer expressément les documents sur lesquels figurent les informations auxquelles elle se réfère à ce sujet.

3.1.10. Droits d'accès, de rectification, d'effacement et d'opposition

88. Dans le cadre juridique coréen, les droits des personnes concernées sont reconnus à l'article 3, paragraphe 5, de la loi PIPA, en vertu duquel le responsable du traitement des informations à caractère personnel garantit les droits des personnes concernées énumérés à l'article 4 de la loi PIPA et précisés aux articles 35 à 37, 39 et 39, paragraphe 2, de ladite loi et, comme pour les «renseignements personnels en matière de crédit» (c'est-à-dire les renseignements en matière de crédit nécessaires pour déterminer la solvabilité des parties à des transactions financières ou commerciales — voir le considérant 3 du projet de décision)», aux articles 37, 38 et 38, paragraphe 3, de la loi CIA.

89. L'EDPB note que le droit d'accès (ainsi que le droit de rectification et d'effacement qui peuvent être exercés par une «*personne concernée ayant accédé à ses informations à caractère personnel en vertu de l'article 35» de la loi PIPA*) peut être limité ou refusé «*lorsque l'accès est interdit ou limité par la loi», «lorsque l'accès peut causer un préjudice à la vie ou à l'intégrité physique d'un tiers, ou une*

atteinte injustifiée aux biens et autres intérêts d'autrui», et, en outre, pour les institutions publiques, lorsque l'octroi de l'accès «*entraînerait de graves difficultés»* dans l'exercice de certaines fonctions, précisées dans l'article 35, paragraphe 4, de la loi PIPA[31]. Des dispositions similaires figurent également à l'article 37 de la loi PIPA concernant le droit de suspension du traitement des informations à caractère personnel.

90. L'article 23 du RGPD autorise le droit de l'Union ou le droit de l'État membre à limiter les droits individuels lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir, entre autres, la protection de la personne concernée ou des droits et libertés d'autrui et «*une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g) [du même article]*».

91. Dans ce contexte, l'EDPB souhaiterait obtenir des assurances générales, dans le projet de décision, sur la nécessité d'une législation limitant les droits des personnes concernées afin de satisfaire aux exigences de la Constitution coréenne selon lesquelles un droit fondamental ne peut être restreint que lorsque cela est nécessaire pour assurer la sécurité nationale ou le maintien de l'ordre public, et cette limitation ne peut affecter l'essence de la liberté ou du droit concerné (article 37, paragraphe 2, de la Constitution coréenne).

92. En outre, en ce qui concerne l'exception relative à «*une atteinte injustifiée aux biens ou à d'autres intérêts d'autrui*», l'EDPB reconnaît que cela «*implique qu'il soit procédé à un équilibre entre les droits et libertés constitutionnellement protégés de la personne, d'une part, et d'autrui, d'autre part*»[32], mais il invite la Commission européenne à surveiller pleinement l'application de cette exception et la jurisprudence pertinente afin de garantir, dans la pratique également, un niveau équivalent de protection des droits des personnes concernées dans le cadre juridique coréen.

93. De même, l'EDPB apprécierait un suivi attentif de l'application de l'exception pour les organismes publics, notamment en ce qui concerne les cas où l'octroi de l'accès serait considéré comme causant de «*graves difficultés*» dans l'exercice de leurs fonctions, étant donné que cette expression semble plus large que celle utilisée dans d'autres dispositions de la loi PIPA, par exemple à l'article 18, paragraphe 2, point 5[33], et devrait être interprétée de manière restrictive afin d'éviter de limiter indûment les droits des personnes concernées.

94. En outre, l'EDPB s'interroge sur la question de savoir si les exceptions en vertu desquelles les dispositions relatives à la transparence sur demande (article 20 de la loi PIPA) et aux droits individuels (articles 35 à 37 de la loi PIPA) — ainsi que les dispositions similaires concernant les exigences applicables aux fournisseurs de services d'information et de communication (article 39, paragraphe 2, 39, paragraphes 6 à 8, de la loi PIPA) et celles qui figurent dans la loi CIA (voir les exceptions prévues à l'article 40, paragraphe 3, de la loi CIA) — ne s'appliquent pas en ce qui concerne les informations pseudonymisées, lorsque celles-ci sont traitées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt public (article 28, paragraphe 7, de la loi PIPA), sont conformes aux garanties fournies par le cadre juridique européen.

95. Ces dispositions semblent introduire une dérogation générale pour ce type de traitement, tandis que le RGPD prévoit que, lorsque des données à caractère personnel (y compris pseudonymisées) sont

[31] Les mêmes conditions et exceptions aux droits d'accès et de rectification prévus par la loi PIPA s'appliquent également en ce qui concerne le droit d'accès et de rectification envisagé par la loi CIA pour les renseignements personnels en matière de crédit (note de bas de page 135 du projet de décision).
[32] Considérant 76 du projet de proposition.
[33] En ce qui concerne les exceptions à la limitation de l'utilisation et de la fourniture d'informations à caractère personnel hors finalité, l'article 18, paragraphe 2, point 5, de la loi PIPA fait référence aux situations dans lesquelles, pour les institutions publiques, «*il est impossible*» d'exercer les fonctions.

traitées à des fins de recherche scientifique ou historique ou à des fins statistiques, le droit de l'Union ou de l'État membre peut prévoir des dérogations aux droits des personnes concernées, mais uniquement «*dans la mesure où ces droits risqueraient de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques et où de telles dérogations sont nécessaires pour atteindre ces finalités*», la pseudonymisation ne constituant qu'une seule des mesures techniques et organisationnelles à adopter pour garantir le respect du principe de minimisation des données (article 89, paragraphe 1, du RGPD).

96. La Commission européenne considère que la dérogation envisagée à l'article 28, paragraphe 7, de la loi PIPA est également justifiée à la lumière de l'article 28, paragraphe 5, de ladite loi, en vertu duquel le responsable du traitement des informations à caractère personnel a l'interdiction expresse de traiter les informations pseudonymisées aux fins de l'identification d'une personne donnée, et elle renvoie à l'approche de l'article 11, paragraphe 2, du RGPD (lu conjointement avec le considérant 57 du RGPD) pour le traitement qui ne nécessite pas d'identification[34].

97. En effet*, conformément à* l'article 11 du RGPD, le responsable du traitement n'est pas tenu de «*conserver, d'obtenir ou de traiter des informations supplémentaires pour identifier la personne concernée*» à la seule fin de respecter le RGPD si, pour les finalités prévues, il peut traiter des données à caractère personnel qui ne nécessitent pas ou plus l'identification d'une personne concernée; dans de tels cas, lorsque le responsable du traitement est à même de démontrer qu'il n'est pas en mesure d'identifier la personne concernée, les droits de cette dernière ne s'appliquent pas. Comme l'a reconnu la Commission européenne[35], le RGPD exige donc, dans de tels cas, une impossibilité «pratique» pour le responsable du traitement et, conformément au principe de minimisation des données, reconnaît qu'aucune donnée supplémentaire ne doit être traitée «en raison» du RGPD.

98. Toutefois, l'EDPB estime que cette situation est différente de celle dans laquelle un responsable du traitement est pratiquement en mesure d'identifier la personne concernée, mais n'est pas autorisé à le faire par une disposition légale telle que celle visée à l'article 28, paragraphe 5, de la loi PIPA. À cet égard, l'EDPB se félicite des précisions apportées par la PIPC dans la notification n° 2021-1[36] confirmant que la section 3 de la loi PIPA (comprenant l'article 28, paragraphe 7) et l'exception prévue à l'article 40, paragraphe 3, de la loi CIA ne s'appliquent que lorsque des informations pseudonymisées sont traitées à des fins de recherche scientifique, de statistiques ou d'archivage dans l'intérêt public. Toutefois — et outre les préoccupations déjà exprimées quant au caractère contraignant effectif de la notification n° 2021-1[37], l'EDPB se demande toujours si les dérogations prévues à l'article 28, paragraphe 7 de la loi PIPA et à l'article 40, paragraphe 3, de la loi CIA pourraient être considérées comme nécessaires et proportionnées dans une société démocratique dans la mesure où elles restreignent les droits de la personne concernée dans tous les cas où des informations pseudonymisées sont traitées à de telles fins, c'est-à-dire même lorsque le responsable du traitement des informations à caractère personnel est pratiquement en mesure d'identifier la personne concernée et que les droits ne risquent pas de rendre impossible ou d'entraver sérieusement la réalisation des finalités spécifiques.

[34] Il convient de noter que le même raisonnement ne serait pas applicable en soi à l'exception prévue à l'article 40, paragraphe 3, de la loi CIA pour le traitement d'informations pseudonymisées en matière de crédit, parce que l'article 40, paragraphes 2 et 6, dispose que: «*Une société* d'*information en matière de crédit, etc., ne doit pas traiter les informations pseudonymisées de manière à ce qu'une personne spécifique puisse être identifiée à des fins lucratives ou déloyales*» et pourrait donc permettre une nouvelle identification à des fins loyales telles que celle de satisfaire à une demande de la personne concernée.

[35] Voir le considérant 82 du projet de décision.

[36] Section 4 de l'annexe I du projet de décision.

[37] Voir la section 3.1.1.1 ci-dessus.

99. En particulier, l'EDPB craint que ces dérogations ne soient pas justifiées et estime qu'elles devraient être examinées de manière plus approfondie, en particulier si elles sont appliquées par le responsable du traitement des informations à caractère personnel qui pseudonyme les données «*à des fins statistiques, de recherche scientifique et d'archivage dans l'intérêt public, etc.*», conformément à l'article 28, paragraphe 2, de la loi PIPA, «*sans le consentement des personnes concernées*» (et sans fournir les informations prévues à l'article 20 de la loi PIPA)[38], dans la mesure où ce responsable du traitement conserve les informations permettant la réidentification. En vertu du RGPD, les particuliers devraient pouvoir exercer leurs droits à l'égard de toute information permettant de les identifier ou de les distinguer, même si cette information est considérée comme «pseudonymisée», à moins que l'article 11 du RGPD ne s'applique. À cet égard, l'EDPB observe que ce n'est que lorsque ces données sont fournies à un tiers aux mêmes fins statistiques, de recherche scientifique et d'archivage que les informations susceptibles d'être utilisées pour identifier une personne donnée ne devraient pas être incluses et que, par conséquent, seul le responsable du traitement des informations à caractère personnel auquel des données pseudonymisées sont fournies conformément à l'article 28-2, paragraphe 2, de la loi PIPA ne serait probablement pas en mesure, «pratiquement», d'identifier la personne concernée sans informations supplémentaires.

