II

(Actes non législatifs)

DÉCISIONS

DÉCISION D'EXÉCUTION (UE) 2022/254 DE LA COMMISSION

du 17 décembre 2021

constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la République de Corée en vertu de la loi sur la protection des informations à caractère personnel

(notified under document C(2021) 9316)

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

LA COMMISSION EUROPÉENNE,

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

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

considérant ce qui suit:

1. INTRODUCTION

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

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

(3) Comme précisé à l'article 45, paragraphe 2, du règlement (UE) 2016/679, l'adoption d'une décision d'adéquation doit reposer sur une analyse approfondie de l'ordre juridique du pays tiers, en ce qui concerne tant les règles applicables aux importateurs de données que les limitations et les garanties en matière d'accès des autorités publiques aux données à caractère personnel. Dans son évaluation, la Commission doit déterminer si le pays tiers en question assure un niveau de protection «substantiellement équivalent» à celui qui est garanti dans l'Union européenne [considérant 104 du règlement (UE) 2016/679]. Cette question doit être évaluée au regard de la législation de l'Union, notamment le règlement (UE) 2016/679, ainsi que de la jurisprudence de la Cour de justice de l'Union européenne ([3]).

([1]) JO L 119 du 4.5.2016, p. 1.
([2]) Voir considérant 101 du règlement (UE) 2016/679.
([3]) Voir, en dernier lieu, arrêt de la Cour dans l'affaire C-311/18, Facebook Ireland et Schrems (ci-après l'«arrêt Schrems II»), ECLI:EU:C:2020:559.

(4) Comme l'a précisé la Cour de justice de l'Union européenne, il n'est pas exigé qu'un pays tiers assure un niveau de protection identique ([4]). En particulier, les moyens auxquels le pays tiers concerné a recours pour protéger les données à caractère personnel peuvent être différents de ceux mis en œuvre au sein de l'Union, pour autant qu'ils s'avèrent, en pratique, effectifs afin d'assurer un niveau de protection adéquat ([5]). Le principe d'adéquation n'exige donc pas que l'on reproduise à l'identique les règles de l'Union. Il s'agit plutôt de déterminer si le système étranger offre, dans son ensemble, par l'essence de ses droits en matière de protection de la vie privée et leur mise en œuvre effective, leur opposabilité et le contrôle de leur application, le niveau de protection requis ([6]). Les critères de référence pour l'adéquation du comité européen de la protection des données, qui ont pour but de préciser davantage ce principe, fournissent également des orientations à cet égard ([7]).

(5) La Commission a soigneusement analysé la législation et les pratiques coréennes. Sur la base des constatations exposées aux considérants 8 à 208, la Commission conclut que la République de Corée assure un niveau adéquat de protection des données à caractère personnel transférées d'un responsable du traitement ou d'un sous-traitant dans l'Union ([8]) à des entités (par exemple, des personnes physiques ou morales, des organisations, des institutions publiques) en Corée relevant du champ d'application de 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). Cela inclut à la fois les responsables du traitement et les sous-traitants [appelés «parties sous-traitantes»/«outsourcees» ([9])] au sens du règlement (UE) 2016/679. Le constat d'adéquation du niveau de protection ne couvre pas le traitement de données à caractère personnel pour des activités de missionnaires par des organisations religieuses ni pour la nomination de candidats par des partis politiques, ni le traitement d'informations personnelles en matière de crédit conformément à la loi sur les informations à caractère personnel en matière de crédit par des responsables du traitement qui sont soumis à la surveillance de la Commission des services financiers.

(6) Cette conclusion tient compte des garanties supplémentaires définies dans la notification n° 2021-5 (annexe I) ainsi que des déclarations, assurances et engagements officiels adressés par le gouvernement coréen à la Commission (annexe II).

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

2. RÈGLES APPLICABLES AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

2.1. Le cadre de la protection des données de la République de Corée

(8) Le régime juridique régissant la protection de la vie privée et la protection des données en Corée trouve son origine dans la Constitution coréenne promulguée le 17 juillet 1948. Bien que le droit à la protection des données à caractère personnel ne soit pas expressément inclus dans la Constitution, il est néanmoins reconnu en tant que droit fondamental, découlant des droits constitutionnels à la dignité humaine et à la poursuite du bonheur (article 10), à la vie privée (article 17) et à la confidentialité des communications (article 18). La Cour suprême ([10]) l'a confirmé, tout comme la Cour constitutionnelle ([11]). Des restrictions aux libertés et droits fondamentaux (y compris le droit au respect de la vie privée) ne peuvent être imposées par la loi que lorsque cela est nécessaire à la sécurité nationale ou au maintien de l'ordre public et ne peuvent pas affecter le contenu essentiel du droit ou de la liberté en cause (article 37, paragraphe 2).

([4]) Affaire C-362/14, Maximillian Schrems/Data Protection Commissioner (ci-après l'«arrêt Schrems»), ECLI:EU:C:2015:650, point 73.
([5]) Arrêt Schrems, point 74.
([6]) Voir communication de la Commission au Parlement européen et au Conseil intitulée «Échange et protection de données à caractère personnel à l'ère de la mondialisation», COM(2017) 7 du 10.1.2017, section 3.1, p. 6.
([7]) Comité européen de la protection des données, Critères de référence pour l'adéquation, WP 254 rév. 01, disponibles à l'adresse suivante: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108
([8]) La présente décision présente un intérêt pour l'EEE. L'accord sur l'Espace économique européen (ci-après l'«accord EEE») prévoit l'extension du marché intérieur de l'Union européenne aux trois pays de l'EEE que sont l'Islande, le Liechtenstein et la Norvège. La décision du Comité mixte intégrant le règlement (UE) 2016/679 dans l'annexe XI de l'accord EEE a été adoptée par le Comité mixte de l'EEE le 6 juillet 2018 et est entrée en vigueur le 20 juillet 2018. Le règlement est donc couvert par ledit accord. Aux fins de la décision, les références faites à l'Union et aux États membres de l'Union doivent donc être comprises comme incluant également les États de l'EEE.
([9]) Voir la section 2.2.3 de la présente décision.
([10]) Voir, par exemple, décision 2014Da77970 de la Cour suprême du 15 octobre 2015 (résumé en anglais disponible en cliquant sur le lien «Lawmaker's disclosure of teachers' trade union members case» à l'adresse suivante: https://www.privacy.go.kr/eng/enforcement_01.do) et jurisprudence citée, notamment la décision 2012Da49933 du 24 juillet 2014.
([11]) Voir, en particulier, décision 99Hun-ma513 de la Cour constitutionnelle du 26 mai 2005 (résumé en anglais disponible à l'adresse suivante: http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2), et décision 2014JHun-ma449 2013Hun-Ba68 (consolidée) du 23 décembre 2015 (résumé en anglais disponible en cliquant sur le lien «Change of resident registration number case» à l'adresse suivante: https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Bien que différents passages de la Constitution fassent référence aux droits des citoyens coréens, la Cour constitutionnelle a jugé que les ressortissants étrangers disposent aussi de droits fondamentaux ([12]). En particulier, la Cour a estimé que la protection de la dignité et de la valeur d'une personne en tant qu'être humain ainsi que le droit à la poursuite du bonheur constituent des droits pour tous les êtres humains et pas uniquement pour les citoyens coréens ([13]). De plus, selon les déclarations officielles du gouvernement coréen ([14]), il est généralement admis que les articles 12 à 22 de la Constitution (qui couvrent les droits à la vie privée) consacrent des droits humains fondamentaux ([15]). Bien qu'il n'existe à ce jour aucune jurisprudence concernant spécifiquement le droit à la vie privée des ressortissants étrangers, le fait que ce droit s'ancre dans la protection de la dignité humaine et de la poursuite du bonheur soutient une telle conclusion ([16]).

(10) De plus, la Corée a adopté un ensemble de lois en matière de protection des données qui fournissent des garanties à chacun, quelle que soit sa nationalité ([17]). Aux fins de la présente décision, les lois pertinentes sont les suivantes:

— la loi sur la protection des informations à caractère personnel (Personal Information Protection Act, ci-après la «PIPA»),

— la loi sur l'utilisation et la protection des informations relatives au crédit ([18]),

— la loi sur la protection de la confidentialité des communications.

(11) La PIPA définit le cadre juridique général de la protection des données en République de Corée. Elle est complétée par un décret d'application (décret présidentiel n° 23169 du 29 septembre 2011, modifié en dernier lieu par le décret présidentiel n° 30892 du 4 août 2020) (ci-après le «décret d'application de la PIPA») qui, à l'instar de la PIPA, est juridiquement contraignant et exécutoire.

(12) De plus, des «notifications» réglementaires adoptées par la Commission de protection des informations à caractère personnel (ci-après la «PIPC») définissent des règles supplémentaires concernant l'interprétation et l'application de la PIPA. S'appuyant sur l'article 5 (obligations de l'État) et l'article 14 (coopération internationale) de la PIPA, la PIPC a adopté la notification n° 2021-5 du 1er septembre 2020 (telle que modifiée par la notification n° 2021-1 du 21 janvier 2021 et la notification n° 2021-5 du 16 novembre 2021, ci-après dénommée la «notification n° 2021-5») relative à l'interprétation, l'application et l'exécution de certaines dispositions de la PIPA. Cette notification apporte des précisions s'appliquant à tout traitement de données à caractère personnel au titre de la PIPA et fournit des garanties supplémentaires pour les données à caractère personnel transférées à la Corée sur la base de la présente décision. La notification est juridiquement contraignante pour les responsables du traitement des informations à caractère personnel et elle est applicable tant par la PIPC que par les juridictions ([19]). Une violation des règles exposées dans la notification entraîne une violation des dispositions applicables de la PIPA qu'elles complètent. Le contenu des garanties supplémentaires est donc analysé dans le cadre de l'évaluation des articles pertinents de la PIPA. Enfin, le guide et les lignes directrices relatifs à la PIPA adoptés par la PIPC fournissent des orientations supplémentaires concernant la PIPA et son décret d'application, qui régit l'application et l'exécution des règles relatives à la protection des données par la PIPC ([20]).

([12]) Décision 93 Hun-MA120 de la Cour constitutionnelle du 29 décembre 1994.
([13]) Décision 99HeonMa494 de la Cour constitutionnelle du 29 novembre 2001.
([14]) Voir section 1.1 de l'annexe II.
([15]) Voir également l'article 1er de la loi sur la protection des informations à caractère personnel, qui fait explicitement mention des «libertés et droits de la personne». Plus précisément, cet article indique que l'objectif de la loi en question consiste à «régir le traitement et la protection des informations à caractère personnel afin de protéger les libertés et les droits des personnes et de faire progresser la dignité et la valeur des personnes». De même, l'article 5, paragraphe 1, de la loi sur la protection des informations à caractère personnel prévoit qu'il est de la responsabilité de l'État de «rédiger des politiques afin de prévenir les conséquences préjudiciables de la collecte injustifiée et de l'utilisation abusive ou détournée des informations à caractère personnel, de la surveillance et des poursuites indiscrètes, entre autres, et afin d'améliorer la dignité humaine et la vie privée».
([16]) De plus, l'article 6, paragraphe 2, de la Constitution prévoit que le statut des ressortissants étrangers est garanti conformément aux dispositions du droit et des traités internationaux. La Corée est partie à plusieurs accords internationaux qui garantissent le droit à 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).
([17]) Cela comprend des règles qui sont pertinentes pour la protection des données à caractère personnel, mais qui ne s'appliquent pas aux cas dans lesquels des données à caractère personnel sont collectées dans l'Union puis transférées en Corée au titre du règlement (UE) 2016/679, par exemple dans la loi sur la protection, l'utilisation, etc. des informations de localisation.
([18]) L'objectif de cette loi est de favoriser des activités portant sur des informations de crédit fiables, d'encourager l'utilisation efficace et la gestion systématique des informations de crédit et de protéger la vie privée contre l'utilisation détournée ou abusive des informations de crédit (article 1er de la loi).
([19]) Par exemple, les tribunaux coréens se sont prononcés sur le respect des notifications réglementaires dans un certain nombre de cas, notamment en tenant les responsables du traitement coréens responsables des violations d'une notification (voir par exemple l'arrêt 2018Da219406 de la Cour suprême du 25 octobre 2018, dans laquelle la Cour a condamné un responsable du traitement à indemniser des particuliers pour les dommages subis en raison d'une violation de la «notification relative à la norme relative aux mesures visant à garantir la sécurité des informations à caractère personnel»; voir également l'arrêt 2018Da219352 de la Cour suprême du 25 octobre 2018, l'arrêt 2011Da24555 de la Cour suprême du 16 mai 2016, la décision 2014Gahap511956 du tribunal central de Séoul du 13 octobre 2016 et la décision 2009Gahap43176 du tribunal central de Séoul du 26 janvier 2010).
([20]) Article 12, paragraphe 1, de la PIPA.

(13) De plus, la loi sur l'utilisation et la protection des informations relatives au crédit (Credit Information Act, ci-après la «CIA») prévoit des règles spécifiques qui s'appliquent tant aux opérateurs économiques «ordinaires» qu'aux entités spécialisées au sein du secteur financier lorsqu'ils traitent des informations à caractère personnel relatives au crédit, c'est-à-dire des informations nécessaires afin de déterminer le degré de solvabilité des parties aux opérations financières ou commerciales. Cela comprend notamment le nom, les coordonnées, les opérations financières, la notation de crédit, le statut en matière d'assurance ou le solde du crédit lorsque de telles informations sont utilisées afin de déterminer le degré de solvabilité d'une personne ([21]). À l'inverse, lorsque ces informations sont utilisées à d'autres fins (par exemple concernant les ressources humaines), la PIPA s'applique dans son intégralité. En ce qui concerne les dispositions spécifiques de la CIA en matière de protection des données, la conformité est contrôlée en partie par la PIPC (pour les organisations commerciales, voir l'article 45-3 de la CIA) et en partie par la Commission des services financiers ([22]) (pour le secteur financier, y compris les agences de notation de crédit, les banques, les compagnies d'assurance, les caisses d'épargne mutuelle, les sociétés de crédit spécialisées, les sociétés de services financiers, les sociétés de financement de valeurs mobilières, les coopératives de crédit, etc., voir l'article 45, paragraphe 1, de la CIA, en liaison avec l'article 36-2, de la CIA et l'article 38 de la loi sur la commission des services financiers). À cet égard, la portée de la présente décision se limite aux opérateurs économiques soumis à la surveillance de la PIPC ([23]). Les règles spécifiques de la CIA qui s'appliquent dans ce contexte (les règles générales de la PIPA s'appliquent lorsqu'aucune règle spécifique n'existe) sont décrites à la section 2.3.11.

2.2. **Champ d'application matériel et personnel de la PIPA**

(14) Sauf dispositions spécifiques contraires contenues dans d'autres lois, la protection des données à caractère personnel est régie par la PIPA (article 6). Le champ d'application matériel et personnel est déterminé par les notions définies d'«informations à caractère personnel», de «traitement» et de «responsable du traitement des informations à caractère personnel».

2.2.1. *Définition des données à caractère personnel*

(15) L'article 2, paragraphe 1, de la PIPA définit les informations à caractère personnel comme les informations relatives à une personne vivante permettant de l'identifier directement, par exemple grâce à son nom, son numéro d'enregistrement comme résident ou son image, ou indirectement, lorsque des informations qui ne permettent pas en elles-mêmes d'identifier une personne spécifique peuvent facilement être combinées à d'autres informations. La possibilité de combiner «facilement» des informations dépend du caractère raisonnablement probable d'une telle combinaison compte tenu de la possibilité d'obtenir d'autres informations, ainsi que du temps, du coût et de la technologie nécessaires pour identifier une personne.

(16) De plus, les informations pseudonymes, c'est-à-dire les informations ne permettant pas d'identifier une personne sans les utiliser ou les combiner avec d'autres informations complémentaires afin d'en rétablir la forme initiale, sont considérées comme des données à caractère personnel au titre de la PIPA [article 2, paragraphe 1, point c), de la PIPA]. À l'inverse, les informations qui sont pleinement «anonymisées» sont exclues du champ d'application de la PIPA (article 58-2 de la PIPA). C'est le cas notamment des informations qui ne permettent pas d'identifier une personne en particulier, même en les combinant à d'autres informations, compte tenu du temps, du coût et de la technologie raisonnablement nécessaires à l'identification.

(17) Cela correspond au champ d'application matériel du règlement (UE) 2016/679 et à ses notions de «données à caractère personnel», «pseudonymisation» ([24]) et «informations rendues anonymes» ([25]).

([21]) Article 2, paragraphe 1, de la CIA.

([22]) La Commission des services financiers est l'autorité de contrôle coréenne du secteur financier et, à ce titre, elle veille également à l'application de la CIA.

([23]) Si cela devait changer à l'avenir, par exemple si la compétence de la PIPC était élargie à l'intégralité du traitement des informations à caractère personnel en matière de crédit au titre de la CIA, il pourrait être envisageable de modifier la décision d'adéquation afin de couvrir aussi les entités qui sont actuellement soumises à la surveillance exercée par la Commission des services financiers.

([24]) La PIPA considère que le «traitement pseudonymisé» correspond au traitement par des méthodes telles que la suppression partielle des données à caractère personnel ou le remplacement total ou partiel des données à caractère personnel de manière à ce qu'aucune personne ne puisse être reconnue sans informations supplémentaires (article 2, paragraphes 1 et 2, de la PIPA). Cela correspond à la définition de la pseudonymisation contenue à l'article 4, paragraphe 5, du règlement (UE) 2016/679, qui fait référence au «traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable».

([25]) Plus particulièrement, le considérant 26 du règlement (UE) 2016/679 précise que ce règlement ne s'applique pas aux informations rendues anonymes, c'est-à-dire aux informations qui ne portent pas sur une personne physique identifiée ou identifiable. Pour le déterminer, il convient de tenir compte de l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement. Pour établir si de tels moyens sont raisonnablement susceptibles d'être utilisés, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci.

2.2.2. *Définition du traitement*

(18) La notion de «traitement» est largement définie dans la PIPA comme couvrant «la collecte, la génération, la connexion, le rapprochement, l'enregistrement, le stockage, la conservation, le traitement à valeur ajoutée, la modification, l'extraction, la production, la rectification, la récupération, l'utilisation, la fourniture, la divulgation et la destruction d'informations à caractère personnel et les autres activités similaires» ([26]). Bien que certaines dispositions de la PIPA fassent uniquement référence à des types spécifiques de traitement, comme l'«utilisation», la «fourniture» ou la «collecte» ([27]), la notion d'«utilisation» est interprétée comme incluant tout type de traitement en dehors de la «collecte» ou de la «fourniture» (par des tiers). Cette interprétation large de la notion d'«utilisation» garantit donc l'absence de toute lacune en matière de protection concernant des activités de traitement spécifiques. La notion de traitement correspond donc à la même notion telle que définie par le règlement (UE) 2016/679.

2.2.3. *Responsable du traitement des informations à caractère personnel et «partie sous-traitante» («outsourcee»)*

(19) La PIPA s'applique aux «responsables du traitement d'informations à caractère personnel» (ci-après les «responsables du traitement»). Comme c'est le cas dans le règlement (UE) 2016/679, cela recouvre toute institution publique, personne morale, organisation ou personne physique qui traite des données à caractère personnel directement ou indirectement afin de gérer des fichiers de données à caractère personnel dans le cadre de leurs activités ([28]). Dans ce contexte, «fichier d'informations à caractère personnel» signifie «tout ensemble d'informations à caractère personnel agencé ou organisé de manière systématique sur la base d'un certain nombre de règles afin de permettre un accès facile aux informations à caractère personnel» (article 2, paragraphe 4, de la PIPA) ([29]). Au sein de son organisation, le responsable du traitement est tenu de former les personnes participant au traitement sous sa direction, comme les agents ou les employés de la société, et d'assurer un contrôle et une surveillance appropriés (article 28, paragraphe 1, de la PIPA).

(20) Des obligations spécifiques s'appliquent lorsqu'un responsable du traitement (le «donneur d'ordre») sous-traite le traitement des données à caractère personnel à un tiers (la «partie sous-traitante»). Plus particulièrement, la sous-traitance doit être régie par un accord juridiquement contraignant (généralement un contrat) ([30]) qui définit la portée des tâches sous-traitées, la finalité du traitement, les garanties techniques et organisationnelles devant être appliquées, la surveillance assurée par le responsable du traitement, la responsabilité (notamment une indemnisation en cas de dommages causés par une violation des obligations contractuelles) ainsi que les limites de toute sous-traitance ([31]) (article 26, paragraphes 1 et 2, de la PIPA, en liaison avec l'article 28, paragraphe 1, du décret d'application) ([32]).

(21) De plus, le responsable du traitement est tenu de publier et de mettre constamment à jour les détails relatifs aux tâches sous-traitées et à l'identité de la partie sous-traitante ou, dans la mesure où le traitement sous-traité concerne des activités de marketing direct, de notifier directement aux personnes les informations pertinentes (article 26, paragraphes 2 et 3, de la PIPA, en liaison avec l'article 28, paragraphes 2 à 5, du décret d'application) ([33]).

(22) En outre, conformément à l'article 26, paragraphe 4, de la PIPA, en liaison avec l'article 28, paragraphe 6, du décret d'application, le responsable du traitement est tenu de «former» la partie sous-traitante aux mesures de sécurité nécessaires et de vérifier, y compris au moyen de contrôles, si celui-ci se conforme bien à toutes les obligations incombant au responsable du traitement au titre de la PIPA ([34]) ainsi que du contrat de sous-traitance. Lorsque la partie sous-traitante cause des dommages en raison d'une violation de la PIPA, ses actions ou son inaction seront imputables au responsable du traitement aux fins de l'établissement de la responsabilité, comme c'est le cas pour un employé (article 26, paragraphe 6, de la PIPA).

([26]) Article 2, paragraphe 2, de la PIPA.

([27]) Par exemple, les articles 15 à 19 de la PIPA font uniquement référence à la collecte, à l'utilisation et à la fourniture d'informations à caractère personnel.

([28]) Article 2, paragraphe 5, de la PIPA. Les institutions publiques au sens de la PIPA incluent l'ensemble des services ou agences administratifs centraux ainsi que les organes qui y sont rattachés, les autorités locales, les écoles et les entreprises locales publiques, les organes administratifs de l'Assemblée nationale et du pouvoir judiciaire (y compris la Cour constitutionnelle) (article 2, paragraphe 6, de la PIPA, en liaison avec l'article 2 du décret d'application de la PIPA).

([29]) Cela correspond au champ d'application matériel du règlement (UE) 2016/679. Selon son article 2, paragraphe 1, le règlement (UE) 2016/679 s'applique au «traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier». L'article 4, paragraphe 6, du règlement (UE) 2016/679 définit le terme «fichier» comme «tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés». Conformément à cette définition, le considérant 15 explique que la protection des personnes devrait s'appliquer «aux traitements de données à caractère personnel à l'aide de procédés automatisés ainsi qu'aux traitements manuels, si les données à caractère personnel sont contenues ou destinées à être contenues dans un fichier. Les dossiers ou ensembles de dossiers, de même que leurs couvertures, qui ne sont pas structurés selon des critères déterminés ne devraient pas relever du champ d'application du présent règlement».

([30]) Voir guide sur la PIPA, chapitre III, section 2, concernant l'article 26 (p. 203 à 212), qui explique que l'article 26, paragraphe 1, de la PIPA fait référence à des accords contraignants, comme des contrats ou d'autres accords similaires.

([31]) Conformément à l'article 26, paragraphe 5, de la PIPA, il est interdit pour le sous-traitant d'utiliser les informations à caractère personnel à des fins dépassant la portée des tâches sous-traitées ou de fournir des informations à caractère personnel à un tiers. Le non-respect de cette exigence peut donner lieu à une sanction pénale, conformément à l'article 71, point 2, de la PIPA.

([32]) Le non-respect de cette exigence peut entraîner l'application d'une amende, voir article 75, paragraphe 4, point 4, de la PIPA.

([33]) Le non-respect de cette exigence peut entraîner l'application d'une amende, voir article 75, paragraphe 2, point 1, et paragraphe 4, point 5, de la PIPA.

([34]) Voir également article 26, paragraphe 7, de la PIPA, selon lequel les articles 15 à 25, 27 à 31, 33 à 38 et 50 s'appliquent mutatis mutandis au sous-traitant.

(23) Bien que la PIPA n'utilise donc pas de notions distinctes pour les «responsables du traitement» et les «sous-traitants», les règles relatives à la sous-traitance prévoient des obligations et des garanties substantiellement équivalentes à celles régissant la relation entre les responsables du traitement et les sous-traitants en vertu du règlement (UE) 2016/679.

2.2.4. *Dispositions spécifiques applicables aux fournisseurs de services d'information et de communication*

(24) Bien que la PIPA s'applique au traitement de données à caractère personnel par tout responsable du traitement, certaines dispositions contiennent des règles spécifiques (en tant que *lex specialis*) régissant le traitement de données à caractère personnel des «utilisateurs» par les «fournisseurs de services d'information et de communication» ([35]). La notion d' «utilisateurs» couvre les personnes qui utilisent des services d'information et de communication (article 2, paragraphe 1, point 4, de la loi sur la promotion de l'utilisation des réseaux d'information et de communication et de la protection des données, ci-après la «loi sur les réseaux»). Cela suppose que la personne utilise soit directement des services de télécommunications fournis par un opérateur coréen de télécommunications, soit des services d'information ([36]) fournis à des fins commerciales (c.-à-d. à des fins lucratives) par une entité qui dépend elle-même des services d'un opérateur de télécommunications titulaire d'une licence en Corée ou enregistré dans ce pays ([37]). Dans les deux cas, l'entité liée par les dispositions spécifiques de la PIPA est celle qui fournit un service en ligne directement à une personne (c'est-à-dire à un utilisateur).

(25) Cependant, une constatation d'adéquation concerne uniquement le niveau de protection assuré aux données à caractère personnel transférées par un responsable du traitement/sous-traitant situé dans l'Union à une entité située dans un pays tiers (en l'occurrence, la République de Corée). Dans ce cas, les personnes se trouvant dans l'Union n'auront normalement de relation directe qu'avec l'«exportateur de données» situé dans l'Union et pas avec les fournisseurs coréens de services d'information et de communication ([38]). Par conséquent, les dispositions spécifiques de la PIPA relatives aux données à caractère personnel des utilisateurs de services d'information et de communication ne s'appliqueront tout au plus qu'à des situations limitées aux données à caractère personnel transférées au titre de la présente décision.

2.2.5. *Exemptions à certaines dispositions de la PIPA*

(26) L'article 58, paragraphe 1, de la PIPA exclut l'application d'une partie de la PIPA (à savoir les articles 15 à 57) en ce qui concerne quatre catégories de traitement des données ([39]). Plus particulièrement, les parties de la PIPA ayant trait aux motifs spécifiques du traitement, à certaines obligations en matière de protection des données, aux règles détaillées applicables à l'exercice des droits individuels ainsi qu'aux règles régissant le règlement des litiges par le comité de médiation des litiges relatifs aux informations à caractère personnel ne s'appliquent pas. Les autres dispositions de base de la PIPA continuent de s'appliquer, notamment les dispositions générales relatives aux principes de la protection des données (article 3 de la PIPA), y compris par exemple les principes de licéité, de précision et de limitation des finalités, de minimisation des données, d'exactitude et de sécurité des données, et aux droits individuels (d'accès, de rectification, de suppression et de suspension, voir article 4 de la PIPA). De plus, l'article 58, paragraphe 4, de la PIPA impose des obligations spécifiques concernant ces activités de traitement, notamment en ce qui concerne la minimisation des données, la limitation de la durée de conservation des données, les mesures de sécurité et la gestion des plaintes ([40]). En conséquence, les personnes peuvent toujours porter plainte auprès de la PIPC en cas de non-respect de ces principes et obligations et la PIPC est habilitée à prendre des mesures d'exécution en cas de non-conformité.

([35]) Voir notamment article 18, paragraphe 2, et chapitre VI de la PIPA.

([36]) Les services d'information incluent tant la fourniture d'informations que les services d'intermédiation pour la fourniture d'informations.

([37]) Voir article 2, paragraphe 1, point 3 (en liaison avec l'article 2, paragraphe 1, points 2 et 4) de la loi sur le réseau et de l'article 2, paragraphes 6 et 8 de la loi sur les activités de télécommunications.

([38]) Dans la mesure où les fournisseurs coréens de services d'information et de communication pourraient avoir une relation directe avec des personnes situées dans l'Union (en leur fournissant des services en ligne), le règlement (UE) 2016/679 serait alors d'application directe, conformément à son article 3, paragraphe 2, point a).

([39]) L'article 58, paragraphe 2, de la PIPA prévoit en outre que les articles 15 et 22, l'article 27, paragraphes 1 et 2, et les articles 34 et 37 ne s'appliquent pas aux informations à caractère personnel traitées par des appareils de traitement des données visuelles installées et exploitées dans des lieux publics. Puisque cette disposition concerne l'utilisation de la vidéosurveillance en Corée, c'est-à-dire la collecte directe d'informations à caractère personnel auprès des personnes en Corée, elle n'est pas pertinente aux fins de la présente décision, qui couvre uniquement les transferts de données à caractère personnel par des responsables du traitement/sous-traitants situés dans l'Union à des entités situées en Corée. De plus, conformément à l'article 58, paragraphe 3, de la PIPA, l'article 15 (collecte et utilisation des informations à caractère personnel), l'article 30 (obligation de mettre en place une politique de confidentialité publique) et l'article 31 (obligation de nommer un responsable de la confidentialité) ne s'appliquent pas aux informations à caractère personnel traitées afin de gérer des associations ou des groupes amicaux (par ex. des clubs de loisirs). Puisque de tels groupes sont considérés comme étant personnels par nature, sans aucun lien avec une activité commerciale ou professionnelle, aucune base juridique spécifique (comme le consentement des personnes concernées) n'est nécessaire afin de pouvoir collecter et utiliser les informations dans ce contexte. Cependant, toutes les autres dispositions de la PIPA (par ex. la minimisation des données, la limitation des finalités, la licéité du traitement, la sécurité et les droits individuels) continuent de s'appliquer. De plus, tout traitement d'informations à caractère personnel qui dépasserait la finalité consistant à créer un groupe social ne bénéficierait pas d'une telle exception.

([40]) Plus précisément, l'article 58, paragraphe 4, de la PIPA prévoit une obligation de limiter le traitement des informations à caractère personnel à ce qui est strictement nécessaire pour atteindre l'objectif visé, de les traiter pendant la durée la plus courte possible et de prendre les dispositions nécessaires pour garantir une gestion sûre et un traitement approprié de ces informations à caractère personnel. Cette dernière obligation inclut des garanties techniques, organisationnelles et physiques ainsi que des mesures permettant de garantir le traitement adéquat des plaintes individuelles.

(27) Premièrement, l'exonération partielle couvre les données à caractère personnel collectées au titre de la loi sur les statistiques en vue de leur traitement par des institutions publiques. Selon les précisions fournies par le gouvernement coréen, les données à caractère personnel traitées dans ce cadre concernent normalement les ressortissants coréens et ne pourraient inclure des informations relatives à des ressortissants étrangers qu'à titre exceptionnel, notamment dans le cas des statistiques relatives à l'entrée sur le territoire et à la sortie du territoire ou aux investissements étrangers. Cependant, même dans ces situations, de telles données ne sont normalement pas transférées par des responsables du traitement/sous-traitants situés dans l'Union, mais elles sont plutôt collectées directement par les autorités publiques en Corée ([41]). En outre, à l'instar de ce qui est prévu au considérant 162 du règlement (UE) 2016/679, le traitement des données dans le cadre de la loi sur les statistiques est soumis à plusieurs conditions et garanties. En particulier, la loi sur les statistiques impose des obligations spécifiques, telles que la garantie de l'exactitude, de la cohérence et de l'impartialité; elle contraint également de protéger les informations des personnes répondant aux enquêtes statistiques, y compris afin d'empêcher que de telles informations soient utilisées à des fins autres que la compilation de statistiques, et de soumettre les membres du personnel à des exigences en matière de confidentialité ([42]). Les autorités publiques qui traitent des statistiques doivent également respecter, entre autres, les principes de minimisation des données, de limitation de la finalité et de sécurité (article 3 et article 58, paragraphe 4, de la PIPA) et permettre aux particuliers d'exercer leurs droits (d'accès, de rectification, de suppression et de suspension, voir article 4 de la PIPA). Enfin, les données doivent être traitées sous une forme anonymisée ou pseudonymisée si cela permet d'atteindre la finalité du traitement (article 3, paragraphe 7, de la PIPA).

(28) Deuxièmement, l'article 58, paragraphe 1, de la PIPA fait référence aux données à caractère personnel collectées ou demandées en vue de l'analyse d'informations liées à la sécurité nationale. La portée et les conséquences de cette exonération partielle sont décrites plus en détail au considérant 149.

(29) Troisièmement, l'exonération partielle s'applique au traitement temporaire de données à caractère personnel lorsque cela est nécessaire de façon urgente à des fins de sécurité et de sûreté publiques, y compris pour des raisons de santé publique. Cette catégorie est interprétée strictement par la PIPC et, selon les informations reçues, n'a jamais été utilisée. La PIPC ne l'applique qu'aux urgences nécessitant une action immédiate, par exemple afin d'assurer le traçage d'agents infectieux ou de porter assistance et secours aux victimes de catastrophes naturelles ([43]). Même dans ces situations, l'exonération partielle ne couvre que le traitement de données à caractère personnel pendant une période limitée pour mener à bien une telle action. Les situations dans lesquelles cette exonération pourrait s'appliquer aux transferts de données couverts par la présente décision sont encore plus limitées, eu égard à la faible probabilité que des données à caractère personnel transférées depuis l'Union à des opérateurs coréens soient d'une nature telle que leur traitement serait «immédiatement nécessaire» dans le cadre de telles urgences.

(30) Enfin, l'exonération partielle s'applique aux données à caractère personnel collectées ou utilisées par la presse, par des organisations religieuses dans le cadre d'activités missionnaires ou par des partis politiques en vue de la nomination de candidats. L'exonération ne s'applique que lorsque la presse, les organisations religieuses ou les partis politiques traitent les données à caractère personnel à ces fins spécifiques (c'est-à-dire les activités journalistiques, le travail missionnaire et la nomination de candidats politiques). Lorsque ces entités traitent des données à caractère personnel à d'autres fins, par exemple la gestion des ressources humaines ou leur organisation interne, la PIPA s'applique intégralement.

(31) En ce qui concerne le traitement des données à caractère personnel par la presse à des fins d'activités journalistiques, l'équilibre entre la liberté d'expression et d'autres droits (y compris le droit à la vie privée) est assurée, entre autres, par la loi d'arbitrage et de recours pour les dommages causés par les articles de presse (ci-après la «loi sur la presse») ([44]). Plus particulièrement, l'article 5 de la loi sur la presse prévoit que la presse (c'est-à-dire tout

([41]) À cet égard, l'article 33 de la loi sur les statistiques impose aux institutions publiques de protéger les informations des personnes répondant aux enquêtes statistiques, notamment afin d'éviter que de telles informations soient utilisées à d'autres fins que la compilation des statistiques.

([42]) Article 2, paragraphes 2 et 3, article 30, paragraphe 2, et articles 33 et 34 de la loi sur les statistiques.

([43]) Guide sur la PIPA, section portant sur l'article 58.

([44]) Par exemple, l'article 4 de la loi sur la presse dispose que les articles de presse doivent être impartiaux et objectifs, conformes à l'intérêt général, respecter la dignité et la valeur de la personne humaine et ne peuvent pas être diffamatoires ni contraires aux droits des personnes, à la morale publique ou à l'éthique sociale.

organisme de radiodiffusion, journal, magazine ou journal en ligne), les services d'actualité en ligne ou les organismes de diffusion multimédia sur l'internet ne peuvent pas porter atteinte à la vie privée. Si, toutefois, une atteinte à la vie privée se produit, il convient d'y remédier rapidement, conformément aux procédures spécifiques définies par la loi. À cet égard, la loi confère aux personnes subissant un préjudice à cause d'un article de presse un certain nombre de droits, notamment celui d'obtenir la publication d'un correctif, d'exercer un droit de réponse ou d'obtenir la publication d'un autre article (lorsqu'un article de presse accuse une personne d'avoir commis une infraction et que la personne est ensuite innocentée) ([45]). Les plaintes formulées par les personnes peuvent être réglées par les organes de presse directement (par l'intermédiaire d'un médiateur) ([46]), par une procédure de conciliation ou d'arbitrage (devant une Commission arbitrale en matière de presse) ([47]) ou devant les tribunaux. Les personnes peuvent également obtenir réparation lorsqu'elles ont subi des dommages financiers, une violation de leurs droits personnels ou toute autre forme de détresse émotionnelle due à un acte illégal de la presse (intentionnel ou par négligence) ([48]). La presse est exonérée de toute responsabilité au titre de la loi lorsqu'un article de presse qui porte atteinte aux droits d'une personne n'est pas contraire aux valeurs sociales et est publié soit avec le consentement de la personne concernée, soit dans l'intérêt général (et qu'il existe suffisamment de raisons de penser que l'article est conforme à la vérité) ([49]).

(32) Si le traitement de données à caractère personnel par la presse dans le cadre d'activités journalistiques bénéficie donc de garanties spécifiques découlant de la loi sur la presse, il n'existe pas de telles garanties supplémentaires pour encadrer le recours aux exceptions prévues pour les activités de traitement par les organisations religieuses et les partis politiques d'une manière comparable à celle prévue par les articles 85, 89 et 91 du règlement (UE) 2016/679. La Commission estime donc qu'il est approprié d'exclure du champ d'application de la présente décision les organisations religieuses dans la mesure où elles traitent des données à caractère personnel dans le cadre de leurs activités missionnaires et les partis politiques dans la mesure où ils traitent des données à caractère personnel dans le cadre de la nomination de candidats.

2.3. **Garanties, droits et obligations**

2.3.1. *Licéité et loyauté du traitement*

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

(34) Ce principe est consacré à l'article 3, paragraphes 1 et 2, de la PIPA et il est renforcé par l'article 59 de la PIPA, qui interdit le traitement de données à caractère personnel «par des moyens frauduleux, inappropriés ou injustes», «sans disposer de l'autorité légale» ou «en outrepassant l'autorité légitime» ([50]). Ces principes généraux de traitement licite sont expliqués en détail aux articles 15 à 19 de la PIPA, qui énoncent les différentes bases juridiques pour le traitement (collecte, utilisation et fourniture à des tiers), y compris les circonstances dans lesquelles un changement de finalité peut se produire (article 18 de la PIPA).

([45]) Articles 15 à 17 de la loi sur la presse.

([46]) Chaque organe de presse ou support médiatique doit avoir son propre médiateur en vue d'éviter et de réparer tout préjudice causé par la presse (par ex. en recommandant la correction des articles de presse qui contiennent des inexactitudes ou qui nuisent à la réputation de tiers), article 6 de la loi sur la presse.

([47]) La Commission d'arbitrage compte 40 à 90 membres, nommés par le ministre de la culture, des sports et du tourisme parmi les personnes exerçant comme juges ou avocats, les personnes actives dans le domaine de la collecte ou les reportages d'actualités depuis au moins 10 ans ou d'autres personnes ayant une expertise dans le domaine de la presse. Les membres de la Commission d'arbitrage ne peuvent pas par ailleurs être dans le même temps fonctionnaires, membres de partis politiques ou journalistes. Conformément à l'article 8 de la loi sur la presse, les membres de la Commission d'arbitrage doivent exercer leurs fonctions de manière indépendante et ne peuvent pas recevoir d'orientations ou d'instructions en lien avec ces fonctions. De plus, des règles spécifiques sont en place afin de prévenir les conflits d'intérêts, par ex. afin d'empêcher les membres de la Commission d'arbitrage de traiter des cas spécifiques auxquels leur conjoint ou leurs proches sont parties (article 10 de la loi sur la presse). La Commission peut régler les litiges par conciliation ou par arbitrage, mais elle peut également formuler des recommandations afin de remédier aux infractions (section 5 de la loi sur la presse).

([48]) Article 30 de la loi sur la presse.

([49]) Article 5 de la loi sur la presse.

([50]) L'article 59 de la PIPA interdit à toute personne «qui traite ou a par le passé traité des informations à caractère personnel» d'«acquérir des informations à caractère personnel ou d'obtenir le consentement au traitement des informations à caractère personnel par des moyens frauduleux, inappropriés ou injustes», de «divulguer des informations à caractère personnel acquises dans le cadre de ses activités ou de les fournir pour utilisation à des tiers qui ne sont pas habilités à cette fin» ou «d'endommager, de détruire, de modifier, de falsifier ou de divulguer les informations à caractère personnel d'autrui sans disposer de l'autorité légale à cet effet ou en outrepassant l'autorité légitime». Une violation de cette interdiction peut entraîner des sanctions pénales, voir article 71, paragraphes 5 et 6, et article 72, paragraphe 2, de la PIPA. L'article 70, paragraphe 2, de la PIPA permet en outre de sanctionner pénalement l'obtention d'informations à caractère personnel traitées par des tiers par des moyens frauduleux ou des méthodes ou moyens injustes, ou la fourniture de telles informations à des tiers à des fins lucratives ou injustes, ou encore le soutien à de tels comportements ou l'organisation de ceux-ci.

(35) Selon l'article 15, paragraphe 1, de la PIPA, un responsable du traitement ne peut collecter des données à caractère personnel (dans le cadre de la finalité de la collecte) qu'en vertu d'un nombre limité de fondements juridiques. Il s'agit 1) du consentement de la personne concernée ([51]) (point 1); 2) de la nécessité d'exécuter un contrat conclu avec la personne concernée (point 4); 3) d'une autorisation spéciale prévue par le droit ou de la nécessité de se conformer à une obligation légale (point 2); de la nécessité ([52]) pour une institution publique de réaliser les tâches qui relèvent légalement de sa compétence; 4) de la nécessité manifeste de protéger la vie, l'intégrité corporelle ou les intérêts matériels de la personne concernée ou d'un tiers contre un danger imminent (seulement si la personne concernée n'est pas en mesure d'exprimer ses intentions ou si son consentement préalable ne peut être obtenu) (point 5); 5) de la nécessité de concourir à l'«intérêt justifiable» poursuivi par le responsable du traitement si cet intérêt est «manifestement supérieur» aux intérêts de la personne concernée (et uniquement lorsque le traitement est «substantiellement lié» à l'intérêt légitime et n'excède pas les limites du raisonnable) (point 6) ([53]). Ces fondements pour le traitement sont substantiellement équivalents à ceux prévus à l'article 6 du règlement (UE) 2016/679, y compris le fondement tiré de l'«intérêt justifiable», qui correspond au fondement tiré de l'«intérêt légitime» prévu à l'article 6, paragraphe 1, point f), dudit règlement.

(36) Une fois collectées, les données à caractère personnel peuvent être utilisées dans le cadre de la finalité de leur collecte (article 15, paragraphe 1, de la PIPA) ou «dans un cadre raisonnablement lié» à la finalité de la collecte, en tenant compte des éventuels préjudices causés aux personnes concernées et à condition que les mesures de sécurité nécessaires (par ex. chiffrement) aient été adoptées (article 15, paragraphe 3, de la PIPA). Pour déterminer si la finalité de l'utilisation est «raisonnablement liée» à la finalité initiale de la collecte, le décret d'application définit des critères spécifiques, semblables à ceux de l'article 6, paragraphe 4, du règlement (UE) 2016/679. En particulier, il doit y avoir une importance considérable par rapport à l'objectif initial; l'utilisation supplémentaire doit être prévisible (par exemple en fonction des circonstances dans lesquelles les informations ont été collectées); et, dans la mesure du possible, les données doivent être pseudonymisées ([54]). Le responsable du traitement doit divulguer à l'avance, dans sa politique de confidentialité, les critères spécifiques qu'il utilise dans le cadre d'une telle évaluation ([55]). De plus, le responsable de la confidentialité (voir considérant 94) est spécifiquement tenu de vérifier si l'utilisation ultérieure a lieu dans le respect de ces paramètres.

([51]) Le consentement doit être donné librement, être éclairé, spécifique et exprimé dans l'une des différentes manières prévues par la loi. En tout état de cause, le consentement ne peut pas être obtenu par des moyens frauduleux, inappropriés ou injustes (article 59, paragraphe 1, de la PIPA). Premièrement, selon l'article 4, point 2, de la PIPA, les personnes concernées ont le droit de «consentir ou ne pas consentir» et de «déterminer la portée de leur consentement» et devraient en être informées (article 15, paragraphe 2, article 16, paragraphes 2 et 3, article 17, paragraphe 2, et article 18, paragraphe 3, de la PIPA). L'article 22, paragraphe 5, de la PIPA prévoit une garantie supplémentaire en interdisant à un responsable du traitement de refuser de fournir des biens ou des services lorsque cela pourrait nuire au libre choix des personnes de donner ou non leur consentement. Cela inclut les situations dans lesquelles seuls certains types de traitement nécessitent un consentement (tandis que les autres se fondent sur un contrat) et couvre également le traitement ultérieur des données à caractère personnel collectées dans le cadre de la fourniture de biens ou de services. Deuxièmement, conformément à l'article 15, paragraphe 2, à l'article 17, paragraphes 2 et 3, et à l'article 18, paragraphe 3, de la PIPA, lorsqu'il demande le consentement, le responsable du traitement doit informer la personne concernée des «caractéristiques» des données à caractère personnel en question [par ex. si des données à caractère personnel sensibles sont concernées, voir article 17, paragraphe 2, point 2 a), du décret d'application de la PIPA], de la finalité du traitement, de la durée de conservation des données et de l'identité de tout destinataire des données. Une telle demande doit être formulée «de manière explicitement reconnaissable», qui fait la distinction entre les matières nécessitant un consentement et les autres (article 22, paragraphes 1 à 4, de la PIPA). Troisièmement, l'article 17, paragraphe 1, points 1 à 6, du décret d'application de la PIPA précise les méthodes spécifiques au moyen desquelles un responsable du traitement obtient le consentement, comme le consentement écrit établi par la signature de la personne concernée ou le consentement par (retour de) courriel. Si la PIPA ne confère pas spécifiquement aux personnes un droit général de retirer leur consentement, celles-ci ont au contraire le droit d'obtenir la suspension du traitement des données les concernant, ce qui, lorsqu'il est exercé, entraînera la cessation du traitement et l'effacement des données (voir considérant 78 sur le droit à la suspension).

([52]) Selon les informations transmises par la PIPC, les institutions publiques ne peuvent invoquer ce fondement que si le traitement des informations à caractère personnel est inévitable, c'est-à-dire qu'il doit être impossible ou déraisonnablement difficile pour l'institution d'effectuer ses missions sans traiter les données.

([53]) L'article 39-3 de la PIPA impose des obligations spécifiques (plus strictes) aux fournisseurs de services d'information et de communication en ce qui concerne la collecte et l'utilisation des informations à caractère personnel de leurs utilisateurs. Plus particulièrement, il exige que le fournisseur obtienne le consentement de l'utilisateur après lui avoir fourni des informations sur la finalité de la collecte/l'utilisation, les catégories d'informations à caractère personnel qui seront collectées et la durée pendant laquelle les informations seront traitées (article 39-3, paragraphe 1, de la PIPA). Il en va de même lorsque l'un quelconque des aspects susmentionnés change. La non-obtention du consentement à la collecte d'informations expose à des sanctions pénales (article 71, paragraphes 4 et 5, de la PIPA). À titre exceptionnel, les fournisseurs de services d'information et de communication peuvent collecter ou utiliser les informations à caractère personnel sans avoir obtenu de consentement préalable. C'est le cas 1) lorsqu'il est manifestement difficile d'obtenir le consentement normal concernant les informations à caractère personnel nécessaires pour exécuter le contrat régissant la fourniture de services d'information et de communication pour des raisons économiques et technologiques (par ex. lorsque des données à caractère personnel sont inévitablement créées dans le cadre de l'exécution du contrat, comme les informations de facturation, les historiques d'accès et les relevés de paiement); 2) lorsque cela est nécessaire pour le règlement des redevances à la suite de la fourniture de services d'information et de communication; ou 3) si d'autres lois le permettent (par exemple, article 21, paragraphe 1, point 6, de la loi sur la protection des consommateurs dans le cadre du commerce en ligne prévoit que les opérateurs économiques peuvent collecter des informations à caractère personnel concernant les tuteurs légaux d'un mineur afin de confirmer l'obtention d'un consentement valable au nom de ce mineur) (article 39-3, paragraphe 2, de la PIPA). Dans tous les cas, les fournisseurs de services d'information et de communication ne peuvent pas refuser de fournir les services pour la simple raison que l'utilisateur ne fournit pas des informations à caractère personnel autres que les informations minimales requises (c'est-à-dire les informations nécessaires à l'exécution des éléments essentiels du service concerné), voir article 39-3, paragraphe 3, de la PIPA.

([54]) Voir article 14-2 du décret d'application de la PIPA.

([55]) Article 14-2, paragraphe 2, du décret d'application de la PIPA.

(37) Des règles semblables (mais légèrement plus strictes) s'appliquent à la fourniture de données à un tiers. Selon l'article 17, paragraphe 1, de la PIPA, la fourniture de données à caractère personnel à un tiers est autorisée sur la base du consentement ([56]) ou, dans le cadre de la finalité de la collecte, lorsque les informations ont été collectées au titre de l'un des fondements juridiques mentionnés à l'article 15, paragraphe 1, points 2, 3 et 5, de la PIPA. Cela exclut notamment toute divulgation fondée sur l'«intérêt justifiable» poursuivi par le responsable du traitement. En outre, l'article 17, paragraphe 4, de la PIPA permet la fourniture aux tiers «dans le cadre raisonnablement lié» à la finalité de la collecte, compte tenu une fois encore des éventuels préjudices causés à la personne concernée et à condition que les mesures de sécurité nécessaires (par ex. le chiffrement) aient été adoptées. Il convient de tenir compte des mêmes facteurs que ceux décrits au considérant 36 afin d'évaluer si la fourniture intervient dans un cadre raisonnablement lié à la finalité de la collecte et si les mêmes garanties (c'est-à-dire les garanties en matière de transparence apportées par la politique de confidentialité et la participation du responsable de la confidentialité) s'appliquent.

(38) La réception de données à caractère personnel en provenance de l'Union par un responsable du traitement coréen est considérée comme une «collecte» au sens de l'article 15 de la PIPA. La notification n° 2021-5 (section I de l'annexe I de la présente décision) précise que la finalité pour laquelle les données ont été transférées par l'entité située dans l'Union concernée constitue la finalité de la collecte pour le responsable du traitement coréen. En conséquence, les responsables du traitement coréens qui reçoivent des données à caractère personnel en provenance de l'Union sont en principe tenus de traiter ces informations dans le cadre de la finalité du transfert, conformément à l'article 17 de la PIPA.

(39) Des limitations spécifiques s'appliquent lorsque le responsable du traitement cherche à utiliser les données à caractère personnel ou à les fournir à un tiers pour une finalité différente de la finalité de la collecte ([57]). Conformément à l'article 18, paragraphe 2, de la PIPA, un responsable du traitement privé peut, à titre exceptionnel ([58]), utiliser les données à caractère personnel ou les fournir à un tiers pour d'autres finalités: 1) sur la base du consentement supplémentaire (c'est-à-dire distinct) de la personne concernée; 2) lorsque cela est prévu par des dispositions légales spéciales; ou 3) lorsque cela est manifestement nécessaire afin de protéger la vie, l'intégrité corporelle ou les intérêts matériels de la personne concernée ou d'un tiers contre un danger imminent (seulement si la personne concernée n'est pas en mesure d'exprimer ses intentions et si son consentement préalable ne peut être obtenu) ([59]).

(40) Les institutions publiques peuvent également utiliser les données à caractère personnel ou les fournir à un tiers pour une finalité différente dans certaines situations. Cela comprend les cas dans lesquels les institutions publiques seraient dans l'impossibilité, s'il en allait autrement, de s'acquitter de leurs missions légales de la manière prescrite par la loi, sous réserve de l'autorisation par la PIPC. En outre, les institutions publiques peuvent fournir des données à caractère personnel à une autre autorité ou juridiction, lorsque cela est nécessaire aux fins de l'enquête et de la poursuite d'infractions ou d'un acte d'accusation, pour permettre à une juridiction d'exercer ses fonctions en lien avec des procédures judiciaires en cours, ou pour faire appliquer une sanction pénale, une ordonnance de prise en charge ou une ordonnance de garde ([60]). Elles peuvent également fournir des données à caractère personnel à un gouvernement étranger ou à une organisation internationale afin de s'acquitter d'une obligation légale découlant d'un traité ou d'une convention internationale, auquel cas elles sont également tenues de respecter les exigences applicables aux transferts transfrontières de données (voir considérant 90).

(41) Les principes de licéité et de loyauté du traitement sont donc mis en œuvre dans le cadre juridique coréen d'une manière substantiellement équivalente à celle du règlement (UE) 2016/679 en ne permettant le traitement que sur la base de fondements légitimes et clairement définis. De plus, dans tous les cas susmentionnés, le traitement n'est permis que s'il n'est pas susceptible de «porter atteinte de manière déloyale» aux intérêts de la personne concernée ou d'un tiers, ce qui nécessite une mise en balance des intérêts. De plus, l'article 18, paragraphe 5, de la PIPA prévoit des garanties supplémentaires lorsque le responsable du traitement fournit les données à caractère personnel à un tiers, qui peuvent inclure une demande de limitation de la finalité et des méthodes d'utilisation ou de mise en place de mesures de sécurité spécifiques. Le tiers est alors tenu de mettre en œuvre les mesures demandées.

([56]) Les violations de l'article 17, paragraphe 1, point 1, de la PIPA exposent à des sanctions pénales.

([57]) La «finalité prévue» est la finalité pour laquelle les informations ont été collectées. Par exemple, lorsque les informations sont collectées sur la base du consentement de la personne concernée, la finalité prévue est celle qui est communiquée à cette personne au titre de l'article 15, paragraphe 2, de la PIPA.

([58]) Voir article 18, paragraphe 1, de la PIPA. Les violations de l'article 18, paragraphes 1 et 2, de la PIPA exposent à des sanctions pénales (article 71, paragraphe 2, de la PIPA).

([59]) L'utilisation des informations à caractère personnel ou leur fourniture à un tiers par les fournisseurs de services d'information et de communication pour une finalité différente de la finalité initiale n'est possible que pour les motifs exposés à l'article 18, paragraphe 2, points 1 et 2, de la PIPA (c'est-à-dire lorsqu'un consentement supplémentaire est obtenu ou que la loi prévoit des dispositions spécifiques). Voir article 18, paragraphe 2, de la PIPA.

([60]) Sauf lorsque le traitement est nécessaire à des fins d'enquête pénale, de mise en accusation et de poursuites, les institutions publiques qui utilisent des informations à caractère personnel ou qui les fournissent à des tiers pour une finalité différente de la finalité de leur collecte (par exemple lorsque cela est spécifiquement permis par la loi ou nécessaire afin d'exécuter un traité) sont tenues de publier les fondements juridiques d'un tel traitement ainsi que sa finalité et sa portée, sur leur site web ou au Journal officiel, et les consignent dans un registre (article 18, paragraphe 4, de la PIPA, en liaison avec l'article 15 du décret d'application de la PIPA).

(42) Enfin, l'article 28-2 de la PIPA permet le traitement (ultérieur) d'informations pseudonymisées sans le consentement de la personne concernée à des fins de statistiques, de recherche scientifique ([61]) et d'archivage dans l'intérêt général, sous réserve de garanties spécifiques. À l'instar du règlement (UE) 2016/679 ([62]), la PIPA facilite donc le traitement (ultérieur) des données à caractère personnel à de telles fins dans un cadre qui prévoit des garanties appropriées afin de protéger les droits des personnes. Au lieu d'invoquer la pseudonymisation comme garantie possible, la PIPA l'impose en tant que condition préalable à la réalisation de certaines activités de traitement à des fins de statistiques, de recherche scientifique et d'archivage dans l'intérêt général (par exemple, afin de pouvoir traiter les données sans consentement, ou de combiner différents ensembles de données).

(43) De plus, la PIPA impose un certain nombre de garanties spécifiques, concernant notamment les mesures techniques et organisationnelles exigées, la tenue de registres, les limitations du partage de données et la prise en compte des risques éventuels de réidentification. La combinaison des différentes garanties décrites aux considérants 44 à 48 permet de garantir que le traitement des données à caractère personnel dans ce contexte fait l'objet de protections substantiellement équivalentes à celles exigées par le règlement (UE) 2016/679.

(44) Premièrement, et surtout, l'article 28-5, paragraphe 1, de la PIPA interdit le traitement d'informations pseudonymisées dans le but d'identifier des personnes en particulier. Si des informations permettant d'identifier une personne sont néanmoins générées lors du traitement des informations pseudonymisées, le responsable du traitement doit immédiatement suspendre le traitement et détruire ces informations (article 28-5, paragraphe 2, de la PIPA). Le non-respect de ces dispositions expose à une amende administrative et constitue une infraction pénale ([63]). Cela signifie que, même dans les situations où il serait *en pratique* possible de réidentifier les personnes, une telle réidentification est *juridiquement* interdite.

(45) Deuxièmement, lorsque le responsable du traitement procède au traitement (ultérieur) d'informations pseudonymisées à de telles fins, il est tenu de mettre en place des mesures technologiques, organisationnelles et physiques spécifiques afin de garantir la sécurité des informations (notamment en conservant et en gérant séparément les informations nécessaires au rétablissement de l'état initial des informations pseudonymisées) ([64]). De plus, il convient de conserver un registre des informations pseudonymisées traitées, de la finalité du traitement, de l'historique d'utilisation et des éventuels tiers destinataires (article 29-5, paragraphe 2, du décret d'application de la PIPA).

(46) Troisièmement et dernièrement, la PIPA prévoit des garanties spécifiques afin d'éviter l'identification de personnes par des tiers dans les cas où les informations sont partagées. Plus particulièrement, lorsqu'ils fournissent des informations pseudonymisées à un tiers à des fins de statistiques, de recherche scientifique ou d'archivage dans l'intérêt général, les responsables du traitement ne peuvent pas inclure d'informations qui pourraient être utilisées pour identifier une personne spécifique (article 28-2, paragraphe 2, de la PIPA) ([65]).

(47) Plus précisément, bien que la PIPA permette de combiner des informations pseudonymisées (traitées par différents responsables du traitement) à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt général, elle réserve ce droit aux institutions spécialisées disposant d'installations de sécurité spécifiques (article 28-3, paragraphe 1, de la PIPA) ([66]). Lorsqu'il demande à pouvoir combiner des données pseudonymisées, un responsable du traitement doit présenter des documents portant notamment sur les données devant être combinées, la

([61]) L'article 2, paragraphe 8, de la PIPA définit la recherche scientifique comme «la recherche appliquant des méthodes scientifiques, comme le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé». Ces catégories correspondent à celles définies au considérant 159 du règlement (UE) 2016/679.

([62]) Voir article 5, paragraphe 1, point b), article 89, paragraphes 1 et 2, et considérants 50 et 157 du règlement (UE) 2016/679.

([63]) Voir article 28-6, paragraphe 1, article 71, paragraphe 4-3, et article 75, paragraphe 2, point 4-4, de la PIPA.

([64]) Article 28-4 de la PIPA et article 29-5 du décret d'application de la PIPA. Le non-respect de cette obligation expose à de sanctions administratives et pénales, voir article 73, paragraphe 1, et article 75, paragraphe 2, point 6, de la PIPA.

([65]) Les violations de ces exigences exposent à des sanctions pénales (article 71, paragraphe 2, de la PIPA). La PIPC a immédiatement commencé à appliquer ces nouvelles règles, par exemple dans sa décision du 28 avril 2021, dans laquelle elle a infligé une amende et imposé des mesures correctrices à une entreprise qui, entre autres violations de la PIPA, n'avait pas respecté les exigences de l'article 28-2, paragraphe 2, de la PIPA — voir à l'adresse suivante: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

([66]) Pour être désigné comme institution spécialisée (une «agence experte en combinaison de données»), il convient d'envoyer une demande à la PIPC, accompagnée de pièces justificatives détaillant notamment les installations et les équipements mis en place afin de combiner en toute sécurité les données pseudonymisées et confirmant que le demandeur emploie à plein temps au moins trois personnes disposant de qualifications et d'une expérience en matière de protection des données à caractère personnel (article 29-2, paragraphes 1 et 2, du décret d'application de la PIPA). Des exigences détaillées, concernant par exemple les qualifications du personnel, les installations disponibles, les mesures de sécurité, les politiques et procédures internes, ainsi que des exigences financières, sont définies dans la notification 2020-9 de la PIPC sur la combinaison et la diffusion d'informations pseudonymisées (annexe I). La PIPC peut révoquer une désignation en tant qu'agence experte en combinaison de données (après avoir organisé une audition) pour certains motifs, par exemple si l'agence ne respecte plus les normes de sécurité exigées pour la désignation ou si une violation de données s'est produite dans le cadre de la combinaison de données (article 29-2, paragraphes 5 et 6, du décret d'application de la PIPA). La PIPC doit publier chaque désignation (ou révocation de la désignation) d'une agence experte en combinaison des données (article 29-2, paragraphe 7, du décret d'application de la PIPA).

finalité de la combinaison, ainsi que les mesures de sécurité proposées concernant le traitement des données combinées ([67]). Afin de permettre la combinaison, le responsable du traitement doit envoyer les données devant être combinées à l'institution spécialisée et fournir une «clé de combinaison» (c'est-à-dire les informations qui ont été utilisées pour la pseudonymisation) à l'agence coréenne de l'internet et de la sécurité ([68]). Celle-ci génère des «données de liaison de la clé de combinaison» (qui permettent de relier les clés de combinaison de différents demandeurs afin de parvenir à combiner les ensembles de données) et les fournit à l'institution spécialisée ([69]).

(48) Le responsable du traitement qui demande la combinaison de données peut analyser les informations combinées dans les locaux de l'institution spécialisée, dans un endroit où sont appliquées des mesures de sécurité techniques, physiques et administratives spécifiques (article 29-3 du décret d'application de la PIPA). Les responsables du traitement qui fournissent un ensemble de données en vue d'une telle combinaison ne peuvent faire sortir les données combinées de l'institution spécialisée qu'une fois les données combinées pseudonymisées ou anonymisées et uniquement avec l'approbation de ladite institution (article 28-3, paragraphe 2, de la PIPA) ([70]). Pour déterminer s'il y lieu ou non de donner son approbation, l'institution évalue le lien entre les données combinées et la finalité du traitement et vérifie si un plan de sécurité spécifique a été élaboré en vue de l'utilisation de ces données ([71]). L'exportation des informations combinées en dehors de l'institution ne sera pas permise si les informations contiennent des données qui permettraient d'identifier une personne ([72]). Enfin, la PIPC supervise la combinaison et la diffusion des données pseudonymisées par l'institution spécialisée (article 29-4, paragraphe 3, du décret d'application de la PIPA).

2.3.2. *Traitement portant sur des catégories particulières de données à caractère personnel*

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

(50) La PIPA contient des règles spécifiques concernant le traitement des données sensibles ([73]), définies comme étant des données à caractère personnel révélant des informations concernant l'idéologie, les croyances, l'adhésion à un syndicat ou à un parti politique ou la cessation d'une telle adhésion, les opinions politiques, la santé et la vie sexuelle d'une personne, ainsi que d'autres informations à caractère personnel susceptibles de menacer «considérablement» la vie privée de la personne concernée, qui ont été désignées comme étant des informations sensibles par un décret présidentiel ([74]). Selon les précisions communiquées par la PIPC, la notion de vie sexuelle est interprétée comme couvrant également l'orientation ou les préférences sexuelles d'une personne ([75]). De plus, l'article 18 du décret d'application ajoute d'autres catégories au champ d'application des données sensibles, notamment les informations sur l'ADN acquises à la suite d'un test génétique et les données qui constituent le casier judiciaire d'une personne. La modification récente apportée au décret d'application de la PIPA a encore élargi la notion de données sensibles, en y incluant également les données à caractère personnel révélant l'origine raciale ou ethnique et les informations biométriques ([76]). À la suite de cette modification, la notion de données sensibles en vertu de la PIPA est substantiellement équivalente à celle qui figure à l'article 9 du règlement (UE) 2016/679.

(51) Conformément à l'article 23, paragraphe 1, de la PIPA et à l'instar des dispositions de l'article 9, paragraphe 1, du règlement (UE) 2016/679, le traitement de données sensibles est interdit de manière générale, sauf si l'une des exceptions prévues s'applique ([77]). Ces exceptions limitent le traitement aux cas dans lesquels le responsable du traitement informe la personne concernée conformément aux articles 15 et 17 de la PIPA et obtient son consentement distinct (c'est-à-dire distinct du consentement au traitement d'autres données à caractère personnel), ou

([67]) Article 8, paragraphes 1 et 2, de la notification 2020-9 sur la combinaison et la diffusion d'informations pseudonymisées.
([68]) Article 2, paragraphes 3 et 6, et article 9, paragraphe 1, de la notification 2020-9 sur la combinaison et la diffusion d'informations pseudonymisées.
([69]) Article 2, paragraphe 4, et article 9, paragraphes 2 et 3, de la notification 2020-9 sur la combinaison et la diffusion d'informations pseudonymisées. L'institution spécialisée doit immédiatement détruire les données de liaison de la clé de combinaison une fois la combinaison réalisée (article 9, paragraphe 4, de la notification).
([70]) Les violations des exigences applicables à la combinaison d'ensembles de données exposent à des sanctions pénales (article 71, paragraphe 4-2, de la PIPA). Voir aussi article 29-2, paragraphe 4, du décret d'application de la PIPA.
([71]) La procédure d'approbation de la diffusion de données combinées est décrite à l'article 11 de la notification 2020-9 sur la combinaison et la diffusion d'informations pseudonymisées. Plus particulièrement, l'institution spécialisée doit mettre en place un «comité d'examen de la diffusion» se composant de membres qui disposent de connaissances et d'une expérience importantes en matière de protection des données.
([72]) Article 29-2, paragraphe 4, du décret d'application de la PIPA et article 11 de la notification 2020-9.
([73]) La Cour constitutionnelle coréenne a également reconnu la nécessité d'accorder des protections spécifiques au traitement des données sensibles, telles que les données concernant la santé ou le comportement sexuel, voir arrêt HunMa 1139 de la Cour constitutionnelle du 31 mai 2007.
([74]) Article 23, paragraphe 1, de la PIPA.
([75]) Voir également guide sur la PIPA, chapitre III, section 2, portant sur l'article 23 (p. 157 à 164).
([76]) C'est-à-dire les informations à caractère personnel découlant d'un traitement technique spécifique des données portant sur les caractéristiques physiques, physiologiques ou comportementales d'une personne afin d'identifier de manière unique cette personne.
([77]) Le non-respect de ces exigences expose à des sanctions conformément à l'article 71, point 3, de la PIPA.

dans lesquels la loi permet ou exige un tel traitement. Les autorités publiques peuvent également traiter les informations biométriques, les informations sur l'ADN acquises à la suite d'un test génétique, les informations à caractère personnel révélant l'origine raciale ou ethnique et les données qui constituent un casier judiciaire pour des motifs qu'elles seules peuvent invoquer (par exemple lorsque cela est nécessaire aux fins d'une enquête pénale ou pour permettre à une juridiction de juger d'une affaire) ([78]). Dès lors, les fondements juridiques disponibles pour le traitement des données sensibles sont plus limités que pour d'autres types de données à caractère personnel et les dispositions du droit coréen à cet égard sont plus restrictives que celles de l'article 9, paragraphe 2, du règlement (UE) 2016/679.

(52) De plus, l'article 23, paragraphe 2, de la PIPA, dont le non-respect expose à des sanctions ([79]), souligne à quel point il est important de garantir une sécurité appropriée lors du traitement de données sensibles, afin d'éviter qu'elles ne soient «perdues, volées, divulguées, falsifiées, modifiées ou endommagées». Bien que l'article 29 de la PIPA donne à cette exigence un caractère général, l'article 3, paragraphe 4, indique clairement que le niveau de sécurité doit être adapté au type de données à caractère personnel traitées, ce qui signifie qu'il faut tenir compte des risques spécifiques liés au traitement de données sensibles. De plus, le traitement des données doit toujours être réalisé «de manière à limiter la possibilité d'atteinte» à la vie privée de la personne concernée et, si possible, «de manière anonyme» (article 3, paragraphes 6 et 7, de la PIPA). Ces exigences sont particulièrement pertinentes lorsque le traitement porte sur des données sensibles.

2.3.3. *Limitation de la finalité*

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

(54) Ce principe est garanti par l'article 3, paragraphes 1 et 2, de la PIPA, selon lequel le responsable du traitement «précise et explicite» la finalité du traitement, traite les données à caractère personnel de façon appropriée et nécessaire à cette finalité et ne les utilise pas d'une manière qui outrepasse cette finalité. L'article 15, paragraphe 1, l'article 18, paragraphe 1, l'article 19 et, pour les sous-traitants (les «parties sous-traitantes»), l'article 26, paragraphe 1, point 1, et l'article 26, paragraphes 5 et 7, de la PIPA confirment également le principe général de limitation de la finalité. Plus particulièrement, les données à caractère personnel ne peuvent en principe être utilisées et fournies à des tiers que dans le cadre de la finalité pour laquelle elles ont été collectées (article 15, paragraphe 1, et article 17, paragraphe 1, point 2). Le traitement pour une finalité compatible, c'est-à-dire «dans un cadre raisonnablement lié à la finalité initiale de la collecte», n'est possible que s'il n'a pas de répercussions négatives sur les personnes concernées et si les mesures de sécurité nécessaires (comme le chiffrement), sont adoptées (article 15, paragraphe 3, et article 17, paragraphe 4, de la PIPA). Afin de déterminer si la finalité d'un traitement ultérieur est compatible, le décret d'application de la PIPA énumère des critères spécifiques semblables à ceux prévus par l'article 6, paragraphe 4, du règlement (UE) 2016/679, voir considérant 36.

(55) Comme expliqué au considérant 38, la finalité de la collecte dans le cas où les responsables du traitement coréens reçoivent des données à caractère personnel provenant de l'Union correspond à la finalité pour laquelle les données sont transférées. Le responsable du traitement ne peut modifier la finalité qu'à titre exceptionnel, dans des cas spécifiques (énumérés) (article 18, paragraphe 2, points 1 à 3, de la PIPA; voir également considérant 39). Dans la mesure où un changement de finalité est autorisé par la loi, ces lois doivent à leur tour respecter le droit fondamental au respect de la vie privée et à la protection des données, ainsi que les principes de nécessité et de proportionnalité énoncés dans la Constitution coréenne. De plus, l'article 18, paragraphes 2 et 5, de la PIPA prévoit des garanties supplémentaires, notamment en exigeant qu'une telle modification de la finalité ne «porte pas atteinte de manière déloyale aux intérêts de la personne concernée», une mise en balance des intérêts en jeu étant dès lors toujours nécessaire. Ces dispositions fournissent un niveau de protection substantiellement équivalent à celui prévu par l'article 5, paragraphe 1, point b), et par l'article 6, en liaison avec le considérant 50, du règlement (UE) 2016/679.

2.3.4. *Exactitude et minimisation des données*

(56) Les données à caractère personnel doivent être exactes et, si nécessaire, mises à jour. Elles doivent également être adéquates, pertinentes et se limiter à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

([78]) L'article 18 du décret d'application de la PIPA prévoit que les catégories de données qu'il énumère sont exclues des dispositions de l'article 23, paragraphe 1, de la loi lorsqu'elles sont traitées par une institution publique en vertu de l'article 18, paragraphe 2, points 5 à 9, de la PIPA.

([79]) Voir l'article 73, point 1, et l'article 75, paragraphe 2, point 6, de la PIPA.

(57) Le principe d'exactitude est reconnu d'une manière similaire à l'article 3, paragraphe 3, de la PIPA, qui exige que les données à caractère personnel soient «exactes, complètes et mises à jour dans la mesure nécessaire aux finalités» pour lesquelles elles ont été collectées. L'article 3, paragraphes 1 et 6, et l'article 16, paragraphe 1, de la PIPA exigent la minimisation des données et précisent que le responsable du traitement limite la collecte des données à caractère personnel «à ce qui est strictement nécessaire» pour parvenir à la finalité prévue, et que la charge de la preuve lui incombe à cet égard. Si la finalité de la collecte peut être atteinte en traitant les informations sous une forme anonymisée, les responsables du traitement doivent s'efforcer de le faire (article 3, paragraphe 7, de la PIPA).

2.3.5. *Limitation de la conservation*

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

(59) Le principe de limitation de la conservation est également prévu par l'article 21, paragraphe 1, de la PIPA ([80]), qui impose au responsable du traitement qu'il «détruise» ([81]) les données à caractère personnel sans délai une fois atteinte la finalité pour laquelle elles ont été collectées ou à l'expiration de la durée de conservation (selon ce qui se produit en premier lieu), sauf si la loi impose de les conserver plus longtemps ([82]). Dans ce dernier cas, les données à caractère personnel concernées «sont conservées et gérées indépendamment des autres informations à caractère personnel» (article 21, paragraphe 3, de la PIPA).

(60) L'article 21, paragraphe 1, de la PIPA ne s'applique pas lorsque des données pseudonymisées sont traitées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt général ([83]). Afin de veiller à l'application du principe de limitation de la conservation des données dans un tel cas également, la notification 2021-5 impose aux responsables du traitement d'anonymiser les informations conformément à l'article 58-2 de la PIPA si les données n'ont pas été détruites une fois atteinte la finalité spécifique du traitement des données ([84]).

2.3.6. *Sécurité des données*

(61) Les données à caractère personnel devraient être traitées d'une manière garantissant leur sécurité, y compris leur protection contre tout traitement non autorisé ou illicite et contre toute perte, toute destruction ou tout dommage d'origine accidentelle. À cette fin, les opérateurs économiques devraient prendre les mesures techniques ou organisationnelles appropriées pour protéger les données à caractère personnel contre d'éventuelles menaces. Ces mesures devraient être évaluées en tenant compte de l'état de la technique, des coûts y afférents ainsi que de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les droits des personnes.

(62) L'article 3, paragraphe 4, de la PIPA prévoit un principe de sécurité similaire et impose aux responsables du traitement de «gérer les informations à caractère personnel en toute sécurité, en fonction des méthodes de traitement, des types, etc. d'informations à caractère personnel, en tenant compte de la possibilité d'atteintes aux droits de la personne concernée et de la gravité des risques pertinents». De plus, le responsable du traitement «traite les informations à caractère personnel de manière à limiter autant que faire se peut la possibilité d'atteinte à la vie privée d'une personne concernée» et s'efforce dans ce cadre de traiter les données à caractère personnel sous forme anonymisée ou pseudonymisée, si possible (article 3, paragraphes 6 et 7, de la PIPA).

(63) L'article 29 de la PIPA décrit plus en détail ces exigences générales et prévoit que chaque responsable du traitement doit «prendre les mesures techniques, organisationnelles et physiques nécessaires, comme créer un plan de gestion interne et conserver des registres d'accès, qui sont nécessaires pour garantir la sécurité de la

([80]) Article 8 (en liaison avec l'article 8-2 du décret d'application), article 11 (en liaison avec l'article 12, paragraphe 2, du décret d'application).

([81]) En ce qui concerne les méthodes de destruction des informations à caractère personnel, voir article 16 du décret d'application de la PIPA. L'article 21, paragraphe 2, de la PIPA précise qu'elles incluent les «mesures nécessaires pour empêcher leur récupération et leur rétablissement».

([82]) Le non-respect de ces exigences expose à des sanctions pénales (article 73, paragraphes 1 et 2, de la PIPA). L'article 39-6 de la PIPA impose une exigence supplémentaire aux fournisseurs de services d'information et de communication, à savoir qu'ils sont tenus de supprimer les informations à caractère personnel des utilisateurs qui n'ont pas utilisé les services d'information et de communication proposés pendant au moins un an (sauf si une conservation plus longue est imposée par la loi ou demandée par la personne concernée). Les personnes doivent être informées de la suppression prévue de leurs informations 30 jours avant l'expiration du délai d'un an (article 39-6, paragraphe 2, de la PIPA et article 48-5, paragraphe 3, du décret d'application de la PIPA). Si la loi exige une conservation plus longue, les données conservées doivent l'être séparément des autres informations des utilisateurs et peuvent uniquement être utilisées ou divulguées conformément à cette loi (article 48-5, paragraphes 1 et 2, du décret d'application de la PIPA).

([83]) Article 28-7 de la PIPA.