100. En résumé, si l'on considère que, comme le reconnaît la Commission européenne, «*au lieu de s'appuyer sur la pseudonymisation comme garantie possible, la loi PIPA l'impose comme condition préalable pour mener à bien certaines activités de traitement à des fins statistiques, de recherche scientifique et d'archivage dans l'intérêt public (par exemple, pour pouvoir traiter les données sans consentement ou combiner différents ensembles de données*)»[39], mais qu'elle envisage, dans de tels cas, des restrictions importantes des droits des personnes concernées, l'EDPB appelle la Commission européenne à poursuivre l'évaluation des dérogations figurant à l'article 28, paragraphe 7, de la loi PIPA et à l'article 40, paragraphe 3, de la loi CIA, et à surveiller attentivement leur application et la jurisprudence pertinente[40] afin de veiller à ce que les droits des personnes concernées ne soient pas indûment restreints lorsque les données à caractère personnel transférées en vertu de la décision d'adéquation sont traitées à ces fins, en tenant compte du fait que dans de nombreux cas, ces droits aident également le responsable du traitement à garantir la qualité des données traitées.

3.1.11. Restrictions applicables aux transferts ultérieurs

101. Les critères de référence pour l'adéquation avec le RGPD précisent que le transfert ultérieur ne doit pas porter atteinte au niveau de protection des personnes physiques dont les données à caractère personnel sont transférées en vertu d'une décision d'adéquation et que, par conséquent, tout transfert ultérieur «*ne [devrait] 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 instructions pertinentes lors du traitement des données pour le compte du responsable du traitement*».

102. En ce qui concerne les transferts ultérieurs vers des prestataires extérieurs (c'est-à-dire des «sous-traitants») établis dans d'autres pays tiers,l'EDPB note qu'aucune règle particulière n'est en place dans le cadre juridique coréen pour couvrir ces cas et que, comme le considère la Commission européenne[41], un responsable coréen du traitement des informations à caractère personnel doit

[38] Voir l'article 28, paragraphe 7, de la loi PIPA, comme expliqué dans la notification n° 2021-1, selon laquelle certaines garanties figurant dans ladite loi, à savoir les «*articles 20, 21, 27, 34 (paragraphe 1), 35 à 37, 39 (paragraphe 3, 4, 6 à 8)*», ne s'appliquent pas aux informations pseudonymisées traitées aux fins de l'établissement de statistiques, de la recherche scientifique, de la conservation des archives publiques, etc.

[39] Considérant 42 du projet de proposition.

[40] Voir, par exemple, les contestations constitutionnelles d'Open Net (informations à l'adresse https://opennet.or.kr/19909 disponibles uniquement en coréen).

[41] Considérant 87 du projet de proposition.

veiller au respect des dispositions de la loi PIPA relatives à l'externalisation (article 26 de la loi PIPA) au moyen d'un instrument juridiquement contraignant, et il sera responsable des informations à caractère personnel qui ont été externalisées (article 26 de la loi PIPA).

103. En ce qui concerne les transferts ultérieurs à des tiers (c'est-à-dire à d'autres responsables du traitement des données à caractère personnel), conformément à l'article 17, paragraphe 3, de la loi PIPA, un responsable coréen du traitement des informations à caractère personnel doit informer les personnes concernées et obtenir leur consentement pour les transferts à l'étranger, et «*ne conclut pas de contrat de transfert transfrontalier d'informations à caractère personnel en violation de la loi PIPA*». L'EDPB note que cette dernière disposition garantira — comme l'envisage la Commission européenne[42] — qu'aucun contrat de transfert transfrontalier ne puisse contenir d'obligations allant à l'encontre des exigences imposées par la loi PIPA au responsable du traitement des informations à caractère personnel, et elle pourrait donc être considérée comme une garantie; toutefois, elle n'impose aucune obligation de mettre en place des garanties pour veiller à assurer au bénéficiaire le même niveau de protection que celui qui est accordé par la loi PIPA. Par conséquent, l'EDPB reconnaît que le consentement éclairé de la personne concernée servira généralement de fondements aux transferts de données d'un responsable du traitement d'informations à caractère personnel établi en Corée vers un destinataire établi dans un pays tiers.

104. À cet égard, les précisions supplémentaires fournies par la PIPC dans la notification n° 2021-1 concernant l'obligation d'informer les personnes sur le pays tiers auquel leurs données seront fournies[43] sont les bienvenues, car comme l'a souligné la Commission européenne[44], cela aiderait les personnes concernées dans l'EEE à prendre une décision en toute connaissance de cause sur l'opportunité de consentir ou non à une disposition étrangère.

105. Toutefois, comme cela a également été indiqué dans l'avis 28/2018 concernant le projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, il convient de souligner que, en vertu du RGPD, les personnes concernées doivent être explicitement informées des risques éventuels impliqués par de tels transferts, découlant de l'absence de protection adéquate dans le pays tiers et de l'absence de garanties appropriées avant le consentement. Cet avertissement devrait par exemple indiquer que le pays tiers est susceptible de ne pas disposer d'une autorité de contrôle et/ou de principes de traitement des données, et/ou de droits des personnes concernées[45]. Pour l'EDPB, il est essentiel de fournir ces informations à la personne concernée afin de lui permettre de donner un consentement éclairé en toute connaissance de ces faits particuliers concernant le transfert[46]. L'EDPB est donc préoccupé par les conclusions de la Commission européenne dans le projet de décision d'adéquation concernant ce type particulier de transferts. Généralement, les personnes concernées ne connaissent pas le cadre de protection des données dans les pays tiers. Par conséquent, une personne concernée ne saurait évaluer le risque d'un transfert par la seule connaissance du pays de destination spécifique. Il serait préférable de disposer d'informations claires sur les risques spécifiques d'un tel transfert de données à caractère personnel vers un pays situé en dehors du territoire de la République de Corée avant que la personne concernée ne donne son consentement.

106. Par conséquent, l'EDPB invite la Commission européenne à veiller à ce que les informations à fournir à la personne concernée «*sur les circonstances du transfert*» incluent des informations sur les risques éventuels du transfert découlant de l'absence de protection adéquate dans le pays tiers et de

[42] Considérant 88 du projet de proposition.

[43] Ibidem.

[44] Ibidem.

[45] Lignes directrices 2/2018 de l'EDPB relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, 25 mai 2018, p. 8.

[46] Lignes directrices 2/2018 de l'EDPB relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, 25 mai 2018, p. 7.

garanties appropriées. Ceci est important pour l'EDPB afin d'évaluer si les exigences en matière de consentement sont essentiellement équivalentes au RGPD.

107. En outre, compte tenu du fait que le consentement doit être donné de façon libre, spécifique, éclairée et univoque, l'EDPB souhaiterait obtenir l'assurance, dans la décision d'adéquation, que les données à caractère personnel ne seront pas transférées à un tiers dans un pays tiers par les responsables coréens du traitement dans une situation où, en vertu du RGPD, un consentement valable ne pourrait être fourni, par exemple en raison d'un déséquilibre des pouvoirs.

108. Dans les cas où le responsable du traitement peut fournir des informations à caractère personnel à un tiers à l'étranger sans le consentement de la personne concernée — c'est-à-dire (1) si des informations à caractère personnel sont fournies lorsque cela est raisonnablement lié à la finalité initiale de la collecte conformément à l'article 17, paragraphe 4, de la loi PIPA; et (2) si des informations à caractère personnel peuvent être fournies à un tiers dans des cas exceptionnels mentionnés à l'article 18, paragraphe 2, de la loi PIPA — l'EDPB prend note des précisions apportées par la PIPC à la section 2 de la notification n° 2021-1 (et se félicite de l'obligation envisagée pour le responsable du traitement établi en Corée et le destinataire à l'étranger de garantir, au moyen d'un acte juridiquement contraignant (tel qu'un contrat), un niveau de protection équivalent à celui de la loi PIPA, y compris en ce qui concerne les droits des personnes concernées).

3.1.12. Démarchage

109. Conformément aux paragraphes 2 et 3 de l'article 21 du RGPD et aux critères de référence pour l'adéquation avec le RGPD, la personne concernée doit toujours être en mesure de s'opposer sans frais au traitement des données à des fins de profilage et de démarchage.

110. En ce qui concerne le droit à la suspension prévu à l'article 37 de la loi PIPA, l'EDPB reconnaît que la Commission européenne considère que ce droit s'applique également lorsque les données sont utilisées à des fins de démarchage[47]. Toutefois, l'EDPB souhaiterait voir figurer dans le projet de décision des informations et des précisions supplémentaires en ce qui concerne cette appréciation et, en particulier, l'application pratique du droit de suspension dans le cadre du démarchage (par exemple, des références à la jurisprudence pertinente, etc.). À cet égard, l'EDPB souligne également que le droit de demander à un fournisseur/utilisateur de renseignements en matière de crédit de cesser de contacter une personne aux fins de la présentation ou d'une sollicitation d'achat de biens ou de services est explicitement énoncé par la loi CIA (article 37, paragraphe 2).

111. En outre, comme l'a reconnu la Commission européenne[48], dans le cadre juridique coréen, un tel traitement requiert généralement le consentement spécifique (supplémentaire) de la personne concernée (voir l'article 15, paragraphe 1, point 1, et l'article 17, paragraphe 2, point 1, de la loi PIPA).

112. Étant donné que l'on se saurait exclure que des données à caractère personnel transférées depuis l'EEE puissent être traitées en Corée à de telles fins, l'EDPB souhaiterait également voir figurer dans la décision d'adéquation des éclaircissements sur l'existence du droit, pour une personne concernée, de retirer son consentement[49],et sur son droit d'obtenir que ses données à caractère personnel soient effacées et ne soient plus traitées, lorsque le traitement est fondé sur le consentement (par exemple dans le cas d'un traitement effectué à des fins de marketing) et que la personne concernée l'a retiré.

[47] Considérant 79 du projet de proposition.
[48] Ibidem.
[49] Voir également ci-dessus, point 67: Bien que la possibilité de révoquer le consentement soit clairement envisagée à l'article 37, paragraphe 1, de la loi CIA, ce droit n'est mentionné qu'à deux reprises dans la loi PIPA pour des circonstances particulières, aux articles 27, paragraphes 1, point 2 et 39, paragraphe 7.