([84]) Notification 2021-5 (annexe I), section 4.

manière prescrite par décret présidentiel afin d'éviter que les informations à caractère personnel ne soient perdues, volées, divulguées, falsifiées, modifiées ou endommagées». L'article 30, paragraphe 1, du décret d'application de la PIPA détaille ces mesures en faisant référence 1) à la formulation et à la mise en œuvre d'un plan de gestion interne pour le traitement en toute sécurité des données à caractère personnel; 2) au contrôle et à la limitation de l'accès; 3) à l'adoption de technologies de chiffrement afin de conserver et de transmettre les données à caractère personnel en toute sécurité; 4) aux registres d'accès; 5) aux programmes de sécurité; et 6) à des mesures physiques telles qu'un stockage sûr ou un système de verrouillage ([85]).

(64) De plus, des obligations spécifiques s'appliquent en cas de violation des données (article 34 de la PIPA, en liaison avec les articles 39 et 40 du décret d'application de la PIPA) ([86]). Plus particulièrement, le responsable du traitement est tenu d'informer sans délai les personnes concernées lésées des détails de la violation ([87]) et notamment de leur fournir des informations concernant les contre-mesures (obligatoires) prises par le responsable du traitement et les mesures que les personnes concernées peuvent prendre pour réduire le plus possible le risque de préjudice (article 34, paragraphes 1 et 2, de la PIPA) ([88]). Lorsqu'au moins 1 000 personnes concernées sont victimes d'une violation, le responsable du traitement signale également, sans délai, la violation de données et les contre-mesures prises à la PIPC et à l'agence coréenne de l'internet et de la sécurité, lesquels peuvent apporter une assistance technique (article 34, paragraphe 3, de la PIPA, en liaison avec l'article 39 du décret d'application de la PIPA). Les responsables du traitement sont responsables des dommages subis du fait des violations de données, conformément aux dispositions du code civil sur la responsabilité délictuelle (voir également section 2.5 sur les recours) ([89]).

(65) Lorsqu'il s'acquitte de ses obligations en matière de sécurité, le responsable du traitement doit être secondé par un responsable de la confidentialité, dont les missions incluent notamment la création d'un système interne de contrôle «afin de prévenir la divulgation et l'utilisation abusive ou détournée des informations à caractère personnel» (article 31, paragraphe 2, point 4, de la PIPA). De plus, le responsable du traitement est tenu d'exercer «un contrôle et une supervision appropriés» des membres de son personnel qui traitent des données à caractère personnel, y compris en ce qui concerne la gestion de celles-ci en toute sécurité. Cela inclut la formation nécessaire formation («éducation») des salariés [article 28, paragraphes 1 et 2 de la PIPA). Enfin, en cas de sous-traitance, le responsable du traitement doit imposer des exigences à la partie sous-traitante, en ce qui concerne notamment la gestion en toute sécurité des données à caractère personnel («mesures techniques et organisationnelles») et doit superviser la manière dont ces exigences sont appliquées grâce à des contrôles (article 26, paragraphes 1 et 4, de la PIPA, en liaison avec l'article 28, paragraphe 1, points 3 et 4, et paragraphe 6, du décret d'exécution de la PIPA).

2.3.7. *Transparence*

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

([85]) En ce qui concerne le traitement des données à caractère personnel par les fournisseurs de services d'information et de communication, l'article 39-5 de la PIPA prévoit explicitement que le nombre de personnes qui manipulent les informations à caractère personnel des utilisateurs doit être limité autant que possible. De plus, les fournisseurs de services d'information et de communication veillent à ce que les informations à caractère personnel des utilisateurs ne soient pas rendues publiques par l'intermédiaire des réseaux d'information et de communication (article 39-10, paragraphe 1, de la PIPA). Les informations rendues publiques doivent être supprimées ou bloquées sur demande de la PIPC (article 39-10, paragraphe 2, de la PIPA). Plus généralement, les fournisseurs de services d'information et de communication (et les tiers qui reçoivent les données à caractère personnel des utilisateurs) sont soumis à des obligations supplémentaires en matière de sécurité, précisées à l'article 48-2 du décret d'application de la PIPA, par exemple la mise au point et l'application d'un plan de gestion interne concernant les mesures de sécurité, les mesures permettant de contrôler les accès, le chiffrement, l'utilisation de logiciels permettant de détecter les programmes malveillants, etc.

([86]) De plus, il est généralement interdit d'endommager, de détruire, de modifier, de falsifier ou de divulguer des informations à caractère personnel sans disposer de l'autorité légale à cet effet, voir article 59, point 3, de la PIPA.

([87]) L'obligation de notification à la personne ne s'applique pas dans la mesure où une violation des données se produit en lien avec des informations pseudonymisées traitées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt général (article 28-7 de la PIPA, qui prévoit une dérogation à l'article 34, paragraphe 1, et à l'article 39-4 de la PIPA). Pour pouvoir procéder aux notifications individuelles, le responsable du traitement concerné devrait identifier les personnes à partir de l'ensemble de données pseudonymisé, ce qui est expressément interdit par l'article 28-5 de la PIPA. Cependant, l'obligation générale de notification de la violation de données (à la PIPC) continue de s'appliquer.

([88]) Les obligations de notification, notamment en ce qui concerne le moment auquel la notification doit intervenir et la possibilité de procéder à la notification «par étapes», sont précisées plus en détail à l'article 40 du décret d'application de la PIPA. Des règles plus strictes s'appliquent aux fournisseurs de services d'information et de communication, qui sont tenus de transmettre une notification aux personnes concernées et à la PIPC dans un délai de 24 heures après avoir pris connaissance du fait que des informations à caractère personnel ont été perdues, volées ou divulguées (article 39-4, paragraphe 1, de la PIPA). Cette notification doit inclure des détails concernant les informations à caractère personnel qui ont été divulguées, le moment auquel cette divulgation s'est produite, les mesures que l'utilisateur peut prendre, les mesures prises pour y faire face par le fournisseur ainsi que les coordonnées du service auquel l'utilisateur peut poser ses questions (article 39-4, paragraphe 1, points 1 à 5, de la PIPA). Si une raison valable le justifie, par exemple le fait de ne pas disposer des coordonnées de l'utilisateur, il est possible d'utiliser d'autres moyens de communication, par ex. en portant les informations à la connaissance du public au moyen d'une publication sur un site web (article 39-4, paragraphe 1, de la PIPA, en liaison avec l'article 48-4, paragraphe 4 et suivants, du décret d'application de la PIPA). Dans ce cas, il convient d'informer la PIPC de ces raisons (article 34-4, paragraphe 3, de la PIPA).

([89]) Voir, par exemple, décisions 2011Da59834, 2011Da59858 et 2011Da59841 de la Cour suprême du 26 décembre 2012. Un résumé en anglais est disponible à l'adresse suivante: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm

(67) Le système coréen prévoir différentes manières de le faire. Outre le droit à l'information prévu à l'article 4, point 1 (en général), et par l'article 20, paragraphe 1 (pour les données à caractère personnel collectées auprès de tiers), de la PIPA et le droit d'accès prévu par l'article 35 de la PIPA, la PIPA inclut une obligation générale de transparence en ce qui concerne la finalité du traitement (article 3, paragraphe 1, de la PIPA) et des obligations spécifiques de transparence lorsque le traitement est fondé sur le consentement (article 15, paragraphe 2, article 17, paragraphe 2, et article 18, paragraphe 3, de la PIPA) ([90]). De plus, l'article 20, paragraphe 2, de la PIPA impose à certains responsables du traitement [ceux pour qui le traitement dépasse certains seuils ([91])] de notifier aux personnes concernées dont il a reçu des données à caractère personnel de la part de tiers la source d'information, la finalité du traitement et le fait qu'elles ont le droit de demander une suspension du traitement, sauf si une telle notification s'avère impossible en raison de l'absence de coordonnées permettant de contacter les personnes. Des exceptions à cette obligation de notification s'appliquent à certains fichiers de données à caractère personnel détenus par les autorités publiques, notamment aux fichiers qui contiennent des données traitées à des fins de sécurité nationale, pour d'autres intérêts nationaux particulièrement importants («sérieux») ou aux fins de l'application du droit pénal, ou lorsqu'une telle notification est susceptible de porter atteinte à la vie ou à l'intégrité corporelle d'une autre personne ou de causer des dommages de manière déloyale aux biens et autres intérêts d'une autre personne, mais uniquement lorsque les intérêts publics ou privés en jeu sont «manifestement supérieurs» aux droits des personnes concernées (article 20, paragraphe 4, de la PIPA). Il convient à cet effet de trouver un équilibre entre les intérêts en jeu.

(68) De plus, l'article 3, paragraphe 5, de la PIPA impose aux responsables du traitement de rendre publique leur politique de confidentialité (et d'autres questions liées au traitement des données à caractère personnel). Cette exigence est décrite plus en détail à l'article 30 de la PIPA, en liaison avec l'article 31 du décret d'application de la PIPA. Selon ces dispositions, la politique de confidentialité portée à la connaissance du public doit notamment indiquer 1) les types de données à caractère personnel traitées; 2) la finalité du traitement; 3) la durée de conservation; 4) si les données à caractère personnel sont fournies à des tiers ([92]); 5) toute sous-traitance; 6) des informations concernant les droits de la personne concernée et la manière de les exercer; et 7) des coordonnées (y compris le nom du responsable de la confidentialité ou du service interne chargé de contrôler le respect des règles en matière de protection des données et de traiter les plaintes). La politique de confidentialité doit être rendue publique de manière à ce que les personnes concernées «puissent aisément la reconnaître» (article 30, paragraphe 2, de la PIPA) ([93]) et doit être constamment mise à jour (article 31, paragraphe 2, du décret d'application de la PIPA).

(69) Les institutions publiques sont soumises à une obligation supplémentaire d'enregistrement auprès de la PIPC, notamment des informations suivantes: 1) le nom de l'institution publique; 2) les fondements et finalités du traitement des fichiers de données à caractère personnel; 3) les caractéristiques des données à caractère personnel enregistrées; 4) la méthode de traitement; 5) la durée de conservation; 6) le nombre de personnes concernées dont les données à caractère personnel sont conservées; 7) le service qui traite les demandes des personnes concernées; et 8) les destinataires des données à caractère personnel lorsque celles-ci sont fournies de manière habituelle ou répétée (article 32, paragraphe 1, de la PIPA) ([94]). Les fichiers de données à caractère personnel enregistrées sont rendus publics par la PIPC et doivent également être référencés par les institutions publiques dans leur politique de confidentialité (article 30, paragraphe 1, et article 32, paragraphe 4, de la PIPA).

(70) Afin d'améliorer la transparence pour les personnes concernées se trouvant dans l'Union dont les données à caractère personnel sont transférées en Corée sur la base de la présente décision, la section 3, points i) et ii), de la notification 2021-5 (annexe I) impose des exigences supplémentaires en matière de transparence. Premièrement, lorsqu'ils reçoivent des données à caractère personnel provenant de l'Union sur la base de la présente décision, les responsables du traitement coréens doivent notifier aux personnes concernées sans retard injustifié (et en tout état

([90]) Plus particulièrement, lorsque des informations à caractère personnel sont traitées avec le consentement d'une personne, le responsable du traitement doit indiquer à cette dernière la finalité du traitement, des détails concernant les informations qui seront traitées, le destinataire des informations, la durée pendant laquelle les informations à caractère personnel sont conservées et utilisées, ainsi que le fait qu'elle a le droit de ne pas donner son consentement (et les inconvénients que cela peut entraîner).

([91]) Conformément à l'article 15-2, paragraphe 1, du décret d'application de la PIPA, cela concerne les responsables du traitement qui traitent des informations sensibles relatives à au moins 50 000 personnes concernées ou des informations à caractère personnel «normales» relatives à au moins un million de personnes concernées. L'article 15-2, paragraphe 2, du décret d'application de la PIPA définit les méthodes de notification et le moment auquel il doit être procédé à ces notifications, et l'article 15-2, paragraphe 3, définit les exigences liées à la tenue de certains registres à cet égard. De plus, des règles spécifiques s'appliquent à certaines catégories de fournisseurs de services d'information et de communication (ceux ayant généré un chiffre d'affaires d'au moins 10 milliards de wons au cours de l'année précédente ou ceux qui conservent/gèrent les données à caractère personnel d'au moins un million d'utilisateurs par jour en moyenne au cours des trois mois précédant la fin de l'année précédente), qui sont tenus de notifier aux utilisateurs l'historique d'utilisation de leurs informations à caractère personnel de manière régulière, sauf si cela s'avère impossible en raison de l'absence de coordonnées permettant de contacter les personnes (article 39-8 de la PIPA et article 48-6 du décret d'application de la PIPA).

([92]) Selon les informations fournies par le gouvernement coréen, cela inclut une obligation de mentionner chacun des destinataires dans la politique de confidentialité.

([93]) L'article 31, paragraphe 3, du décret d'application de la PIPA définit des modalités supplémentaires.

([94]) L'obligation d'enregistrement ne s'applique pas à certains types de fichiers d'informations à caractère personnel, par exemple ceux qui contiennent des données relatives à la sécurité nationale, aux secrets diplomatiques, aux enquêtes pénales, aux enquêtes, poursuites ou sanctions en matière fiscale, ni aux fichiers portant exclusivement sur les performances professionnelles internes (article 32, paragraphe 2, de la PIPA).

de cause dans un délai maximal d'un mois à compter du transfert) le nom et les coordonnées des entités transférant et recevant les informations, les données (ou catégories de données) à caractère personnel transférées, la finalité de la collecte par le responsable du traitement coréen, la durée de conservation et les droits que leur confère la PIPA. Deuxièmement, lorsque des données à caractère personnel provenant de l'Union sont fournies à des tiers sur la base de la présente décision, les personnes concernées doivent notamment être informées du destinataire, des données à caractère personnel ou des catégories de données à caractère personnel devant être fournies, du pays auquel ces données sont fournies (le cas échéant), ainsi que des droits que leur confère la PIPA ([95]). De cette manière, la notification garantit que les personnes se trouvant dans l'Union continuent d'être informées des responsables du traitement spécifiques qui traitent leurs informations et sont en mesure d'exercer leurs droits vis-à-vis des entités pertinentes.

(71) La section 3, point iii), de la notification (annexe I) permet certaines exceptions limitées et spécifiques à ces obligations supplémentaires en matière de transparence, qui sont substantiellement équivalentes à celles prévues par le règlement (UE) 2016/679. Plus particulièrement, la notification des personnes concernées se trouvant dans l'Union n'est pas requise 1) lorsqu'il convient de restreindre les notifications pour des raisons d'intérêt général (par exemple lorsque les informations sont traitées aux fins de la sécurité nationale ou d'enquêtes pénales en cours) et pour la durée nécessaire à cet effet, dans la mesure où les objectifs d'intérêt général sont manifestement supérieurs aux droits de la personne concernée; 2) lorsque la personne concernée dispose déjà de ces informations; 3) lorsque et dans la mesure où la notification est susceptible de porter atteinte à la vie ou à l'intégrité corporelle de la personne concernée ou d'une autre personne, ou de porter atteinte de manière déloyale aux intérêts matériels d'une autre personne, lorsque de tels droits ou intérêts sont manifestement supérieurs aux droits de la personne concernée; ou 4) lorsqu'on ne dispose pas des coordonnées des personnes concernées ou que leur envoyer une notification nécessiterait un effort disproportionné. Afin de déterminer s'il est ou non possible de contacter la personne concernée ou si des efforts excessifs sont nécessaires à cet effet, il convient de tenir compte de la possibilité de coopérer avec l'exportateur des données situé dans l'Union.

(72) Les règles prévues aux considérants 67 à 71 assurent donc un niveau de protection en matière de transparence substantiellement équivalent à celui que prévoit le règlement (UE) 2016/679.

2.3.8. *Droits individuels*

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

(74) Selon l'article 3, paragraphe 5, de la PIPA, le responsable du traitement garantit les droits des personnes concernées énumérés à l'article 4 de la PIPA et détaillés dans les articles 35 à 37, 39 et 39-2 de la PIPA.

(75) Premièrement, les personnes disposent d'un droit à l'information et d'un droit d'accès. Lorsque le responsable du traitement a collecté les données à caractère personnel auprès d'un tiers (ce qui sera toujours le cas lorsque les données sont transférées depuis l'Union), les personnes concernées disposent généralement du droit de recevoir des informations concernant 1) la «source» de leurs données à caractère personnel transférées (c'est-à-dire l'entité qui les a transférées), 2) la finalité du traitement et 3) le fait qu'elles ont le droit de demander la suspension du traitement (article 20, paragraphe 1, de la PIPA). Des limitations s'appliquent, notamment lorsqu'une telle notification est susceptible de porter atteinte à la vie ou à l'intégrité corporelle d'une autre personne ou «de causer de manière déloyale des dommages aux biens et autres intérêts» d'une autre personne, mais seulement lorsque les intérêts de ces tiers sont «explicitement supérieurs» aux droits de la personne concernée (article 20, paragraphe 4, point 2, de la PIPA).

(76) De plus, l'article 35, paragraphes 1 et 3, de la PIPA, en liaison avec l'article 41, paragraphe 4, du décret d'application de la PIPA, confère aux personnes concernées un droit d'accès à leurs informations à caractère personnel ([96]). Le droit d'accès couvre la confirmation du traitement, les informations concernant le type de données traitées, la finalité du traitement, la durée de conservation et toute divulgation à un tiers, ainsi que la

([95]) Notification 2021-5, section 3, point ii) (annexe I).

([96]) Selon l'article 35, paragraphe 3, de la PIPA, en liaison avec l'article 42, paragraphe 2, du décret d'application de la PIPA, le responsable du traitement peut reporter l'octroi de l'accès pour de «bonnes raisons» (c'est-à-dire des raisons dûment justifiées, par exemple si un délai supplémentaire est nécessaire pour évaluer si l'accès peut être accordé), mais il doit informer la personne concernée de cette raison dans les 10 jours et lui préciser la manière dont elle peut former un recours contre une telle décision; aussitôt que la raison justifiant le report cesse d'exister, l'accès doit être accordé.

fourniture d'une copie des informations à caractère personnel traitées (article 4, point 3, de la PIPA, en liaison avec l'article 41, paragraphe 1, du décret d'application de la PIPA) ([97]). L'accès ne peut être limité (accès partiel) ([98]) ou refusé que lorsque la loi le prévoit ([99]), lorsqu'il est susceptible de porter atteinte à la vie ou à l'intégrité corporelle d'un tiers ou de causer une atteinte injustifiée aux biens et autres intérêts d'une autre personne (article 35, paragraphe 4, de la PIPA) ([100]). Ce dernier cas nécessite de mettre en balance les droits et libertés constitutionnels de la personne, d'une part, et ceux d'autres personnes, d'autre part. Lorsque l'accès est limité ou refusé, le responsable du traitement doit en indiquer les motifs à la personne concernée et lui préciser la manière dont elle peut former un recours contre une telle décision (article 41, paragraphe 5, et article 42, paragraphe 2, du décret d'application de la PIPA).

(77) Deuxièmement, les personnes concernées disposent du droit à la rectification ou à l'effacement ([101]) de leurs données à caractère personnel, «sauf si d'autres dispositions légales en disposent spécifiquement autrement» (article 36, paragraphes 1 et 2, de la PIPA) ([102]). À la réception d'une demande, le responsable du traitement doit réaliser une enquête sans retard, prendre les mesures nécessaires ([103]) et les notifier à la personne concernée dans un délai de dix jours; lorsqu'il n'est pas possible de donner suite à la demande, cette obligation de notification porte sur les raisons du refus et la manière de former un recours (voir article 36, paragraphe 4, de la PIPA, en liaison avec l'article 43, paragraphe 3, du décret d'application de la PIPA) ([104]).

(78) Enfin, les personnes concernées ont droit à la suspension du traitement de leurs données à caractère personnel sans retard ([105]), sauf si l'une des exceptions prévues s'applique (article 37, paragraphes 1 et 2, de la PIPA) ([106]). Le responsable du traitement peut rejeter la demande 1) lorsque la loi le permet expressément ou lorsque cela est nécessaire («inévitable») afin de s'acquitter d'obligations juridiques; 2) lorsque la suspension demandée est susceptible de porter atteinte à la vie ou à l'intégrité corporelle d'un tiers ou de causer une atteinte injustifiée aux biens et autres intérêts d'une autre personne; 3) lorsqu'il serait impossible pour une institution publique de réaliser ses missions telles que prévues par la loi sans traiter les informations; ou 4) lorsque la personne concernée ne résilie pas expressément le contrat sous-jacent conclu avec le responsable du traitement alors même qu'il serait impossible d'exécuter ce contrat sans traiter les données. Dans ce cas, le responsable du traitement doit, sans retard, notifier à la personne concernée les motifs du rejet et l'informer de la manière dont elle peut former un recours (article 37, paragraphe 2, de la PIPA, en liaison avec l'article 44, paragraphe 2, du décret d'application de la PIPA). Selon l'article 37, paragraphe 4, de la PIPA, le responsable du traitement doit, sans retard, «prendre les mesures nécessaires, y compris la destruction des informations à caractère personnel concernées» lorsqu'il exécute la demande de suspension ([107]).

(79) Le droit à la suspension s'applique également lorsque les données à caractère personnel sont utilisées à des fins de marketing direct, c'est-à-dire afin de promouvoir des biens ou des services ou d'en encourager l'acquisition. De plus, un tel traitement ultérieur nécessite en général le consentement spécifique (supplémentaire) de la personne concernée (voir article 15, paragraphe 1, point 1, et article 17, paragraphe 2, point 1, de la PIPA) ([108]). Lorsqu'il demande un tel consentement, le responsable du traitement doit spécifiquement informer la personne concernée

([97]) L'accès aux informations à caractère personnel traitées par une institution publique peut être obtenu directement auprès de l'institution ou indirectement en adressant une demande à la PIPC, qui la transmettra sans retard (article 35, paragraphe 2, de la PIPA et article 41, paragraphe 3, du décret d'application de la PIPA).

([98]) Selon l'article 42, paragraphe 1, du décret d'application de la PIPA, le responsable du traitement est tenu d'accorder un accès partiel lorsqu'une partie au moins des informations n'est pas couverte par les motifs de refus.

([99]) Ces lois doivent à leur tour respecter le droit fondamental au respect de la vie privée et à la protection des données, ainsi que les principes de nécessité et de proportionnalité énoncés dans la constitution coréenne.

([100]) De plus, les institutions publiques peuvent refuser l'accès si l'accorder entraînerait de graves difficultés pour réaliser certaines tâches, notamment les audits en cours de réalisation ou l'imposition, la collecte ou le remboursement d'impôts (article 35, paragraphe 4, de la PIPA).

([101]) Dans un tel cas, le responsable du traitement doit prendre des mesures empêchant la récupération des informations à caractère personnel, voir article 36, paragraphe 3, de la PIPA.

([102]) De telles dispositions légales doivent respecter les exigences de la Constitution qui prévoient qu'un droit fondamental peut uniquement être restreint lorsque cela s'avère nécessaire pour des raisons de sécurité nationale ou pour le maintien de l'ordre public et du bien-être social, et ne peuvent pas affecter l'essence même d'une liberté ou d'un droit (article 37, paragraphe 2, de la Constitution).

([103]) L'article 43, paragraphe 2, du décret d'application de la PIPA prévoit une procédure spéciale lorsque le responsable du traitement traite des fichiers d'informations à caractère personnel fournis par un autre responsable du traitement.

([104]) Le non-respect de l'obligation de prendre les mesures nécessaires pour rectifier ou effacer les informations à caractère personnel et la poursuite de l'utilisation ou de la fourniture à un tiers de ces informations exposent à des sanctions pénales (article 73, paragraphe 2, de la PIPA).

([105]) Selon l'article 44, paragraphe 2, du décret d'application de la PIPA, le responsable du traitement informe la personne concernée du fait qu'il a bien suspendu le traitement dans un délai de dix jours à compter de la réception de la demande.

([106]) En ce qui concerne les institutions publiques, le droit à la suspension du traitement peut être exercé à l'égard des informations contenues dans les fichiers d'informations à caractère personnel enregistrés (article 37, en liaison avec l'article 32, de la PIPA). Un tel enregistrement n'est pas obligatoire dans un nombre limité de situations, par ex. lorsque les fichiers d'informations à caractère personnel portent sur des questions de sécurité nationale, des enquêtes pénales, des relations diplomatiques, etc. (article 32, paragraphe 2, de la PIPA).

([107]) La poursuite du traitement expose à des sanctions pénales (article 73, paragraphe 3, de la PIPA).

([108]) Le comité de médiation des litiges (voir considérant 133) a traité plusieurs cas dans lesquels des personnes se sont plaintes de l'utilisation de leurs données à des fins de marketing direct sans consentement, ce qui a donné lieu, par exemple, au paiement d'une compensation et à la suppression de données à caractère personnel par le responsable du traitement concerné [voir par exemple le comité de médiation des litiges 20R10-024 (2020.11.18), 20R08-015, (2020.8.28), et 20R07-031 (2020.9.1)].

de l'utilisation prévue des données à des fins de marketing direct (c'est-à-dire du fait qu'il ou elle pourra être contacté en vue de la promotion de biens ou de services ou d'être encouragé à en faire l'acquisition) d'une «manière explicitement reconnaissable» (article 22, paragraphes 2 et 4, de la PIPA, en liaison avec l'article 17, paragraphe 2, point 1, du décret d'exécution de la PIPA).

(80) Afin de faciliter l'exercice des droits individuels, le responsable du traitement doit mettre au point des procédures spécifiques et les porter à la connaissance du public (article 38, paragraphe 4, de la PIPA) ([109]). Cela comprend notamment des procédures permettant de contester le rejet d'une demande (article 38, paragraphe 5, de la PIPA). Le responsable du traitement doit veiller à ce que la procédure d'exercice des droits soit «conviviale» et ne soit pas plus difficile que celle de la collecte des données à caractère personnel. Cela inclut également l'obligation de fournir des informations sur la procédure sur son site web (article 41, paragraphe 2, article 43, paragraphe 1, et article 44, paragraphe 1, du décret d'application de la PIPA) ([110]). Les personnes peuvent désigner un représentant et l'autoriser à présenter une telle demande (article 38, paragraphe 1, de la PIPA, en liaison avec l'article 45 du décret d'application de la PIPA). Bien que le responsable du traitement puisse imposer des frais (et, dans le cas d'une demande de copies par courrier de données à caractère personnel, des frais postaux), le montant doit en être déterminé «conformément aux dépenses réellement nécessaires au traitement de [la demande]»; aucuns frais (ni aucuns frais postaux) ne peuvent être imposés lorsque le responsable du traitement est à l'origine de la demande (article 38, paragraphe 3, de la PIPA, en liaison avec l'article 47 du décret d'application de la PIPA).

(81) La PIPA et son décret d'application ne comportent pas de dispositions générales traitant de la question des décisions relatives à la personne concernée et reposant uniquement sur le traitement automatisé de données à caractère personnel. Cependant, pour ce qui est des données à caractère personnel qui ont été collectées dans l'Union, toute décision fondée sur un traitement automatisé sera généralement prise par le responsable du traitement de l'Union (qui est en relation directe avec la personne concernée) et relève par conséquent du règlement (UE) 2016/679 ([111]). Cela inclut les cas de transfert dans lesquels le traitement est effectué par un opérateur économique étranger (coréen, par exemple) en tant qu'agent (sous-traitant) agissant au nom du responsable du traitement de l'Union (ou en tant que sous-traitant agissant au nom du sous-traitant de l'Union ayant obtenu les données auprès d'un responsable du traitement de l'Union qui les a collectées) qui prend ensuite la décision sur cette base. Il est donc peu probable que l'absence de règles spécifiques applicables à la prise de décisions automatisée dans la PIPA porte préjudice au niveau de protection des données à caractère personnel transférées sur la base de la présente décision.

(82) À titre exceptionnel, les dispositions relatives à la transparence concernant les demandes (article 20) et les droits individuels (articles 35 à 37), ainsi que l'obligation de notification individuelle pour les fournisseurs de services d'information et de communication (article 39-8 de la PIPA), ne s'appliquent pas aux informations pseudonymisées lorsqu'elles sont traitées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt général (article 28-7 de la PIPA) ([112]). Conformément à l'approche de l'article 11, paragraphe 2 (en liaison avec le considérant 57) du règlement (UE) 2016/679, cela se justifie par le fait que, pour garantir la transparence ou accorder des droits individuels, le responsable du traitement devrait déterminer si des données (et, le cas échéant, lesquelles) sont liées à la personne à l'origine de la demande, ce qui est expressément interdit en vertu de la PIPA (article 28-5, paragraphe 1, de la PIPA). En outre, lorsque cette réidentification implique de renoncer à la pseudonymisation pour la totalité de l'ensemble de données (pseudonymisées), elle exposerait les informations à caractère personnel de toutes les autres personnes concernées à des risques accrus. Tandis que le règlement (UE) 2016/679 fait référence à des situations dans lesquelles la réidentification est pratiquement impossible, la PIPA adopte une approche plus stricte en interdisant expressément la réidentification dans tous les cas où des informations pseudonymisées sont traitées.

(83) Le système coréen, tel que décrit aux considérants 74 à 82, contient donc des règles relatives aux droits des personnes concernées qui assurent un niveau de protection substantiellement équivalent à celui prévu par le règlement (UE) 2016/679.

([109]) Voir article 30, paragraphe 1, point 5, de la PIPA concernant la politique de confidentialité, qui contient entre autres des informations sur les droits dont disposent les personnes et sur la manière dont elles peuvent les exercer.

([110]) Voir également article 39-7, paragraphe 2, de la PIPA en ce qui concerne les fournisseurs de services d'information et de communication.

([111]) Inversement, il peut exister exceptionnellement un lien direct entre l'opérateur économique coréen et la personne concernée dans l'UE, ce qui découle généralement du fait que cet opérateur cible cette personne dans l'UE en lui offrant des biens ou des services ou en suivant son comportement. Dans un tel scénario, l'opérateur économique coréen lui-même relèvera du règlement (UE) 2016/679 (article 3, paragraphe 2); il doit donc se conformer directement au droit de l'UE en matière de protection des données.

([112]) Voir également notification 2021-5, qui confirme que la section 3 de la PIPA (y compris l'article 28-7) ne s'applique que lorsque les informations pseudonymisées sont traitées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt général, voir section 4 de l'annexe I de la présente décision.

2.3.9. *Transferts ultérieurs*

(84) Le niveau de protection conféré aux données à caractère personnel qui sont transférées depuis l'Union vers des responsables du traitement en République de Corée ne doit pas être compromis par le transfert ultérieur de ces mêmes données vers des destinataires se trouvant dans un pays tiers.

(85) De tels «transferts ultérieurs» constituent des transferts à partir de la République de Corée du point de vue du responsable du traitement. À cet égard, la PIPA opère une distinction entre le fait de sous-traiter le traitement à une partie sous-traitante (c'est-à-dire un sous-traitant) et la fourniture de données à caractère personnel à des tiers ([113]).

(86) Premièrement, lorsque le traitement des données à caractère personnel est sous-traité à une entité se situant dans un pays tiers, le responsable du traitement coréen doit veiller au respect des dispositions de la PIPA en matière de sous-traitance (article 26 de la PIPA). Cela comprend la mise en place d'un instrument juridiquement contraignant qui, entre autres, limite le traitement réalisé par la partie sous-traitante à la finalité des tâches sous-traitées, impose des garanties techniques et organisationnelles et limite la sous-traitance (voir article 26, paragraphe 1, de la PIPA), et la publication d'informations sur les tâches sous-traitées. De plus, le responsable du traitement est tenu d'«éduquer» la partie sous-traitante concernant les mesures de sécurité nécessaires et de surveiller, y compris au moyen de contrôles, le respect de toutes les obligations incombant au responsable du traitement au titre de la PIPA ([114]) ainsi que du contrat de sous-traitance.

(87) Tout préjudice causé par la partie sous-traitante en raison du non-respect de la PIPA dans le cadre du traitement des données à caractère personnel est imputable au responsable du traitement à des fins de responsabilité, tout comme si le préjudice était causé par un employé de ce dernier (article 26, paragraphe 6, de la PIPA). Le responsable du traitement coréen reste donc responsable des données à caractère personnel sous-traitées et doit garantir que le sous-traitant se trouvant à l'étranger traite les informations conformément à la PIPA. Si la partie sous-traitante traite les informations en violation de la PIPA, le responsable du traitement coréen peut être tenu pour responsable du non-respect de son obligation d'assurer la conformité avec la PIPA, notamment via le contrôle exercé sur la partie sous-traitante. Les garanties incluses dans le contrat de sous-traitance et la responsabilité du responsable du traitement coréen pour les actions de sa partie sous-traitante assurent la continuité de la protection lorsque le traitement de données à caractère personnel est sous-traité à une entité se trouvant en dehors de la Corée.

(88) Deuxièmement, les responsables du traitement coréens peuvent fournir les données à caractère personnel à un tiers situé en dehors de la Corée. Bien que la PIPA comprenne un certain nombre de fondements juridiques permettant la fourniture à des tiers de manière générale, si le tiers en question se trouve en dehors de la Corée, le responsable du traitement doit en principe ([115]) obtenir le consentement ([116]) de la personne concernée après lui avoir fourni des informations concernant 1) le type de données à caractère personnel; 2) le destinataire des données à caractère personnel; 3) la finalité du transfert au regard de la finalité du traitement recherchée par le destinataire; 4) la durée de conservation aux fins du traitement par le destinataire; et 5) le fait que la personne concernée peut refuser de donner son consentement (article 17, paragraphes 2 et 3, de la PIPA). Dans sa section sur la transparence (voir considérant 70), la notification 2021-5 exige que les personnes soient informées du pays tiers vers lequel leurs données seront transférées. Cela permet de garantir que les personnes concernées dans l'Union peuvent prendre une décision éclairée s'agissant de consentir ou non à la fourniture à l'étranger de leurs données. De plus, le responsable du traitement ne doit pas conclure de contrat qui enfreindrait la PIPA avec un tiers destinataire, ce qui signifie que le contrat ne doit pas contenir d'obligations contraires aux exigences incombant au responsable du traitement en vertu de la PIPA ([117]).

([113]) Des règles spécifiques s'appliquent aux fournisseurs de services d'information et de communication. Conformément à l'article 39-12 de la PIPA, les fournisseurs de services d'information et de communication doivent en principe obtenir le consentement de l'utilisateur pour tout transfert d'informations à caractère personnel à l'étranger. Lorsque les informations à caractère personnel sont transférées dans le cadre de la sous-traitance d'opérations de traitement, y compris à des fins de conservation, le consentement n'est pas nécessaire si les personnes concernées ont été informées à l'avance, directement ou par un avis public facilement consultable, 1) des caractéristiques des informations transférées; 2) du pays vers lequel les informations seront transférées (ainsi que la date et la méthode du transfert); 3) du nom du destinataire; et 4) de la finalité de l'utilisation et de la conservation par le destinataire (article 39-12, paragraphe 3, de la PIPA). De plus, les exigences générales en matière de sous-traitance s'appliqueront dans ce cas. Pour chaque transfert, des garanties spécifiques doivent être mises en place en ce qui concerne la sécurité, le traitement des plaintes et des litiges, ainsi que d'autres mesures nécessaires à la protection des informations des utilisateurs (article 48-10 du décret d'application de la PIPA).

([114]) Voir également article 26, paragraphe 7, de la PIPA, selon lequel les articles 15 à 25, 27 à 31, 33 à 38 et 50 s'appliquent mutatis mutandis au sous-traitant.

([115]) Si des fournisseurs de services d'information et de communication fournissent à des tiers les informations à caractère personnel de leurs utilisateurs, le consentement de l'utilisateur final est toujours nécessaire (article 39-12, paragraphe 2, de la PIPA).

([116]) Comme expliqué plus en détail dans la note de bas de page 51, pour que ce consentement soit valable, il doit être donné librement, éclairé et spécifique.

([117]) Voir également article 39-12, paragraphe 1, de la PIPA en ce qui concerne les fournisseurs de services d'information et de communication.

(89) En l'absence de consentement de la personne, les données à caractère personnel peuvent être fournies à un tiers (à l'étranger) lorsque l'objectif de la divulgation reste «dans un cadre raisonnablement lié» à la finalité initiale de la collecte (article 17, paragraphe 4, de la PIPA, voir considérant 36). Cependant, lorsqu'il décide de divulguer (ou non) des données à caractère personnel pour une finalité «liée», le responsable du traitement doit se demander si la divulgation entraînerait des inconvénients pour la personne et si les mesures de sécurité nécessaires (comme le chiffrement) ont été prises. Puisqu'il est possible que le pays tiers vers lequel des données à caractère personnel sont transférées ne prévoie pas de protections semblables à celles contenues dans la PIPA, la section 2 de la notification 2021-5 reconnaît que de tels inconvénients peuvent survenir et ne peuvent être évités que si le responsable du traitement coréen et le destinataire se trouvant à l'étranger assurent, au moyen d'un instrument juridiquement contraignant (comme un contrat), un niveau de protection équivalent à celui prévu par la PIPA, y compris en ce qui concerne les droits des personnes concernées.

(90) Des règles spécifiques s'appliquent à la divulgation «ne relevant pas de la finalité», c'est-à-dire à la fourniture de données à un tiers pour une nouvelle finalité (non liée), qui ne peut avoir lieu que pour l'un des motifs indiqués à l'article 18, paragraphe 2, de la PIPA, comme le décrit le considérant 39. Cependant, même dans de telles conditions, toute fourniture à des tiers est exclue si elle est susceptible de «porter atteinte de manière déloyale» aux intérêts de la personne concernée ou d'un tiers, ce qui nécessite une mise en balance des intérêts. De plus, conformément à l'article 18, paragraphe 5, de la PIPA, le responsable du traitement doit appliquer des garanties supplémentaires, qui peuvent notamment consister à demander au tiers de limiter la finalité et la méthode du traitement ou de mettre en place des mesures de sécurité spécifiques. Une fois encore, puisqu'il est possible que le pays tiers vers lequel des données à caractère personnel sont transférées ne prévoie pas de protections semblables à celles contenues dans la PIPA, la section 2 de la notification 2021-5 reconnaît qu'une telle «atteinte déloyale» aux intérêts de la personne ou d'un tiers peut survenir et ne peut être évitée que si le responsable du traitement coréen et le destinataire se trouvant à l'étranger assurent, au moyen d'un instrument juridiquement contraignant (comme un contrat), un niveau de protection équivalent à celui prévu par la PIPA, y compris en ce qui concerne les droits des personnes concernées.

(91) Les règles mentionnées aux considérants 86 à 90 assurent donc la continuité de la protection lorsque les données à caractère personnel font l'objet d'un transfert ultérieur (à une «partie sous-traitante» ou à un tiers) depuis la République de Corée d'une manière substantiellement équivalente à celle prévue par le règlement (UE) 2016/679.

2.3.10. *Responsabilité*

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

(93) Selon l'article 3, paragraphes 6 et 8, de la PIPA, le responsable du traitement doit traiter les données à caractère personnel «de manière à réduire au minimum la possibilité d'atteinte» à la vie privée de la personne concernée et s'efforce d'obtenir la confiance de la personne concernée en respectant et en exécutant les obligations et les responsabilités telles que prévues par la PIPA et d'autres lois connexes. Cela comprend la création d'un plan de gestion interne (article 29 de la PIPA), ainsi qu'une formation et une supervision appropriées des employés (article 28 de la PIPA).

(94) Afin d'assurer la responsabilité, l'article 31 de la PIPA, en liaison avec l'article 32 du décret d'application de la PIPA, oblige les responsables du traitement à désigner un responsable de la confidentialité qui «prend en charge de manière exhaustive le traitement des informations à caractère personnel». Plus particulièrement, ce responsable de la confidentialité est chargé des missions suivantes: 1) la création et la mise en œuvre d'un plan de protection des données à caractère personnel et la rédaction de la politique de confidentialité; 2) la réalisation d'études régulières sur le statut du traitement des données à caractère personnel et sur les bonnes pratiques en la matière, afin de remédier aux éventuelles lacunes; 3) la gestion des plaintes et des indemnités octroyées à titre de réparation; 4) la création d'un système interne de contrôle afin d'empêcher la divulgation ou l'utilisation abusive ou détournée de données à caractère personnel; 5) la préparation et la mise en œuvre d'un programme de formation; 6) la protection, le contrôle et la gestion des fichiers de données à caractère personnel; et 7) la destruction des données à caractère personnel une fois que la finalité du traitement est réalisée ou que la durée de conservation est arrivée à son terme. Lorsqu'il exécute ces missions, le responsable de la confidentialité peut contrôler le statut du traitement des données à caractère personnel et des systèmes y afférents et réclamer des informations à cet égard (article 31, paragraphe 3, de la PIPA). Si le responsable de la confidentialité prend connaissance de toute infraction à la PIPA ou à toute autre loi pertinente en matière de protection des données, il doit immédiatement prendre des mesures correctrices et les notifier à la direction du responsable du traitement, si nécessaire (article 31, paragraphe 4, de la PIPA). Selon l'article 31, paragraphe 5, de la PIPA, le responsable de la confidentialité ne doit pas subir des inconvénients injustifiés du fait de l'exercice de ces missions.

(95) De plus, les responsables du traitement doivent s'efforcer de manière proactive de réaliser une analyse d'impact relative à la confidentialité lorsque l'exploitation de fichiers de données à caractère personnel comprend un risque en matière de confidentialité (article 33, paragraphe 8, de la PIPA). Sur la base de l'article 33, paragraphes 1 et 2, de la PIPA, en liaison avec les articles 35, 36 et 38 du décret d'application de la PIPA, des facteurs tels que le type et la nature des données traitées (notamment s'il s'agit d'informations sensibles), leur volume, la durée de conservation et la probabilité que des violations de données se produisent sont pertinents afin d'apprécier le degré de risque pour les droits des personnes concernées. L'objectif de l'analyse d'impact relative à la confidentialité est de garantir que les facteurs de risque en matière de confidentialité, ainsi que les contre-mesures de sécurité ou autres, sont analysés et de signaler les aspects qui nécessitent une amélioration (voir article 33, paragraphe 1, de la PIPA, en liaison avec l'article 38 du décret d'application de la PIPA).

(96) Les institutions publiques sont tenues de réaliser une analyse d'impact lorsqu'elles traitent certains fichiers de données à caractère personnel qui présentent un risque plus élevé de violation de la confidentialité (article 33, paragraphe 1, de la PIPA). Conformément à l'article 35 du décret d'application de la PIPA, c'est notamment le cas des fichiers contenant des informations sensibles sur au moins 50 000 personnes concernées, des fichiers qui seront combinés à d'autres fichiers et qui contiendront en conséquence de cela des informations sur au moins 500 000 personnes concernées ou des fichiers contenant des informations sur au moins un million de personnes concernées. Une institution qui réalise une analyse d'impact doit en communiquer les résultats à la PIPC (article 33, paragraphe 1, de la PIPA), qui peut rendre un avis sur la question (article 33, paragraphe 3, de la PIPA).

(97) Enfin, l'article 13 de la PIPA prévoit que la PIPC élabore les politiques nécessaires afin de promouvoir et de soutenir des «activités de protection des données autorégulées» réalisées par les responsables du traitement, notamment par la formation à la protection des données, par la promotion et l'appui d'organisations actives dans le domaine de la protection des données et par l'aide apportée aux responsables du traitement s'agissant de créer et de mettre en place des règles autorégulées. De plus, elle présente le système de symbole ePRIVACY et en facilite l'application. À cet égard, l'article 32, paragraphe 2, de la PIPA, en liaison avec les articles 34-2 à 34-8 du décret d'application de la PIPA, prévoit la possibilité de certifier que le traitement des données à caractère personnel et le système de protection d'un responsable du traitement sont conformes aux exigences de la PIPA. Selon ces règles, il est possible d'accorder une certification ([118]) (pour une durée de trois ans) au responsable du traitement qui remplit les critères de certification définis par la PIPC, notamment la mise en place de mesures organisationnelles, techniques et physiques pour protéger les données à caractère personnel ([119]). La PIPC doit examiner les systèmes du responsable du traitement pertinents pour la certification au moins une fois par an afin d'en assurer l'efficacité, ce qui peut conduire à la révocation de la certification (article 32, paragraphe 4, de la PIPA, en liaison avec l'article 34-5 du décret d'application de la PIPA, la «gestion de suivi»).

(98) Le cadre coréen met donc en place le principe de responsabilité d'une manière qui garantit un niveau de protection substantiellement équivalent à celui prévu par le règlement (UE) 2016/679, y compris en prévoyant différents mécanismes permettant de vérifier et de démontrer la conformité avec la PIPA.

2.3.11. *Règles spéciales pour le traitement des informations à caractère personnel en matière de crédit*

(99) Comme décrit au considérant 13, la CIA prévoit des règles spécifiques pour le traitement des informations à caractère personnel en matière de crédit par les opérateurs économiques. Lorsqu'ils traitent des informations à caractère personnel en matière de crédit, les opérateurs économiques doivent donc respecter les dispositions générales de la PIPA, sauf si la CIA prévoit des règles plus spécifiques. C'est par exemple le cas lorsqu'ils traitent des informations relatives à une carte de crédit ou à un compte bancaire dans le cadre d'une opération commerciale avec une personne. En tant que législation sectorielle pour le traitement d'informations (à caractère personnel et non personnel) en matière de crédit, la CIA impose non seulement des garanties spécifiques en matière de protection des données (par exemple en ce qui concerne la transparence ou la sécurité), mais elle régit également de manière plus générale les circonstances particulières dans lesquelles il est possible de traiter des informations à caractère personnel en matière de crédit. Cela se traduit notamment dans les exigences détaillées concernant l'utilisation, la fourniture à un tiers ou la conservation de telles données.

(100) Tout comme la PIPA, la CIA consacre les principes de licéité et de proportionnalité. Premièrement, à titre d'exigence générale, l'article 15, paragraphe 1, de la CIA n'autorise à collecter des informations à caractère personnel en matière de crédit que par des moyens raisonnables et loyaux et que dans la moindre mesure nécessaire pour réaliser une finalité spécifique, conformément à l'article 3, paragraphes 1 et 2, de la PIPA. Deuxièmement, la CIA régit spécifiquement la licéité du traitement des informations à caractère personnel en matière de crédit en restreignant leur collecte, leur utilisation et leur fourniture à un tiers et, de manière générale, en soumettant ces activités de traitement à l'obligation de disposer du consentement de la personne concernée.

([118]) De plus, si le responsable du traitement souhaite mentionner la certification dans le cadre de ses activités ou s'en prévaloir, il peut utiliser le symbole de la protection des informations à caractère personnel créé par la PIPC. Voir article 34-7, du décret d'application de la PIPA.

([119]) Depuis novembre 2018, un «système de gestion des informations à caractère personnel et de la sécurité des informations» (ISMS-P) a été mis au point et certifie que les responsables du traitement disposent d'un système de gestion complet.

(101) Les informations à caractère personnel en matière de crédit peuvent être collectées sur la base de l'un des fondements prévus par la PIPA, ou de l'un des fondements spécifiques prévus par la CIA. Puisque l'article 45 du règlement (UE) 2016/679 présuppose un transfert de données à caractère personnel par un responsable du traitement ou un sous-traitant se trouvant dans l'Union, mais ne couvre pas la collecte directe (auprès de la personne ou d'un site internet par exemple) par un responsable du traitement en Corée, seuls le consentement et les fondements prévus par la PIPA sont pertinents pour la présente décision. Ces fondements incluent notamment des scénarios dans lesquels le transfert est nécessaire à l'exécution d'un contrat conclu avec la personne ou conforme aux intérêts légitimes du responsable du traitement coréen (article 15, paragraphe 1, points 4 et 6, de la PIPA) ([120]).

(102) Une fois collectées, les informations à caractère personnel en matière de crédit peuvent être utilisées 1) pour la finalité initiale pour laquelle elles ont été (directement) fournies par la personne concernée ([121]); 2) pour une finalité compatible avec la finalité initiale de la collecte ([122]); 3) pour décider d'établir ou de conserver une relation commerciale demandée par la personne concernée ([123]); 4) à des fins statistiques, de recherche et d'archivage dans l'intérêt général ([124]) si les informations ont été pseudonymisées ([125]); 5) si un consentement supplémentaire a été obtenu; ou 6) conformément à la législation.

(103) Si un opérateur économique souhaite divulguer des informations à caractère personnel en matière de crédit à un tiers, il doit obtenir le consentement de la personne concernée ([126]), après l'avoir informée du destinataire des données, de la finalité du traitement par le destinataire, des détails concernant les données qui seront transférées, de la durée de conservation par le destinataire et de son droit à ne pas consentir à ce transfert (article 32, paragraphe 1, de la CIA et article 28, paragraphe 2, du décret d'application de la CIA) ([127]). Cette obligation de consentement ne s'applique pas dans certaines situations spécifiques, notamment lorsque les informations à caractère personnel en matière de crédit sont divulguées ([128]): 1) à une partie sous-traitante à des fins de sous-traitance ([129]); à un tiers en cas de transfert, de division ou de fusion d'une entreprise; 3) à des fins statistiques, de recherche et d'archivage dans l'intérêt général, lorsque les informations ont été pseudonymisées; 4) pour une finalité compatible avec la finalité initiale de la collecte; 5) à un tiers qui utilise les informations afin de recouvrer une dette due par la personne ([130]); 6) afin d'exécuter une ordonnance judiciaire; 7) à un procureur ou un agent de

([120]) La CIA prévoit également d'autres fondements juridiques pour la collecte, notamment lorsque la loi l'exige, lorsque les informations sont publiées par une institution publique en vertu de la législation relative à la liberté d'information ou lorsque les informations sont mises à disposition sur un réseau social. Pour que l'opérateur économique puisse se prévaloir de ce dernier fondement, il doit être en mesure de démontrer que la collecte relève du consentement de la personne concernée, en se fondant sur une interprétation raisonnable («objective») et en tenant compte de la nature des données, de l'intention et de la motivation sous-tendant leur publication sur le réseau social, de la «forte pertinence» de la collecte eu égard à la finalité, etc. (article 13 du décret d'application de la CIA). Cependant, comme expliqué au considérant 101, ces fondements ne sont en principe pas pertinents dans le cadre d'un transfert.

([121]) Par exemple, lorsque des informations en matière de crédit sont générées/fournies dans le cadre d'une opération commerciale avec la personne. Cependant, il n'est pas possible d'invoquer ce fondement pour utiliser des informations à caractère personnel en matière de crédit à des fins de marketing direct (voir article 33, paragraphe 1, point 3, de la CIA).

([122]) Pour déterminer si la finalité de l'utilisation est compatible avec la finalité initiale de la collecte, il convient de tenir compte des facteurs suivants: 1) la relation («pertinence») entre les deux finalités; 2) la manière dont les informations ont été collectées; 3) l'incidence de l'utilisation sur la personne et 4) si des mesures de sécurité appropriées, telles que la pseudonymisation, ont été mises en œuvre (voir article 32, paragraphe 6, point 9-4, de la CIA).

([123]) Par exemple, un responsable du traitement peut se voir obligé de prendre en considération des informations à caractère personnel en matière de crédit qu'il a reçues d'une personne afin de décider de prolonger l'échéance d'un prêt accordé à celle-ci.

([124]) Article 33 de la CIA, en liaison avec l'article 32, paragraphe 6, points 9-2, 9-4 et 10, de la CIA.

([125]) L'article 2, paragraphe 15, de la CIA définit la pseudonymisation comme le traitement d'informations à caractère personnel en matière de crédit de manière à ce qu'il ne soit plus possible d'identifier les personnes à partir des informations, à moins de les combiner à d'autres informations. Bien que la CIA contienne des garanties spécifiques pour le traitement des informations pseudonymisées à des fins statistiques, de recherche et d'archivage dans l'intérêt général (article 40-2 de la CIA), ces règles ne s'appliquent pas aux organisations commerciales. Celles-ci sont plutôt soumises aux exigences spécifiques de la section III de la PIPA, comme expliqué aux considérants 42 à 48. L'article 40-3 de la CIA exonère en outre le traitement des informations à caractère personnel en matière de crédit, lorsqu'il est réalisé à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt général, des exigences en matière de transparence et de droits individuels, à l'instar de l'exception prévue par l'article 28-7 de la PIPA et sous réserve des garanties prévues par la section III de la PIPA, comme décrit plus en détail aux considérants 42 à 48.

([126]) Cela ne s'applique pas lorsque les informations sont fournies à un tiers afin d'assurer que les informations à caractère personnel en matière de crédit restent exactes et mises à jour tant que cette fourniture relève de la finalité initiale du traitement (article 32, paragraphe 1, de la CIA). C'est par exemple le cas lorsque des informations mises à jour sont fournies à une agence de notation du crédit afin de vérifier que les registres sont exacts.

([127]) S'il est compliqué de fournir les informations susmentionnées, il peut être suffisant de renvoyer la personne vers le tiers destinataire qui fournira les informations nécessaires.

([128]) Puisque la CIA ne régit pas spécifiquement la divulgation à l'étranger d'informations à caractère personnel en matière de crédit, de telles divulgations doivent respecter les garanties applicables aux transferts ultérieurs prévues par la section 2 de la notification 2021-5.

([129]) Il n'est possible de sous-traiter le traitement des informations à caractère personnel en matière de crédit que sur la base d'un contrat écrit et dans le respect des exigences de l'article 26, paragraphes 1 à 3 et 5, de la PIPA, telles que décrites au considérant 20 (article 17 de la CIA et article 14 du décret d'application de la CIA). La partie sous-traitante ne peut pas utiliser les informations en dehors de la portée des missions qui lui sont sous-traitées et l'entreprise donneuse d'ordre doit mettre en place des mesures de sécurité spécifiques (par exemple le chiffrement) et former la partie sous-traitante sur la manière d'éviter la perte, le vol, la divulgation, la modification ou la compromission des informations en matière de crédit.

([130]) Voir article 28, paragraphe 10, point 1, 2 et 6, du décret d'exécution de la CIA.

police judiciaire en cas d'urgence lorsque la vie de la personne est en danger ou que la personne est susceptible de subir un préjudice corporel et qu'il n'y a pas assez de temps pour délivrer un mandat judiciaire ([131]); 8) aux autorités fiscales compétentes afin de se conformer au droit fiscal; ou 9) conformément à tout autre acte législatif. En cas de divulgation sur la base de l'un de ces fondements, il convient d'en informer à l'avance la personne concernée (article 32, paragraphe 7, de la CIA).

(104) La CIA régit aussi spécifiquement la durée du traitement des informations à caractère personnel en matière de crédit sur la base de l'un de ces fondements en vue de leur utilisation ou de leur fourniture à un tiers une fois que la relation commerciale avec la personne est terminée ([132]). Seules les informations qui étaient nécessaires à l'établissement ou à la conservation de cette relation peuvent être conservées, sous réserve de l'application de garanties supplémentaires (elles doivent être conservées séparément des informations en matière de crédit portant sur des personnes avec lesquelles une relation commerciale est en cours, protégées par des mesures spécifiques de sécurité et seulement accessibles aux personnes autorisées) ([133]). Toutes les autres données doivent être supprimées (article 17-2, paragraphe 1, point 2, du décret d'application de la CIA). Afin de déterminer quelles données étaient nécessaires à la relation commerciale, il convient de tenir compte de différents facteurs, notamment s'il aurait été possible d'établir la relation sans ces données et si ces données portent directement sur les biens ou les services fournis à la personne (article 17-2, paragraphe 2, du décret d'application de la CIA).

(105) Même dans les cas où les informations à caractère personnel en matière de crédit peuvent en principe être conservées après la fin de la relation commerciale, elles doivent être supprimées dans un délai de trois mois après la réalisation de la finalité supplémentaire du traitement ([134]) ou, en tout état de cause, après cinq ans (article 20-2 de la CIA). Dans un nombre limité de circonstances, les informations personnelles sur le crédit peuvent être conservées pendant plus de cinq ans, en particulier lorsque cela est nécessaire pour se conformer à une obligation légale; lorsque cela est nécessaire pour les intérêts vitaux, l'intégrité corporelle ou les biens d'une personne; aux fins de l'archivage d'informations pseudonymisées (qui ont été utilisées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt général); ou à des fins d'assurance (notamment pour le paiement d'assurances ou pour prévenir la fraude à l'assurance) ([135]). Dans ces cas exceptionnels, des garanties spécifiques s'appliquent (comme la notification de l'utilisation ultérieure à la personne, la séparation des informations conservées et des informations portant sur des personnes avec qui une relation commerciale existe encore, la limitation des droits d'accès, voir article 17-2, paragraphes 1 et 2, du décret d'application de la CIA).

(106) La CIA donne également des précisions concernant les principes d'exactitude et de qualité des données en exigeant que les informations à caractère personnel en matière de crédit soient «enregistrées, modifiées et gérées» de manière à assurer qu'elles sont exactes et mises à jour (article 18, paragraphe 1, de la CIA et article 15, paragraphe 3, du décret d'application de la CIA) ([136]). Lorsqu'ils fournissent des informations en matière de crédit à certaines autres entités (comme des agences de notation du crédit), les opérateurs économiques sont également spécifiquement tenus de vérifier l'exactitude des informations afin de garantir que le destinataire enregistre et gère uniquement des informations exactes (article 15, paragraphe 1, du décret d'application de la CIA, en liaison avec l'article 18, paragraphe 1, de la CIA). Plus généralement, la CIA impose la tenue de registres concernant la collecte, l'utilisation, la divulgation à des tiers et la destruction d'informations à caractère personnel en matière de crédit (article 20, paragraphe 2, de la CIA) ([137]).

(107) De plus, le traitement d'informations à caractère personnel en matière de crédit est soumis à des exigences spécifiques en ce qui concerne la sécurité des données. Plus particulièrement, la CIA impose la mise en œuvre de mesures technologiques, physiques et organisationnelles afin de prévenir tout accès illicite aux systèmes informatiques, et d'empêcher que les données traitées soient exposées à la modification, à la destruction ou à tout autre risque (par exemple grâce à la mise en place de contrôles de l'accès, voir article 19 de la CIA et article 16 du décret d'application de la CIA). De plus, lorsque des informations à caractère personnel en matière de crédit sont partagées avec un tiers, il convient de conclure un accord prévoyant des mesures de sécurité spécifiques (article 19, paragraphe 2, de la CIA). En cas de violation des informations à caractère personnel en matière de crédit, il convient de prendre des mesures visant à réduire au minimum tout dommage et d'en informer sans retard les personnes concernées (article 39-4, paragraphes 1 et 2, de la CIA). De plus, la PIPC doit être informée de la notification adressée aux personnes concernées et des mesures mises en œuvre (article 39-4, paragraphe 4, de la CIA).

([131]) Dans ce cas, un mandat doit être demandé sans délai. Si le mandat n'est pas délivré dans les 36 heures, les données reçues doivent être supprimées sans délai (article 32, paragraphe 6, point 6, de la CIA).

([132]) Par exemple parce que les obligations contractuelles ont été exécutées, parce que l'une des parties a exercé son droit de résiliation, etc., voir article 17-2, paragraphe 5, du décret d'application de la CIA.

([133]) Article 20-2, paragraphe 1, de la CIA et article 17-2, paragraphe 1, point 1, du décret d'application de la CIA.

([134]) Cette période tient compte du fait que, bien souvent, la suppression n'est pas immédiatement possible, mais nécessite généralement plusieurs étapes (par exemple la séparation des données à supprimer des autres données et la réalisation de la suppression sans affecter la stabilité des systèmes d'information) dont la mise en œuvre nécessite un certain temps.

([135]) Article 20-2, paragraphe 2, de la CIA.

([136]) L'article 18, paragraphe 2, de la CIA et l'article 15, paragraphe 4, du décret d'application de la CIA définissent des règles plus spécifiques concernant cette obligation de tenue de registres, par exemple pour les registres portant sur des informations qui pourraient nuire à une personne, comme des informations en matière de délinquance ou de faillite.

([137]) En ce qui concerne d'autres mécanismes de responsabilité, la CIA impose à certaines organisations (par exemple les coopératives et les entreprises publiques, voir article 21, paragraphe 2, du décret d'application de la CIA) de nommer un «responsable/gestionnaire des informations en matière de crédit», qui est chargé de veiller au respect de la CIA et réalise les missions d'un «responsable de la confidentialité» au titre de la PIPA (article 20, paragraphes 3 et 4, de la CIA).

(108) La CIA impose également des obligations spécifiques en matière de sécurité au moment de l'obtention du consentement à l'utilisation ou à la fourniture d'informations à caractère personnel en matière de crédit (article 32, paragraphe 4, et article 34-2 de la CIA et article 30-3 du décret d'application de la CIA) et, plus généralement, avant la fourniture d'informations à un tiers (article 32, paragraphe 7, de la CIA) ([138]). De plus, les personnes ont le droit d'obtenir sur demande des informations concernant l'utilisation et la fourniture de leurs informations en matière de crédit à des tiers au cours des trois années précédant la demande (y compris concernant la finalité et les dates de telles utilisations/fournitures) ([139]).

(109) Au titre de la CIA, les personnes ont également le droit d'avoir accès à leurs informations à caractère personnel en matière de crédit (article 38, paragraphe 1, de la CIA) et d'obtenir la rectification des données inexactes (article 38, paragraphes 2 et 3, de la CIA) ([140]). De plus, outre le droit général à l'effacement prévu par la PIPA (voir considérant 77), la CIA prévoit un droit spécifique à l'effacement des informations à caractère personnel en matière de crédit qui ont été conservées plus longtemps que les durées de conservation mentionnées au considérant 104, c'est-à-dire cinq ans (pour les informations à caractère personnel en matière de crédit nécessaires à l'établissement ou au maintien d'une relation commerciale) ou trois mois (pour les autres types d'informations à caractère personnel en matière de crédit) ([141]). Il est possible, à titre exceptionnel, qu'une demande d'effacement soit rejetée lorsqu'une plus longue durée de conservation est nécessaire dans les cas décrits au considérant 105. Si une personne demande l'effacement de ses données, mais que l'une des exceptions s'applique, des garanties spécifiques doivent être appliquées aux informations à caractère personnel en matière de crédit concernées (article 38-3, paragraphe 3, de la CIA et article 33-3 du décret d'application de la CIA). Par exemple, ces informations doivent être conservées séparément des autres informations, elles doivent faire l'objet de mesures de sécurité spécifiques et seules les personnes autorisées peuvent y avoir accès.

(110) Outre les droits mentionnés au considérant 109, la CIA donne aux personnes le droit de demander à un responsable du traitement de cesser de les contacter à des fins de marketing direct (article 37, paragraphe 2, de la CIA) et le droit à la portabilité des données. En ce qui concerne ce droit à la portabilité, la CIA permet aux personnes de demander la transmission de leurs informations à caractère personnel en matière de crédit à elles-mêmes ou à certains tiers (par exemple des institutions financières ou des agences de notation du crédit). Les informations à caractère personnel en matière de crédit doivent être traitées et transmises au tiers dans un format permettant leur traitement par un appareil de traitement des données (comme un ordinateur).

(111) Dans la mesure où la CIA contient des règles spécifiques par rapport à la PIPA, la Commission estime donc que ces règles assurent également un niveau de protection substantiellement équivalent à celui prévu par le règlement (UE) 2016/679.

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

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

2.4.1. *Surveillance indépendante*

(113) En République de Corée, l'autorité indépendante chargée de surveiller l'application de la PIPA et de la faire respecter est la PIPC. La PIPC se compose d'un président, d'un vice-président et de sept commissaires. Le président et le vice-président sont nommés par le président de la République sur recommandation du Premier ministre. Parmi les commissaires, deux sont nommés par le président de la République sur recommandation du président de la PIPC et cinq sur recommandation de l'Assemblée nationale [dont deux sur recommandation du parti

([138]) Cela comprend une obligation générale de notification (article 32, paragraphe 7, de la CIA) et une obligation spécifique de transparence dans le cas où des informations permettant de déterminer la solvabilité d'une personne sont fournies à certaines entités, comme des agences de notation du crédit et des agences de collecte d'informations en matière de crédit (article 35-3 de la CIA et article 30-3 du décret d'application de la CIA) ou lorsqu'une relation commerciale est refusée ou résiliée sur la base d'informations à caractère personnel en matière de crédit reçues de la part d'un tiers (article 36 de la CIA et article 31 du décret d'application de la CIA).

([139]) Article 35 de la CIA. Certaines organisations commerciales, par exemple les coopératives et les entreprises publiques (article 21, paragraphe 2, du décret d'application de la CIA) sont soumises à des exigences supplémentaires en matière de transparence; elles doivent notamment s'assurer que les informations sont accessibles au public (article 31 de la CIA) et informer les personnes des éventuels inconvénients pour leur notation de crédit auxquels elles sont exposées lorsqu'elles réalisent des opérations financières comportant des risques de crédit (article 35-2 de la CIA).

([140]) En ce qui concerne les conditions et les exceptions relatives aux droits d'accès et de rectification, les règles de la PIPA (décrites aux considérants 76 et 77) s'appliquent. De plus, l'article 38, paragraphes 4 à 8, de la CIA et l'article 33 du décret d'application de la CIA définissent des modalités supplémentaires. Plus particulièrement, un opérateur économique qui a rectifié ou effacé des informations inexactes en matière de crédit doit le notifier à la personne. De plus, tout tiers auquel les informations ont été divulguées au cours des six mois précédents doit recevoir une notification et la personne concernée doit en être informée. Si une personne n'est pas satisfaite de la manière dont a été traitée sa demande de rectification, elle peut se plaindre auprès de la PIPC, qui contrôle les actions du responsable du traitement et peut imposer des mesures correctrices.

([141]) Article 38-3 de la CIA.

politique auquel appartient le président de la République et trois sur recommandation d'autres partis politiques (article 7-2, paragraphe 2, de la PIPA), ce qui contribue à contrebalancer la partialité dans le processus de nomination] ([142]). Cette procédure est conforme aux exigences applicables à la nomination des membres des autorités chargées de la protection des données dans l'Union [article 53, paragraphe 1, du règlement (UE) 2016/679]. De plus, tous les commissaires doivent s'abstenir de participer à des activités à but lucratif ou politiques et d'occuper des postes dans l'administration publique ou à l'Assemblée nationale (article 7-6 et article 7-7, paragraphe 1, point 3, de la PIPA) ([143]). Tous les commissaires sont soumis à des règles spécifiques leur interdisant de prendre part aux délibérations en cas de possible conflit d'intérêts (article 7-11 de la PIPA). La PIPC bénéficie de l'aide d'un secrétariat (article 7-13) et peut créer des sous-commissions (se composant de trois commissaires) qui géreront les infractions mineures et les problèmes récurrents (article 7-12 de la PIPA).

(114) Chaque membre de la PIPC est nommé pour un mandat de trois ans renouvelable une seule fois (article 7-4, paragraphe 1, de la PIPA). Les commissaires ne peuvent être révoqués que dans des circonstances particulières, notamment s'ils ne sont plus en mesure d'assurer leurs fonctions en raison d'une incapacité mentale ou physique durable, s'ils enfreignent la loi ou s'ils remplissent l'un des critères d'interdiction d'exercer leurs fonctions ([144]) (article 7-5 de la PIPA). Cela leur assure une protection institutionnelle dans l'exercice de leurs fonctions.

(115) De manière plus générale, l'article 7, paragraphe 1, de la PIPA garantit explicitement l'indépendance de la PIPC et l'article 7-5, paragraphe 2, de la PIPA impose aux commissaires d'exercer leurs fonctions de manière indépendante, dans le respect de la loi et de leur conscience ([145]). Les garanties institutionnelles et procédurales décrites ci-dessus, notamment en ce qui concerne la nomination et la révocation de ses membres, assurent que la PIPC agit en toute indépendance, sans influence ou instructions extérieures. En outre, en tant qu'agence administrative centrale, la PIPC propose chaque année son propre budget (qui est réexaminé par le ministère des finances dans le cadre du budget national global avant son adoption par l'Assemblée nationale) et est chargée de sa propre gestion du personnel. La PIPC est dotée d'un budget actuel d'environ 35 millions d'euros et compte 154 membres du personnel (dont 40 employés spécialisés dans les technologies de l'information et de la communication, 32 employés spécialisés dans les enquêtes et 40 experts juridiques).

(116) Les missions et pouvoirs de la PIPC sont principalement prévus aux articles 7-8, 7-9 et 61 à 66 de la PIPA ([146]). Plus particulièrement, la PIPC est notamment chargée de fournir des conseils sur les lois et règlements portant sur la protection des données, de mettre au point des politiques et orientations en matière de protection des données, d'enquêter sur les violations des droits des personnes, de gérer les plaintes et d'arbitrer les conflits, de veiller à la conformité avec la PIPA, d'assurer la formation et la promotion en matière de protection des données, et de communiquer et de coopérer avec les autorités de protection des données de pays tiers ([147]).

(117) Sur la base de l'article 68 de la PIPA, en liaison avec l'article 62 du décret d'application de la PIPA, certaines missions de la PIPC ont été déléguées à l'agence coréenne de l'internet et de la sécurité, à savoir: 1) la formation et les relations publiques; 2) la formation de spécialistes et la mise au point de critères pour les analyses d'impact relatives à la confidentialité; 3) le traitement des demandes de désignation d'une «institution réalisant des analyses d'impact relatives à la confidentialité»; 4) le traitement de demandes d'accès indirect aux données à caractère

([142]) Seules les personnes qui remplissent les critères suivants peuvent être nommées commissaires PIPC: les hauts fonctionnaires chargés de questions liées aux informations à caractère personnel; d'anciens juges, procureurs ou avocats ayant pratiqué pendant au moins 10 ans; d'anciens gestionnaires disposant d'une expérience en matière de protection des données et ayant travaillé dans une institution ou organisation publique pendant plus de trois ans, ou qui ont été recommandés par une telle institution ou organisation; et d'anciens professeurs associés disposant de connaissances professionnelles en matière de protection des données ayant travaillé pendant au moins cinq ans dans un établissement universitaire (article 7-2 de la PIPA).

([143]) Voir également article 4-2 du décret d'application de la PIPA.

([144]) Voir article 7-7 de la PIPA, qui dispose que les ressortissants étrangers et les membres de partis politiques ne peuvent pas devenir membres de la PIPC. Il en va de même pour les personnes contre qui ont été prononcées certaines sanctions pénales, qui ont été démises de leurs fonctions à la suite d'une procédure disciplinaire au cours des cinq dernières années, etc. (article 7-7 de la PIPA, en liaison avec l'article 33 de la loi sur la fonction publique).

([145]) Bien que l'article 7, paragraphe 2, de la PIPA fasse référence au pouvoir conféré au Premier ministre par l'article 18 de la loi sur l'organisation du gouvernement de suspendre ou de révoquer, avec l'approbation du président de la République, toute disposition illégale ou injuste d'une agence administrative centrale, aucun pouvoir similaire n'est accordé en ce qui concerne les pouvoirs d'enquête ou d'exécution de la PIPC (voir article 7, paragraphe 2, points 1 et 2, de la PIPA). Selon les explications fournies par le gouvernement coréen, l'article 18 de la loi sur l'organisation du gouvernement a pour objectif de donner au Premier ministre la possibilité d'agir dans des cas extraordinaires, par exemple afin d'arbitrer un désaccord entre différentes agences gouvernementales. Cependant, le Premier ministre n'a jamais fait usage de ce pouvoir depuis l'adoption de cette disposition en 1963.

([146]) Lorsque cela est nécessaire pour accomplir les tâches prévues à l'article 7-9, paragraphe 1, de la PIPA, la PIPC peut demander leur avis à des fonctionnaires compétents, des experts en matière de protection des données, des organisations de la société civile et des opérateurs économiques concernés. De plus, la PIPC peut demander des documents pertinents, émettre des recommandations d'amélioration et contrôler l'application de ces recommandations (article 7-9, paragraphes 2 à 5, de la PIPA).

([147]) Voir également article 9 de la PIPA (plan directeur triennal pour la protection des informations à caractère personnel), article 12 de la PIPA (orientations concernant les normes en matière de protection des informations à caractère personnel), et article 13 de la PIPA (politiques pour la promotion et le soutien de l'autorégulation).

personnel détenues par les autorités publiques (article 35, paragraphe 2, de la PIPA); et 5) la mission consistant à demander des documents et à réaliser des contrôles concernant les plaintes reçues via le «centre d'appel consacré à la protection de la vie privée». Dans le cadre de la gestion des plaintes via le centre d'appel consacré à la protection de la vie privée, l'agence coréenne de l'internet et de la sécurité transfère les affaires dans lesquelles elle estime que la loi a été violée à la PIPC ou au ministère public. La possibilité de soumettre une plainte au centre d'appel consacré à la protection de la vie privée n'empêche pas les personnes de présenter directement une plainte à la PIPC ou de s'adresser à celle-ci si elles estiment ne pas être satisfaites de la manière dont l'agence coréenne de l'internet et de la sécurité a traité leur plainte.

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

(118) Afin de garantir le respect de la PIPA, le législateur a accordé à la PIPC des pouvoirs d'enquête et d'exécution, allant de recommandations à des amendes administratives. Un régime de sanctions pénales vient compléter ces pouvoirs.

(119) En ce qui concerne les pouvoirs d'enquête, si l'existence d'une violation de la PIPA est présumée ou a été signalée, ou lorsque cela est nécessaire à la protection des droits des personnes concernées contre les infractions, la PIPC peut réaliser des contrôles sur place et demander tout élément pertinent (comme des articles ou des documents) aux responsables du traitement (article 63 de la PIPA, en liaison avec l'article 60 du décret d'application de la PIPA) ([148]).

(120) En ce qui concerne l'exécution, au titre de l'article 61, paragraphe 2, de la PIPA, la PIPC peut donner des conseils aux responsables du traitement concernant la manière dont ils peuvent améliorer le niveau de protection des données à caractère personnel dans le cadre d'activités de traitement spécifiques. Les responsables du traitement doivent s'efforcer de bonne foi d'appliquer ces conseils et sont tenus d'informer la PIPC de leurs résultats. De plus, lorsque des raisons suffisantes laissent à penser qu'une violation de la PIPA a été commise et que toute inaction est susceptible de causer des préjudices difficiles à réparer, la PIPC peut imposer des mesures correctrices (article 64, paragraphe 1, de la PIPA) ([149]). La section 5 de la notification 2021-5 (annexe I) précise, de manière contraignante, que ces conditions sont remplies en ce qui concerne la violation de toute disposition de la PIPA protégeant les droits des personnes en matière de confidentialité portant sur des informations à caractère personnel ([150]). La PIPC peut notamment prendre les mesures suivantes: ordonner la cessation du comportement causant la violation, la suspension temporaire du traitement des données ou toute autre mesure nécessaire. Le non-respect d'une mesure corrective peut entraîner une peine d'amende d'un montant maximal de 50 millions de wons (article 75, paragraphe 2, point 13, de la PIPA).

(121) En ce qui concerne certaines autorités publiques (telles que l'Assemblée nationale, les agences administratives centrales, les administrations locales et les juridictions), l'article 64, paragraphe 4, de la PIPA prévoit que la PIPC peut «recommander» l'une des mesures correctives mentionnées au considérant 120 et que ces autorités doivent se conformer à cette recommandation, sauf dans des circonstances extraordinaires. Conformément à la section 5 de la notification 2021-5, il s'agit de circonstances de fait ou de droit dont la PIPC n'avait pas connaissance au moment de formuler sa recommandation. L'autorité publique concernée ne peut invoquer de telles circonstances extraordinaires que si elle démontre clairement qu'aucune violation n'a eu lieu et la PIPC établit que ce n'est effectivement pas le cas. Sinon, l'autorité publique doit suivre la recommandation de la PIPC et «prendre une mesure corrective, y compris cesser immédiatement l'action en cause et réparer le préjudice subi dans le cas exceptionnel où un acte illicite aurait néanmoins été commis».

(122) La PIPC peut également demander à d'autres organismes administratifs dotés de compétences spécifiques en vertu de la législation sectorielle (par exemple, santé, éducation) de mener une enquête — seule ou conjointement avec la PIPC — sur les violations (présumées) de la vie privée commises par des responsables du traitement opérant dans ces secteurs relevant de leur compétence, et d'imposer des mesures correctives (article 63, paragraphes 4 et 5, de la PIPA). Dans ce cas, la PIPC détermine les motifs, l'objet et la portée de l'enquête ([151]). Ensuite, l'agence administrative concernée doit soumettre un plan d'inspection à la PIPC et communiquer à cette dernière le résultat de l'inspection. La PIPC peut recommander une mesure corrective spécifique à prendre, que l'agence compétente doit s'efforcer de mettre en œuvre. En tout état de cause, une telle demande ne limite pas le pouvoir de la PIPC de mener sa propre enquête ou d'imposer des sanctions.