3.1.13. Prise de décision et profilage automatisés

113. Comme l'a reconnu la Commission européenne dans son projet de décision[50], la loi PIPA et son décret d'application ne contiennent pas de dispositions générales traitant de la question des décisions affectant la personne concernée et fondées uniquement sur le traitement automatisé de données à caractère personnel. Néanmoins, le système juridique coréen envisage ce droit dans la loi CIA, qui contient des règles sur les décisions automatisées (article 36, paragraphe 2), même si leur application semble se situer hors du champ d'application de la supervision par la PIPC (et, par conséquent, hors de celui du présent projet de décision — voir la section 2.3.2 ci-dessus concernant le champ d'application du projet de décision).

114. Comme l'ont déjà souligné le groupe de travail «article 29»[51] dans son avis 1/2016 sur le bouclier de protection des données et l'EDPB dans son avis précédent sur la décision d'adéquation concernant le Japon[52], l'importance croissante de la prise de décision automatisée, du profilage et de l'I.A. suggère d'adopter une approche plus protectrice à cet égard. Contrairement aux arguments de la Commission européenne[53] selon lesquels l'absence de règles spécifiques sur la prise de décision automatisée dans la loi PIPA ne devrait pas avoir d'incidence sur le niveau de protection des données à caractère personnel collectées dans l'Union (étant donné que toute décision fondée sur un traitement automatisé serait généralement prise par le responsable du traitement dans l'Union qui a un lien direct avec la personne concernée), l'EDPB considère qu'il ne peut être exclu que la prise de décision automatisée puisse être utilisée par un responsable du traitement des données à caractère personnel établi en Corée en cas de transfert de données en vertu de la décision d'adéquation (par exemple, dans le cadre d'un emploi, pour évaluer les performances au travail, la fiabilité, le comportement, etc.).

115. Le développement des nouvelles technologies facilite, pour les entreprises, la mise en œuvre ou les projets de mise en œuvre de systèmes de prise de décision automatisés, ce qui pourrait affaiblir la position des personnes. Lorsque des décisions prises uniquement par ces systèmes automatisés ont une incidence sur la situation juridique des personnes ou les affectent de manière significative (par exemple, en les inscrivant sur une liste noire et en privant ainsi les personnes de leurs droits), il est essentiel de prévoir des garanties suffisantes, notamment le droit d'être informé des raisons spécifiques qui sous-tendent la décision et de la logique sous-jacente, de corriger des informations inexactes ou incomplètes et de contester la décision lorsqu'elle a été adoptée sur une base factuelle erronée[54].

116. Dans ce contexte, L'EDPB s'inquiète de l'absence de dispositions juridiques, dans la loi PIPA, sur la prise de décision automatisée, et invite par conséquent la Commission européenne à répondre à cette préoccupation et à continuer à suivre l'évolution du cadre législatif coréen à cet égard.

3.1.14. Obligation de rendre des comptes

117. Le cadre juridique coréen contient plusieurs règles visant à garantir que les responsables du traitement des informations à caractère personnel mettent en place des mesures techniques et organisationnelles appropriées pour se conformer efficacement à leurs obligations en matière de

[50] Voir le considérant 81 du projet de décision.
[51] Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agissait d'un organe consultatif européen indépendant sur la protection des données et le respect de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE. Le groupe de travail «article 29» est devenu l'actuel comité européen de la protection des données.
[52] Avis 28/2018 relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, adopté le 5 décembre 2018.
[53] Considérant 81 du projet de proposition.
[54] WP254, p. 7.

protection des données et qu'ils soient en mesure de démontrer cette conformité, entre autres à l'autorité de contrôle compétente. En particulier, l'EDPB se félicite de l'existence de règles prévoyant l'adoption d'un plan de gestion interne (article 29 de la loi PIPA), de l'obligation de procéder à une «analyse d'impact sur la vie privée» («**PIA**») dans les cas où le traitement présente un risque plus élevé de violation de la vie privée (article 33, paragraphe 1, de la loi PIPA et article 35 du décret d'application de la loi PIPA), ainsi que de l'obligation de désigner un responsable de la protection de la vie privée (article 31 de la loi PIPA lu conjointement avec l'article 32 de son décret d'application).

118. L'EDPB partage le point de vue de la Commission européenne en ce qui concerne la protection essentiellement équivalente garantie par ces dispositions — même dans les cas où les règles semblent relativement différentes de celles prévues par le RGPD; par exemple, aucune disposition n'indique que le responsable de la protection de la vie privée doit être indépendant; toutefois, il est clairement indiqué qu'il doit rendre compte à la direction du responsable du traitement des informations à caractère personnel (article 31, paragraphe 4, de la loi PIPA) et qu'il ne doit pas subir d'inconvénients injustifiés du fait de l'exercice de ces fonctions (article 31, paragraphe 5, de la loi PIPA) — et le comité propose que la Commission européenne surveille, dans le cadre de l'examen de la décision d'adéquation, l'application effective de ces dispositions afin d'évaluer l'efficacité de leur mise en œuvre.

3.2. Mécanismes en matière de procédure et d'application

119. Sur la base des principes établis dans les critères de référence pour l'adéquation avec le RGPD, l'EDPB a analysé les aspects suivants du cadre coréen de protection des données visé par le projet de décision: l'existence d'une autorité de contrôle indépendante fonctionnant de manière efficace, l'existence d'un système garantissant un niveau de conformité satisfaisant et l'existence d'un système d'accès aux mécanismes de recours appropriés permettant aux personnes situées dans l'EEE d'exercer leurs droits et de disposer de voies de recours administratives et judiciaires sans être confrontés à des obstacles majeurs.

120. Conformément au chapitre VI du RGPD et au chapitre 3 des critères de référence pour l'adéquation avec le RGPD, il doit exister dans un pays tiers une ou plusieurs autorités de contrôle indépendantes chargées de surveiller, de garantir et de faire respecter les dispositions relatives à la protection des données et au respect de la vie privée afin d'assurer un niveau de protection équivalent à celui de l'EEE.

121. Dans ce contexte, l'autorité de contrôle du pays tiers doit agir en toute indépendance et impartialité dans l'exercice de ses fonctions et de ses pouvoirs et, ce faisant, ne sollicite ni n'accepte d'instructions. En outre, l'autorité de contrôle devrait disposer de tous les pouvoirs et mandats nécessaires et disponibles pour garantir le respect des droits en matière de protection des données et sensibiliser à ces droits. Il convient également de tenir compte du personnel et du budget de l'autorité de contrôle. L'autorité de contrôle doit également pouvoir engager une procédure de sa propre initiative.

3.2.1. Autorité de contrôle indépendante compétente

122. En République de Corée, l'autorité indépendante chargée du suivi et de l'application de la loi PIPA est la PIPC. La PIPC se compose d'un président de séance, d'un vice-président et de sept commissaires. Le président de séance et le vice-président de séance sont nommés par le président sur recommandation du Premier ministre. Parmi les commissaires, deux sont nommés sur recommandation du président, deux sur recommandation des représentants du parti politique auquel le président appartient et les trois autres membres sur recommandation des représentants d'autres partis politiques (article 7, paragraphe 2, point 2), de la loi PIPA). La PIPC est assistée d'un secrétariat (article 7, paragraphe 13) et peut créer des sous-commissions (composées de trois commissaires) chargées de traiter les infractions mineures et les questions récurrentes (article 7, paragraphe 12, de la loi PIPA).

123. À cet égard, l'EDPB reconnaît qu'en dépit de sa récente réorganisation, qui a profondément modifié son statut et ses pouvoirs, la PIPC a déployé des efforts considérables pour mettre en place les infrastructures nécessaires à la mise en œuvre de la loi PIPA et de ses dernières modifications. Parmi ces efforts, il convient de noter l'établissement des règles de la PIPC, l'élaboration de lignes directrices pour fournir des orientations sur l'interprétation de la loi PIPA et la mise en place d'une ligne d'assistance téléphonique pour conseiller les opérateurs économiques et les particuliers sur les dispositions en matière de protection des données, ainsi que d'un service de médiation pour traiter les réclamations. Les tâches de la PIPC consistent en particulier à fournir des conseils sur les lois et règlements relatifs à la protection des données, à élaborer des politiques et des lignes directrices en matière de protection des données, à enquêter sur les violations des droits individuels, à traiter les réclamations et à assurer la médiation des litiges, à veiller au respect de la loi PIPA, à assurer l'éducation et la promotion dans le domaine de la protection des données, ainsi qu'à échanger et coopérer avec les autorités de protection des données des pays tiers[55].

124. La désignation et la composition de la PIPC sont énoncées à l'article 7, paragraphe 2, de la loi PIPA. Bien que la PIPC relève de la compétence du premier ministre (et que le président de séance et le vice-président de séance soient nommés par le président sur recommandation du premier ministre), le cadre juridique prévoit que les commissaires exercent leurs fonctions en toute indépendance, conformément à la loi et à leur conscience. L'EDPB reconnaît les garanties institutionnelles et procédurales figurant dans la loi PIPA et, en particulier, dans les paragraphes 4 à 7 de l'article 7. Néanmoins, l'EDPB souhaiterait que la Commission européenne surveille toute évolution susceptible d'affecter l'indépendance des membres de l'autorité de contrôle sud-coréenne.

125. En outre, le projet de décision ne comporte pas encore d'analyse du budget de la PIPC, notamment des sources de financement et de la transparence budgétaire. L'EDPB estime que cet élément, qui est mentionné à la fois à l'article 56, paragraphe 1, du RGPD, ainsi que dans les principes et mécanismes de procédure et d'exécution en matière de protection des données à prendre en considération dans le cadre des critères de référence pour l'adéquation avec le RGPD lors de l'évaluation du système d'un pays ou d'une organisation internationale, doit être pris en compte de manière approfondie, car il constitue un indicateur des ressources économiques et humaines dont dispose l'autorité de contrôle pour s'acquitter de ses obligations et missions légales en matière de protection des données de manière indépendante, et recommande donc à la Commission européenne d'en rendre compte de manière plus détaillée dans le projet de décision.

3.2.2. Existence d'un système de protection des données garantissant un bon niveau de conformité

126. Dans le domaine de l'application de la législation, l'EDPB reconnaît l'éventail des pouvoirs d'exécution et des sanctions de la PIPC prévus dans les lois PIPA et CIA et prend acte des précisions figurant dans la notification n° 2021-1 selon lesquelles les conditions visées aux articles 64, paragraphe 1, de la loi PIPA et 45, paragraphe 4, de la loi CIA[56] seront applicables en cas de violation de tous principes, droits et devoirs prévus par la législation pour protéger les informations à caractère personnel. Il recommande toutefois à la Commission européenne de surveiller de près l'application pratique des pouvoirs de la PIPC d'ordonner au contrevenant de prendre la mesure qu'il juge appropriée parmi celles qui sont énumérés à l'article 64, paragraphe 1, ou à l'article 45, paragraphe 4, de la loi CIA.

[55] Les tâches et compétences de la PIPC sont principalement prévues aux paragraphes 8 et 9 de l'article 7 ainsi qu'aux articles 61 à 66 de la loi PIPA.

[56] C'est-à-dire qu'«une *violation de la loi est réputée être susceptible de porter atteinte aux droits et à la liberté des personnes à l'égard des informations à caractère personnel et l'inaction est susceptible de causer un préjudice difficilement réparable».*

127. En outre, en ce qui concerne les mesures correctives prévues à l'article 64, paragraphe 1, de la loi PIPA, en cas de non-respect d'une mesure corrective, la PIPC est habilitée à infliger une amende d'un montant maximal de 50 millions de wons coréens (article 75, paragraphe 2, point. 13 de la loi PIPA). Ce montant équivaut à 36 564 EUR. L'EDPB estime et craint qu'un éventail aussi limité de sanctions pécuniaires n'ait pas un fort effet dissuasif sur les contrevenants, comme le prévoit la loi, afin de garantir l'application des règles en matière de protection des données, étant donné qu'il ne semble pas suffisant pour dissuader, en particulier dans le cas de grandes organisations ou d'entreprises disposant de ressources financières importantes.

128. En ce qui concerne la possibilité que la PIPC demande au directeur d'un service administratif central d'enquêter sur le responsable du traitement des informations à caractère personnel ou de procéder conjointement à une enquête sur des violations de la PIPA, voire même, impose des mesures correctives à l'égard des responsables du traitement des informations à caractère personnel relevant de leur compétence (article 63, paragraphe 4, point 5), de la loi PIPA), l'EDPB observe que, même si certaines informations ont été fournies au considérant 122 du projet de décision, globalement, la nature de ces autres agences et leurs relations juridiques avec la PIPC restent plutôt floues. En outre, l'article 68, paragraphe 1, de la loi PIPA fait référence à de nombreuses entités auxquelles il serait possible de déléguer l'autorité de la PIPC. Même s'il semble que cette disposition n'ait été appliquée qu'en ce qui concerne l'Agence coréenne pour l'internet et la sécurité[57], l'EDPB souhaiterait obtenir des éclaircissements sur la nature des interactions possibles entre ces entités et recommande un suivi attentif de l'application de cette disposition à l'avenir afin de garantir l'indépendance des entités chargées d'appliquer les règles sur la protection des données.

129. En ce qui concerne les sanctions, le système coréen semble combiner différents types de sanctions, allant des mesures correctives et des amendes administratives aux sanctions pénales, qui sont susceptibles d'avoir un fort effet dissuasif, et les autorités coréennes ont présenté plusieurs exemples d'amendes infligées récemment par la PIPC, notamment une amende de 6,7 milliards de wons coréens, imposée en décembre 2020 à une société pour violation des différentes dispositions de la loi PIPA, et une autre amende de 103,3 millions de wons coréens le 28 avril 2021, infligée à une société technologique d'intelligence artificielle pour violation des règles de licéité du traitement, en particulier du consentement, et pour le traitement d'informations pseudonymisées.

130. Bien que les montants susmentionnés puissent avoir un effet dissuasif, l'EDPB souhaiterait recevoir des informations supplémentaires sur la méthode utilisée par la PIPC pour calculer le montant des amendes administratives, par exemple en ce qui concerne les amendes infligées en cas de non-respect d'une mesure corrective adoptée en vertu de l'article 64, paragraphe 1, de la loi PIPA (voir l'article 75, paragraphe 2, point 13 de la loi PIPA). Ceci est particulièrement important en ce qui concerne les sanctions pénales et l'application de la loi pénale (coréenne).

3.2.3. Le système de protection des données doit soutenir et aider les personnes concernées dans l'exercice de leurs droits et fournir des mécanismes de recours appropriés

131. En ce qui concerne les recours, le système coréen semble offrir diverses voies pour assurer une protection adéquate et, en particulier, faire respecter les droits individuels grâce à un recours administratif et judiciaire effectif, comprenant la réparation des dommages subis.

132. Le système coréen offre également d'autres mécanismes auxquels les particuliers peuvent avoir recours pour obtenir réparation, outre les voies administratives et judiciaires, comme expliqué aux considérants 132 et 133 du projet de décision, concernant respectivement le Centre d'appel pour la protection de la vie privée et le Comité de médiation des litiges. Étant donné qu'il s'agit de voies de recours supplémentaires, l'EDPB souhaiterait obtenir des explications plus détaillées sur la manière

[57] Voir le considérant 117 du projet de décision et l'article 62 du décret d'application.

dont elles complètent les possibilités de recours devant la PIPC et les tribunaux pour les personnes concernées dont les données à caractère personnel sont transférées à la Corée en vertu de la décision d'adéquation.

4. ACCÈS AUX DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES DEPUIS L'UNION EUROPÉENNE PAR LES AUTORITÉS PUBLIQUES EN CORÉE DU SUD, ET UTILISATION DE CES DONNÉES

133. En ce qui concerne l'évaluation du niveau de protection des données dans les domaines de l'application de la loi et de la sécurité nationale, la Commission européenne a fourni des informations complètes dans son projet de décision et dans les annexes mises à disposition. Par conséquent, l'EDPB s'abstient de reproduire la plupart des constatations et appréciations factuelles dans le présent avis.

134. La Commission européenne conclut que, dans les domaines susmentionnés, il existe un niveau de protection des données qui correspond aux exigences fixées par la jurisprudence de la CJUE et peut donc être considéré comme essentiellement équivalent à celui de l'Union européenne.

135. De manière générale, l'EDPB tient à souligner que, même dans les cas où il semble que, comme la Commission européenne l'affirme, les données transférées de l'UE vers la Corée du Sud sont peu susceptibles d'être affectées par la législation coréenne applicable, il est toujours opportun d'évaluer le caractère adéquat du niveau coréen de protection des données en ce qui concerne ces cas. Leur pertinence est également démontrée par le fait que la Commission européenne les a elle-même abordées dans le projet de décision.

4.1. Cadre général de protection des données dans le contexte de l'accès du gouvernement

136. En ce qui concerne l'accès des autorités publiques aux données à caractère personnel, diverses lois coréennes doivent être examinées afin d'évaluer le niveau de protection du droit au respect de la vie privée et à la protection des données. Tout d'abord, l'EDPB observe que la loi PIPA, en tant que législation essentielle en matière de protection des données, revendique une large applicabilité. Toutefois, si la loi PIPA est pleinement applicable au domaine répressif, son application au traitement des données à des fins de sécurité nationale est limitée. Conformément à l'article 58, paragraphe 1, point 2), de la loi PIPA, les chapitres III à VII ne s'appliquent pas au traitement de données à caractère personnel à des fins de sécurité nationale. Toutefois, les chapitres I, II, IX et X restent applicables dans le domaine de la sécurité nationale. Ainsi, les principes centraux de la loi PIPA ainsi que les garanties fondamentales pour les droits des personnes concernées et les dispositions relatives à la surveillance, à l'application et aux voies de recours s'appliquent à l'accès aux données à caractère personnel et à leur utilisation par les autorités nationales de sécurité.

137. La constitution sud-coréenne consacre également des principes essentiels de protection des données, à savoir les principes de légalité, de nécessité et de proportionnalité. Ces principes s'appliquent également à l'accès des autorités publiques sud-coréennes aux données à caractère personnel dans les domaines de l'application de la loi et de la sécurité nationale[58].

138. Dans le domaine répressif, la police, les procureurs, les tribunaux et d'autres organismes publics peuvent collecter des données à caractère personnel sur la base d'une législation spécifique, à savoir la loi sur la procédure pénale («**CPA**»), la loi sur la protection de la confidentialité des communications («**CPPA**»), la loi sur les activités de télécommunications («**TBA**») et la loi sur la déclaration et

[58] Voir le considérant 145 du projet de décision.

l'utilisation d'informations spécifiques sur les transactions financières («**ARUSFTI**»), qui s'applique aux poursuites judiciaires et à la prévention du blanchiment de capitaux et du financement du terrorisme. Ces lois particulières fixent des limites, des garanties et des exemptions supplémentaires.

139. Dans le domaine de la sécurité nationale, sur la base de la loi sur les services de renseignement nationaux («**NISA**») et des autres «lois sur la sécurité nationale»[59], le service national de renseignement («**NIS**») peut collecter des données à caractère personnel et intercepter les communications. Dans l'exercice de ses pouvoirs, l'EDPB croit savoir que le NIS doit se conformer aux dispositions juridiques susmentionnées ainsi qu'à la loi PIPA.

140. L'EDPB demande à la Commission de préciser s'il existe en Corée d'autres autorités, outre le NIS, qui sont responsables du domaine de la sécurité nationale, étant donné qu'à l'annexe I, section 6, la Commission européenne donne l'impression que le NIS constitue un exemple pour les agences nationales de sécurité.

1.2. Protection et garanties pour les données de confirmation de la communication dans le cadre de l'accès du gouvernement aux données à des fins répressives

141. Sur la base de la loi pertinente, la CPPA, les services répressifs peuvent prendre deux types de mesures pour l'accès aux informations de communication. La loi CPPA établit une distinction entre les mesures de restriction de la communication, qui couvrent à la fois la collecte du contenu du courrier ordinaire et l'interception directe du contenu des télécommunications[60], et la collecte de données dites de confirmation de communication. Ces dernières incluent la date des télécommunications, leur heure de début et de fin, le nombre d'appels entrants et sortants ainsi que le numéro d'abonné de l'interlocuteur, la fréquence d'utilisation, les fichiers journaux sur l'utilisation des services de télécommunication et les informations de localisation[61]

142. L'EDPB note que les données de confirmation de la communication ne semblent pas bénéficier des mêmes garanties que les données collectées au moyen de mesures de restriction de la communication, c'est-à-dire des données relatives au contenu. En effet, l'EDPB constate que la collecte de contenus bénéficie de davantage de garanties que la collecte de données de confirmation de communication à des fins répressives: Premièrement, contrairement à la collecte de données relatives au contenu, la collecte de données de confirmation de communication ne se limite pas à l'enquête sur certains crimes graves, mais peut être effectuée lorsqu'elle est jugée nécessaire pour mener «toute enquête ou exécuter une sanction» (article 13, paragraphe 1, de la loi CPPA). Deuxièmement, la collecte de données de confirmation de communication n'est en principe pas structurée comme une mesure de dernier recours et ne doit être utilisée que lorsqu'il est difficile d'éviter autrement la commission d'une infraction pénale, d'arrêter le criminel ou de recueillir des preuves[62]. Des données de confirmation de communication peuvent être collectées chaque fois qu'un procureur ou un officier de police judiciaire «le juge nécessaire» pour enquêter sur une infraction pénale ou exécuter une sanction. Toutefois, il existe à cet égard une exception pour les données de suivi en temps réel et les données de confirmation de communication concernant une station de base spécifique conformément à l'article 13, paragraphe 2, de la loi CPPA. Troisièmement, les services répressifs qui collectent le contenu de la communication doivent cesser immédiatement de le faire

[59] Les lois sur la sécurité nationale comprennent, par exemple, la loi sur la protection de la confidentialité des communications, la loi sur la lutte contre le terrorisme pour la protection des citoyens et de la sécurité publique ou la loi sur les activités de télécommunications.
[60] Articles 3, paragraphe 2, et 2, paragraphes 6 et 7, de la loi CPPA.
[61] Article 2, paragraphe 11, de la loi CPPA.
[62] C'est le cas pour les données relatives au contenu conformément aux articles 3, paragraphe 2 et 5, paragraphe 1, de la loi CPPA.

une fois que l'accès en continu n'est plus jugé nécessaire[63]. En ce qui concerne les données de confirmation de la communication, ceci n'est du moins pas explicitement stipulé dans la loi CPPA ou son décret d'application.