([148]) La PIPC peut également pénétrer dans les locaux du responsable du traitement afin de contrôler l'état des activités, des registres, des documents, etc. de l'entreprise (article 63, paragraphe 2, de la PIPA). Voir également article 45-3 de la CIA et article 36-4 du décret d'application de la CIA en ce qui concerne les pouvoirs de la PIPC en vertu de cette loi.

([149]) Voir également article 45-4 de la CIA en ce qui concerne les pouvoirs de la PIPC en vertu de cette loi.

([150]) La section 5 de la notification précise qu'«un motif sérieux de considérer qu'il y a eu une violation d'informations à caractère personnel pour laquelle l'absence de mesures est susceptible d'entraîner un préjudice difficilement réparable au sens des paragraphes 1 et 2 de l'article 64 de la PIPA renvoie à une violation de l'un des principes, droits et devoirs contenus dans la loi qui visent à protéger les droits des personnes à des informations à caractère personnel». Il en va de même pour les pouvoirs de la PIPC en vertu de l'article 45-4 de la CIA.

([151]) Article 60 du décret d'application de la PIPA.

(123) Outre son pouvoir d'adopter des mesures correctives, la PIPC peut imposer des amendes administratives d'un montant de 10 à 50 millions de wons en cas d'infraction aux diverses exigences de la PIPA (article 75 de la PIPA) ([152]). Ces infractions incluent, entre autres, le non-respect des exigences relatives à la licéité du traitement, la non-adoption des mesures de sécurité nécessaires, l'absence de notification à la personne concernée en cas de violation de données à caractère personnel, le non-respect des exigences en matière de sous-traitance ultérieure, le non-établissement et la non-communication d'une politique de confidentialité, l'absence de désignation d'un responsable de la protection de la vie privée ou l'inaction à la suite d'une demande d'une personne concernée exerçant ses droits individuels, ainsi que certaines infractions procédurales (non-coopération au cours d'une enquête). En cas de violation de plusieurs dispositions de la PIPA par le même responsable du traitement, une amende peut être infligée pour chaque infraction et le nombre de personnes concernées sera pris en compte lors de la fixation du montant de l'amende.

(124) En outre, lorsqu'il existe des motifs raisonnables de soupçonner une violation de la PIPA ou de toute autre «loi relative à la protection des données», la PIPC peut introduire une plainte pénale auprès de l'autorité enquêtrice compétente (comme un procureur, voir article 65, paragraphe 1, de la PIPA). La PIPC peut également recommander au responsable du traitement de prendre des mesures disciplinaires à l'encontre de la personne responsable (y compris du gestionnaire, voir article 65, paragraphe 2, de la PIPA). Lorsqu'il reçoit une telle recommandation, le responsable du traitement doit s'y conformer ([153]) et informer par écrit la PIPC du résultat (article 65 de la PIPA, en liaison avec l'article 58 du décret d'application de la PIPA).

(125) S'agissant de la recommandation visée à l'article 61, des mesures correctives visées à l'article 64, de la saisine ou de la recommandation de mesures disciplinaires visées à l'article 65 et de l'imposition d'amendes administratives visée à l'article 75 de la PIPA, la PIPC peut rendre publics les faits — à savoir, l'infraction, l'entité ayant commis l'infraction et la ou les mesures imposées — en les publiant sur son site internet ou, généralement, dans un quotidien national (article 66 de la PIPA, en liaison avec l'article 61, paragraphe 1, du décret d'application de la PIPA) ([154]).

(126) Pour finir, le respect des exigences en matière de protection des données figurant dans la PIPA (ainsi que dans les autres «lois relatives à la protection des données») est renforcé par un régime de sanctions pénales. À cet égard, les articles 70 à 73 de la PIPA contiennent des dispositions en matière de sanctions qui peuvent donner lieu à l'imposition d'une amende (entre 20 et 100 millions de wons) ou d'une peine d'emprisonnement (dont la durée maximale se situe entre deux et 10 ans). Les infractions concernées comprennent, entre autres, l'utilisation de données à caractère personnel ou la transmission de telles données à un tiers sans le consentement nécessaire, le traitement d'informations sensibles contraire à l'interdiction visée à l'article 23, paragraphe 1, de la PIPA, le non-respect des exigences de sécurité applicables entraînant la perte, le vol, la divulgation, la falsification, l'altération ou la détérioration des données à caractère personnel, la non-adoption des mesures nécessaires en vue de rectifier ou d'effacer des données à caractère personnel ou de suspendre leur utilisation, ou le transfert illicite de données à caractère personnel vers un pays tiers ([155]). Conformément à l'article 74 de la PIPA, dans chacun de ces cas, la responsabilité de l'employé, de l'agent ou du représentant du responsable du traitement, y compris de ce dernier, est engagée ([156]).

(127) Outre les sanctions pénales prévues par la PIPA, l'utilisation détournée de données à caractère personnel peut également constituer une infraction en vertu du code pénal. C'est le cas en particulier en ce qui concerne la violation de la confidentialité de lettres, de documents ou de dossiers électroniques (article 316), la divulgation d'informations couvertes par le secret professionnel (article 317), la fraude informatique (article 347-2) ainsi que le détournement de fonds et l'abus de confiance (article 355).

(128) Le système coréen combine donc différents types de sanctions, allant des mesures correctives et des amendes administratives aux sanctions pénales, qui sont susceptibles d'avoir un effet dissuasif particulièrement fort pour les

([152]) De plus, lorsque des systèmes de traitement et de protection des informations à caractère personnel opérés par un responsable du traitement ont été certifiés conformément à la PIPA, mais que les critères de certification visés à l'article 34-2, paragraphe 1, du décret d'application de la PIPA n'ont en réalité pas été respectés, ou dans le cas d'une violation grave de toute «loi relative à la protection des informations [à caractère personnel]», la PIPC peut révoquer la certification (article 32-2, paragraphes 3 et 5, de la PIPA). La PIPC notifie cette révocation au responsable du traitement et l'annonce publiquement, ou la publie sur son site internet ou au Journal officiel (article 34-4 du décret d'application de la PIPA). Des amendes administratives (article 52 de la CIA) et des sanctions pénales (article 50 de la CIA) sont également prévues en cas de violation de la CIA.

([153]) Conformément à l'article 58, paragraphe 2, du décret d'application de la PIPA, si le respect de la recommandation est «impossible» en raison de circonstances particulières, le responsable du traitement doit fournir une justification motivée à la PIPC.

([154]) Lorsqu'elle prend la décision d'une telle divulgation au public, la PIPC tient compte des éléments de fond et de la gravité de la violation, de sa durée et de sa fréquence, ainsi que de ses conséquences (ampleur du préjudice). L'entité concernée est informée au préalable et a la possibilité de se défendre. Voir article 61, paragraphes 2 et 3, du décret d'application de la PIPA.

([155]) Voir l'article 71, point 2, en liaison avec l'article 18, paragraphe 1, de la PIPA (non-respect des conditions énoncées à l'article 17, paragraphe 3, de la PIPA auxquelles l'article 18, paragraphe 1, renvoie). Voir également l'article 75, paragraphe 2, point 1, en liaison avec l'article 17, paragraphe 2, de la PIPA (non-fourniture à la personne concernée des informations nécessaires visées à l'article 17, paragraphe 2, de la PIPA auxquelles l'article 17, paragraphe 3, renvoie).

([156]) En outre, l'article 74-2 de la PIPA autorise la confiscation des fonds, biens ou autres bénéfices acquis à la suite de la violation ou, si la confiscation n'est pas possible, la «perception» du bénéfice obtenu de manière illicite.

responsables du traitement et les personnes traitant les données. Immédiatement après son institution en 2020, la PIPC a commencé à faire usage de ses pouvoirs. Le rapport annuel 2021 de la PIPC montre que celle-ci a déjà émis un certain nombre de recommandations, d'amendes administratives et d'injonctions correctives, tant à l'encontre du secteur public (environ 34 autorités publiques) que d'opérateurs privés (environ 140 entreprises) ([157]). La PIPC a notamment infligé à une société une amende d'un montant de 6,7 milliards de wons en décembre 2020 pour violation de plusieurs dispositions de la PIPA (notamment des exigences en matière de sécurité, de consentement à la fourniture de données à un tiers et de transparence) ([158]). Elle a imposé également à une société spécialisée dans les technologies de l'IA une amende d'un montant de 103,3 millions de wons le 28 avril 2021 pour violation, entre autres dispositions, des règles relatives à la licéité du traitement, en particulier au consentement, et au traitement d'informations pseudonymisées ([159]). En août 2021, la PIPC a achevé une autre enquête sur les activités de trois entreprises, qui a donné lieu à des mesures correctives et à l'imposition d'amendes allant jusqu'à 6.47 milliards de wons (notamment pour n'avoir pas informé les particuliers de la divulgation de données à caractère personnel à des tiers, y compris des transferts vers des pays tiers) ([160]). De même, avant la réforme récente, la Corée du Sud était déjà très active en matière de répression, dans la mesure où les autorités responsables recouraient à l'éventail complet des mesures de répression, notamment aux amendes administratives, aux mesures correctives et à la «désignation et [au] partage» à l'égard de divers responsables du traitement, y compris des fournisseurs de services de communication (Commission coréenne des communications), ainsi que des opérateurs commerciaux, des institutions financières, des autorités publiques, des universités et des hôpitaux (ministère de l'intérieur et de la sécurité) ([161]). Sur cette base, la Commission conclut que le système coréen garantit en pratique l'application effective des règles en matière de protection des données, assurant ainsi un niveau de protection substantiellement équivalent à celui garanti par le règlement (UE) 2016/679.

2.5. **Recours**

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

(130) Le système coréen offre aux particuliers divers mécanismes leur permettant de faire valoir effectivement leurs droits et d'obtenir réparation (en justice).

(131) Dans un premier temps, les personnes qui considèrent que leurs droits ou intérêts en matière de protection des données ont été violés peuvent s'adresser au responsable du traitement concerné. Conformément à l'article 30, paragraphe 1, point 5, de la PIPA, la politique de confidentialité du responsable du traitement contient, entre autres, des informations concernant les droits des personnes concernées et leurs modalités d'exercice. En outre, elle fournit des coordonnées — telles que le nom et le numéro de téléphone du responsable de la protection de la vie privée ou du service chargé de la protection des données — afin de permettre le dépôt des plaintes («réclamations»). Au sein de l'organisation du responsable du traitement, le responsable de la protection de la vie privée est chargé de traiter les plaintes, d'adopter des mesures correctives en cas d'atteinte à la vie privée et de veiller à la réparation du préjudice subi (article 31, paragraphe 2, point 3, et article 31, paragraphe 4, de la PIPA). Ce dernier point est pertinent, par exemple, dans le cas d'une violation de données, car le responsable du traitement doit informer la personne concernée, entre autres, du ou des points de contact à qui signaler tout préjudice (article 34, paragraphe 1, point 5, de la PIPA).

(132) En outre, la PIPA offre aux particuliers plusieurs voies de recours contre les responsables du traitement. Premièrement, toute personne qui estime que ses droits ou intérêts en matière de protection des données ont été violés par le responsable du traitement peut signaler cette violation directement à la PIPC et/ou à l'une des institutions spécialisées désignées par le PIPC pour recevoir et traiter les plaintes; il s'agit notamment de l'Agence coréenne pour l'internet et la sécurité, qui gère à cette fin un centre d'appels d'informations à caractère personnel (le «centre d'appel concernant la protection de la vie privée») (article 62, paragraphes 1 et 2, de la PIPA, en liaison avec

([157]) Voir le rapport annuel de la PIPC 2021, pp. 50-55 (disponible uniquement en coréen), à l'adresse suivante: https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Voir affaire à l'adresse (disponible uniquement en coréen) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK

([159]) Voir affaire à l'adresse (disponible uniquement en coréen) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8

([160]) Voir affaire à l'adresse (disponible uniquement en coréen): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK

([161]) Voir, par exemple, rapport annuel 2020 à l'adresse (disponible uniquement en coréen) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 et exemples fournis en anglais à l'adresse https://www.privacy.go.kr/eng/enforcement_02.do

l'article 59 du décret d'application de la PIPA). Le centre d'appel concernant la protection de la vie privée enquête et constate les infractions, fournit des conseils en matière de traitement des données à caractère personnel (article 62, paragraphe 3, de la PIPA) et peut signaler des infractions à la PIPC (mais ne peut prendre lui-même de mesures d'exécution). Le centre d'appel concernant la protection de la vie privée reçoit un grand nombre de plaintes/demandes (par exemple, 177 457 en 2020, 159 255 en 2019 et 164 497 en 2018) ([162]). Selon les informations reçues de la PIPC elle-même, cette dernière a reçu un millier de plaintes entre août 2020 et août 2021. En réponse à une plainte, la PIPC peut adresser un avis d'amélioration, des mesures correctives, une «accusation» à l'organisme d'enquête compétent (y compris un procureur) ou des conseils en matière de sanctions disciplinaires (voir articles 61, 64 et 65 de la PIPA). Les décisions de la PIPC (telles que le refus de traiter une plainte ou le rejet d'une plainte sur le fond) peuvent être contestées en vertu de la loi sur le contentieux administratif ([163]).

(133) Deuxièmement, conformément aux articles 40 à 50 de la PIPA, en liaison avec les articles 48-14 à 57 du décret d'application de la PIPA, les personnes concernées peuvent introduire une réclamation auprès d'un «comité de médiation des litiges» composé de représentants nommés par le président de la PIPC parmi les hauts fonctionnaires (membres du service d'encadrement supérieur) de la PIPC et de personnes nommées sur la base de leur expérience dans le domaine de la protection des données parmi certains groupes éligibles (voir article 40, paragraphes 2, 3 et 7, de la PIPA et article 48-14 du décret d'application de la PIPA) ([164]). La possibilité de recourir à la médiation devant le comité de médiation des litiges offre une autre voie de recours, mais ne limite pas le droit de la personne de s'adresser à la PIPC ou aux tribunaux. Afin d'examiner l'affaire, le comité peut demander aux parties au litige de fournir les éléments nécessaires et/ou faire comparaître les témoins concernés devant lui (article 45 de la PIPA). Une fois l'affaire clarifiée, le comité prépare un projet de décision de médiation ([165]) qui doit être approuvé par une majorité de ses membres. Le projet de médiation peut inclure la suspension de la violation, les mesures correctives nécessaires (y compris une restitution ou une indemnisation) ainsi que toute mesure nécessaire pour éviter que de telles violations ne se reproduisent (article 47, paragraphe 1, de la PIPA). Lorsque les deux parties acceptent la décision de médiation, cette dernière produira les mêmes effets qu'une transaction judiciaire (article 47, paragraphe 5, de la PIPA). Chacune des parties est autorisée à intenter une action en justice pendant le processus de médiation, auquel cas cette dernière sera suspendue (voir article 48, paragraphe 2, de la PIPA) ([166]). Les chiffres annuels publiés par la PIPC montrent que les particuliers recourent régulièrement à la procédure devant le comité de médiation des litiges, ce qui aboutit souvent à un résultat positif. Par exemple, en 2020, le comité a traité 126 dossiers, dont 89 ont été résolus devant le comité (77 cas dans lesquels les parties étaient déjà parvenues à un accord avant la fin du processus de médiation et 12 cas dans lesquels les parties ont accepté la proposition de médiation), ce qui a conduit à un taux de médiation de 70,6 % ([167]). De même, en 2019, le comité a traité 139 dossiers, dont 92 ont été résolus, ce qui a conduit à un taux de médiation de 62,2 %.

(134) Par ailleurs, lorsqu'au moins 50 personnes ont subi un préjudice, ou si leurs droits en matière de protection des données ont été violés de la même manière ou de façon similaire à la suite du même incident (ou d'incidents du même type) ([168]), une personne concernée ou une organisation de protection des données peut introduire une demande de médiation collective pour le compte d'un tel collectif; les autres personnes concernées peuvent demander à rejoindre cette médiation, laquelle sera annoncée publiquement par le comité de médiation des litiges (article 49, paragraphes 1 à 3, de la PIPA, en liaison avec les articles 52 à 54 du décret d'application de la PIPA) ([169]). Le comité de médiation des litiges peut désigner en tant que partie représentante au moins une

([162]) Voir le rapport annuel de la PIPC du 2021, p. 174. En 2020, ces plaintes concernaient, par exemple, la collecte de données sans consentement, le non-respect des obligations de transparence, les violations de la PIPA par des sous-traitants, l'insuffisance des mesures de sécurité, l'absence de réponse aux demandes des personnes concernées, ainsi que des enquêtes générales.

([163]) En particulier, les personnes peuvent former un recours contre l'exercice de la puissance publique par une agence administrative ou le refus de celle-ci de l'exercer (article 2, paragraphe 1, point 1, et article 3, point 1, de la loi sur le contentieux administratif). De plus amples informations sur les aspects de cette procédure, notamment les critères de recevabilité, sont fournies au considérant 181.

([164]) Tous les membres exercent un mandat d'une durée fixe et ils ne peuvent être révoqués que pour une raison valable (voir article 40, paragraphe 5, et article 41 de la PIPA). De plus, l'article 42 de la PIPA prévoit des garanties afin d'éviter tout conflit d'intérêts.

([165]) Voir article 44 de la PIPA. Le comité peut en outre proposer un projet de transaction et recommander une transaction sans médiation (voir article 46 de la PIPA).

([166]) De plus, le comité peut refuser la médiation s'il la juge inadaptée à la résolution du litige au vu de sa nature, ou parce que la demande de médiation a été introduite à des fins déloyales (article 48 de la PIPA).

([167]) Voir le rapport annuel de la PIPC pour 2021, p. 179-180. Ces affaires concernaient, entre autres, des violations de l'obligation d'obtenir un consentement pour la collecte des données, du principe de limitation de la finalité et des droits des personnes concernées.

([168]) Voir l'article 49, paragraphe 1, de la PIPA, selon lequel les personnes concernées doivent subir un préjudice ou une violation de leurs droits «d'une manière identique ou similaire», et l'article 52, point 2, du décret d'exécution de la PIPA, qui exige que «[l]es questions importantes relatives à l'incident soient communes en fait ou en droit».

([169]) En outre, même des parties tierces peuvent bénéficier d'une décision de médiation collective acceptée par le responsable du traitement dans la mesure où le comité de médiation des litiges peut conseiller au responsable du traitement de préparer et de soumettre un plan d'indemnisation les concernant (également) (article 49, paragraphe 5, de la PIPA).

personne parmi celles qui représentent au mieux les intérêts collectifs (article 49, paragraphe 4, de la PIPA). Si le responsable du traitement refuse la médiation collective ou n'accepte pas la décision de médiation, certaines organisations ([170]) peuvent introduire un recours collectif afin de remédier à la violation (articles 51 à 57 de la PIPA).

(135) Troisièmement, dans le cas d'une atteinte à la vie privée entraînant un «préjudice» pour l'individu, la personne concernée a le droit à un recours approprié dans le cadre d'une «procédure rapide et équitable» (article 4, point 5, en liaison avec article 39 de la PIPA) ([171]). Le responsable du traitement peut se disculper en prouvant l'absence de faute («intention fautive» ou négligence). Lorsque la personne concernée subit un préjudice du fait de la perte, du vol, de la divulgation, de la falsification, de l'altération ou de la détérioration de ses données à caractère personnel, la juridiction peut fixer le montant de l'indemnisation jusqu'à trois fois celui du préjudice réel, en tenant compte d'un certain nombre de facteurs (article 39, paragraphes 3 et 4, de la PIPA). À titre subsidiaire, la personne concernée peut réclamer un «montant raisonnable» d'indemnisation inférieur ou égal à 3 millions de wons (article 39-2, paragraphes 1 et 2, de la PIPA). De plus, conformément au code civil, une indemnisation peut être réclamée à toute personne «qui a causé des pertes ou des préjudices à une autre personne en commettant un acte illicite, intentionnellement ou par négligence» ([172]) ou à une personne «qui a porté préjudice à la personne, qui a porté atteinte à la liberté ou à la réputation d'une autre personne, ou qui a infligé une souffrance morale à une autre personne» ([173]). Cette responsabilité délictuelle découlant de la violation des règles en matière de protection des données a été confirmée par la Cour suprême ([174]). Si un préjudice a été causé du fait d'un acte illicite commis par une autorité publique, une demande en réparation peut en outre être introduite en vertu de la loi sur l'indemnisation publique ([175]). Une demande au titre de la loi sur l'indemnisation publique peut être introduite auprès d'un «conseil de l'indemnisation» spécialisé ou directement auprès des juridictions coréennes ([176]). La responsabilité de l'État s'étend également aux préjudices non matériels (tels que la souffrance morale) ([177]). Si la victime est un ressortissant étranger, la loi sur l'indemnisation publique s'applique, pour autant que son pays d'origine garantisse de la même manière l'indemnisation publique des ressortissants coréens ([178]).

(136) Quatrièmement, la Cour suprême a reconnu que les particuliers ont le droit de réclamer une mesure injonctive en cas de violation de leurs droits découlant de la Constitution, y compris du droit à la protection des données à caractère personnel ([179]). Dans ce contexte, une juridiction peut, par exemple, ordonner à des responsables du traitement de suspendre ou de cesser toute activité illicite. En outre, les droits en matière de protection des données, notamment les droits protégés par la PIPA, peuvent être exercés au moyen d'actions civiles. Cette application horizontale de la protection constitutionnelle de la vie privée aux relations entre les parties privées a été reconnue par la Cour suprême ([180]).

([170]) À savoir, les groupes de consommateurs ou les ONG à but non lucratif possédant un certain nombre de membres dont l'objectif déclaré est la protection des données [bien que, dans ce dernier cas, la demande de recours collectif doive en outre avoir été introduite par au moins 100 personnes victimes de la même violation (ou de violations du même type)]. Voir article 51 de la PIPA.

([171]) Les articles 43 à 43-3 de la CIA prévoient également l'obligation d'indemniser les dommages résultant de violations de cette loi.

([172]) Article 750 du code civil.

([173]) Article 751, paragraphe 1, du code civil.

([174]) Voir, par exemple, arrêts 2015Da251539, 251546, 251553, 251560, 251577 de la Cour suprême du 30 mai 2018. La Cour suprême a par ailleurs confirmé que les violations de données peuvent ouvrir le droit au versement de dommages-intérêts en vertu du code civil, voir arrêt 2011Da59834, 59858, 59841 de la Cour suprême du 26 décembre 2012 (résumé en anglais disponible à l'adresse http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). Dans cette affaire, la Cour suprême a précisé que, aux fins d'apprécier si une personne a subi une souffrance morale qui peut être assimilée à un préjudice réparable, il convient de tenir compte de plusieurs facteurs, comme le type et les caractéristiques des informations divulguées, le caractère identifiable de la personne à la suite de la violation, la possibilité pour des tiers d'accéder aux données, la mesure dans laquelle les informations à caractère personnel ont été diffusées, le fait que la violation a entraîné ou non d'autres violations de droits individuels, la façon dont les informations à caractère personnel étaient gérées et protégées, etc.

([175]) Sur la base de la loi sur l'indemnisation publique, les particuliers peuvent demander à être indemnisés des préjudices causés par des agents publics dans l'exercice de leurs fonctions officielles en violation de la loi (article 2, paragraphe 1, de la loi sur l'indemnisation publique).

([176]) Articles 9 et 12 de la loi sur l'indemnisation publique. Cette loi institue des conseils de district (présidés par le procureur adjoint du parquet correspondant), un conseil central (présidé par le vice-ministre de la justice) et un conseil spécial (présidé par le vice-ministre de la défense nationale et chargé des demandes de réparation des préjudices causés par des militaires ou des employés civils de l'armée). Les demandes d'indemnisation sont en principe traitées par les conseils de district, qui, dans certaines circonstances, doivent transmettre l'affaire au conseil central/spécial, par exemple si l'indemnisation dépasse un certain montant ou si une personne demande une nouvelle délibération. Tous les conseils sont composés de membres nommés par le ministre de la justice (par exemple, parmi les fonctionnaires du ministère de la justice, des officiers ministériels, des avocats et des personnes possédant une expertise en matière d'indemnisation publique) et sont soumis à des règles spécifiques en matière de conflit d'intérêts (voir article 7 du décret d'application de la loi sur l'indemnisation publique).

([177]) Voir article 8 de la loi sur l'indemnisation publique (qui renvoie au code civil) et article 751 du code civil.

([178]) Article 7 de la loi sur l'indemnisation publique.

([179]) Arrêts de la Cour suprême 93Da40614 du 12 avril 1996 et 2008Da42430 du 2 septembre 2011 (résumé en anglais disponible à l'adresse https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Voir, par exemple, arrêt 2008Da42430 de la Cour suprême du 2 septembre 2011 (résumé en anglais disponible à l'adresse https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Enfin, les particuliers peuvent introduire une plainte pénale conformément au code de procédure pénale (article 223) auprès d'un procureur ou d'un officier de police judiciaire ([181]).

(138) Le système coréen offre donc diverses possibilités d'obtenir réparation, allant des options peu coûteuses et facilement accessibles [par exemple, en contactant le centre d'appel consacré à la protection de la vie privée ou par le biais de la médiation (collective)] aux voies de recours administratif (devant la PIPC) et judiciaire, y compris la possibilité d'obtenir une indemnisation.

3. ACCÈS ET UTILISATION PAR LES AUTORITÉS PUBLIQUES EN RÉPUBLIQUE DE CORÉE DE DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES À PARTIR DE L'UNION EUROPÉENNE

(139) La Commission a également évalué les limitations et les garanties prévues, y compris les mécanismes de surveillance et de recours individuel prévus par le droit coréen en ce qui concerne la collecte et l'utilisation ultérieure par les autorités publiques coréennes de données à caractère personnel transférées à des responsables du traitement en Corée pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale (ci-après l'«accès des pouvoirs publics»). À cet égard, le gouvernement coréen a fourni à la Commission des déclarations, des assurances et des engagements officiels souscrits au plus haut niveau ministériel et des services, qui figurent à l'annexe II de la présente décision.

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

(141) Premièrement, toute limitation du droit à la protection des données à caractère personnel doit être prévue par la loi et la base juridique qui permet l'ingérence dans ce droit doit définir elle-même la portée de la limitation de l'exercice du droit concerné ([182]).

(142) Deuxièmement, pour satisfaire à l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire dans une société démocratique pour répondre à des objectifs spécifiques d'intérêt général équivalents à ceux reconnus par l'Union, la réglementation du pays tiers en cause permettant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ([183]). Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise ([184]), ainsi que soumettre le respect de ces exigences à une surveillance indépendante ([185]).

(143) Troisièmement, la législation et ses exigences doivent être juridiquement contraignantes en vertu du droit national. Cela concerne en premier lieu toutes les autorités du pays tiers en question, mais ces exigences légales doivent également être opposables à ces autorités devant les tribunaux ([186]). En particulier, les personnes concernées doivent disposer de la possibilité d'exercer des voies de droit devant un tribunal indépendant et impartial afin d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données ([187]).

3.1. **Cadre juridique général**

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

([181]) Comme expliqué au considérant 127, l'utilisation détournée de données peut constituer une infraction pénale en vertu du code pénal.

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

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

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

([185]) Voir arrêt Schrems II, point 179.

([186]) Voir arrêt Schrems II, points 181 et 182.

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

(145) Premièrement, l'accès des autorités publiques coréennes aux données à caractère personnel est régi par les principes généraux de légalité, de nécessité et de proportionnalité issus de la Constitution coréenne ([188]). En particulier, les libertés et les droits fondamentaux (notamment le droit au respect de la vie privée et le droit au secret de la correspondance) ([189]) ne peuvent être limités que conformément au droit et lorsque cela est nécessaire pour la sécurité nationale ou le maintien de l'ordre aux fins du bien-être public. De telles limitations ne sauraient porter atteinte à l'essence du droit ou de la liberté en jeu. En particulier, en ce qui concerne les perquisitions et les saisies, la Constitution prévoit qu'elles ne peuvent avoir lieu que dans les conditions prévues par le droit, sur la base d'un mandat délivré par un juge et dans le respect d'une procédure régulière ([190]). Enfin, les particuliers peuvent faire valoir leurs droits et leurs libertés devant la Cour constitutionnelle s'ils estiment qu'ils ont été violés par des autorités publiques dans l'exercice de leurs pouvoirs ([191]). De la même manière, les personnes qui ont subi un préjudice du fait d'un acte illicite commis par un agent public dans l'exercice de ses fonctions officielles ont le droit de réclamer une juste réparation ([192]).

(146) Deuxièmement, comme décrit plus en détail dans les sections 3.2.1 et 3.3.1, les principes généraux mentionnés au considérant 145 sont également consacrés dans les lois spécifiques qui régissent les pouvoirs des autorités répressives et des autorités nationales de sécurité. Par exemple, s'agissant des enquêtes pénales, le code de procédure pénale (ci-après le «CPP») dispose que des mesures de contrainte ne peuvent être prises que dans les cas expressément prévus dans le CPP et dans la stricte mesure du nécessaire pour parvenir à l'objectif de l'enquête ([193]). De même, l'article 3 de la loi sur la protection de la confidentialité des communications (ci-après la «CPPA») interdit l'accès aux communications privées, sauf sur la base du droit et sous réserve des limitations et des garanties prévues par le droit. Dans le domaine de la sécurité nationale, la loi sur le Service national de renseignement (ci-après la «loi sur le NIS») dispose que tout accès à des communications ou à des informations de localisation doit être conforme au droit et punit de sanctions pénales les abus de pouvoir et les violations de la loi ([194]).

(147) Troisièmement, le traitement des données à caractère personnel par les autorités publiques, y compris à des fins répressives et à des fins de sécurité nationale, est soumis aux règles en matière de protection des données fixées par la PIPA ([195]). En règle générale, l'article 5, paragraphe 1, de la PIPA impose aux autorités publiques d'élaborer des politiques visant à prévenir «l'utilisation abusive et détournée des informations à caractère personnel, la surveillance et le traçage indiscrets, etc. et à renforcer la dignité des êtres humains et le respect de la vie privée des personnes». En outre, tout responsable du traitement doit traiter les données à caractère personnel de manière à réduire au minimum la possibilité d'empiéter sur la vie privée de la personne concernée (article 3, paragraphe 6, de la PIPA).

(148) Toutes les exigences de la PIPA, telles que décrites en détail à la section 2, s'appliquent au traitement des données à caractère personnel à des fins répressives. Cela inclut les principes (tels que les principes de licéité et de loyauté, de limitation des finalités, d'exactitude, de minimisation des données, de limitation de la conservation, de sécurité et de transparence), les obligations (par exemple, en ce qui concerne la notification des violations de données et les données sensibles) et les droits fondamentaux (droits d'accès, de rectification, de suppression et de suspension).

(149) Bien que le traitement des données à caractère personnel à des fins de sécurité nationale soit soumis à un ensemble plus restreint de dispositions en vertu de la PIPA, les principes fondamentaux, ainsi que les règles en matière de surveillance, de contrôle du respect des règles et de recours, s'appliquent ([196]). Plus précisément, les articles 3 et 4 de la PIPA énoncent les principes généraux en matière de protection des données (licéité et loyauté, limitation des finalités, exactitude, minimisation des données, sécurité et transparence) et les droits individuels (le droit d'être informé, le droit d'accès et les droits de rectification, de suppression et de suspension) ([197]). L'article 4, paragraphe 5, de la PIPA prévoit en outre pour les particuliers, en cas de préjudice résultant du traitement de leurs

([188]) Voir annexe II, section 1.1.
([189]) Article 37, paragraphe 2, de la Constitution.
([190]) Article 16 et article 12, paragraphe 3, de la Constitution. L'article 12, paragraphe 3, de la Constitution décrit en outre les circonstances exceptionnelles dans lesquelles une perquisition ou une saisie sans mandat peut avoir lieu (bien qu'un mandat ex post soit toujours nécessaire), c'est-à-dire en cas de flagrant délit ou d'infraction passible d'une peine d'emprisonnement d'au moins trois ans, s'il existe un risque que les preuves soient détruites ou que le suspect s'échappe.
([191]) Article 68, paragraphe 1, de la loi sur la Cour constitutionnelle.
([192]) Article 29, paragraphe 1, de la Constitution.
([193]) Article 199, paragraphe 1, du CPP. Plus généralement, lorsqu'elles exercent leurs pouvoirs en vertu du CPP, les autorités publiques doivent respecter les droits fondamentaux des suspects et de toute autre personne concernée (article 198, paragraphe 2, du CPP).
([194]) Article 14 de la loi sur le NIS.
([195]) Voir annexe II, section 1.2.
([196]) Article 58, paragraphe 1, point 2, de la PIPA. See also Section 6 of Notification No 2021-5 (Annex I). Cette dérogation à certaines dispositions de la PIPA ne s'applique que lorsque des données à caractère personnel sont traitées «à des fins de sécurité nationale». Dès que la situation en matière de sécurité nationale justifiant le traitement des données a pris fin, la dérogation ne peut plus être invoquée et toutes les exigences de la PIPA s'appliquent.
([197]) Ces droits ne peuvent être limités que dans les cas prévus par le droit, dans la mesure où et aussi longtemps que cela est nécessaire et proportionné à la protection d'un objectif d'intérêt public important ou lorsque l'octroi de ce droit peut porter atteinte à la vie ou à l'intégrité physique d'un tiers, ou entraîner la violation injustifiée des droits de propriété et d'autres intérêts d'un tiers. Voir également section 6 de la notification 2021-5.

données à caractère personnel, le droit à un recours approprié dans le cadre d'une procédure rapide et équitable. Ces droits et principes sont complétés par les obligations plus spécifiques de limiter le traitement des données à caractère personnel à la portée et à la durée minimales nécessaires pour atteindre la finalité visée, de mettre en place les mesures nécessaires pour garantir la gestion sûre et le traitement approprié des données (telles que des garanties techniques, administratives et physiques), ainsi que de mettre en place des mesures aux fins du traitement approprié des réclamations individuelles (plaintes) ([198]). Pour finir, les principes généraux de légalité, de nécessité et de proportionnalité découlant de la Constitution coréenne (voir considérant 145) s'appliquent également au traitement de données à caractère personnel à des fins de sécurité nationale.

(150) Les particuliers peuvent invoquer ces limitations et garanties générales devant les organismes de surveillance indépendants (par exemple, la PIPC et/ou la Commission nationale des droits de l'homme, voir considérants 177 et 178) et les juridictions (voir considérants 179 à 183) pour obtenir réparation.

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

(151) Le droit de la République de Corée impose un certain nombre de limitations à l'accès aux données à caractère personnel et à l'utilisation de celles-ci à des fins répressives. Il prévoit également des mécanismes de surveillance et de recours dans ce domaine qui sont conformes aux exigences visées aux considérants 141 à 143 de la présente décision. Les conditions dans lesquelles un tel accès peut intervenir et les garanties applicables à l'utilisation de ces pouvoirs sont évaluées en détail dans les sections suivantes.

3.2.1. *Bases juridiques, limitations et garanties*

(152) Les données à caractère personnel traitées par des responsables du traitement coréens qui seraient transférées depuis l'Union sur la base de la présente décision ([199]) peuvent être collectées par les autorités coréennes à des fins répressives dans le cadre d'une perquisition ou d'une saisie (sur la base du CPP), en accédant aux informations de communications (sur la base de la CPPA) ou en obtenant les données d'abonnés par voie de demandes de divulgation volontaire (sur la base de la loi sur les activités de télécommunications, ci-après la «TBA») ([200]).

3.2.1.1. Perquisitions et saisies

(153) En vertu du CPP, une perquisition ou une saisie ne peut avoir lieu que si une personne est soupçonnée d'avoir commis une infraction, la perquisition ou la saisie est nécessaire aux fins de l'enquête et un lien est établi entre l'enquête et la personne faisant l'objet de la perquisition ou le bien à inspecter ou à saisir ([201]). En outre, une perquisition ou une saisie (en tant que mesure de contrainte) ne peut être autorisée/effectuée que dans la stricte mesure du nécessaire ([202]). Si une perquisition concerne une disquette ou un autre support de stockage de données, en principe seules les données nécessaires (copiées ou imprimées) seront saisies et non le support entier ([203]). Ce dernier ne peut être saisi que si l'impression ou la copie séparée des données nécessaires, ou la réalisation de l'objectif de la perquisition, est considérée comme fondamentalement impossible ([204]). Le CPP fixe par conséquent des règles claires et précises concernant la portée et l'application de ces mesures, garantissant ainsi que l'ingérence dans les droits des personnes, dans le cas d'une perquisition ou d'une saisie, sera limitée à ce qui est nécessaire aux fins d'une enquête pénale spécifique et proportionné à l'objectif visé.

([198]) Article 58, paragraphe 4, de la PIPA.

([199]) Voir annexe II, section 2.1. La déclaration officielle du gouvernement coréen (section 2.1 de l'annexe II) mentionne également la possibilité de collecter les informations sur les opérations financières aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme sur la base de la loi sur la communication et l'utilisation de certaines informations sur les opérations financières (ARUSFTI). Toutefois, l'ARUSFTI n'impose des obligations de divulgation qu'aux responsables du traitement qui traitent des informations à caractère personnel en matière de crédit conformément à la CIA et sont soumis à la surveillance de la Commission des services financiers (voir considérant 13). Étant donné que le traitement des informations à caractère personnel en matière de crédit par ces responsables du traitement est exclu du champ d'application de la présente décision, l'ARUSFTI n'est pas pertinente pour la présente évaluation.

([200]) L'article 3 de la CPPA mentionne également la loi sur les tribunaux militaires comme base juridique éventuelle de la collecte de données de communications. Toutefois, cette loi régit la collecte d'informations sur le personnel militaire et ne peut s'appliquer aux civils que dans un nombre limité de cas (par exemple, si des militaires et des civils commettent ensemble une infraction, ou si un individu commet une infraction contre les forces armées, une procédure peut être engagée devant un tribunal militaire, voir article 2 de la loi sur les tribunaux militaires). En tout état de cause, la loi contient des dispositions générales régissant les perquisitions et les saisies qui sont similaires à celles du CPP (voir articles 146 à 149 et 153 à 156 de la loi sur les tribunaux militaires). Elle prévoit par exemple que le courrier postal ne peut être collecté que lorsque cela est nécessaire aux fins d'une enquête et sur la base d'un mandat délivré par le tribunal militaire. Dans la mesure où des communications électroniques seraient collectées sur la base de cette loi, les limitations et les garanties de la CPPA s'appliqueraient. Voir annexe II, section 2.2.2, et note de bas de page 50.

([201]) Article 215, paragraphes 1 et 2, du CPP. Voir également article 106, paragraphe 1, et articles 107 et 109 du CPP, qui disposent que les juridictions peuvent effectuer des perquisitions et des saisies dès lors que les biens ou les personnes concernées sont considérés comme ayant un lien avec une affaire spécifique. Voir annexe I, section 2.2.1.2.

([202]) Article 199, paragraphe 1, du CPP.

([203]) Article 106, paragraphe 3, du CPP.

([204]) Article 106, paragraphe 3, du CPP.

(154) Pour ce qui est des garanties procédurales, le CPP exige qu'un mandat soit obtenu auprès d'une juridiction pour effectuer une perquisition ou une saisie ([205]). Une perquisition ou une saisie sans mandat n'est autorisée qu'à titre exceptionnel, à savoir dans des circonstances urgentes ([206]), in loco au moment de l'arrestation ou de la détention d'un suspect ([207]), ou lorsqu'un bien est jeté ou volontairement produit par un suspect ou un tiers (dans le cas de données à caractère personnel, par l'individu concerné lui-même) ([208]). Les perquisitions et les saisies illégales sont passibles de sanctions pénales ([209]) et tout élément de preuve obtenu en violation du CPP est considéré comme irrecevable ([210]). Enfin, les individus concernés doivent toujours être informés de la perquisition ou de la saisie (y compris de la saisie de leurs données) sans délai ([211]), ce qui facilitera l'exercice de leurs droits substantiels et de leur droit de recours (en particulier sur la possibilité de contester l'exécution d'un mandat de saisie, voir considérant 180).

3.2.1.2. Accès aux informations de communications

(155) Sur la base de la CPPA, les autorités répressives coréennes peuvent adopter deux types de mesures ([212]): d'une part, la collecte de «données de confirmation des communications» ([213]), qui comprennent la date, l'heure de début et l'heure de fin des télécommunications, le nombre d'appels sortants et entrants ainsi que le numéro d'abonné de l'autre partie, la fréquence d'utilisation, les journaux relatifs à l'utilisation des services de télécommunications et les informations de localisation (par exemple, à partir des pylônes de transmission où les signaux sont reçus); et, d'autre part, les «mesures de restriction des communications» qui couvrent aussi bien la collecte du contenu du courrier traditionnel que l'interception directe du contenu des télécommunications ([214]).

(156) Les données de confirmation des communications ne peuvent être consultées que lorsque cela est nécessaire aux fins de la réalisation d'une enquête pénale ou de l'exécution d'une peine ([215]), sur la base d'un mandat délivré par une juridiction ([216]). À cet égard, la CPPA exige que des informations détaillées soient fournies tant dans la demande de mandat (par exemple, concernant les raisons de la demande, le lien avec la cible/l'abonné et les données nécessaires) que dans le mandat lui-même (par exemple, concernant l'objectif, la cible et la portée de la mesure) ([217]). La collecte de données sans mandat ne peut avoir lieu que lorsque, pour des motifs d'urgence, il

([205]) Article 215, paragraphes 1 et 2, et article 113 du CPP. Lorsqu'elle introduit une demande de mandat, l'autorité concernée doit présenter des éléments démontrant les motifs permettant de soupçonner un individu d'avoir commis une infraction, que la perquisition, l'inspection ou la saisie est nécessaire et que les biens pertinents à saisir existent (article 108, paragraphe 1, du règlement sur la procédure pénale). Le mandat lui-même doit préciser, entre autres, le nom du suspect et l'infraction; le lieu, la personne ou les objets à fouiller, ou les objets à saisir; la date de délivrance; et la période d'application effective (article 114, paragraphe 1, en liaison avec l'article 219 du CPP). Voir annexe I, section 2.2.1.2.

([206]) C'est-à-dire, lorsqu'il n'est pas possible d'obtenir un mandat en raison d'une urgence sur le lieu de l'infraction (article 216, paragraphe 3, du CPP), auquel cas un mandat doit toujours être obtenu par la suite sans délai (article 216, paragraphe 3, du CPP).

([207]) Article 216, paragraphes 1 et 2, du CPP.

([208]) Article 218 du CPP. En outre, comme expliqué à la section 2.2.1.2 de l'annexe II, les biens produits volontairement ne sont admis comme preuves dans une procédure judiciaire que s'il n'existe aucun doute raisonnable quant au caractère volontaire de la divulgation, ce qu'il appartient au procureur de démontrer.

([209]) Article 321 du code pénal.

([210]) Article 308-2 du CPP. De plus, un individu (et son avocat) peut être présent au cours de l'exécution d'un mandat de perquisition ou de saisie et peut donc également s'y opposer au moment où le mandat est exécuté (articles 121 et 219 du CPP).

([211]) Articles 121 et 122 du CPP (en ce qui concerne les perquisitions), et article 219 en liaison avec l'article 106, paragraphe 4, du CPP (en ce qui concerne les saisies).

([212]) Voir également annexe II, section 2.2.2.1. De telles mesures peuvent être adoptées en sollicitant par voie de contrainte l'assistance des opérateurs de télécommunications sur présentation à ces derniers d'une autorisation écrite obtenue auprès d'une juridiction (article 9, paragraphe 2, de la CPPA), qui doit être conservée par les opérateurs (article 15-2 de la CPPA et article 12 du décret d'application de la CPPA). Les opérateurs de télécommunications peuvent refuser de coopérer lorsque les informations concernant l'individu ciblé qui figurent sur l'autorisation écrite de la juridiction (par exemple, le numéro de téléphone de l'individu) sont inexactes. Ils ont dans tous les cas l'interdiction de divulguer les mots de passe utilisés aux fins des télécommunications (article 9, paragraphe 4, de la CPPA).

([213]) Article 2, paragraphe 11, de la CPPA.

([214]) Voir article 2, paragraphe 6, de la CPPA, qui fait référence à la «censure» (ouvrir le courrier sans le consentement de la partie concernée ou prendre connaissance de son contenu, l'enregistrer ou le conserver par d'autres moyens) et article 2, paragraphe 7, de la CPPA, qui fait référence à l'«écoute téléphonique» (obtenir ou enregistrer le contenu de télécommunications en écoutant ou en interprétant collectivement les sons, les mots, les symboles ou les images des communications au moyen de dispositifs électroniques et mécaniques sans le consentement de la partie concernée, ou interférer avec leur transmission et leur réception).

([215]) Article 13, paragraphe 1, de la CPPA. Voir également annexe II, section 2.2.2.3. En outre, les données de localisation en temps réel et les données de confirmation des communications concernant une station de base précise ne peuvent être collectées qu'aux fins des enquêtes relatives à des infractions graves ou si, dans le cas contraire, il serait difficile de prévenir la commission d'une infraction ou de recueillir des preuves (article 13, paragraphe 2, de la CPPA). Cette limitation reflète la nécessité de prévoir des garanties supplémentaires dans le cas de mesures particulièrement intrusives pour la vie privée, conformément au principe de proportionnalité.

([216]) Articles 13 et 6 de la CPPA.

([217]) Voir article 13, paragraphes 3 et 9, en liaison avec l'article 6, paragraphes 4 et 6, de la CPPA.

n'est pas possible d'obtenir l'autorisation d'une juridiction, auquel cas le mandat doit être obtenu et transmis à l'opérateur de télécommunications immédiatement après que les données ont été demandées ([218]). Si la juridiction refuse d'accorder une autorisation par la suite, les informations recueillies doivent être détruites ([219]).

(157) En ce qui concerne les garanties supplémentaires relatives à la collecte de données de confirmation des communications, la CPPA impose des exigences spécifiques en matière de tenue de registres et de transparence ([220]). En particulier, les autorités répressives ([221]) et les opérateurs de télécommunications ([222]) doivent tenir des registres relatifs aux demandes et aux divulgations effectuées. De plus, les autorités répressives doivent notifier en principe aux personnes le fait que leurs données de confirmation des communications ont été collectées ([223]). Une telle notification ne peut être différée que dans des circonstances exceptionnelles, sur la base d'une autorisation du directeur d'un parquet de district compétent ([224]). Cette autorisation ne peut être accordée que lorsque la notification est susceptible 1) de menacer la sécurité nationale, la sécurité publique et l'ordre public; 2) de causer un décès ou un préjudice corporel; 3) d'entraver la tenue d'une procédure judiciaire équitable (par exemple, parce qu'elle entraîne la destruction de preuves ou l'intimidation de témoins); ou 4) de nuire à la réputation du suspect, des victimes ou d'autres personnes liées à l'affaire, ou d'empiéter sur leur vie privée. Dans ces cas, la notification doit être effectuée dans un délai de 30 jours à partir du moment où le ou les motifs du report cessent d'exister ([225]). Une fois informées, les personnes ont le droit d'obtenir des informations sur les raisons de la collecte de leurs données ([226]).

(158) Des règles plus strictes s'appliquent en ce qui concerne les mesures de restriction des communications, auxquelles il ne peut être fait recours que lorsqu'il existe des raisons sérieuses de soupçonner que certaines infractions graves spécifiquement énumérées dans la CPPA sont en train d'être planifiées ou commises ou ont été commises ([227]). En outre, les mesures de restriction des communications ne peuvent être prises qu'en dernier recours et si, dans le cas contraire, il est difficile de prévenir la commission d'une infraction, d'arrêter un criminel ou de recueillir des preuves ([228]). Elles doivent être immédiatement abandonnées lorsqu'elles ne sont plus nécessaires afin de limiter autant que possible la violation de la confidentialité des communications ([229]). Les informations qui ont été illégalement obtenues par le biais de mesures de restriction des communications ne sont pas admises comme preuves dans les procédures judiciaires ou disciplinaires ([230]).

(159) Pour ce qui est des garanties procédurales, la CPPA exige qu'un mandat judiciaire soit obtenu aux fins de la mise en œuvre des mesures de restriction des communications ([231]). De la même manière, la CPPA exige que la demande de mandat et le mandat lui-même contiennent des informations détaillées ([232]), notamment la justification de la demande, ainsi que les communications à collecter (qui doivent être celles du suspect faisant l'objet de l'enquête) ([233]). De telles mesures ne peuvent être prises sans un mandat que dans le cas d'une menace imminente

([218]) Article 13, paragraphe 2, de la CPPA.
([219]) Article 13, paragraphe 3, de la CPPA.
([220]) Voir annexe II, section 2.2.2.3.
([221]) Article 13, paragraphes 5 et 6, de la CPPA.
([222]) Article 13, paragraphe 7, de la CPPA. De plus, les opérateurs de télécommunications doivent rendre compte deux fois par an de la divulgation de données de confirmation des communications au ministère des sciences et des TIC.
([223]) Voir article 13-3, paragraphe 7, en liaison avec l'article 9-2 de la CPPA. En particulier, les personnes doivent être informées dans un délai de 30 jours à compter de la décision d'engager (ou non) des poursuites ou dans un délai de 30 jours un an après la décision de suspendre la mise en accusation (bien qu'une notification doive dans tous les cas être effectuée dans un délai de 30 jours un an après la collecte des informations), voir article 13-3, paragraphe 1, de la CPPA.
([224]) Article 13-3, paragraphes 2 et 3, de la CPPA.
([225]) Article 13-3, paragraphe 4, de la CPPA.
([226]) Article 13-3, paragraphe 5, de la CPPA. À la demande de la personne, un procureur ou un officier de police judiciaire doit exposer par écrit les raisons de la collecte dans un délai de 30 jours à partir de la réception de la demande, à moins que l'une des exceptions concernant le report de la notification ne s'applique (article 13-3, paragraphe 6, de la CPPA).
([227]) Par exemple, les infractions liées à l'insurrection et à la drogue, les infractions impliquant des explosifs, ainsi que les infractions liées à la sécurité nationale, aux relations diplomatiques ou aux bases et installations militaires, voir article 5, paragraphe 1, de la CPPA. Voir également annexe II, section 2.2.2.2.
([228]) Article 3, paragraphe 2, et article 5, paragraphe 1, de la CPPA.
([229]) Article 2 du décret d'application de la CPPA.
([230]) Article 4 de la CPPA.
([231]) Article 6, paragraphes 1, 2, 5 et 6, de la CPPA.
([232]) Une demande de mandat doit décrire 1) les raisons sérieuses conduisant à suspecter que l'une des infractions énumérées est planifiée, est en train d'être commise ou a été commise, ainsi que tout élément justificatif; 2) les mesures de restriction des communications ainsi que leur cible, leur portée, leur objectif et leur période d'effet; et 3) le lieu où les mesures seraient exécutées et la façon dont elles seraient mises en œuvre (article 6, paragraphe 4, de la CPPA et article 4, paragraphe 1, du décret d'application de la CPPA). Le mandat lui-même doit préciser les mesures ainsi que leur cible, leur portée, leur période d'effet, leur lieu d'exécution et leurs modalités de mise en œuvre (article 6, paragraphe 6, de la CPPA).
([233]) La cible d'une mesure de restriction des communications doit consister dans des envois postaux ou des télécommunications spécifiques envoyés ou reçus par le suspect, ou des envois postaux ou des télécommunications envoyés ou reçus par le suspect pendant une période déterminée (article 5, paragraphe 2, de la CPPA).

de crime organisé, ou lorsqu'une autre infraction grave susceptible de causer un décès ou un préjudice grave est imminente, et si une urgence ne permet pas d'appliquer la procédure normale ([234]). Toutefois, dans ce cas, une demande de mandat doit être immédiatement introduite après que la mesure a été prise ([235]). Les mesures de restriction des communications ne doivent être mises en œuvre que dans une période maximale de deux mois ([236]) et ne peuvent être prolongées qu'avec l'accord d'une juridiction si les conditions de mise en œuvre des mesures continuent d'être remplies ([237]). La période prolongée ne saurait dépasser un an au total, ou trois ans pour certaines infractions particulièrement graves (par exemple, les infractions liées à une insurrection, à une agression étrangère et à la sécurité nationale) ([238]).

(160) Comme pour la collecte de données de confirmation des communications, la CPPA exige des opérateurs de télécommunications ([239]) et des autorités répressives ([240]) qu'ils tiennent des registres relatifs à l'exécution des mesures de restriction des communications. La loi prévoit également la notification des mesures à l'individu concerné, laquelle peut être différée à titre exceptionnel, lorsque cela est nécessaire pour des motifs d'intérêt public importants ([241]).

(161) Enfin, le non-respect de plusieurs des limitations et garanties prévues par la CPPA (notamment, par exemple, les obligations relatives à l'obtention d'un mandat, à la tenue de registres et à la notification à la personne), en ce qui concerne tant la collecte de données de confirmation des communications que le recours à des mesures de restriction des communications, est passible de sanctions pénales ([242]).

(162) Le pouvoir des autorités répressives de collecter des données de communication sur la base de la CPPA (aussi bien le contenu des communications que les données de confirmation des communications) est donc encadré par des règles claires et précises et est soumis à un certain nombre de garanties. Ces garanties assurent en particulier le contrôle de l'exécution de ces mesures, aussi bien ex ante (par le biais de l'autorisation préalable d'une juridiction) qu'ex post (par le biais des exigences en matière de tenue de registres et de déclaration), et facilitent l'accès des personnes à des recours effectifs (en veillant à ce qu'elles soient informées de la collecte de leurs données).

3.2.1.3. Demandes de divulgation volontaire de données d'abonnés

(163) En plus de s'appuyer sur les mesures de contrainte décrites aux considérants 153 à 162, les autorités répressives coréennes peuvent demander aux opérateurs de télécommunications des «données de communication» sur une base volontaire, à l'appui d'un procès pénal, d'une enquête pénale ou de l'exécution d'une peine (article 83, paragraphe 3, de la TBA). Cette possibilité n'existe qu'en ce qui concerne des ensembles de données limités, c'est-à-dire le nom, le numéro d'enregistrement résidentiel, l'adresse et le numéro de téléphone des utilisateurs, les dates auxquelles ces derniers ont souscrit ou résilié leur abonnement ainsi que leurs codes d'identification (à savoir les codes utilisés pour identifier l'utilisateur légitime des systèmes informatiques ou des réseaux de communication) ([243]). Étant donné que seules les personnes qui concluent directement un contrat de service avec un opérateur de télécommunications coréen sont considérées comme des «utilisateurs» ([244]), les citoyens de l'Union dont les données ont été transférées vers la République de Corée ne relèvent normalement pas de cette catégorie ([245]).

(164) Différentes limitations s'appliquent à de telles divulgations volontaires, en ce qui concerne aussi bien l'exercice des pouvoirs par l'autorité répressive que la réponse de l'opérateur de télécommunications. En règle générale, les autorités répressives doivent agir conformément aux principes constitutionnels de nécessité et de proportionnalité (article 12, paragraphe 1, et article 37, paragraphe 2, de la Constitution), notamment lorsqu'elles demandent des informations sur une base volontaire. En outre, elles doivent se conformer à la PIPA, en particulier en ne

([234]) Article 8, paragraphe 1, de la CPPA. Toutefois, la collecte d'informations dans des situations d'urgence doit toujours avoir lieu conformément à une «déclaration de censure/d'écoute d'urgence» et l'autorité effectuant la collecte doit tenir un registre des mesures d'urgence prises (article 8, paragraphe 4, de la CPPA).

([235]) La collecte doit être immédiatement abandonnée si l'autorité répressive n'obtient pas l'autorisation d'une juridiction dans un délai de 36 heures (article 8, paragraphe 2, de la CPPA), auquel cas, comme expliqué à la section 2.2.2.2 de l'annexe II, les informations recueillies seront en principe détruites. La juridiction doit également être prévenue lorsque des mesures d'urgence ont été mises en œuvre dans un délai si court que l'autorisation n'est plus nécessaire (par exemple, si le suspect est arrêté immédiatement après le début de l'interception, voir article 8, paragraphe 5, de la CPPA). Dans ce cas, elle doit être informée de l'objectif, de la cible, de la portée, de la durée, du lieu d'exécution de la collecte et de la méthode de collecte, ainsi que des motifs justifiant l'absence de demande d'autorisation auprès d'une juridiction (article 8, paragraphes 6 et 7, de la CPPA).

([236]) Article 6, paragraphe 7, de la CPPA. Si l'objectif des mesures est atteint plus tôt dans cette période, les mesures doivent être abandonnées immédiatement.

([237]) Article 6, paragraphes 7 et 8, de la CPPA.

([238]) Article 6, paragraphe 8, de la CPPA.

([239]) Article 9, paragraphe 3, de la CPPA.

([240]) Article 18, paragraphe 1, du décret d'application de la CPPA.

([241]) En particulier, le procureur doit informer la personne dans un délai de 30 jours à compter de l'établissement de l'acte d'accusation ou de la décision de ne pas l'inculper ou l'arrêter (article 9-2, paragraphe 1, de la CPPA). La notification peut être différée avec l'accord du chef du parquet de district si elle est susceptible de menacer gravement la sécurité nationale ou de perturber la sécurité et l'ordre publics, ou si elle est susceptible d'entraîner un préjudice important pour la vie et l'intégrité physique d'autrui (article 9-2, paragraphes 4 à 6, de la CPPA).

([242]) Articles 16 et 17 de la CPPA.

([243]) Article 83, paragraphe 3, de la TBA. Voir également annexe II, section 2.2.3.

([244]) Article 2, paragraphe 9, de la TBA.

([245]) Voir également annexe II, section 2.2.3.

collectant qu'un minimum de données à caractère personnel, dans la mesure nécessaire pour atteindre une finalité légitime et de manière à réduire au minimum l'incidence de la collecte sur la vie privée des personnes (comme prévu à l'article 3, paragraphes 1 et 6, de la PIPA). Plus précisément, les demandes visant à obtenir des données de communication sur la base de la TBA doivent être effectuées par écrit et indiquer les raisons de la demande, le lien avec l'utilisateur concerné et la portée des données demandées ([246]).

(165) Les opérateurs de télécommunications ne sont pas tenus de satisfaire à de telles demandes et ne peuvent le faire que conformément à la PIPA. Cela signifie, en particulier, qu'ils doivent mettre en balance les différents intérêts en jeu et peuvent ne pas fournir les données si cela est susceptible de porter atteinte de manière déloyale aux intérêts de la personne ou d'un tiers ([247]). Cela serait par exemple le cas s'il apparaissait clairement que l'autorité à l'origine de la demande a abusé de son autorité ([248]). Les opérateurs de télécommunications doivent tenir des registres relatifs aux divulgations effectuées au titre de la TBA et rendre compte de celles-ci deux fois par an au ministère des sciences et des TIC ([249]).

(166) De plus, conformément à la section 3 de la notification 2021-5 (annexe 1), les opérateurs de télécommunications doivent en principe informer la personne concernée lorsqu'ils répondent volontairement à une demande ([250]). La personne sera alors en mesure d'exercer ses droits et, dans le cas où ses données seraient divulguées illégalement, de former un recours contre le responsable du traitement (par exemple, pour avoir divulgué les données en violation de la PIPA ou pour avoir répondu à une demande qui était visiblement disproportionnée) ou contre l'autorité répressive (par exemple, pour avoir agi au-delà des limites de ce qui est nécessaire et proportionné, ou pour ne pas avoir respecté les exigences procédurales de la TBA).

3.2.2. *Utilisation ultérieure des informations recueillies*

(167) Le traitement des données à caractère personnel collectées par les autorités répressives coréennes est soumis à l'ensemble des exigences de la PIPA, notamment en ce qui concerne la limitation des finalités (article 3, paragraphes 1 et 2, de la PIPA), la licéité de l'utilisation et de la fourniture des données aux tiers (articles 15, 17 et 18 de la PIPA), les transferts internationaux (articles 17 et 18 de la PIPA, en liaison avec la section 2 de la notification 2021-5) ([251]), la proportionnalité/minimisation des données (article 3, paragraphes 1 et 6, de la PIPA) et la limitation de la conservation (article 21 de la PIPA) ([252]).

(168) S'agissant du contenu des communications acquises par l'exécution de mesures de restriction des communications, la CPPA limite spécifiquement l'utilisation possible de ces communications à la prévention des infractions graves et aux enquêtes et poursuites en la matière ([253]); aux procédures disciplinaires relatives aux mêmes infractions; aux demandes d'indemnisation introduites par une partie aux communications ou lorsque cela est spécifiquement autorisé par d'autres lois ([254]). En outre, le contenu de télécommunications transmises sur l'internet qui est collecté ne peut être conservé qu'avec l'accord de la juridiction ayant autorisé les mesures de restriction des communications ([255]), en vue de leur utilisation aux fins de la prévention d'infractions graves et des enquêtes et poursuites en la matière ([256]). Plus généralement, la CPPA interdit la divulgation des informations confidentielles obtenues par le biais de mesures de restriction des communications, ainsi que l'utilisation de ces informations dans le but de porter atteinte à la réputation des personnes visées par les mesures ([257]).

3.2.3. *Surveillance*

(169) En Corée, les activités des autorités répressives sont supervisées par différents organismes ([258]).

([246]) Article 83, paragraphe 4, de la TBA. Lorsqu'il n'est pas possible de présenter une demande écrite du fait d'une urgence, la demande écrite doit être fournie dès que la raison de l'urgence cesse d'exister (article 83, paragraphe 4, de la TBA).

([247]) Article 18, paragraphe 2, de la PIPA.

([248]) Arrêt 2012Da105482 de la Cour suprême du 10 mars 2016. Voir également annexe II, section 2.2.3, concernant cet arrêt.

([249]) Article 83, paragraphes 5 et 6, de la TBA.

([250]) Cette exigence est soumise à des exceptions limitées et précises, en particulier si et aussi longtemps que la notification compromet une enquête pénale en cours ou porte atteinte à la vie ou à l'intégrité physique d'une autre personne, lorsque ces droits ou intérêts sont manifestement supérieurs aux droits de la personne concernée. Voir section 3, paragraphe iii), point 1), de la notification.

([251]) Les autorités publiques coréennes sont tenues en particulier de garantir, au moyen d'un instrument juridiquement contraignant, un niveau de protection équivalent à celui de la PIPA, voir également le considérant 90.

([252]) Voir également annexe II, section 1.2.

([253]) Voir considérant 158.

([254]) Article 12 de la CPPA. Voir annexe I, section 2.2.2.2.

([255]) Le procureur ou l'agent de police exécutant les mesures de restriction des communications doit sélectionner les télécommunications à conserver dans un délai de 14 jours à compter de la fin des mesures et demander l'autorisation de la juridiction (dans le cas d'un agent de police, la demande doit être présentée à un procureur qui la soumet ensuite à la juridiction), voir article 12-2, paragraphes 1 et 2, de la CPPA.

([256]) La demande d'une telle autorisation doit contenir des informations sur les mesures de restriction des communications, un résumé du résultat des mesures, les raisons de la conservation (ainsi que les éléments justificatifs) et les télécommunications à conserver (article 12-2, paragraphe 3, de la CPPA). En l'absence de demande, les données recueillies doivent être supprimées dans un délai de 14 jours à partir de la fin des mesures de restriction des communications (article 12-2, paragraphe 5, de la CPPA) et, si la demande est rejetée, dans un délai de sept jours (article 12-2, paragraphe 5, de la CPPA). Dans les deux cas, un rapport sur la suppression doit être remis à la juridiction qui a autorisé la collecte dans un délai de sept jours.

([257]) Article 11, paragraphe 2, du décret d'application de la CPPA.

([258]) Voir annexe II, section 2.3.

(170) Premièrement, la police est soumise au contrôle interne de l'inspecteur général ([259]), qui est chargé du contrôle de la légalité, notamment en ce qui concerne les éventuelles violations des droits de l'homme. La fonction d'inspecteur général a été établie aux fins de la mise en œuvre de la loi sur les audits du secteur public, qui encourage la création d'organismes d'autocontrôle et fixe les exigences spécifiques relatives à leur composition et à leurs missions. En particulier, la loi prévoit que le directeur d'un organisme d'autocontrôle est nommé en dehors de l'autorité concernée (par exemple, parmi des anciens juges ou professeurs) pour une période de deux à cinq ans ([260]), qu'il ne peut être révoqué que pour des motifs justifiés (par exemple, lorsqu'il n'est plus en mesure d'exercer ses fonctions pour des raisons de santé, ou lorsqu'il fait l'objet d'une mesure disciplinaire) ([261]) et que son indépendance est garantie dans la plus large mesure possible ([262]). L'entrave à un autocontrôle est passible d'amendes administratives ([263]). Les rapports d'audit (qui peuvent inclure des recommandations, des demandes de mesures disciplinaires et des demandes d'indemnisation ou de correction) sont communiqués au directeur de l'autorité publique concernée et au comité d'audit et d'inspection (ci-après le «BAI») ([264]), et sont généralement rendus publics ([265]). Les résultats de la mise en œuvre du rapport doivent également être transmis au BAI ([266]) (voir considérant 173 en ce qui concerne la fonction de surveillance et les pouvoirs du BAI).

(171) Deuxièmement, la PIPC contrôle la conformité du traitement des données par les autorités répressives avec la PIPA et d'autres lois qui protègent la vie privée des personnes, notamment les lois qui régissent la collecte de preuves (électroniques) à des fins répressives, comme décrit à la section 3.2.1 ([267]). En particulier, dans la mesure où la surveillance de la PIPC s'étend aux principes de licéité et de loyauté de la collecte et du traitement des données (article 3, paragraphe 1, de la PIPA), lesquels seront violés en cas d'accès aux données à caractère personnel et d'utilisation de celles-ci en violation de ces lois ([268]), la PIPC peut également mener des enquêtes et faire respecter les limitations et garanties décrites à la section 3.2.1 ([269]). Dans l'exercice de sa fonction de surveillance, la PIPC peut utiliser l'ensemble des pouvoirs d'investigation et de correction à sa disposition, tels que détaillés à la section 2.4.2. Avant même la réforme récente de la PIPA (c'est-à-dire, dans le cadre de sa précédente fonction de supervision pour le secteur public), la PIPC réalisait plusieurs activités de surveillance liées au traitement de données à caractère personnel par les autorités répressives, par exemple, dans le cadre de l'interrogation de suspects (affaire n° 2013-16 du 26 août 2013), en ce qui concerne l'envoi de notifications aux personnes concernant l'imposition d'amendes administratives (affaire n° 2015-02-04 du 26 janvier 2015), le partage de données avec d'autres autorités (affaire n° 2018-15-146 du 9 juillet 2018; affaire n° 2018-25-308 du 10 décembre 2018; affaire n° 2019-02-015 du 29 janvier 2019), la collecte d'empreintes digitales ou de photographies (affaire n° 2019-17-273 du 9 septembre 2019) et l'utilisation de drones (affaire n° 2020-01-004 du 13 janvier 2020). Dans ces cas, la PIPC a examiné le respect de plusieurs dispositions de la PIPA (par exemple, la licéité du traitement, les principes de limitation des finalités et de minimisation des données), mais également des dispositions pertinentes d'autres lois, comme le code de procédure pénale, et, lorsque cela était nécessaire, a formulé des recommandations en vue de remettre le traitement en conformité avec les exigences en matière de protection des données.

(172) Troisièmement, une surveillance indépendante est exercée par la Commission nationale des droits de l'homme (ci-après la «CNDH») ([270]), qui peut enquêter sur les violations des droits au respect de la vie privée et au secret de la correspondance dans le cadre de sa mission générale visant à protéger les droits fondamentaux consacrés par les articles 10 à 22 de la Constitution. La CNDH est composée de 11 commissaires qui doivent posséder des qualifications spécifiques ([271]) et sont nommés par le président de la République, conformément aux procédures prévues par le droit. En particulier, quatre commissaires sont nommés sur proposition de l'Assemblée nationale, quatre autres sur proposition du président de la République et les trois derniers sur proposition du président de la Cour suprême ([272]). Le président est nommé par le président de la République parmi les commissaires et cette nomination doit être confirmée par l'Assemblée nationale ([273]). Les commissaires (y compris le président) sont

([259]) Voir annexe II, section 2.3.1. Voir également à l'adresse https://www.police.go.kr/eng/knpa/org/org01.jsp
([260]) De la même manière, les auditeurs sont nommés sur la base de conditions spécifiques énoncées dans la loi, voir articles 16 et suivants de la loi sur les audits du secteur public.
([261]) Articles 8 à 11 de la loi sur les audits du secteur public.
([262]) Article 7 de la loi sur les audits du secteur public.
([263]) Article 41 de la loi sur les audits du secteur public.
([264]) Article 23, paragraphe 1, de la loi sur les audits du secteur public.
([265]) Article 26 de la loi sur les audits du secteur public.
([266]) Article 23, paragraphe 3, de la loi sur les audits du secteur public.
([267]) Voir article 7-8, paragraphes 3 et 4, et article 7-9, paragraphe 5, de la PIPA.
([268]) Voir notification 2021-5 de la PIPC, section 6 (annexe I).
([269]) Voir également annexe II, section 2.3.4.
([270]) Article 1er de la loi sur la Commission des droits de l'homme (la «loi sur la CNDH»).
([271]) Pour être nommé, un commissaire doit 1) avoir exercé au moins la fonction de professeur associé pendant au moins dix ans dans une université ou un institut de recherche agréé; 2) avoir assumé les fonctions de juge, de procureur ou d'avocat pendant au moins dix ans; 3) avoir participé à des activités liées aux droits de l'homme pendant au moins dix ans (par exemple, pour une organisation à but non lucratif, une organisation non gouvernementale ou une organisation internationale); ou 4) avoir été recommandé par des groupes de la société civile (article 5, paragraphe 3, de la loi sur la CNDH). De plus, après leur nomination, les commissaires ont l'interdiction d'exercer simultanément un mandat à l'Assemblée nationale, dans des conseils locaux ou dans toute administration de l'État ou locale (en qualité de fonctionnaire), voir article 10 de la loi sur la CNDH.
([272]) Article 5, paragraphes 1 et 2, de la loi sur la CNDH.
([273]) Article 5, paragraphe 5, de la loi sur la CNDH.

nommés pour un mandat renouvelable d'une durée de trois ans et ne peuvent être révoqués que s'ils sont condamnés à une peine de prison ou ne sont plus en mesure d'exercer leurs fonctions en raison d'un handicap physique ou mental prolongé (auquel cas les deux tiers des commissaires doivent approuver la révocation) ([274]). Dans le cadre d'une enquête, la CNDH peut demander la présentation d'éléments pertinents, mener des inspections et convoquer des personnes afin qu'elles témoignent ([275]). Pour ce qui est de ses pouvoirs de correction, la CNDH peut formuler des recommandations (publiques) en vue d'améliorer ou de corriger certaines politiques et pratiques, auxquelles les autorités publiques doivent répondre par une proposition de plan de mise en œuvre ([276]). Si l'autorité concernée ne met pas en œuvre les recommandations, elle doit en informer la commission ([277]), qui, à son tour, peut notifier ce défaut à l'Assemblée nationale et/ou le rendre public. Selon la déclaration officielle du gouvernement coréen (section 2.3.5 de l'annexe II), les autorités coréennes se conforment généralement aux recommandations de la CNDH et y sont fortement incitées dans la mesure où leur mise en œuvre a été évaluée dans le cadre d'une évaluation générale continue sous l'autorité du cabinet du Premier ministre. Les chiffres annuels relatifs à ces activités montrent que la CNDH contrôle activement les activités des autorités répressives, sur la base de demandes individuelles ou au moyen d'enquêtes d'office ([278]).

(173) Quatrièmement, la surveillance générale de la légalité des activités des autorités publiques est exercée par le BAI, qui examine les recettes et les dépenses de l'État, mais aussi, plus généralement, qui contrôle le respect des devoirs des autorités publiques en vue d'améliorer le fonctionnement de l'administration publique ([279]). Le BAI est formellement établi par le président de la République de Corée, mais il conserve un statut d'indépendance en ce qui concerne ses devoirs ([280]). En outre, il jouit d'une indépendance totale pour ce qui est de la nomination, du congédiement et de l'organisation de son personnel, ainsi que de l'établissement de son budget ([281]). Le BAI se compose d'un président (nommé par le président de la République, avec le consentement de l'Assemblée nationale) ([282]) et de six commissaires (nommés par le président de la République sur recommandation du président du BAI) ([283]), qui doivent posséder les qualifications spécifiques fixées par la législation ([284]) et qui ne peuvent être révoqués qu'en cas de destitution, de peine de prison ou d'incapacité à exercer leurs fonctions en raison d'un handicap mental ou physique durable ([285]). Le BAI réalise un audit général tous les ans, mais il peut également mener des audits spécifiques concernant des questions revêtant un intérêt particulier. Lorsqu'il procède à un audit ou à une inspection, le BAI peut demander qu'on lui fournisse des documents et que certaines personnes soient présentes ([286]). Le BAI peut formuler des recommandations, demandes des mesures disciplinaires ou déposer une plainte pénale ([287]).

(174) Enfin, l'Assemblée nationale exerce un contrôle parlementaire sur les autorités publiques au moyen d'enquêtes et d'inspections ([288]) portant sur leurs activités ([289]). Elle peut demander la communication de documents, contraindre des témoins à comparaître ([290]), recommander des mesures correctives (si elle conclut que des activités

([274]) Article 7, paragraphe 1, et article 8 de la loi sur la CNDH.
([275]) Article 36 de la loi sur la CNDH. En vertu de l'article 6, paragraphe 7, de la loi, la présentation d'éléments ou d'objets peut être refusée si cela risque de porter atteinte à un secret d'État susceptible d'affecter substantiellement la sécurité nationale ou les relations diplomatiques ou de constituer un obstacle sérieux à une enquête pénale ou à un procès en cours. Dans de tels cas, la Commission peut demander des informations complémentaires au directeur de l'agence concernée (qui doit satisfaire à cette demande de bonne foi) lorsque cela est nécessaire pour examiner si le refus de fournir les informations est justifié.
([276]) Article 25, paragraphes 1 et 3, de la loi sur la CNDH.
([277]) Article 25, paragraphe 4, de la loi sur la CNDH.
([278]) Par exemple, de 2015 à 2019, la CNDH a reçu chaque année entre 1 380 à 1 699 demandes contre des autorités répressives et en a traité un nombre tout aussi élevé (par exemple, elle a traité 1 546 plaintes déposées contre la police en 2018 et 1 249 en 2019); elle a également mené plusieurs enquêtes d'office, telles que décrites plus en détail dans son rapport annuel 2018 (disponible à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) et dans son rapport annuel 2019 (disponible à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Articles 20 et 24 de la loi sur le comité d'audit et d'inspection (la «loi sur le BAI»). Voir annexe II, section 2.3.2.
([280]) Article 2, paragraphe 1, de la loi sur le BAI.
([281]) Article 2, paragraphe 2, de la loi sur le BAI.
([282]) Article 4, paragraphe 1, de la loi sur le BAI.
([283]) Article 5, paragraphe 1, et article 6 de la loi sur le BAI.
([284]) Par exemple, avoir assumé les fonctions de juge, de procureur ou d'avocat pendant au moins dix ans, avoir été fonctionnaire, avoir exercé la fonction de professeur ou occupé un poste de niveau supérieur dans une université pendant au moins huit ans, ou avoir travaillé pendant au moins dix ans dans une entreprise cotée en bourse ou dans une institution financée par les pouvoirs publics (dont cinq ans au moins en qualité de directeur), voir article 7 de la loi sur le BAI. En outre, les commissaires ont l'interdiction de participer à des activités politiques et d'exercer simultanément un mandat au sein de l'Assemblée nationale, d'agences administratives, d'organisations soumises aux audits et aux inspections du BAI ou d'occuper toute autre fonction ou tout autre poste rémunéré(e) (article 9 de la loi sur le BAI).
([285]) Article 8 de la loi sur le BAI.
([286]) Voir, par exemple, article 27 de la loi sur le BAI.
([287]) Articles 24 et 31 à 35 de la loi sur le BAI.
([288]) Article 128 de la loi sur l'Assemblée nationale et articles 2, 3 et 15 de la loi sur les inspections et les enquêtes relatives à l'administration de l'État. Ces inspections incluent les inspections annuelles des affaires gouvernementales dans leur ensemble, mais également les enquêtes relatives à des questions particulières.
([289]) Voir annexe II, section 2.2.3.
([290]) Article 10, paragraphe 1, de la loi sur les inspections et les enquêtes relatives à l'administration de l'État. Voir également articles 128 et 129 de la loi sur l'Assemblée nationale.

illicites ou illégitimes ont eu lieu) ([291]) et rendre public le résultat de ses constatations ([292]). Lorsque l'Assemblée nationale demande que des mesures correctives soient prises — lesquelles peuvent inclure, par exemple, l'octroi d'une indemnisation, l'adoption de mesures disciplinaires ou l'amélioration de procédures internes —, l'autorité publique concernée est tenue d'agir sans délai et de rendre compte du résultat des mesures à l'Assemblée nationale ([293]).