143. L'EDPB note que la collecte des données de confirmation de communication ne peut avoir lieu que sur le fondement d'un mandat délivré par un tribunal. En outre, la loi CPPA exige que des informations détaillées soient fournies tant dans la demande de mandat que dans le mandat lui-même[64]. Cette autorisation judiciaire préalable sert à limiter le pouvoir discrétionnaire des services répressifs dans l'application de la loi et à vérifier si, dans chaque cas, il existe des motifs suffisants pour recueillir des données de confirmation de communication. L'EDPB reconnaît également que le droit de la République de Corée ne semble pas prévoir la conservation générale et indifférenciée des données de confirmation de communication. Ainsi, l'accès du gouvernement à ces données se rapporte toujours à des données qui sont encore conservées aux fins de la facturation et de la fourniture des services de communication eux-mêmes.

144. Toutefois, l'EDPB souligne que la CJUE a remis en question le fait que les données relatives au trafic soient moins sensibles que d'autres, et en particulier que les données relatives au contenu[65]. Compte tenu du fait que les données de confirmation de communication bénéficient à plusieurs égards d'un niveau de protection inférieur à celui des données relatives au contenu, l'EDPB invite la Commission européenne à surveiller attentivement si les garanties prévues par la législation coréenne pour cette catégorie de données à caractère personnel assurent un niveau de protection essentiellement équivalent à celui garanti dans l'UE, notamment en ce qui concerne la proportionnalité et la prévisibilité de la loi.

4.3. Accès des autorités publiques coréennes aux informations de communication à des fins de sécurité nationale

145. En ce qui concerne le cadre juridique régissant l'accès des autorités nationales de sécurité aux informations de communication transférées de l'EEE vers la Corée, l'EDPB a identifié deux points de préoccupation, tous deux liés au régime d'accès aux communications entre ressortissants non coréens qui relèvent d'un ensemble spécifique de cas d'utilisation (voir point 29). Dans ces cas, en ce qui concerne tant les données de confirmation de la communication que les données relatives au contenu, certaines garanties prévues par ailleurs ne sont pas applicables. En d'autres termes, dans ces cas particuliers, ces données ne bénéficient pas des mêmes garanties que les données communiquées lorsqu'au moins un ressortissant coréen est impliqué dans la communication.

[63] Article 2 du décret d'application de la loi CPPA.
[64] Voir le considérant 156 du projet de décision.
[65] Voir CJUE, C-623/17, *Privacy International*, 6 octobre 2020, ECLI:EU:C:2020:790, point 71: «*L'ingérence que comporte la transmission des données relatives au trafic et des données de localisation aux services de sécurité et de renseignement dans le droit consacré à l'article 7 de la Charte doit être considérée comme étant particulièrement grave, compte tenu notamment du caractère sensible des informations que peuvent fournir ces données et, notamment, de la possibilité d'établir à partir de celles-ci le profil des personnes concernées, une telle information étant tout aussi sensible que le contenu même des communications. En outre, elle est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 27 et 37, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 99 et 100).*»

4.3.1. Absence d'obligation d'informer les particuliers de l'accès du gouvernement aux communications entre ressortissants étrangers

146. Dans un scénario tel que décrit ci-dessus, c'est-à-dire lorsqu'aucune des parties à une communication n'est un ressortissant coréen, les autorités nationales de sécurité ne sont pas tenues d'informer les personnes de la collecte et du traitement de leurs données. L'EDPB reconnaît que cette question ne concerne que certains cas. Premièrement, comme cela a déjà été souligné, chaque fois qu'au moins un ressortissant coréen est impliqué dans une communication, les exigences de notification prévues par la loi CPPA s'appliquent à toutes les parties à la communication, quelle que soit leur nationalité[66]. Deuxièmement, la collecte de données à caractère personnel provenant exclusivement de communications entre ressortissants étrangers est soumise à un ensemble spécifique de cas d'utilisation. En particulier, dans de tels cas, le droit d'accès s'étend aux communications a) de pays hostiles à la République de Corée, b) d'agences, de groupes ou de ressortissants étrangers soupçonnés d'exercer des activités anticoréennes[67], ou c) de membres de groupes opérant dans la péninsule coréenne, mais qui dépassent effectivement la souveraineté de la République de Corée, et de leurs groupes de tutelle établis dans des pays étrangers. Les communications entre des particuliers de l'UE transférées de l'EEE vers la Corée ne peuvent donc être collectées à des fins de sécurité nationale que si elles relèvent de l'une des trois catégories susmentionnées[68]. À titre de facteur restrictif supplémentaire, l'EDPB a compris, à la lecture des explications complémentaires de la Commission européenne, que le cadre juridique applicable ne prévoit pas l'interception de données en transit en dehors de la Corée.

147. Par conséquent, la pertinence critique de l'absence d'obligation de notification pourrait, du point de vue de ses incidences pratiques, être considérée comme limitée. Toutefois, l'EDPB souligne l'importance de la notification (ultérieure) de l'accès du gouvernement, en particulier pour ce qui est de garantir des voies de recours efficaces. Selon la CJUE, la notification est nécessaire «*pour permettre à ces personnes d'exercer leurs droits, découlant des articles 7 et 8 de la Charte, de demander l'accès à leurs données à caractère personnel faisant l'objet de ces mesures et, le cas échéant, la rectification ou la suppression de celles-ci, ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte, un recours effectif devant un tribunal*»[69]. L'accès du gouvernement à des fins de sécurité nationale comporte souvent des mesures de surveillance secrète, ce qui signifie que les objets de la surveillance, à savoir les personnes concernées, n'ont pas connaissance du traitement de leurs données. Ainsi, «*la personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci ou si – autre cas de figure –, soupçonnant que ses communications font ou ont fait l'objet d'interceptions, la personne a la faculté de saisir les tribunaux, ceux-ci étant compétents même si le sujet de l'interception n'a pas été informé de cette mesure*»[70]. Dans ce contexte et en cohérence avec ce qui précède, l'EDPB a exprimé à de nombreuses reprises son inquiétude quant à l'existence de voies de recours efficaces dans les affaires de surveillance. L'EDPB souligne que le secret des mesures gouvernementales ne doit pas conduire à ce que de telles mesures soient effectivement inattaquables. Dans ce contexte, la question de savoir si l'absence d'obligation de notification pour les communications entre

[66] Voir le considérant 192 du projet de décision.

[67] Voir l'annexe II, note de bas de page n° 244, selon laquelle la notion d'activités anticoréennes fait référence à des activités qui menacent l'existence et la sécurité de la nation, l'ordre démocratique ou la survie et la liberté du peuple.

[68] Voir le considérant 187 du projet de décision.

[69] CJUE, affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, 6 octobre 2020, ECLI:EU:C:2020:791, point 190.

[70] Cour EDH, *Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, point 337, et Cour EDH, *affaire Roman Zakharov c. Russie*, 4 décembre 2015, ECLI:CE:ECHR:2015:1204JUD004714306, point 234.

ressortissants étrangers a ou non une incidence sur le niveau de protection des données tel qu'il est évalué dans le projet de décision doit être appréciée dans le cadre d'une évaluation globale portant en particulier sur les mécanismes de contrôle et de recours prévus par le droit coréen (voir les sections 4.7 et 4.8).

148. En outre, l'EDPB relève dans ce contexte que la loi fait référence à des termes assez généraux tels que les activités anticoréennes ou antinationales[71] et qu'il est difficile de prévoir comment ces notions sont interprétées en droit coréen. L'EDPB invite la Commission européenne à vérifier comment ces termes sont développés dans le droit coréen et si leur application dans la pratique répond aux exigences de proportionnalité découlant du droit de l'Union.

4.3.2. Absence d'autorisation préalable indépendante pour la collecte d'informations de communication entre ressortissants étrangers

149. Lorsque des données à caractère personnel de l'EEE provenant de communications entre des ressortissants non coréens (et relevant de l'un des cas d'utilisation susmentionnés) doivent être traitées en Corée à des fins de sécurité nationale, la collecte de ces données n'est pas soumise à l'approbation préalable d'un organisme indépendant (comme c'est le cas pour les communications dont au moins une des personnes concernées est un ressortissant coréen).[72]

150. En particulier, à la lumière des récentes décisions de la Cour européenne des droits de l'homme (la «**Cour EDH**») «Big Brother Watch et autres c. Royaume-Uni» et «Centrum för Rättvisa c. Suède», l'EDPB juge nécessaire d'examiner si cela constitue une lacune critique du cadre coréen en matière de protection des données. À cet égard, l'EDPB rappelle que, comme il l'a souligné dans ses recommandations actualisées sur les garanties essentielles européennes pour les mesures de surveillance[73], l'article 6, paragraphe 3, du traité sur l'Union européenne dispose que les droits fondamentaux énoncés dans la CEDH constituent des principes généraux du droit de l'Union alors que, comme le rappelle la CJUE dans sa jurisprudence, la CEDH ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement intégré à l'ordre juridique de l'Union[74]. Dès lors, le niveau de protection des droits fondamentaux exigé par l'article 45 du RGPD doit être déterminé sur la base des dispositions dudit règlement, lues à la lumière des droits fondamentaux consacrés par la Charte. Cela étant dit, conformément à l'article 52, paragraphe 3, de la Charte, les droits qui y sont énoncés et qui correspondent à des droits garantis par la CEDH ont le même sens et la même portée que ceux qui sont énoncés par cette convention. Par conséquent, la jurisprudence de la Cour EDH concernant les droits qui sont également prévus dans la Charte doit être prise en compte, en tant que seuil de protection minimale en vue de l'interprétation des droits correspondants de la Charte, c'est-à-dire dans la mesure où cette dernière, telle qu'interprétée par la CJUE, ne prévoit pas un niveau de protection plus élevé[75].

151. L'EDPB note que si l'approbation préalable (indépendante) des mesures de surveillance est considérée comme une importante garantie contre l'arbitraire, cette approbation ne saurait être déduite de la jurisprudence de la CJUE comme étant une exigence absolue pour la proportionnalité des mesures de

[71] La Commission européenne a expliqué que, selon les explications du gouvernement coréen, il s'agit d'«activités qui menacent l'existence et la sécurité de la nation, l'ordre démocratique ou la survie et la liberté du peuple», voir également la note de bas de page 319 du projet de décision d'adéquation.
[72] Voir le considérant 190 du projet de décision.
[73] Voir les recommandations 02/2020 de l'EDPB sur les garanties essentielles européennes pour les mesures de surveillance, points 10, 11.
[74] Voir CJUE, C-311/18, *Data Protection Commissioner contre Facebook Ireland Ltd. et Maximilian Schrems*, 16 juillet 2020, ECLI:EU:C:2020:559 (ci-après «*Schrems II*»), point 98.
[75] Voir CJUE, affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, 6 octobre 2020, point 124.

surveillance. Toutefois, la Cour EDH a désormais explicitement établi l'exigence d'une autorisation indépendante ex ante pour les interceptions en masse[76]. Bien que le projet de décision ne le précise pas explicitement, l'EDPB croit comprendre que le cadre juridique de la République de Corée ne prévoit pas l'interception en masse, mais uniquement l'interception ciblée des télécommunications[77]. La Commission européenne a confirmé cette interprétation.

152. Cela étant dit, les décisions susmentionnées de la Cour EDH, conformément à la jurisprudence de la CJUE[78] et à la jurisprudence antérieure de la Cour EDH[79], montrent une fois de plus l'importance d'un contrôle exhaustif par des autorités de contrôle indépendantes. L'EDPB souligne qu'un contrôle indépendant à toutes les étapes du processus d'accès du gouvernement à des fins répressives et de sécurité nationale constitue une garantie importante contre les mesures de surveillance arbitraire et, partant, pour l'évaluation d'un niveau adéquat de protection des données. La garantie d'indépendance des autorités de contrôle au sens de l'article 8, paragraphe 3, de la Charte vise à assurer un contrôle efficace et fiable du respect des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Ceci vaut en particulier lorsque, en raison de la nature de la surveillance secrète, la personne est empêchée de demander un réexamen ou de participer directement à toute procédure de réexamen avant ou pendant l'exécution de la mesure de surveillance.

153. L'absence d'approbation préalable indépendante ne saurait en soi être considérée comme une lacune importante du droit coréen en ce qui concerne l'appréciation d'un niveau de protection des données essentiellement équivalent. L'évaluation de l'adéquation dépend, là encore, de toutes les circonstances de l'espèce, en particulier de l'efficacité du contrôle ex post et des voies de recours prévues par le cadre juridique coréen (voir les sections 4.7 et 4.8).

4.4. Divulgations volontaires

154. Conformément à l'article 83, paragraphe 3, de la loi TBA, les fournisseurs de services de télécommunications peuvent, sur demande, transmettre volontairement les «données relatives aux abonnés»[80] aux autorités nationales de sécurité et de répression. Bien que l'EDPB note que les affaires concernant des données à caractère personnel qui ont été transférées de l'EEE vers la Corée sont susceptibles d'être rares, elles doivent encore être analysées afin d'évaluer le niveau de protection des données, comme cela a déjà été mentionné ci-dessus.

155. L'EDPB croit savoir que, dans ces cas, les garanties en matière de protection des données prévues par la loi PIPA s'appliquent et les autorités publiques, ainsi que les fournisseurs de télécommunications,

---

[76] Voir Cour EDH, *Big Brother Watch et autres c.* Royaume-Uni, 25 mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, point 351: «Les activités d'interception en masse devraient être soumises à l'autorisation d'une autorité indépendante dès le départ»; «l'interception en masse devrait [...] être autorisée par un organe indépendant, c'est-à-dire un organe indépendant du pouvoir exécutif».

[77] Seule l'annexe II, section 3.2, contient une déclaration explicite à des fins de sécurité nationale lorsqu'il est précisé que les limitations et garanties «*garantissent que la collecte et le traitement des informations sont limités à ce qui est strictement nécessaire pour atteindre un objectif légitime. Cela exclut toute collecte massive et indifférenciée d'informations à caractère personnel à des fins de sécurité nationale*».

[78] Voir, par exemple, les affaires jointes de la CJUE C-203/15 et C-698/15, *Tele2 Sverige AB* e.a., ECLI:EU:C:2016:970.

[79] Voir, par exemple, Cour EDH, *affaire Roman Zakharov c. Russie*, 4 décembre 2015, ECLI:CE:ECHR:2015:1204JUD004714306.

[80] Les ensembles de données concernés seraient les suivants: le nom, le numéro d'enregistrement de résident, l'adresse et le numéro de téléphone des utilisateurs, les dates auxquelles les utilisateurs souscrivent ou annulent leur abonnement, ainsi que les codes d'identification de l'utilisateur (utilisés pour identifier l'utilisateur légitime de systèmes informatiques ou de réseaux de communication).

doivent se conformer à ces exigences[81], les deux pouvant être tenus pour responsables de toute violation des droits et libertés des personnes concernées[82]. En outre, l'EDPB croit savoir que les fournisseurs de télécommunications ne sont pas tenus de satisfaire à ces demandes.

156. Toutefois, en ce qui concerne la notion de l'accès des autorités nationales aux données relatives aux abonnés à des fins répressives et, en particulier, à des fins de sécurité nationale par le biais de la «divulgation volontaire» effectuée par les opérateurs du secteur des télécommunications, il existe un risque accru pour les droits et libertés des personnes concernées, notamment en ce qui concerne leur droit à l'information.

157. Conformément à l'article 58, paragraphe 1, point 2, de la loi PIPA, les dispositions des chapitres III à VII ne s'appliquent pas aux informations à caractère personnel dont la communication est demandée pour des motifs liés à la sécurité nationale. À cet égard, par exemple, les dispositions de l'article 18 (Limitation de l'utilisation et de la fourniture d'informations à caractère personnel hors finalité) et de l'article 20 (Notification des sources, etc. des informations à caractère personnel collectées auprès de tiers) de la loi PIPA ne sont pas applicables à de telles demandes. Dans les cas où une demande émane d'une autorité nationale de sécurité, cela soulève la question, d'une part, de savoir si l'article 58, paragraphe 1, point 2 exclut également l'application de la loi PIPA aux fournisseurs de télécommunications. D'autre part, l'on peut se demander si l'exclusion de l'application de l'article 20 de la loi PIPA dans de tels cas s'applique également à la disposition correspondante de la section 3 de l'annexe I (Notification pour les données lorsque des données à caractère personnel n'ont pas été collectées auprès de la personne concernée (article 20 de la loi)). Si tel était le cas et si l'article 58, paragraphe 1, point 2 concernait également les fournisseurs de télécommunications, il y aurait un risque, selon les informations disponibles, qu'il n'y ait pas d'obligation légale d'informer les personnes concernées de la divulgation volontaire.

158. L'EDPB est donc préoccupé par le fait que les exigences en matière d'information pourraient être rendues inefficaces, ce qui accroît considérablement la difficulté, pour les personnes concernées de faire valoir leurs droits en matière de protection des données, en particulier en ce qui concerne le recours juridictionnel. À cet égard, l'EDPB invite la Commission européenne à préciser le champ d'application des dispositions pertinentes.

4.5. Utilisation ultérieure des informations

159. Le principe de limitation de la finalité est une exigence juridique fondamentale de la protection des données. Il exige que les données à caractère personnel soient collectées uniquement pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement de manière incompatible avec ces finalités. En outre, le droit de l'Union autorise les autorités publiques à traiter des données à caractère personnel à des fins de prévention d'infractions pénales, ou d'enquêtes ou de poursuites en la matière, même si ces données ont été obtenues initialement à des fins différentes, si ces autorités s'appuient sur un fondement juridique pour traiter ces données en vertu de la législation applicable et si le traitement ultérieur n'est pas disproportionné[83].

160. Selon ce rapport, l'EDPB note que le cadre coréen en matière de protection des données prévoit des garanties et des limitations similaires à celles prévues par le droit de l'Union en ce qui concerne l'utilisation ultérieure des informations collectées à des fins répressives et de sécurité nationale, par exemple le principe de la limitation de la finalité, visé à l'article 3, paragraphes 1 et 2, de la loi PIPA.

[81] Voir les considérants 164 et 194 du projet de décision.
[82] Voir le considérant 166 du projet de décision.
[83] Voir l'article 4, paragraphe 2, de la directive en matière de protection des données dans le domaine répressif.

1.6. Transferts ultérieurs et partage de renseignements

161. L'article 44 du RGPD prévoit que les transferts et les transferts ultérieurs de données à caractère personnel n'ont lieu que si le niveau de protection garanti par le RGPD n'est pas compromis. Par conséquent, le niveau de protection accordé aux données à caractère personnel transférées de l'EEE vers la Corée ne doit pas être compromis par le transfert ultérieur à des destinataires situés dans un pays tiers, c'est-à-dire que les transferts ultérieurs ne devraient être autorisés que lorsqu'un niveau constant de protection substantiellement équivalent à celui prévu par le droit de l'Union est assuré. Par conséquent, pour évaluer si un pays tiers garantit un niveau adéquat de protection des données, il convient de tenir compte du cadre juridique du pays pour les transferts ultérieurs. Ceci est incontestable et conforme à l'avis de la Commission européenne[84] et de l'EDPB.