3.2.4. *Voies de recours*

(175) Le système coréen offre différentes possibilités de recours (juridictionnel), notamment d'indemnisation.

(176) Premièrement, la PIPA confère aux particuliers des droits d'accès, de rectification, de suppression et de suspension en ce qui concerne les données à caractère personnel traitées à des fins répressives ([294]).

(177) Deuxièmement, les particuliers peuvent utiliser les différents mécanismes de recours offerts par la PIPA si leurs données ont été traitées par une autorité répressive en violation de la PIPA ou en violation des limitations et des garanties régissant la collecte des données à caractère personnel prévues dans d'autres lois (à savoir, le CPP ou la CPPA, voir considérant 171). En particulier, les personnes peuvent introduire une plainte auprès de la PIPC [notamment par le biais du centre d'appel consacré à la protection de la vie privée opéré par l'agence coréenne de l'internet et de la sécurité ([295])] ou du comité de médiation des litiges relatifs aux informations à caractère personnel ([296]). Ces possibilités de recours ne sont pas soumises à d'autres exigences en matière de recevabilité. Sur la base de la loi sur le contentieux administratif, les personnes peuvent en outre former un recours contre les décisions ou l'inaction de la PIPC (voir considérant 132).

(178) Troisièmement, toute personne ([297]) peut déposer plainte auprès de la CNDH pour violation du droit à la protection de la vie privée et des données par une autorité répressive coréenne. La CNDH peut recommander la rectification ou l'amélioration de toute législation, institution, politique ou pratique en cause ([298]), ou la mise en œuvre de voies de recours comme la médiation ([299]), la cessation de la violation des droits de l'homme, la réparation du préjudice subi et des mesures visant à éviter la répétition de ce type de violations ([300]). Selon la déclaration officielle du gouvernement coréen (section 2.4.2 de l'annexe II), ces recommandations peuvent inclure la suppression des données à caractère personnel collectées de manière illicite. Bien que la CNDH n'ait pas le pouvoir de prononcer des décisions contraignantes, elle offre des voies de recours plus informelles, abordables et facilement accessibles, en particulier car, comme expliqué à l'annexe II, section 2.4.2, il n'est pas nécessaire de démontrer qu'un préjudice réel a eu lieu pour qu'une plainte soit examinée ([301]). Cela permet de garantir que les plaintes de particuliers portant sur la collecte de leurs données seront examinées, même si la personne concernée n'est pas en mesure de démontrer que ses données ont effectivement été collectées (par exemple parce que la notification à cette personne n'a pas encore eu lieu). Les rapports annuels d'activités de la CNDH montrent que les individus utilisent également cette voie de recours en pratique pour contester les activités des autorités répressives, notamment en ce qui concerne le traitement de leurs données à caractère personnel ([302]). Si une personne n'est

([291]) Article 16, paragraphe 2, de la loi sur les inspections et les enquêtes relatives à l'administration de l'État.
([292]) Article 12-2 de la loi sur les inspections et les enquêtes relatives à l'administration de l'État.
([293]) Article 16, paragraphe 3, de la loi sur les inspections et les enquêtes relatives à l'administration de l'État.
([294]) Ces droits peuvent être exercés directement à l'égard de l'autorité compétente, ou indirectement par l'intermédiaire de la PIPC (article 35, paragraphe 2, de la PIPA). Comme décrit plus en détail aux considérants 76 à 78, les dérogations à ces droits ne s'appliqueront que lorsque cela est nécessaire pour protéger des intérêts (publics) importants.
([295]) Article 62 de la PIPA.
([296]) Articles 40 à 50 de la PIPA et articles 48-2 à 57 du décret d'application de la PIPA. Voir également annexe II, section 2.4.1.
([297]) Comme précisé à l'annexe II, section 2.4.2, bien que l'article 4 de la loi sur la CNDH fasse référence aux citoyens et étrangers résidant en République de Corée, le terme «résidant» renvoie à la notion de juridiction plutôt qu'à celle de territoire. Par conséquent, si les droits fondamentaux d'un étranger résidant hors de Corée sont violés par des institutions nationales en Corée, cette personne peut déposer une plainte auprès de la CNDH. Tel serait le cas si les données à caractère personnel d'un étranger transférées vers la Corée étaient consultées de manière illicite par des autorités publiques coréennes. Voir en particulier les explications fournies à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2
([298]) Article 44 de la loi sur la CNDH.
([299]) Une personne peut également demander le règlement de la plainte par voie de médiation, voir articles 42 et suivants de la loi sur la NRHC.
([300]) Article 42, paragraphe 4, de la loi sur la CNDH. En outre, la CNDH peut adopter des mesures correctives urgentes dans le cas d'une violation continue qui est susceptible de causer un préjudice difficilement réparable si rien n'est fait, voir article 48 de la loi sur la CNDH.
([301]) Une plainte doit en principe être introduite dans un délai d'un an à partir de la violation, mais la CNDH peut néanmoins décider d'enquêter sur une plainte introduite après cette période pour autant que le délai de prescription prévu par le droit pénal ou civil n'ait pas expiré (article 32, paragraphe 1, point 4, de la loi sur la CNDH).
([302]) Par exemple, la CNDH a, dans le passé, traité des plaintes et formulé des recommandations concernant des saisies illicites et une violation de l'obligation d'informer les personnes de la saisie (voir p. 80 et 91 du rapport annuel 2018 de la CNDH, disponible à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), ainsi que le traitement illicite d'informations à caractère personnel par la police, le ministère public et les juridictions (voir p. 157 et 158 du rapport annuel 2019 de la CNDH, disponible à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, et p. 76 de ce rapport, disponible à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

pas satisfaite de l'issue d'une procédure devant la CNDH, elle peut contester les décisions [telles que la décision de ne pas poursuivre l'enquête sur une plainte ([303])] et les recommandations de la CNDH devant les juridictions coréennes en vertu de la loi sur le contentieux administratif (voir considérant 181) ([304]). En outre, une procédure devant la CNDH peut faciliter encore davantage l'accès à la justice, dans la mesure où un individu peut obtenir d'autres recours contre l'autorité publique qui a traité ses données de manière illicite sur la base des conclusions de la CNDH, conformément aux procédures décrites aux considérants 181 à 183.

(179) Pour finir, les personnes ont accès à différentes voies de recours qui leur permettent d'invoquer les limitations et les garanties décrites à la section 3.2.1 pour obtenir réparation ([305]).

(180) S'agissant des saisies (y compris de données), le CPP prévoit la possibilité de s'opposer à l'exécution d'un mandat ou de la contester au moyen d'une «quasi-plainte» en déposant une requête auprès de la juridiction compétente en vue d'annuler ou de modifier une disposition prise par un procureur ou un agent de police ([306]).

(181) Plus généralement, les particuliers peuvent contester les actions ([307]) ou les omissions ([308]) des autorités publiques (y compris des autorités répressives) en vertu de la loi sur le contentieux administratif ([309]). Une action administrative est considérée comme une «disposition contestable» si elle a une incidence directe sur les droits et les devoirs civils ([310]), ce qui, comme l'a confirmé le gouvernement coréen (section 2.4.3 de l'annexe II), est le cas des mesures visant à collecter des données à caractère personnel, que ce soit directement (par exemple, en interceptant des communications) ou par le biais d'une demande de divulgation contraignante (par exemple, auprès d'un fournisseur de services) ou d'une demande de coopération volontaire. Pour qu'une plainte introduite sur la base de la loi sur le contentieux administratif soit recevable, une personne doit avoir un intérêt juridique à poursuivre la demande ([311]). Conformément à la jurisprudence de la Cour suprême, un «intérêt juridique» est interprété comme un «intérêt protégé par le droit», à savoir un intérêt direct et spécifique protégé par les lois et réglementations sur lesquelles les dispositions administratives sont fondées (par opposition aux intérêts généraux, indirects et abstraits du public) ([312]). Les personnes ont un tel intérêt juridique en cas de violation des limitations et des garanties qui s'appliquent à la collecte de leurs données à caractère personnel à des fins répressives (en vertu de lois spécifiques ou de la PIPA). Sur la base de la loi sur le contentieux administratif, une juridiction peut décider d'annuler ou de modifier une disposition illégale, prononcer sa nullité (c'est-à-dire, déclarer que la disposition n'a pas d'effets juridiques ou n'existe pas dans l'ordre juridique) ou conclure qu'une omission est illégale ([313]). Un jugement définitif rendu au titre de la loi sur le contentieux administratif est contraignant pour les parties ([314]).

([303]) Par exemple, si la CNDH n'est exceptionnellement pas en mesure d'inspecter certains éléments ou équipements, car ces derniers concernent ou contiennent des secrets d'État susceptibles d'affecter substantiellement la sécurité nationale ou les relations diplomatiques, ou lorsque l'inspection risque de constituer un obstacle sérieux à une enquête pénale ou un procès en cours et que cela l'empêche de conduire l'enquête nécessaire pour évaluer le bien-fondé de la demande reçue, elle informera la personne des raisons pour lesquelles la plainte a été rejetée, conformément à l'article 39 de la loi sur la CNDH. Dans ce cas, la personne pourrait contester la décision de la CNDH sur la base de la loi sur le contentieux administratif.

([304]) Voir, par exemple, arrêt 2007Nu27259 de la Haute Cour de Séoul du 18 avril 2008, confirmé par l'arrêt 2008Du7854 de la Cour suprême du 9 octobre 2008; et décision 2017Nu69382 de la Haute Cour de Séoul du 2 février 2018.

([305]) Voir annexe II, section 2.4.3.

([306]) Article 417 du CPP, en liaison avec son article 414, paragraphe 2. Voir également décision 97Mo66 de la Cour suprême du 29 septembre 1997.

([307]) La loi sur le contentieux administratif fait référence à des «dispositions», à savoir l'exercice de la puissance publique, ou le refus d'exercer celle-ci, dans un cas précis.

([308]) En vertu de la loi sur le contentieux administratif, une omission désigne le fait qu'une agence administrative ne prenne pas une certaine disposition pendant une période prolongée contrairement à une obligation légale en la matière.

([309]) Un recours administratif peut en premier lieu être introduit devant une commission des recours administratifs établie par certaines autorités publiques (par exemple, le NIS, la CNDH) ou, de manière plus informelle, devant la commission centrale des recours administratifs instituée par la Commission pour la lutte contre la corruption et les droits civils (article 6 de la loi sur les recours administratifs et article 18, paragraphe 1, de la loi sur le contentieux administratif). Toutefois, une demande peut également être directement introduite devant les juridictions coréennes sur la base de la loi sur le contentieux administratif.

([310]) Arrêts de la Cour suprême 98Du18435 du 22 octobre 1999, 99Du1113 du 8 septembre 2000 et 2010Du3541 du 27 septembre 2012.

([311]) Articles 12, 35 et 36 de la loi sur le contentieux administratif. En outre, une demande d'annulation/de modification d'une disposition et une demande de confirmation de l'illégalité d'une omission doivent être introduites dans un délai de 90 jours à compter de la date à laquelle la personne a eu connaissance de la disposition/l'omission et, en principe, au plus tard un an à partir de la date d'exécution de la disposition ou de survenance de l'omission, sauf s'il existe des raisons justifiables (article 20 et article 38, paragraphe 2, de la loi sur le contentieux administratif). La notion de «raisons justifiables» a été interprétée au sens large par la Cour suprême et nécessite d'évaluer s'il est socialement acceptable d'autoriser l'introduction d'une plainte en retard, à la lumière des circonstances de l'affaire (arrêt 90Nu6521 de la Cour suprême du 28 juin 1991). Ainsi que l'a confirmé le gouvernement coréen à la section 2.4.3 de l'annexe II, cette notion inclut (entre autres) des motifs de retard pour lesquels la partie concernée ne saurait être tenue pour responsable (c'est-à-dire, une situation échappant au contrôle du plaignant, par exemple lorsqu'il n'a pas été informé de la collecte de ses informations à caractère personnel) ou un cas de force majeure (par exemple, une catastrophe naturelle, une guerre, etc.).

([312]) Arrêt 2006Du330 de la Cour suprême du dimanche 26 mars 2006.

([313]) Articles 2 et 4 de la loi sur le contentieux administratif.

([314]) Article 30, paragraphe 1, de la loi sur le contentieux administratif.

(182) En plus de contester les actions du gouvernement par voie de procédure administrative, les particuliers peuvent également introduire une plainte constitutionnelle auprès de la Cour constitutionnelle concernant toute violation de leurs droits fondamentaux résultant de l'exercice ou de l'absence d'exercice d'un pouvoir gouvernemental (à l'exclusion des jugements des juridictions) ([315]). Si d'autres voies de recours sont disponibles, celles-ci doivent être épuisées en premier lieu. Conformément à la jurisprudence de la Cour constitutionnelle, les ressortissants étrangers peuvent déposer une plainte constitutionnelle dans la mesure où leurs droits fondamentaux sont reconnus par la Constitution coréenne (voir explications figurant à la section 1.1) ([316]). La Cour constitutionnelle peut invalider l'exercice du pouvoir gouvernemental ayant entraîné la violation ou confirmer le caractère non constitutionnel d'un défaut d'action particulier ([317]). Dans ce cas, l'autorité concernée doit prendre des mesures en vue de se conformer à la décision de la Cour.

(183) Par ailleurs, les personnes peuvent obtenir une indemnisation devant les juridictions coréennes. Cette voie de recours inclut avant tout la possibilité de réclamer des dommages-intérêts en cas de violations de la PIPA commises par des autorités répressives, conformément à son article 39 (voir également considérant 135). Plus généralement, les personnes peuvent demander la réparation des préjudices causés par des agents publics dans l'exercice de leurs fonctions officielles en violation du droit, sur la base de la loi sur l'indemnisation publique (voir également considérant 135) ([318]).

(184) Les mécanismes décrits aux considérants 176 à 183 mettent à la disposition des personnes concernées des moyens de recours administratif et judiciaire effectif, qui leur permettent en particulier de faire valoir leurs droits, notamment le droit d'accéder aux données à caractère personnel les concernant ou d'obtenir la rectification ou l'effacement de ces données.

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

(185) Le droit de la République de Corée impose un certain nombre de limitations et de garanties en ce qui concerne l'accès aux données à caractère personnel et l'utilisation de celles-ci à des fins de sécurité nationale. Il prévoit également des mécanismes de surveillance et de recours qui sont conformes aux exigences visées aux considérants 141 à 143 de la présente décision. Les conditions dans lesquelles un tel accès peut intervenir et les garanties applicables à l'utilisation de ces pouvoirs sont évaluées en détail dans les sections suivantes.

3.3.1. *Bases juridiques, limitations et garanties*

(186) En République de Corée, les données à caractère personnel peuvent être consultées à des fins de sécurité nationale sur la base de la CPPA, de la TBA et de la loi sur la lutte contre le terrorisme pour la protection des citoyens et de la sécurité publique (la «loi antiterroriste») ([319]). L'autorité principale ([320]) compétente en matière de sécurité nationale est le Service national de renseignement (le «NIS») ([321]). La collecte et l'utilisation des données à caractère

([315]) Article 68, paragraphe 1, de la loi sur la Cour constitutionnelle. Les plaintes constitutionnelles doivent être introduites dans un délai de 90 jours à compter de la date à laquelle la personne a eu connaissance de la violation, et dans un délai d'un an après sa survenance. Comme expliqué également à l'annexe II, section 2.4.3, étant donné que la procédure prévue par la loi sur le contentieux administratif s'applique aux litiges relevant de la loi sur la Cour constitutionnelle conformément à son article 40, une plainte sera toujours recevable s'il existe des «raisons justifiables», telles qu'interprétées conformément à la jurisprudence de la Cour suprême décrite à la note de bas de page 312. Tandis que d'autres voies de recours doivent être épuisées en premier lieu, une plainte constitutionnelle doit être introduite dans un délai de 30 jours à compter de la décision définitive concernant ladite voie de recours (article 69 de la loi sur la Cour constitutionnelle).

([316]) Arrêt 99HeonMa194 de la Cour constitutionnelle du 29 novembre 2001.

([317]) Article 75, paragraphe 3, de la loi sur la Cour constitutionnelle.

([318]) Article 2, paragraphe 1, de la loi sur l'indemnisation publique.

([319]) Voir annexe II, section 3.1.

([320]) À titre exceptionnel, la police et le ministère public peuvent également collecter des informations à caractère personnel à des fins de sécurité nationale (voir note de bas de page 327 et annexe II, section 3.2.1.2). En outre, l'agence de renseignement militaire coréenne (le commandement du soutien de la défense et de la sécurité, qui est établi par le ministère de la défense) dispose de pouvoirs dans le domaine de la sécurité nationale. Toutefois, comme expliqué à l'annexe II, section 3.1, le commandement du soutien de la défense et de la sécurité est responsable uniquement du renseignement militaire et n'exerce une surveillance sur les civils que lorsque cela est nécessaire à l'exercice de ses fonctions militaires. En particulier, il ne peut enquêter que sur le personnel militaire, les salariés civils des forces armées, les personnes suivant une formation militaire, les réservistes, les nouvelles recrues et les prisonniers de guerre (article 1er de la loi sur les tribunaux militaires). Lorsqu'il collecte des informations de communications à des fins de sécurité nationale, le commandement du soutien de la défense et de la sécurité est soumis aux limitations et aux garanties prévues par la CPPA et son décret d'application.

([321]) Le mandat du NIS consiste à collecter, à compiler et à diffuser des informations sur les pays étrangers (à savoir, des informations générales concernant les tendances et les évolutions liées aux pays étrangers, ou les activités d'acteurs publics); des renseignements liés au contre-espionnage (y compris à l'espionnage militaire et industriel), au terrorisme et aux activités d'organisations criminelles internationales; des renseignements sur certains types d'infractions visant le public et la sécurité nationale (par exemple, l'insurrection nationale, l'agression étrangère) et des renseignements liés à la mission visant à assurer la cybersécurité et à prévenir les cyberattaques et les cybermenaces ou à lutter contre celles-ci (article 4, paragraphe 2, de la loi sur le NIS). Voir également annexe II, section 3.1.

personnel par le NIS doivent être conformes aux exigences légales applicables (y compris à la PIPA et à la CPPA) ([322]) et aux lignes directrices générales élaborées par le président de la République et examinées par l'Assemblée nationale ([323]). En règle générale, le NIS doit maintenir la neutralité politique et protéger les libertés et les droits des personnes ([324]). En outre, le personnel du NIS ne doit pas abuser de son autorité officielle en vue de contraindre une institution, une organisation ou une personne à accomplir une action sans qu'elle y soit (légalement) tenue ni empêcher une personne d'exercer ses droits ([325]).

3.3.1.1. Accès aux informations de communications

(187) Sur la base de la CPPA, les autorités publiques coréennes ([326]) peuvent collecter des données de confirmation des communications (à savoir, la date, l'heure de début et l'heure de fin des télécommunications, le nombre d'appels sortants et entrants ainsi que le numéro d'abonné de l'autre partie, la fréquence d'utilisation, les journaux relatifs à l'utilisation des services de télécommunications et les informations de localisation, voir considérant 155) et le contenu des communications (par le biais de mesures de restriction des communications, voir considérant 155) à des fins de sécurité nationale (telles que déterminées par le mandat du NIS, voir note de bas de page 322 ci-dessus). Ces pouvoirs s'étendent à deux types d'informations: 1) les communications dont une ou les deux partie (s) sont des ressortissants coréens ([327]); et 2) les communications a) de pays hostiles à la République de Corée, b) d'agences, de groupes ou de ressortissants étrangers soupçonnés d'être impliqués dans des activités préjudiciables à la Corée ([328]), ou c) de membres de groupes opérant au sein de la péninsule coréenne, mais hors de la souveraineté de la République de Corée, et dont les groupes centraux sont établis dans des pays étrangers ([329]). Les communications des citoyens de l'UE transférées depuis l'Union vers la République de Corée sur la base de la présente décision peuvent donc être collectées en vertu de la CPPA à des fins de sécurité nationale (sous réserve des conditions énoncées aux considérants 188 à 192) si elles ont lieu entre un citoyen de l'UE et un ressortissant coréen ou, lorsque les communications ont lieu exclusivement entre des ressortissants non coréens, si elles relèvent de l'une des trois catégories mentionnées au point 2 a), b) et c).

(188) Dans ces deux scénarios, la collecte de données de confirmation des communications ne peut avoir lieu que dans le but de prévenir les menaces pour la sécurité nationale ([330]), tandis que les mesures de restriction des communications ne peuvent être prises que s'il existe un risque grave pour la sécurité nationale et si la collecte est nécessaire pour prévenir celui-ci ([331]). En outre, le contenu des communications ne peut être consulté qu'en dernier recours et des efforts doivent être déployés pour réduire au minimum la violation de la confidentialité des communications ([332]), de manière à garantir qu'elle reste proportionnée à l'objectif de sécurité nationale poursuivi. La collecte du contenu des communications et des données de confirmation des communications ne peut se prolonger au-delà d'une période maximale de quatre mois, et doit être immédiatement abandonnée si l'objectif poursuivi est atteint plus tôt ([333]). Si les conditions pertinentes continuent d'être remplies, la période peut être prolongée moyennant l'autorisation préalable d'une juridiction (pour les mesures décrites au considérant 189) ou du président de la République (pour les mesures décrites au considérant 190) ([334]), pour une durée maximale de quatre mois.

(189) Les mêmes garanties procédurales s'appliquent à la collecte des données de confirmation des communications et du contenu des communications ([335]). En particulier, si au moins une des personnes participant à la communication est un ressortissant coréen, l'agence de renseignement doit présenter une demande écrite au parquet

([322]) Voir également articles 14, 22 et 23 de la loi sur le NIS.
([323]) Article 4, paragraphe 2, de la loi sur le NIS.
([324]) Article 3, paragraphe 1, article 6, paragraphe 2, et articles 11 et 21 de la loi sur le NIS. Voir également les règles relatives aux conflits d'intérêts, en particulier les articles 10 et 12 de la loi sur le NIS.
([325]) Article 13 de la loi sur le NIS.
([326]) Cela inclut les agences de renseignement (à savoir, le NIS et le commandement du soutien de la défense et de la sécurité) et la police/le ministère public.
([327]) Article 7, paragraphe 1, point 1, de la CPPA.
([328]) Comme l'a expliqué le gouvernement coréen dans la note de bas de page 244 de l'annexe II, il s'agit d'activités qui menacent l'existence et la sécurité de la nation, l'ordre démocratique ou la survie et la liberté des personnes.
([329]) Article 7, paragraphe 1, point 2, de la CPPA.
([330]) Article 13-4 de la CPPA.
([331]) Article 7, paragraphe 1, de la CPPA.
([332]) Article 3, paragraphe 2, de la CPPA. En outre, les mesures de restriction des communications doivent être immédiatement abandonnées lorsqu'elles ne sont plus nécessaires, de manière à garantir que toute violation de la confidentialité des communications de la personne est limitée au minimum (article 2 du décret d'application de la CPPA).
([333]) Article 7, paragraphe 2, de la CPPA.
([334]) La demande visant à obtenir l'autorisation de prolonger les mesures de surveillance doit être effectuée par écrit, en indiquant les raisons de la prolongation demandée et en fournissant des éléments justificatifs (article 7, paragraphe 2, de la CPPA et article 5 du décret d'application de la CPPA).
([335]) Voir article 13-4, paragraphe 2, de la CPPA et article 37, paragraphe 4, du décret d'application de la CPPA, en vertu desquels les procédures applicables à la collecte du contenu des communications s'appliquent également à la collecte des données de confirmation des communications. Voir également annexe II, section 3.2.1.1.1.

supérieur, qui doit à son tour introduire une demande de mandat auprès d'un haut magistrat de la Haute Cour ([336]). La CPPA dresse la liste des informations qui doivent être fournies dans la demande adressée au procureur, la demande de mandat ou le mandat lui-même. Ces informations incluent, en particulier, la justification de la demande et les principaux motifs de suspicion, des éléments justificatifs, ainsi que des informations concernant l'objectif, la cible (c'est-à-dire la ou les personnes ciblées), la portée et la durée de la mesure proposée ([337]). Une collecte sans mandat peut également avoir lieu s'il existe une entente menaçant la sécurité nationale et une urgence qui ne permet pas de passer par les procédures susmentionnées ([338]). Toutefois, dans ce cas également, une demande de mandat doit être immédiatement introduite après que la mesure a été prise ([339]). La CPPA définit donc clairement le champ d'application et les conditions de ces types de collectes et les soumet à des garanties (procédurales) spécifiques (y compris à l'autorisation préalable d'une juridiction) afin de garantir que l'utilisation de telles mesures soit limitée à ce qui est nécessaire et proportionné. En outre, l'obligation de fournir des informations détaillées aussi bien dans la demande de mandat que dans le mandat lui-même exclut la possibilité d'un accès indifférencié aux données.

(190) Dans le cas des communications entre des ressortissants non coréens qui relèvent de l'une des trois catégories spécifiques énumérées au considérant 187, une demande doit être introduite auprès du directeur du NIS, qui, après avoir examiné le caractère approprié des mesures proposées, doit solliciter l'approbation préalable écrite du président de la République de Corée ([340]). La demande préparée par l'agence de renseignement doit inclure les mêmes informations détaillées que celles figurant dans une demande de mandat judiciaire (voir considérant 189), en particulier la justification de la demande et les principaux motifs de suspicion, des éléments justificatifs et des informations concernant les objectifs, la portée et la durée des mesures proposées, ainsi que la ou les personnes ciblées par celles-ci ([341]). Dans des situations d'urgence ([342]), l'autorisation préalable du ministre auquel l'agence de renseignement est rattachée doit être obtenue, bien que l'agence de renseignement doive solliciter l'approbation du président de la République immédiatement après que les mesures d'urgence ont été prises ([343]). En ce qui concerne également la collecte des communications qui ont lieu exclusivement entre des ressortissants non coréens, la CPPA limite donc l'utilisation de ces mesures à ce qui est nécessaire et proportionné, en définissant clairement les catégories restreintes de personnes qui peuvent faire l'objet de telles mesures et en précisant les critères détaillés dont les agences de renseignement doivent démontrer le respect pour justifier une demande de collecte d'informations. En outre, cette limitation exclut de nouveau la possibilité d'un accès indifférencié aux données. En l'absence d'approbation préalable indépendante de ces mesures, une supervision indépendante est assurée ex post par, en particulier, la PIPC et la CNDH (voir, par exemple, considérants 199 et 200).

(191) La CPPA impose en outre plusieurs garanties supplémentaires qui contribuent au contrôle ex post et facilitent l'accès des personnes à des voies de recours effectif. Premièrement, pour tous les types de collectes à des fins de sécurité nationale, la CPPA prévoit différentes exigences en matière de tenue de registres et de déclaration. En particulier, lorsqu'elles adressent une demande de coopération à des opérateurs privés, les agences de renseignement doivent fournir le mandat/l'autorisation présidentielle ou une copie de la couverture d'une déclaration de censure d'urgence que l'entité contrainte doit conserver dans ses dossiers ([344]). Dans le cadre d'une coopération

([336]) Article 6, paragraphes 5 et 8, article 7, paragraphe 1, point 1, et article 7, paragraphe 3, de la CPPA, en liaison avec l'article 7, paragraphes 3 et 4, du décret d'application de la CPPA.

([337]) Voir article 7, paragraphe 3, et article 6, paragraphe 4, de la CPPA (pour les demandes émanant des agences de renseignement), article 4 du décret d'application de la CPPA (pour les demandes introduites par le procureur) et article 7, paragraphe 3, et article 6, paragraphe 6, de la CPPA (pour le mandat).

([338]) Article 8 de la CPPA.

([339]) Article 8, paragraphes 2 et 8, de la CPPA. La collecte doit être immédiatement abandonnée si l'autorisation de la juridiction n'est pas obtenue dans un délai de 36 heures à compter de l'adoption de la mesure. Si la mesure de surveillance est mise en œuvre sur une courte période, excluant ainsi l'autorisation de la juridiction, le chef du bureau du procureur général compétent doit transmettre un avis de mesure d'urgence préparé par l'agence de renseignement au président de la juridiction compétente, lequel, sur cette base, peut examiner la légalité de la collecte (article 8, paragraphes 5 et 7, de la CPPA). Cet avis doit indiquer l'objectif, la cible, la portée, la période, le lieu d'exécution de la surveillance et la méthode de surveillance, ainsi que les motifs justifiant l'absence de demande avant l'adoption de la mesure (article 8, paragraphe 6, de la CPPA). Plus généralement, les agences de renseignement ne doivent prendre des mesures d'urgence qu'en conformité avec une «déclaration de censure/d'écoute d'urgence» et doivent tenir des registres relatifs à ces mesures (article 8, paragraphe 4, de la CPPA).

([340]) Article 8, paragraphes 1 et 2, du décret d'application de la CPPA.

([341]) Article 8, paragraphe 3, du décret d'application de la CPPA, en liaison avec l'article 6, paragraphe 4, de la CPPA.

([342]) C'est-à-dire des situations dans lesquelles, lorsque la mesure vise une entente qui menace la sécurité nationale, il n'y a pas suffisamment de temps pour obtenir l'approbation du président de la République et la non-adoption des mesures d'urgence peut porter atteinte à la sécurité nationale (article 8, paragraphe 8, de la CPPA).

([343]) Article 8, paragraphe 9, de la CPPA. La collecte doit être immédiatement abandonnée si l'autorisation n'est pas obtenue dans un délai de 36 heures à partir du moment où la demande est introduite.

([344]) Article 9, paragraphe 2, de la CPPA et article 12 du décret d'application de la CPPA. Voir article 13 du décret d'application de la CPPA concernant la possibilité d'obtenir par voie de contrainte l'aide des bureaux de poste et des fournisseurs de services de télécommunications. Les opérateurs privés auxquels il est demandé de divulguer des informations peuvent refuser lorsque le mandat/l'autorisation ou la déclaration de censure d'urgence mentionne un identifiant erroné (par exemple, un numéro de téléphone appartenant à une personne autre que celle identifiée). En tout état de cause, il leur est interdit de divulguer les mots de passe utilisés pour les communications (article 9, paragraphe 4, de la CPPA).

par voie de contrainte, l'autorité publique à l'origine de la demande et l'opérateur concerné doivent conserver les documents relatifs à l'objectif et à l'objet des mesures, ainsi qu'à la date d'exécution ([345]). En outre, les agences de renseignement doivent rendre compte des informations recueillies et du résultat de l'activité de surveillance au directeur du NIS ([346]).

(192) Deuxièmement, les personnes doivent être informées par notification de la collecte de leurs données (données de confirmation ou contenu des communications) à des fins de sécurité nationale si celle-ci concerne des communications dont au moins l'une des parties est un ressortissant coréen ([347]). Cette notification doit être effectuée par écrit dans un délai de 30 jours à compter de la date de fin de la collecte (y compris lorsque les données ont été obtenues conformément à la procédure d'urgence) et ne peut être différée que si et aussi longtemps qu'elle menace la sécurité nationale ou porte atteinte à la vie et à la sécurité physique des personnes ([348]). Indépendamment de cette notification, les personnes disposent de différentes voies de recours, comme expliqué plus en détail à la section 3.3.4.

3.3.1.2. Collecte d'informations sur les individus soupçonnés d'activités terroristes

(193) La loi antiterroriste dispose que le NIS peut collecter des données concernant des individus soupçonnés d'activités terroristes ([349]) dans le respect des limitations et des garanties prévues par d'autres lois ([350]). En particulier, le NIS peut obtenir des données de communications (sur la base de la CPPA) et d'autres informations à caractère personnel (par le biais d'une demande de divulgation volontaire) ([351]). En ce qui concerne la collecte d'informations de communications (à savoir, le contenu ou les données de confirmation des communications), les limitations et les garanties décrites à la section 3.3.1.1 s'appliquent, notamment l'obligation d'obtenir un mandat approuvé par une juridiction. S'agissant des demandes de divulgation volontaire d'autres types de données à caractère personnel concernant des individus soupçonnés d'activités terroristes, le NIS doit se conformer aux exigences de nécessité et de proportionnalité prévues dans la Constitution et la PIPA (voir considérant 164) ([352]). Les responsables du traitement recevant de telles demandes peuvent satisfaire à celles-ci sur une base volontaire dans les conditions énoncées dans la PIPA (par exemple, conformément au principe de minimisation des données et en limitant l'incidence sur la vie privée de la personne) ([353]). Dans ce cas, ils doivent également se conformer à l'obligation d'informer la personne concernée imposée par la notification 2021-5 (voir considérant 166).

([345]) S'agissant des mesures de restriction des communications, ces documents doivent être conservés pendant trois ans, voir article 9, paragraphe 3, de la CPPA et article 17, paragraphe 2, du décret d'application de la CPPA. Pour ce qui est des données de confirmation des communications, les agences de renseignement doivent conserver les documents attestant du fait qu'une demande relative à de telles données a été effectuée, ainsi que la demande écrite elle-même, et de l'institution qui s'appuie sur celle-ci (article 13, paragraphe 5, et article 13-4, paragraphe 3, de la CPPA). Les fournisseurs de services de télécommunications doivent conserver ces documents pendant sept ans et rendre compte deux fois par an au ministre des sciences et des TIC de la fréquence de ces divulgations (article 9, paragraphe 3, de la CPPA, en liaison avec l'article 13, paragraphe 7, de la CPPA, et article 37, paragraphe 4, et article 39 du décret d'application de la CPPA).

([346]) Article 18, paragraphe 3, du décret d'application de la CPPA.

([347]) Article 9-2, paragraphe 3, et article 13-4 de la CPPA. La notification doit mentionner 1) le fait que les informations ont été collectées, 2) l'agence d'exécution et 3) la période d'exécution.

([348]) Article 9-2, paragraphe 4, de la CPPA. Dans ce cas, la notification doit être envoyée dans un délai de 30 jours dès que les motifs du report cessent d'exister, voir article 13-4, paragraphe 2, et article 9-2, paragraphe 6, de la CPPA.

([349]) C'est-à-dire, les membres d'un groupe terroriste (tel que désigné par les Nations unies, voir article 2, paragraphe 2, de la loi antiterroriste); les personnes qui promeuvent et diffusent les idées ou les tactiques d'un groupe terroriste, qui collectent des fonds destinés à des activités terroristes ou qui contribuent à ces fonds, ou celles qui se livrent à d'autres activités de préparation, de conspiration, de propagande ou d'incitation en vue de la commission d'actes terroristes; ou les personnes pour lesquelles il existe de bonnes raisons de soupçonner qu'elles se sont livrées à de telles activités (article 2, paragraphe 3, de la loi antiterroriste). Le «terrorisme» est défini par l'article 2, paragraphe 1, de la loi antiterroriste comme une conduite visant à entraver l'exercice de l'autorité de l'État, d'un pouvoir public local ou d'un pouvoir public étranger (y compris d'une organisation internationale), à obliger celui-ci à prendre des mesures sans qu'il y soit légalement tenu ou à menacer le public. Une telle conduite peut inclure, par exemple, le meurtre, le kidnapping ou la prise d'otage; le détournement/la capture illicite, la destruction ou l'endommagement d'un navire ou d'un aéronef; l'utilisation d'armes biochimiques, explosives ou incendiaires dans le but de causer la mort, des blessures graves ou des dommages; et l'utilisation malveillante de matières nucléaires ou radioactives.

([350]) Article 9, paragraphes 1 et 3, de la loi antiterroriste.

([351]) Bien que la loi antiterroriste mentionne la possibilité de collecter des informations à l'entrée en République de Corée et à la sortie de celle-ci sur la base de la loi sur l'immigration et de la loi douanière, ces lois ne prévoient pas une telle habilitation (voir section 3.2.2.1 de l'annexe II). En tout état de cause, elles ne s'appliqueraient pas en principe aux données transférées sur la base de la présente décision, car elles concernent généralement des informations qui sont directement collectées par les autorités coréennes (et non l'accès à des données qui ont été préalablement transférées depuis l'Union vers des responsables du traitement coréens). De plus, la loi antiterroriste cite entre autres l'ARUSFTI comme base légale de la collecte des informations sur les transactions financières. Toutefois, comme expliqué à la note de bas de page 200, les types de données qui peuvent être obtenues sur la base de cette loi ne relèvent pas du champ d'application de la présente décision. Enfin, la loi antiterroriste prévoit également que le NIS peut collecter des informations de localisation par le biais de demandes non contraignantes, auquel cas les fournisseurs d'informations de localisation pourraient volontairement divulguer ces informations dans les conditions énoncées dans la PIPA (telles que décrites au considérant 193) et la loi sur les informations de localisation. Cependant, comme expliqué à la note de bas de page 17, les informations de localisation ne seraient pas transférées depuis l'Union vers des responsables du traitement coréens sur la base de la présente décision, mais seraient plutôt générées à l'intérieur de la Corée.

([352]) Voir annexe II, section 3.2.2.2.

([353]) Voir article 58, paragraphe 4, de la PIPA, qui exige que le traitement des informations à caractère personnel soit limité au minimum nécessaire pour atteindre la finalité visée, et article 3, paragraphe 6, de la PIPA, qui dispose que les informations à caractère personnel doivent être traitées de manière à réduire au minimum la possibilité de violer la vie privée de la personne. Voir également article 59, points 2 et 3, de la PIPA, qui interdit aux responsables du traitement de divulguer des informations à caractère personnel à des tiers sans autorisation.

3.3.1.3. Demandes de divulgation volontaire de données d'abonnés

(194) Sur la base de la TBA, les opérateurs de télécommunications peuvent divulguer volontairement des données d'abonnés (voir considérant 163) à la demande d'une agence de renseignement qui souhaite collecter ces informations en vue de prévenir une menace pour la sécurité nationale ([354]). Dans le cas de telles demandes du NIS, les mêmes limitations (découlant de la Constitution, de la PIPA et de la TBA) que celles prévues dans le domaine répressif, telles que décrites au considérant 164, s'appliquent ([355]). Les opérateurs de télécommunications ne sont pas tenus de satisfaire auxdites demandes et ne peuvent le faire que dans les conditions énoncées dans la PIPA (en particulier, conformément au principe de minimisation des données et en limitant l'incidence sur la vie privée de la personne, voir également considérant 193). Les mêmes obligations que celles prévues dans le domaine répressif en matière de tenue de registres et de notification de la personne concernée s'appliquent (voir considérants 165 et 166).