162. Dans ce contexte, l'EDPB note que, dans ses récentes décisions «Big Brother Watch et autres c. Royaume-Uni» et «Centrum för Rättvisa c. Suède», la Cour EDH a fourni des orientations[85] concernant les précautions à observer en matière de protection des données dans les États contractants lors de la communication des données à caractère personnel à d'autres parties à des fins répressives et de sécurité nationale dans les affaires de collecte en masse: «*Premièrement, les circonstances dans lesquelles pareil transfert peut avoir lieu doivent être clairement énoncées dans le droit interne. Deuxièmement, l'État qui transfère les informations en question doit s'assurer que l'État destinataire a mis en place, pour la gestion des données, des garanties de nature à prévenir les abus et les ingérences disproportionnées. L'État destinataire doit, en particulier, garantir la conservation sécurisée des données et restreindre leur divulgation à d'autres parties.* [...] *Troisièmement, des garanties renforcées sont nécessaires lorsqu'il est clair que les éléments transférés appellent une confidentialité particulière – par exemple s'il s'agit de communications journalistiques confidentielles*.»[86]

163. En appliquant ces normes, la Cour EDH a conclu dans «Centrum för Rättvisa c. Suède» que l'absence, dans le régime d'interception, de toute obligation légale expresse d'apprécier la nécessité et la proportionnalité du partage de renseignements au regard de son possible impact sur le droit au respect de la vie privée constituait une violation de l'article 8 de la Convention européenne des droits de l'homme. La Cour EDH a critiqué le fait que, en raison du niveau de généralité de la loi, les éléments issus de l'interception des communications puissent généralement être envoyés à l'étranger chaque fois que cela est considéré comme étant dans l'intérêt national, indépendamment de la question de savoir si le destinataire étranger offre des garanties d'un niveau minimum acceptable[87].

164. Reconnaissant que le cadre juridique de la Corée du Sud ne permet pas l'interception en masse, toujours à la lumière des implications de la jurisprudence de la Cour EDH, comme indiqué ci-dessus, l'EDPB estime que, outre les exigences découlant du droit de l'Union tel qu'interprété par la CJUE, l'argumentation de la Cour EDH devrait être prise en considération pour déterminer si le cadre juridique pour les transferts ultérieurs vers un pays tiers prévoit des normes adéquates en matière de protection des données.

[84] Voir les considérants 84 et suivants du projet de décision.

[85] Les éléments suivants ont été établis à l'occasion des affaires *Big Brother Watch* et *Centrum för Rättvisa*, qui concernent des régimes d'interception de masse. L'exigence de précautions à prendre lors de la communication de documents à d'autres parties figurait déjà dans les critères élaborés par la Cour EDH dans le cadre d'une interception ciblée et n'avait pas été précisée plus avant par la Cour EDH (voir l'arrêt *Big Brother Watch et autres c. Royaume-Uni*, points 335 et 362).

[86] Cour EDH, *Big Brother Watch et autres c. Royaume-Uni*, 25 mai 2021, ECLI:CE:ECHR:2021:0525JUD005817013, point 362.

[87] Voir Cour EDH, *Centrum för Rättvisa c. Suède*, 25 mai 2021, ECLI:CE:ECHR:2021:0525JUD003525208, point 326.

1.6.1. Cadre juridique applicable aux transferts ultérieurs effectués par les services répressifs

165. En ce qui concerne les transferts ultérieurs effectués par les autorités compétentes à des fins répressives, l'EDPB comprend, à la lecture des explications de la Commission européenne, que la section 2 de l'annexe I du projet de décision concernant la limitation des transferts ultérieurs est applicable, y compris lorsque le transfert est effectué sur la base d'une législation autre que la loi PIPA. Selon cette règle, «*si des informations à caractère personnel sont fournies à un tiers à l'étranger, elles ne peuvent pas bénéficier du niveau de protection garanti par la loi coréenne sur la protection des informations à caractère personnel, en raison des différences entre les pays en termes de systèmes de protection de ces informations. Par conséquent, ces cas seront considérés comme des «cas dans lesquels la personne concernée peut subir des inconvénients» mentionnés à l'article 17, paragraphe 4, de la loi ou comme des «cas de violation déloyale de l'intérêt d'une personne concernée ou d'un tiers» mentionnés à l'article 18, paragraphe 2, de la loi et à l'article 14, paragraphe 2, du décret d'application de la même loi. Pour satisfaire aux exigences de ces dispositions, le responsable du traitement des informations à caractère personnel et le tiers doivent donc explicitement garantir un niveau de protection équivalent à la loi, comprenant la garantie de l'exercice de ses droits par la personne concernée dans des documents juridiquement contraignants tels que des contrats, même après le transfert à l'étranger d'informations à caractère personnel»*[88].

166. L'EDPB se félicite de cette disposition qui, en supposant l'adéquation du niveau de protection des données en Corée à cette fin, garantit la continuité d'un niveau de protection tel qu'il est essentiellement garanti par le droit de l'Union pour les transferts ultérieurs. La Commission a confirmé que l'interprétation du comité, à savoir que cette section de l'annexe I s'applique à tous les transferts ultérieurs effectués par les autorités compétentes à des fins répressives, est correcte. Toutefois, l'EDPB souligne qu'il convient de veiller à ce que le présent règlement prévoie un niveau de protection constant dans la pratique, étant donné qu'il peut y avoir une incertitude quant aux garanties et obligations contractuelles ou à d'autres mécanismes similaires pouvant être utilisés pour atteindre un tel niveau de protection en cas de traitement à des fins répressives. À cet égard, il convient en outre de préciser, par exemple, que les données à caractère personnel ne peuvent être partagées qu'avec les autorités compétentes concernées du pays tiers.

167. Sous réserve des éclaircissements demandés ci-dessus quant à la question de savoir si la KOFIU est couverte par le projet de décision, l'EDPB note que la déclaration officielle sur l'accès du gouvernement[89] explique que, conformément à l'article 8, paragraphe 1, de la loi ARUSFTI, le commissaire de la KOFIU peut fournir aux services de renseignement financier étrangers des informations spécifiques sur les transactions financières, si cela est jugé nécessaire pour atteindre la finalité de la loi ARUSFTI[90]. L'article 8 de la loi ARUSFTI lui-même ne prévoit pas l'obligation de déterminer si le pays étranger offre des garanties adéquates en matière de protection des données, et de veiller à ce qu'il en soit ainsi. L'annexe II ne fait pas référence à la nouvelle section de l'annexe I à cet égard. Par conséquent, l'EDPB invite la Commission européenne à clarifier les liens entre la section correspondante de l'annexe I relative à la limitation des transferts ultérieurs et le fondement juridique des transferts ultérieurs conformément à la loi ARUSFTI.

[88] Projet de décision, annexe I, p. 7.

[89] Voir le projet de décision, annexe II.

[90] Voir le projet de décision, annexe II, section 2.2.3.2. Si un tel échange ne peut avoir lieu qu'à la condition que le service étranger ne puisse utiliser les informations à des fins autres que la finalité initiale de la divulgation, et notamment pas aux fins d'une enquête ou d'un procès au pénal (article 8, paragraphe 2, de la loi ARUSFTI), le commissaire de la KOFIU peut, à la réception d'une demande d'un pays étranger, donner son consentement à l'utilisation de ces données à des fins d'enquêtes ou de procès pénaux pour des infractions pénales avec le consentement préalable du ministre de la justice (article 8, paragraphe 3, de la loi ARUSFTI).

4.6.2. Cadre juridique applicable aux transferts ultérieurs à des fins de sécurité nationale

168. Le projet de décision ne contient aucune information sur le cadre juridique des transferts ultérieurs dans le domaine de la sécurité nationale. À cette fin, l'EDPB croit comprendre que la section 2 de l'annexe I s'applique aux transferts ultérieurs à des fins répressives, mais non à des fins de sécurité nationale. Les articles 17 et 18 de la loi PIPA qui font l'objet de la section en question de l'annexe I font partie du chapitre III de la PIPA, qui n'est pas applicable au traitement des données à caractère personnel à des fins de sécurité nationale (article 58, paragraphe 1, de la loi PIPA).

169. Toutefois, l'EDPB part du principe que la Corée peut avoir besoin de transmettre des données à caractère personnel aux services de renseignement étrangers à des fins de sécurité nationale et qu'elle les transmet effectivement, par exemple afin de coopérer pour lutter contre les menaces transfrontalières pesant sur la sécurité nationale, d'avertir les gouvernements étrangers ou de solliciter leur aide pour détecter de telles menaces.

170. L'EDPB a compris que, de l'avis de la Commission européenne, les transferts ultérieurs sont suffisamment réglementés en droit coréen par les garanties découlant du cadre constitutionnel global, en particulier les principes de nécessité et de proportionnalité, ainsi que par les principes fondamentaux de protection des données régis par la loi PIPA, tels que la licéité et l'équité du traitement, la limitation de la finalité, la minimisation des données, la sécurité et les obligations générales de prévention de l'utilisation abusive d'informations à caractère personnel.

171. L'EDPB reconnaît l'applicabilité générale de ces principes essentiels (de protection des données), mais craint que ces garanties soient de nature très générale et qu'elles ne fassent pas explicitement référence ou n'abordent pas, dans une base légale, les circonstances et conditions spécifiques applicables aux transferts ultérieurs, à des fins de sécurité nationale, de données transférées dans l'EEE. Bien que ces principes généraux et globaux soient largement applicables, l'EDPB se demande si l'on peut considérer que les critères de règles claires et précises sont remplis et si les textes prévoient suffisamment des garanties effectives et exécutoires. En particulier, lorsque l'accès aux données à caractère personnel et leur traitement par le gouvernement sont exercés de manière secrète et que les déductions qui pourraient être tirées de ces données sont particulièrement graves, il est essentiel de disposer de règles claires et détaillées. La loi devrait indiquer la portée de tout pouvoir discrétionnaire conféré aux autorités compétentes et les modalités de son exercice avec suffisamment de clarté pour que la personne concernée bénéficie d'une protection adéquate. Dans l'arrêt *Schrems II*, la CJUE rappelle qu'une base légale permettant une ingérence dans les droits fondamentaux doit, pour satisfaire aux exigences des principes de nécessité et de proportionnalité, définir elle-même la portée de la limitation de l'exercice du droit concerné, prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposer des exigences minimales[91]. L'EDPB est donc préoccupé par le fait qu'il ne suffit pas que de telles garanties soient généralement inscrites dans le droit de rang supérieur si la notion de proportionnalité n'est pas mise œuvre spécifiquement dans la base légale.

172. Ces préoccupations sont corroborées par la décision susmentionnée de la Cour EDH, dans laquelle la Cour a jugé qu'une règle générale sans obligation expresse d'évaluer la nécessité et la proportionnalité ou de prendre en considération les préoccupations en matière de respect de la vie privée n'était pas compatible avec le droit au respect de la vie privée prévu à l'article 8 de la Convention européenne des droits de l'homme. À cet égard, l'EDPB observe que, dans le droit de l'affaire en cause (ainsi que dans le droit coréen), il existe des principes généraux (garantis par la Constitution) de nécessité et de proportionnalité, par exemple en vertu de la Charte et par le biais de l'adhésion à la CEDH.

173. L'EDPB invite la Commission européenne à préciser la base légale, les modalités, la portée et les conditions spécifiques dans lesquelles les services de renseignement sont tenus de prendre en

[91] Voir l' arrêt *Schrems II*, points 175 et 180.

considération les préoccupations en matière de respect de la vie privée et les garanties de protection des données avant de divulguer des données à caractère personnel à des partenaires étrangers à des fins de sécurité nationale. Si cette obligation découle directement des principes constitutionnels, la Commission européenne devrait évaluer de manière plus approfondie les exigences de précision et de clarté de la loi applicable et confirmer que les principes généraux de la constitution et de la protection des données sont correctement appliqués et mis en œuvre.

4.6.3. Accords internationaux

174. L'EDPB note que la Commission européenne n'a pas tenu compte, dans le cadre de son évaluation de l'adéquation, de l'existence d'accords internationaux conclus entre la Corée et des pays tiers ou des organisations internationales susceptibles de prévoir des dispositions particulières pour le transfert international de données à caractère personnel par les services répressifs et/ou de renseignement vers des pays tiers. L'EDPB estime que la conclusion d'accords bilatéraux ou multilatéraux avec des pays tiers à des fins de coopération en matière répressive ou de renseignement est susceptible d'affecter le cadre juridique de la Corée en matière de protection des données tel qu'il a été évalué.

175. L'EDPB invite donc la Commission européenne à préciser s'il existe de tels accords, dans quelles conditions ils peuvent être conclus, et à évaluer si les dispositions des accords internationaux peuvent avoir une incidence sur le niveau de protection garanti pour les données à caractère personnel transférées de l'EEE vers la Corée par le cadre législatif et les pratiques en matière de divulgation à l'étranger à des fins répressives et de sécurité nationale.

4.7. Contrôle

176. L'EDPB note que le contrôle de l'application du droit pénal et des autorités nationales de sécurité est assuré par une combinaison de différents organes internes et externes.

177. Dans ce contexte, il convient de noter que la CJUE a souligné à plusieurs reprises la nécessité d'un contrôle indépendant en tant qu'élément essentiel de la protection des personnes physiques à l'égard du traitement de leurs données à caractère personnel. Le concept d'indépendance englobe les domaines de l'autonomie institutionnelle, du non-assujettissement aux instructions et de l'indépendance matérielle. Afin d'assurer un contrôle et une application cohérents de la législation en matière de protection des données, les autorités de contrôle doivent disposer de pouvoirs effectifs, notamment de pouvoirs correctifs et réparatoires.

178. L'EDPB souscrit à la conclusion de la Commission européenne selon laquelle, dans le cadre d'une évaluation globale, la Corée peut être considérée comme disposant d'un système de surveillance indépendant et efficace, même si plusieurs organes dudit système ne satisfont pas à proprement parler aux exigences susmentionnées. Par exemple, la plupart d'entre eux ne disposent pas de pouvoirs exécutifs, mais se limitent à émettre de simples recommandations, par exemple la Commission nationale des droits de l'homme ou le Conseil d'audit et d'inspection. En outre, la plupart des organismes publics respectifs ne sont pas exclusivement des institutions de protection des données, mais sont généralement chargés d'autres missions dans le domaine de la protection des droits fondamentaux.

179. Toutefois, selon les explications de la Commission européenne, l'EDPB note que la surveillance des services répressifs est garantie de manière exhaustive et sans exception par la PIPC. Par conséquent, la PIPC dispose de pouvoirs d'enquête, de réparation et d'exécution en vertu de la loi PIPA et d'autres lois en matière de protection des données (par exemple, la loi CPPA) qui s'appliquent à l'ensemble du domaine de l'accès des services répressifs et des autorités nationales de sécurité aux données à caractère personnel

180. Dans ce contexte, l'EDPB tient à souligner une nouvelle fois que les autorités de surveillance doivent disposer de ressources humaines, techniques et financières suffisantes pour s'acquitter de leurs missions et exercer leurs pouvoirs. À cet égard, il y a malheureusement un manque d'informations sur les organismes de contrôle désignés, en particulier la PIPC. Par conséquent, l'EDPB réitère sa demande à la Commission européenne de fournir de plus amples informations à ce sujet.

181. Dans l'ensemble, l'EDPB souhaite faire observer qu'il n'existe pratiquement aucune déclaration, aucun exemple ni aucun chiffre dans le projet de décision en ce qui concerne les activités de surveillance et l'application légale de la législation en matière de protection des données par les organes de contrôle dans le domaine de la répression et de la sécurité nationale. Ceux-ci seraient utiles dans le cadre de l'évaluation de l'efficacité des organes de surveillance.

4.8. Recours juridictionnel

182. L'EDPB rappelle qu'il est essentiel, pour assurer un niveau adéquat de protection des données, que les personnes concernées disposent de voies de recours étendues contre tout accès ou traitement non autorisé de données. Ces voies de recours doivent être suffisantes pour permettre à la personne concernée d'accéder aux données conservées la concernant et de demander leur rectification ou leur suppression.

183. À la lumière des arrêts *Schrems I* et *Schrems II* de la CJUE, il est clair qu'outre le droit de s'adresser aux autorités compétentes, une protection juridictionnelle effective au sens de l'article 47, paragraphe 1, de la Charte revêt une importance fondamentale pour l'hypothèse d'une adéquation du droit d'un pays tiers.

184. L'EDPB reconnaît que la Corée a mis en place diverses voies pour l'exécution des droits d'accès, de conservation, de suppression et de suspension exercés par les personnes dans le cadre de la loi PIPA. Ces droits peuvent être exercés à l'égard du responsable du traitement lui-même ou au moyen d'une réclamation déposée auprès de la PIPC ou d'autres organes de contrôle, par exemple la Commission nationale des droits de l'homme. En outre, l'EDPB reconnaît la possibilité de contester la décision des responsables du traitement ou des autorités publiques, en réponse à leur demande, sur la base de la Loi sur le contentieux administratif.

185. En outre, l'EDPB comprend, à la lecture des explications fournies par la Commission européenne, que les particuliers peuvent contester les actions des autorités répressives et de sécurité nationale devant les tribunaux compétents en vertu de la loi sur le contentieux administratif et de la loi sur la Cour constitutionnelle, et avoir la possibilité d'obtenir réparation en vertu de la loi sur l'indemnisation accordée par l'État[92].

186. Dans ce contexte, toutefois, l'EDPB s'inquiète quant à l'efficacité des voies de recours pour les citoyens de l'UE dans les affaires de sécurité nationale où aucun citoyen coréen n'est impliqué. Comme indiqué aux points 33 et suivants, les autorités nationales de sécurité ne sont pas tenues de notifier aux personnes concernées la collecte et le traitement de leurs données à caractère personnel. Étant donné qu'il est beaucoup plus difficile d'obtenir une protection juridique effective dans ces cas, l'EDPB tient à souligner que certaines garanties juridiques sont requises en l'espèce si des données transférées depuis l'EEE sont concernées. Ces garanties doivent permettre aux personnes concernées de prendre des mesures efficaces contre le traitement illicite de données d'une manière juridiquement sûre, sans être entravées par des exigences procédurales excessivement strictes, par exemple une charge de la preuve qu'elles ne peuvent pas satisfaire sans avoir connaissance du traitement. En outre, les personnes concernées doivent pouvoir s'adresser à un organisme compétent qui satisfait aux exigences de l'article 47 de la Charte, c'est-à-dire qui est compétent pour déterminer qu'un traitement est effectué, vérifier sa licéité et disposer de pouvoirs réparatoires exécutoires en cas de traitement

[92] Voir l'annexe II, point 3.2.4, en liaison avec le point 2.4.3.

illicite. Dans ce contexte, un simple droit de réclamation auprès de la Commission nationale des droits de l'homme, par exemple, ne serait pas suffisant. L'EDPB invite donc la Commission à expliquer plus en détail comment ces exigences sont mises en œuvre en termes de procédure et de fond, par exemple s'il est possible pour les personnes concernées de s'adresser à la PIPC ainsi qu'à un tribunal sans devoir prouver le traitement des données en question.

187. En outre, l'EDPB observe que le projet de décision prévoit un mécanisme de renvoi des réclamations, c'est-à-dire que les citoyens de l'UE peuvent déposer une réclamation auprès de la PIPC par l'intermédiaire de leur autorité nationale chargée de la protection des données ou par le biais de l'EDPB. La PIPC informe ensuite la personne concernée par le même canal une fois l'enquête terminée[93]. L'EDPB se félicite des efforts déployés pour faciliter l'accès aux voies de recours contre les autorités de sécurité nationales coréennes. Dans le même temps, l'EDPB préconise qu'un tel mécanisme de renvoi transite par les autorités nationales européennes chargées de la protection des données plutôt que par l'EDPB, étant donné qu'elles sont compétentes et plus proches du traitement des réclamations individuelles.

188. En outre, l'EDPB relève une éventuelle contradiction en ce qui concerne les divulgations volontaires. D'une part, le projet de décision indique que les personnes physiques peuvent obtenir réparation en cas de divulgation illicite de leurs données à la suite d'une demande de divulgation volontaire, y compris à l'encontre de l'autorité répressive qui émet la demande[94]. D'autre part, le projet de décision fait référence à l'exigence d'une incidence directe en ce qui concerne le droit de la personne de contester les actes des autorités publiques, en énumérant (uniquement) les demandes de divulgation contraignantes comme exemples dans lesquels une action administrative est réputée avoir un impact direct sur le droit au respect de la vie privée[95]. L'EDPB comprend, à la lecture des explications de la Commission européenne, qu'il n'y a en fait aucune restriction des possibilités de recours contre les demandes de divulgation volontaire, et demande par conséquent à la Commission européenne de clarifier davantage ce point dans la décision, tant dans les domaines de l'application de la loi que de la sécurité nationale (contrairement à la section consacrée à l'application de la loi, la section sur les divulgations volontaires à des fins de sécurité nationale ne contient aucune déclaration explicite sur les voies de recours dans ce contexte).

[93] Voir le considérant 205 et l'annexe I, p. 19 du projet de décision.
[94] Voir le considérant 166 du projet de décision.
[95] Voir le considérant 181 (services répressifs) et les considérants 208 et 181 (sécurité nationale) du projet de décision.