3.3.2. *Utilisation ultérieure des informations recueillies*

(195) Le traitement des données à caractère personnel collectées par les autorités coréennes à des fins de sécurité nationale est soumis aux principes de limitation des finalités (article 3, paragraphes 1 et 2, de la PIPA), de licéité et de loyauté du traitement (article 3, paragraphe 1, de la PIPA), de proportionnalité/minimisation des données (article 3, paragraphes 1 et 6, et article 58 de la PIPA), d'exactitude (article 3, paragraphe 3, de la PIPA), de transparence (article 3, paragraphe 5, de la PIPA), de sécurité (article 58, paragraphe 4, de la PIPA), et de limitation de la conservation (article 58, paragraphe 4, de la PIPA) ([356]). La divulgation possible de données à caractère personnel à des tiers (y compris à des pays tiers) ne peut avoir lieu que dans le respect de ces principes (en particulier de ceux de limitation des finalités et de minimisation des données), après examen du respect des principes de nécessité et de proportionnalité (article 37, paragraphe 2, de la Constitution) et compte tenu de l'incidence sur les droits des personnes concernées (article 3, paragraphe 6, de la PIPA).

(196) En ce qui concerne le contenu des communications et les données de confirmation des communications, la CPPA limite en outre l'utilisation de ces données aux procédures judiciaires, lorsqu'une partie liée à la communication se fonde sur celles-ci dans le cadre d'une demande d'indemnisation; ou autorise leur utilisation en vertu d'autres lois ([357]).

3.3.3. *Surveillance*

(197) Les activités des autorités nationales de sécurité coréennes sont supervisées par différents organismes ([358]).

(198) Premièrement, la loi antiterroriste prévoit des mécanismes de surveillance pour les activités de lutte contre le terrorisme, notamment la collecte des données concernant les individus soupçonnés d'activités terroristes. En particulier, au niveau de l'exécutif, les activités de lutte antiterroriste sont supervisées par la Commission de lutte contre le terrorisme ([359]), à laquelle le directeur du NIS doit rendre compte du traçage des individus soupçonnés d'activités terroristes et des enquêtes les concernant pour collecter des informations ou des éléments nécessaires aux activités de lutte antiterroriste ([360]). En outre, le délégué à la protection des droits de l'homme (ci-après le «HRPO») surveille spécifiquement le respect des droits fondamentaux dans les activités de lutte antiterroriste ([361]). Le HRPO est nommé par le président de la Commission de lutte contre le terrorisme parmi des personnes qui possèdent les qualifications spécifiques énumérées dans le décret d'application de la loi antiterroriste ([362]) pour un mandat (renouvelable) d'une durée de deux ans, et ne peut être démis de ses fonctions que pour des motifs spécifiques et limités et pour une raison valable ([363]). Dans l'exercice de sa fonction de surveillance, le HRPO peut

([354]) Article 83, paragraphe 3, de la TBA.
([355]) Voir également annexe II, section 3.2.3.
([356]) Voir annexe II, section 1.2.
([357]) Article 5, paragraphes 1 et 2, et articles 12 et 13-5 de la CPPA.
([358]) Voir annexe II, section 3.3.
([359]) Article 5, paragraphe 3, de la loi antiterroriste. La Commission est présidée par le Premier ministre et se compose de plusieurs ministres et directeurs d'agences gouvernementales, tels que les ministres des affaires étrangères, de la justice, de la défense nationale et de l'intérieur et de la sécurité, le directeur du NIS et le commissaire général de la police nationale (article 3, paragraphe 1, du décret d'application de la loi antiterroriste).
([360]) Article 9, paragraphe 4, de la loi antiterroriste.
([361]) Article 7 de la loi antiterroriste.
([362]) C'est-à-dire, toute personne qualifiée en tant qu'avocat ayant au moins dix ans d'expérience professionnelle, ou ayant des connaissances spécialisées dans le domaine des droits de l'homme et exerçant ou ayant exercé (au moins) la fonction de professeur associé pendant au moins dix ans, ou ayant exercé la fonction de haut fonctionnaire dans des agences d'État ou des pouvoirs locaux, ou ayant au moins dix ans d'expérience professionnelle dans le domaine des droits de l'homme, par exemple dans une organisation non gouvernementale (article 7, paragraphe 1, du décret d'application de la loi antiterroriste).
([363]) Par exemple, en cas de mise en accusation dans une affaire pénale liée à ses fonctions, en cas de divulgation d'informations confidentielles, ou en raison d'une incapacité mentale ou physique (article 7, paragraphe 3, du décret d'application de la loi antiterroriste).

formuler des recommandations générales en vue d'améliorer la protection des droits de l'homme ([364]) et des recommandations spécifiques de mesures correctives si une violation des droits de l'homme a été établie ([365]). Les autorités publiques doivent informer le HRPO du suivi assuré concernant ses recommandations ([366]).

(199) Deuxièmement, la PIPC surveille le respect par les autorités nationales de sécurité des règles en matière de protection des données, qui comprennent à la fois les dispositions applicables de la PIPA (voir considérant 149) et les limitations et garanties qui s'appliquent à la collecte de données à caractère personnel sur la base d'autres lois (la CPPA, la loi antiterroriste et la TBA, voir considérant 171) ([367]). Dans l'exercice de sa fonction de surveillance, la PIPC peut utiliser l'ensemble des pouvoirs d'investigation et de correction à sa disposition, tels que détaillés à la section 2.4.2.

(200) Troisièmement, les activités des autorités nationales de sécurité sont soumises à la surveillance indépendante de la CNDH, conformément aux procédures décrites au considérant 172 ([368]).

(201) Quatrièmement, la fonction de supervision du BAI s'étend également aux autorités nationales de sécurité, bien que le NIS puisse, dans des circonstances exceptionnelles, refuser de fournir certaines informations ou certains éléments, c'est-à-dire lorsque ces derniers constituent des secrets d'État et que leur divulgation entraînerait des conséquences graves pour la sécurité nationale ([369]).

(202) Enfin, le contrôle parlementaire des activités du NIS est exercé par l'Assemblée nationale (par le biais d'un comité du renseignement spécialisé) ([370]). La CPPA attribue à l'Assemblée nationale une fonction de supervision spécifique en ce qui concerne le recours à des mesures de restriction des communications à des fins de sécurité nationale ([371]). En particulier, l'Assemblée nationale peut procéder à des inspections sur place du matériel d'écoute et exiger tant du NIS que des opérateurs de télécommunications ayant divulgué le contenu des communications qu'ils lui en rendent compte. L'Assemblée nationale peut également exercer ses fonctions générales de supervision (conformément aux procédures décrites au considérant 174). La loi sur le NIS impose au directeur du NIS de répondre sans délai à la Commission du renseignement lorsque celle-ci lui demande un rapport sur une question spécifique ([372]), en fixant des règles spécifiques concernant certaines informations particulièrement sensibles. Concrètement, le directeur du NIS peut également refuser de répondre ou de témoigner devant le comité dans des circonstances exceptionnelles, c'est-à-dire si la demande concerne des secrets d'État relatifs à des questions militaires, diplomatiques ou liées à la Corée du Nord, lorsque leur divulgation pourrait avoir de graves conséquences pour le «destin national» du pays ([373]). Dans ce cas, la Commission du renseignement peut demander une explication au Premier ministre et, si aucune explication n'est fournie dans un délai de sept jours, la réponse ou le témoignage ne saurait être refusé.

3.3.4. *Voies de recours*

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

(204) Premièrement, conformément à l'article 3, paragraphe 5, et à l'article 4, paragraphes 1, 3 et 4, de la PIPA, les particuliers peuvent exercer leurs droits d'accès, de rectification, de suppression et de suspension à l'égard des autorités nationales de sécurité. La section 6 de la notification 2021-5 (annexe 1 de la présente décision) précise

([364]) Article 8, paragraphe 1, du décret d'application de la loi antiterroriste.
([365]) Article 9, paragraphe 1, du décret d'application de la loi antiterroriste. Le HRPO décide de manière autonome de l'adoption des recommandations, mais il doit rendre compte de ces recommandations au président de la Commission de lutte contre le terrorisme.
([366]) Article 9, paragraphe 2, du décret d'application de la loi antiterroriste. D'après la déclaration officielle du gouvernement coréen, l'absence de mise en œuvre d'une recommandation du HRPO serait signalée à la Commission de lutte contre le terrorisme, y compris au Premier ministre, bien que, jusqu'à présent, il n'y ait pas eu de cas où les recommandations du HRPO n'ont pas été mises en œuvre (voir section 3.3.1 de l'annexe II).
([367]) Annexe II, section 3.3.4.
([368]) Plus précisément, en ce qui concerne le NIS, la CNDH a, dans le passé, mené des enquêtes d'office et traité un certain nombre de plaintes individuelles. Voir, par exemple, rapport annuel 2018 de la CNDH, p. 128 (disponible à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) et son rapport annuel 2019, p. 70 (disponible à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Article 13, paragraphe 1, de la loi sur le NIS.
([370]) Article 36 et article 37, paragraphe 1, point 15, de la loi sur l'Assemblée nationale.
([371]) Article 15 de la CPPA.
([372]) Article 15, paragraphe 2, de la loi sur le NIS.
([373]) Article 17, paragraphe 2, de la loi sur le NIS. Les «secrets d'État» sont définis comme «des faits, des biens ou des connaissances (classés comme tels) qui ne doivent pas être divulgués à un autre pays ou une autre organisation, afin d'éviter tout préjudice grave pour la sécurité nationale, et dont l'accès n'est autorisé qu'à un nombre limité de personnes. Voir article 13, paragraphe 4, de la loi sur le NIS.

davantage la façon dont ces droits s'appliquent dans le cadre du traitement des données à des fins de sécurité nationale. En particulier, une autorité nationale de sécurité ne peut limiter ou refuser l'exercice de l'un de ces droits que dans la mesure où et aussi longtemps que cela est nécessaire et proportionné pour protéger un objectif important d'intérêt public (par exemple, dans la mesure où et aussi longtemps que l'octroi de ce droit compromettrait une enquête en cours ou menacerait la sécurité nationale), ou lorsque l'octroi de ce droit peut porter atteinte à la vie ou à l'intégrité physique d'un tiers. Invoquer une telle restriction nécessite par conséquent de mettre en balance les droits et les intérêts de la personne avec l'intérêt public concerné et ne saurait en aucun cas porter atteinte à l'essence de ce droit (article 37, paragraphe 2, de la Constitution). Lorsque la demande est refusée ou restreinte, la personne doit être informée sans délai des raisons.

(205) Deuxièmement, les particuliers ont le droit d'obtenir réparation en vertu de la PIPA si leurs données ont été traitées par une autorité nationale de sécurité en violation de cette loi ou des limitations et garanties prévues dans d'autres lois régissant la collecte des données à caractère personnel (en particulier, la CPPA, voir considérant 171) ([374]). Ce droit peut être exercé en introduisant une plainte auprès de la PIPC (y compris par l'intermédiaire du centre d'appel consacré à la protection de la vie privée opéré par l'agence coréenne de l'internet et de la sécurité) ([375]). En outre, afin de faciliter l'accès aux voies de recours contre les autorités nationales de sécurité coréennes, les citoyens de l'UE peuvent déposer plainte auprès de la PIPC par l'intermédiaire de leur autorité nationale de protection des données ([376]). Dans ce cas, la PIPC préviendra la personne concernée (autorité nationale de protection des données) une fois l'enquête terminée (y compris, le cas échéant, en l'informant sur les mesures correctives imposées). Sur la base de la loi sur le contentieux administratif, les personnes peuvent en outre former un recours contre les décisions ou l'inaction de la PIPC (voir considérant 132).

(206) Troisièmement, les particuliers peuvent introduire une plainte auprès du HRPO concernant la violation de leur droit à la protection de la vie privée/des données dans le cadre d'activités de lutte antiterroriste (c'est-à-dire, sur la base de la loi antiterroriste) ([377]), lequel peut recommander une mesure corrective. Étant donné qu'il n'existe aucune exigence en matière de recevabilité devant le HRPO, une plainte sera traitée même si la personne concernée ne peut pas démontrer qu'elle a subi un préjudice réel (par exemple, du fait de la collecte illicite présumée de ses données par une autorité nationale de sécurité) ([378]). L'autorité concernée doit informer le HRPO de toute mesure prise aux fins de la mise en œuvre de ses recommandations.

(207) Quatrièmement, les personnes peuvent introduire une plainte auprès de la CNDH concernant la collecte de leurs données par des autorités nationales de sécurité et obtenir réparation conformément à la procédure décrite au considérant 178 ([379]).

(208) Pour finir, les personnes ont accès à différentes voies de recours ([380]), qui leur permettent d'invoquer les limitations et les garanties décrites à la section 3.3.1 pour obtenir réparation. En particulier, elles peuvent contester la légalité des actions des autorités nationales de sécurité sur la base de la loi sur le contentieux administratif (conformément à la procédure décrite au considérant 181) ou de la loi sur la Cour constitutionnelle (voir considérant 182). Par ailleurs, elles peuvent obtenir réparation du préjudice subi sur la base de la loi sur l'indemnisation publique (telle que décrite plus en détail au considérant 183).

4. **CONCLUSIONS**

(209) La Commission considère que la République de Corée — au moyen de la PIPA, des règles particulières applicables à certains secteurs (telles qu'analysées à la section 2) et des garanties supplémentaires prévues dans la notification 2021-5 (annexe 1) — assure un niveau de protection des données à caractère personnel transférées de l'Union européenne qui est substantiellement équivalent à celui garanti par le règlement (UE) 2016/679.

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

([374]) Article 58, paragraphe 4, et article 4, paragraphe 5, de la PIPA. Voir annexe II, section 3.4.2.
([375]) Article 62 et article 63, paragraphe 2, de la PIPA.
([376]) Notification 2021-5 (annexe I, section 6).
([377]) Article 8, paragraphe 1, point 2, du décret d'application de la loi antiterroriste.
([378]) Voir annexe II, section 3.4.1.
([379]) Par exemple, la CNDH reçoit régulièrement des plaintes contre le Service national de renseignement, voir chiffres relatifs au nombre de plaintes reçues entre 2015 et 2019 dans le rapport annuel 2019 de la CNDH, p. 70 (disponible à l'adresse https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Voir annexe II, section 3.4.4.

(211) Enfin, sur la base des informations disponibles concernant l'ordre juridique coréen, y compris les déclarations, assurances et engagements du gouvernement coréen figurant à l'annexe II, la Commission considère que toute atteinte aux droits fondamentaux des particuliers dont les données à caractère personnel sont transférées de l'Union européenne vers la République de Corée par des autorités publiques coréennes pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale, sera limitée à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridique effective contre les atteintes de cette nature.

(212) Par conséquent, à la lumière des constatations contenues dans la présente décision, il convient de décider que la République de Corée assure un niveau de protection adéquat, au sens de l'article 45 du règlement (UE) 2016/679, interprété à la lumière de la Charte des droits fondamentaux de l'Union européenne, des données à caractère personnel transférées de l'Union européenne vers la République de Corée à des responsables du traitement des données/informations à caractère personnel situés en République de Corée et soumis à la PIPA, à l'exception des organisations religieuses dans la mesure où elles traitent des données à caractère personnel aux fins de leurs activités missionnaires; des partis politiques dans la mesure où ils traitent des données à caractère personnel dans le cadre de la nomination de candidats; et des responsables du traitement qui sont soumis à la surveillance de la Commission des services financiers en ce qui concerne le traitement des informations à caractère personnel en matière de crédit conformément à la loi sur les informations en matière de crédit, dans la mesure où ils traitent de telles informations.

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

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

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

(215) Il convient de rappeler que, comme prévu à l'article 58, paragraphe 5, du règlement (UE) 2016/679 et ainsi que la Cour de justice l'a expliqué dans l'arrêt Schrems ([381]), lorsqu'une autorité nationale chargée de la protection des données met en cause, notamment après avoir été saisie d'une plainte, la compatibilité d'une décision d'adéquation de la Commission avec la protection des droits fondamentaux que constituent le respect de la vie privée et la protection des données, le droit national doit prévoir des voies de recours lui permettant de faire valoir ces griefs devant les juridictions nationales, qui, en cas de doute, doivent surseoir à statuer et procéder à un renvoi préjudiciel devant la Cour de justice ([382]).

6. SUIVI ET EXAMEN DE LA PRÉSENTE DÉCISION

(216) Conformément à la jurisprudence de la Cour de justice ([383]), et comme consacré par l'article 45, paragraphe 4, du règlement (UE) 2016/679, la Commission devrait suivre, de manière permanente, les évolutions dans le pays tiers après l'adoption d'une décision d'adéquation, afin de déterminer si le pays tiers continue de garantir un niveau de protection substantiellement équivalent. Une telle vérification s'impose, en tout état de cause, lorsque la Commission reçoit des informations faisant naître un doute justifié à cet égard.

(217) Par conséquent, la Commission devrait surveiller de manière permanente la situation en République de Corée en ce qui concerne le cadre juridique et la pratique proprement dite de traitement des données à caractère personnel tels qu'évalués dans la présente décision, notamment le respect, par les autorités coréennes, des déclarations, assurances et engagements contenus dans l'annexe II. Pour faciliter ce processus, il est attendu des autorités coréennes qu'elles informent rapidement la Commission de toute évolution importante en rapport avec la présente décision, concernant tant le traitement des données à caractère personnel par les opérateurs économiques et les autorités publiques que les limitations et garanties applicables à l'accès des autorités publiques aux données à caractère personnel.

([381]) Arrêt Schrems, point 65.

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

([383]) Arrêt Schrems, point 76.

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

(219) En application de l'article 45, paragraphe 3, du règlement (UE) 2016/679 ([384]), et au regard du fait que le niveau de protection assuré par l'ordre juridique de la Corée est susceptible d'évoluer, la Commission, après l'adoption de la présente décision, devrait vérifier de manière périodique si les conclusions relatives au niveau adéquat de la protection assurée par la République de Corée sont toujours justifiées en fait et en droit.

(220) À cette fin, la présente décision devrait faire l'objet d'un premier examen dans un délai de trois ans après son entrée en vigueur. Après ce premier examen, et en fonction de son résultat, la Commission se prononcera, en étroite concertation avec le comité institué en vertu de l'article 93, paragraphe 1, du règlement (UE) 2016/679, sur l'opportunité de maintenir, ou non, le cycle de trois ans. En tous les cas, les examens ultérieurs devraient avoir lieu au moins une fois tous les quatre ans ([385]). L'examen devrait couvrir tous les aspects relatifs au fonctionnement de la présente décision et, en particulier, l'application des garanties supplémentaires contenues dans l'annexe I de la présente décision (en accordant une attention particulière aux protections accordées en cas de transferts ultérieurs); les évolutions pertinentes de la jurisprudence; les règles relatives au traitement des informations pseudonymisées à des fins statistiques, de recherche scientifique ou d'archivage dans l'intérêt général, ainsi que l'application des exceptions prévues à l'article 28, paragraphe 7, de la PIPA; le caractère effectif de l'exercice des droits individuels, y compris avant la réforme récente de la PIPC, et l'application des exceptions à ces droits; l'application des dérogations partielles prévues par le PIPA; ainsi que les limitations et garanties en ce qui concerne l'accès des pouvoirs publics aux données (telles qu'exposées à l'annexe II de la présente décision), y compris la coopération de la PIPC avec les autorités européennes de protection des données dans le cadre du traitement des plaintes des particuliers. Il devrait également englober l'efficacité de la surveillance et du contrôle du respect des règles applicables eu égard à la PIPA et dans le domaine de la répression et de la sécurité nationale (en particulier par la PIPC et la CNDH).

(221) En vue de la réalisation de cet examen, la Commission devrait rencontrer la PIPC, accompagnée, le cas échéant, d'autres autorités coréennes responsables de l'accès des pouvoirs publics aux données, y compris les organismes de surveillance concernés. La participation à cette réunion devrait être ouverte aux représentants des membres du comité européen de la protection des données. Dans le cadre de l'examen, la Commission devrait demander à la PIPC de fournir des informations exhaustives sur tous les aspects pertinents pour le constat d'adéquation, y compris sur les limitations et les garanties en ce qui concerne l'accès des pouvoirs publics aux données ([386]). La Commission devrait également demander des explications sur toute information reçue présentant de l'intérêt pour la présente décision, notamment des rapports publics établis par les autorités coréennes ou d'autres parties prenantes en Corée, par le comité européen de la protection des données, par diverses autorités de protection des données, par des groupes de la société civile, ainsi que des informations relayées par les médias ou toute autre source d'informations disponible.

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

7. SUSPENSION, ABROGATION OU MODIFICATION DE LA PRÉSENTE DÉCISION

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

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

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

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

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

([386]) Voir annexe II de la présente décision.

(226) Plus particulièrement, la Commission devrait lancer la procédure de suspension ou d'abrogation en présence d'éléments indiquant que les garanties supplémentaires figurant à l'annexe I ne sont pas respectées par les opérateurs économiques recevant des données à caractère personnel sur la base de la présente décision et/ou que leur mise en œuvre n'est pas effectivement garantie, ou encore que les autorités coréennes ne respectent pas les déclarations, assurances et engagements contenus dans l'annexe II de la présente décision.

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

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

8. **CONSIDÉRATIONS FINALES**

(229) Le comité européen de la protection des données a publié son avis ([387]), dont il a été tenu compte dans l'élaboration de la présente décision.

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

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

1. Aux fins de l'article 45 du règlement (UE) 2016/679, la République de Corée assure un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne à des entités situées en République de Corée et soumises à la loi sur la protection des informations à caractère personnel, telle que complétée par les garanties supplémentaires figurant à l'annexe I, ainsi que par les déclarations, les assurances et les engagements officiels contenus dans l'annexe II.

2. La présente décision ne concerne pas les données à caractère personnel transférées à des destinataires relevant de l'une des catégories suivantes, dans la mesure où la finalité du traitement des données à caractère personnel correspond en tout ou en partie à l'une des finalités énumérées, à savoir:

a) les organisations religieuses dans la mesure où elles traitent des données à caractère personnel aux fins de leurs activités missionnaires;

b) les partis politiques dans la mesure où ils traitent des données à caractère personnel dans le cadre de la nomination de candidats;

c) les entités qui sont soumises à la surveillance de la Commission des services financiers en ce qui concerne le traitement des informations à caractère personnel en matière de crédit conformément à la loi sur les informations en matière de crédit, dans la mesure où elles traitent de telles informations.

Article 2

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

Article 3

1. La Commission suit de manière permanente l'application du cadre juridique sur lequel se fonde la présente décision, notamment les conditions dans lesquelles les transferts ultérieurs sont effectués, les droits individuels sont exercés et les autorités publiques coréennes ont accès aux données transférées sur la base de la présente décision, dans le but de déterminer si la République de Corée continue d'assurer un niveau de protection adéquat au sens de l'article 1er.

([387]) Avis 32/2021 concernant le projet de décision d'exécution de la Commission européenne conformément au règlement (UE) 2016/679 constatant le niveau de protection adéquat des données à caractère personnel assuré par la République de Corée (Opinion 32/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the Republic of Korea), disponible à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en

2. Les États membres et la Commission s'informent mutuellement des cas dans lesquels la Commission de protection des informations à caractère personnel, ou toute autre autorité coréenne compétente, échoue à faire respecter le cadre juridique sur lequel se fonde la présente décision.

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

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

5. Lorsqu'elle est en possession d'éléments indiquant qu'un niveau de protection adéquat n'est plus assuré, la Commission en informe les autorités coréennes compétentes. Si nécessaire, elle peut décider de suspendre, de modifier ou d'abroger la présente décision, ou d'en restreindre le champ d'application, conformément à l'article 45, paragraphe 5, du règlement (UE) 2016/679, notamment en présence d'éléments indiquant:

a) que les responsables du traitement en Corée ayant reçu des données à caractère personnel en provenance de l'Union européenne sur la base de la présente décision ne respectent pas les garanties supplémentaires figurant à l'annexe I, ou que la surveillance et le contrôle du respect des règles sont insuffisants à cet égard;

b) que les autorités publiques coréennes ne respectent pas les déclarations, les assurances et les engagements contenus dans l'annexe II, notamment en ce qui concerne les conditions et les limitations relatives à la collecte de données à caractère personnel transférées sur la base de la présente décision par les autorités publiques coréennes et l'accès de celles-ci à ces données, à des fins répressives ou à des fins de sécurité nationale.

La Commission peut également adopter de telles mesures si le défaut de coopération de la part des autorités coréennes l'empêche de déterminer si la République de Corée continue d'assurer un niveau de protection adéquat.

Article 4

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 17 décembre 2021.

Par la Commission
Didier REYNDERS
Membre de la Commission

ANNEXE I

RÈGLES SUPPLÉMENTAIRES POUR L'INTERPRÉTATION ET L'APPLICATION DE LA LOI SUR LA PROTECTION DES INFORMATIONS À CARACTÈRE PERSONNEL RELATIVES AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES EN CORÉE

Table des matières

I. **Aperçu**

La Corée et l'Union européenne (ci-après l'«UE») ont engagé des discussions portant sur la constatation d'un niveau de protection adéquat, à la suite desquelles la Commission européenne a déterminé que la Corée garantissait un niveau adéquat de protection des données à caractère personnel conformément à l'article 45 du RGPD.

Dans ce contexte, la Commission de protection des informations à caractère personnel a adopté la présente notification sur la base de l'article 5 (Obligations de l'État, etc.) et de l'article 14 (Coopération internationale) ([1]) de la loi sur la protection des informations à caractère personnel afin de clarifier l'interprétation, l'application et la mise en œuvre de certaines dispositions de la loi, notamment en ce qui concerne le traitement des données à caractère personnel transférées en Corée sur la base de la décision d'adéquation de l'UE.

Comme la présente notification a le statut d'une règle administrative que l'agence administrative compétente établit et annonce aux fins de clarifier les normes d'interprétation, d'application et de mise en œuvre de la loi sur la protection des informations à caractère personnel dans le système juridique coréen, elle a une force juridiquement contraignante pour le responsable du traitement des informations à caractère personnel dans le sens où toute violation de cette notification peut être considérée comme une violation des dispositions pertinentes de la PIPA. En outre, si les droits et intérêts personnels sont enfreints en raison d'une violation de la présente notification, les personnes concernées ont le droit d'obtenir réparation auprès de la Commission de protection des informations à caractère personnel ou du tribunal.

Par conséquent, si le responsable du traitement des informations à caractère personnel, qui traite les informations à caractère personnel transférées en Corée conformément à la décision d'adéquation de l'UE, ne prend pas de mesures conformes à cette notification, il sera considéré «qu'il y a des raisons sérieuses de considérer qu'il y a eu une infraction concernant les informations à caractère personnel, et que l'absence de mesures est susceptible de causer des dommages difficilement réparables», conformément aux paragraphes 1 et 2 de l'article 64 de la loi. Dans ce cas, la Commission de protection des informations à caractère personnel ou les agences administratives centrales concernées peuvent ordonner

([1]) L'article 14 de la loi sur la protection des informations à caractère personnel [PIPA, de l'anglais Personal Information Protection Act] enjoint à l'autorité du gouvernement coréen d'élaborer des politiques visant à améliorer le niveau de protection des informations à caractère personnel dans l'environnement international et à éviter la violation des droits des personnes concernées à la suite du transfert transfrontière d'informations à caractère personnel.

au responsable du traitement des informations à caractère personnel concerné de prendre des mesures correctives, etc. conformément à l'autorité conférée par le présent texte et, en fonction des violations spécifiques de la loi, des sanctions correspondantes (pénalités, amendes administratives, etc.) peuvent également être imposées.

II. **Définition de termes**

Les définitions des termes utilisés dans le présent texte sont les suivantes:

i) loi: loi sur la protection des informations à caractère personnel (loi n° 16930, modifiée le 4 février 2020 et entrée en vigueur le 5 août 2020);

ii) décret présidentiel: décret d'application de la loi sur la protection des informations à caractère personnel (décret présidentiel n° 30509, 3 mars 2020, modifiant d'autres lois);

iii) personne concernée: un individu qui est identifiable par les informations traitées et qui est le sujet de ces informations;

iv) responsable du traitement des informations à caractère personnel: une institution publique, une personne morale, une organisation, un individu, etc. qui traite des informations à caractère personnel directement ou indirectement dans le cadre de ses activités;

v) UE: Union européenne (à la fin du mois de février 2020, 27 pays membres [2], à savoir la Belgique, l'Allemagne, la France, l'Italie, le Luxembourg, les Pays-Bas, le Danemark, l'Irlande, la Grèce, le Portugal, l'Espagne, l'Autriche, la Finlande, la Suède, Chypre, la Tchéquie, l'Estonie, la Hongrie, la Lettonie, la Lituanie, Malte, la Pologne, la Slovaquie, la Slovénie, la Roumanie, la Bulgarie et la Croatie) ainsi que les pays associés à l'UE par l'intermédiaire de l'accord EEE (Islande, Liechtenstein, Norvège);

vi) RGPD: la loi générale de l'UE sur la protection des informations à caractère personnel, le règlement général sur la protection des données [règlement (UE) 2016/679];

vii) décision d'adéquation (décision constatant un niveau de protection adéquat): conformément à l'article 45, paragraphe 3, du RGPD, la Commission européenne a décidé qu'un pays tiers, le territoire d'un pays tiers, une ou plusieurs zones ou une organisation internationale garantissent un niveau adéquat de protection des informations à caractère personnel.

III. **Règles supplémentaires**

1. **Limitation de l'utilisation et de la fourniture d'informations à caractère personnel à des fins non prévues (articles 3, 15 et 18 de la loi)**

<Loi sur la protection des informations à caractère personnel

(Loi n° 16930, partiellement modifiée le 4 février 2020)>

Article 3 (Principes de protection des informations à caractère personnel) 1) Le responsable du traitement des informations à caractère personnel doit préciser explicitement les finalités pour lesquelles les informations à caractère personnel sont traitées; il est également tenu de collecter les informations à caractère personnel de manière licite et loyale et de limiter cette collecte au minimum nécessaire pour atteindre ces finalités.

2) Le responsable du traitement des informations à caractère personnel traite les informations à caractère personnel de la manière appropriée nécessaire aux finalités pour lesquelles les informations à caractère personnel sont traitées, et ne les utilise pas au-delà de ces fins.

Article 15 (Collecte et utilisation des informations à caractère personnel) 1) Un responsable du traitement des informations à caractère personnel est habilité à collecter des informations à caractère personnel dans les cas suivants, et à les utiliser dans le cadre de la finalité de la collecte:

1. lorsque le consentement d'une personne concernée a été obtenu;

2. lorsque des dispositions spéciales existent dans les lois ou que la collecte est inévitable pour respecter les obligations légales;

3. lorsque la collecte est inévitable aux fins de l'exécution, par une institution publique, des tâches qui lui incombent en vertu de sa compétence, comme le prescrivent les lois, etc.;

4. lorsque la collecte est inévitablement nécessaire pour signer et exécuter un contrat avec une personne concernée;

[2] Jusqu'à la fin de la période de transition, cela inclut également le Royaume-Uni, comme le prévoient les articles 126, 127 et 132 de l'accord sur le retrait du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de l'Union européenne et de la Communauté européenne de l'énergie atomique (2019/C 384 I/01).

5. lorsque la collecte est jugée manifestement nécessaire à la protection de la vie, des intérêts corporels ou matériels de la personne concernée ou d'un tiers contre un danger imminent, lorsque la personne concernée ou son représentant légal n'est pas en mesure d'exprimer sa volonté, ou que le consentement préalable ne peut être obtenu en raison d'adresses inconnues, etc.;
6. lorsque la collecte est nécessaire pour répondre à l'intérêt justifié d'un responsable du traitement des informations à caractère personnel, cet intérêt étant manifestement supérieur aux droits de la personne concernée. Dans ces cas, le traitement n'est autorisé que dans la mesure où il est substantiellement lié à l'intérêt justifié du responsable du traitement des informations à caractère personnel et ne dépasse pas une portée raisonnable.

Article 18 (Limitation de l'utilisation et de la fourniture d'informations à caractère personnel à des fins non prévues) 1) Un responsable du traitement des informations à caractère personnel ne doit pas utiliser les informations à caractère personnel au-delà de la portée prévue à l'article 15, paragraphe 1, et à l'article 39-3, paragraphes 1 et 2, ni les fournir à un tiers au-delà de la portée prévue à l'article 17, paragraphes 1 et 3.

2) Nonobstant le paragraphe 1, lorsque l'un des points suivants s'applique, le responsable du traitement des informations à caractère personnel peut utiliser les informations à caractère personnel ou les fournir à un tiers à d'autres fins, à moins que cela ne soit susceptible de porter atteinte de manière déloyale aux intérêts d'une personne concernée ou d'un tiers: à condition que les fournisseurs de services d'information et de communication (tels que définis à l'article 2, paragraphe 1, point 3, de la loi sur la promotion de l'utilisation des réseaux d'information et de communication et la protection des informations, etc.; ci-après les mêmes dispositions s'appliquent) traitant les informations à caractère personnel des utilisateurs (comme indiqué à l'article 2, paragraphe 1, point 4, de la loi sur la promotion de l'utilisation des réseaux d'information et de communication et la protection des informations, etc.; ci-après les mêmes dispositions s'appliquent) ne soient soumis qu'aux points 1 et 2, et que les points 5 à 9 ne soient applicables qu'aux institutions publiques:

1. lorsque le consentement supplémentaire de la personne concernée a été obtenu;
2. lorsqu'il existe d'autres dispositions spéciales dans les lois;
3. lorsque ladite fourniture est jugée manifestement nécessaire à la protection de la vie, des intérêts corporels ou matériels de la personne concernée ou d'un tiers contre un danger imminent, lorsque la personne concernée ou son représentant légal n'est pas en mesure d'exprimer sa volonté, ou que le consentement préalable ne peut être obtenu en raison d'adresses inconnues;
4. supprimé; <par la loi n° 16930 du 4 février 2020>
5. lorsqu'il est impossible d'exercer les fonctions relevant de sa compétence, comme le prévoit toute loi, à moins que le responsable du traitement des informations à caractère personnel n'utilise les informations à caractère personnel à des fins autres que celles prévues, ou ne les fournisse à un tiers, et qu'il soit soumis à la délibération et à la résolution de la Commission;
6. lorsqu'il est nécessaire de fournir des informations à caractère personnel à un gouvernement étranger ou à une organisation internationale pour exécuter un traité ou une autre convention internationale;
7. lorsque cela est nécessaire pour l'enquête sur une infraction, une mise en accusation et des poursuites;
8. lorsque la fourniture est nécessaire pour permettre à un tribunal de s'acquitter d'obligations liées à un procès;
9. lorsque la fourniture est nécessaire à l'application d'une peine, d'une probation ou d'une détention.

Paragraphes 3 et 4 omis

5) Lorsqu'un responsable du traitement des informations à caractère personnel fournit des informations à caractère personnel à un tiers à des fins autres que celles visées dans les cas prévus au paragraphe 2, le responsable du traitement des informations à caractère personnel doit demander au destinataire des informations à caractère personnel de limiter la finalité et la méthode d'utilisation ainsi que les autres questions nécessaires, ou de préparer les mesures de protection nécessaires pour assurer la sécurité des informations à caractère personnel. Dans ce cas, la personne qui reçoit cette demande doit prendre les mesures nécessaires pour assurer la sécurité des informations à caractère personnel.

i) L'article 3, paragraphes 1 et 2, de la loi définit le principe selon lequel un responsable du traitement d'informations à caractère personnel doit limiter la collecte des informations à caractère personnel au minimum nécessaire pour traiter ces informations de manière légale et licite et conformément à la finalité prévue, et ne doit pas les utiliser à une autre fin ([3]).

ii) Selon ce principe, le paragraphe 1 de l'article 15 de la loi dispose que lorsqu'un responsable du traitement d'informations à caractère personnel recueille des informations à caractère personnel, celles-ci peuvent être utilisées dans le cadre de la finalité de la collecte, et le paragraphe 1 de l'article 18 dispose que les informations à caractère personnel ne doivent pas être utilisées au-delà de la finalité de la collecte ni être fournies à un tiers.

([3]) Étant donné que ces dispositions énoncent des principes généraux qui s'appliquent à tout traitement d'informations à caractère personnel, y compris lorsque ce traitement est spécifiquement réglementé par d'autres lois, les précisions apportées dans cette section s'appliquent également lorsque des données à caractère personnel sont traitées sur la base d'autres lois (voir par exemple article 15, paragraphe 1, de la loi sur les informations en matière de crédit, qui fait spécifiquement référence à ces dispositions).

iii) Par ailleurs, même si les informations à caractère personnel peuvent être utilisées à des fins autres que celles prévues ou fournies à un tiers dans les cas exceptionnels ([4]) décrits aux points énumérés à l'article 18, paragraphe 2, de la loi, il faut demander que la finalité ou la méthode d'utilisation soit limitée afin que les informations à caractère personnel puissent être traitées en toute sécurité conformément au paragraphe 5, ou que les mesures nécessaires pour assurer la sécurité des informations à caractère personnel soient prises.

iv) Les dispositions ci-dessus s'appliquent également au traitement de toutes les informations à caractère personnel reçues dans la zone de compétence juridique de la Corée en provenance d'un pays tiers, quelle que soit la nationalité de la personne concernée.

v) Par exemple, si un responsable du traitement d'informations à caractère personnel de l'UE transfère des informations à caractère personnel à un responsable du traitement d'informations à caractère personnel coréen conformément à la décision d'adéquation de la Commission européenne, la finalité du transfert des informations à caractère personnel par le responsable du traitement d'informations à caractère personnel de l'UE sera considérée comme la finalité de la collecte des informations à caractère personnel par le responsable du traitement d'informations à caractère personnel coréen, et dans ce cas, le responsable du traitement d'informations à caractère personnel coréen ne peut utiliser les informations à caractère personnel ou les fournir à un tiers que dans le cadre de la finalité de la collecte, sauf dans les cas exceptionnels décrits aux points du paragraphe 2 de l'article 18 de la loi.

2. **Limitation du transfert ultérieur de données à caractère personnel (article 17, paragraphes 3 et 4, et article 18 de la loi)**

<Loi sur la protection des informations à caractère personnel (Loi n° 16930, partiellement modifiée le 4 février 2020)>

Article 17 (Fourniture d'informations à caractère personnel) 1) Paragraphe omis.

2) Un responsable du traitement d'informations à caractère personnel doit informer une personne concernée des points suivants lorsqu'il obtient le consentement en vertu du paragraphe 1, point 1. Il en va de même lorsque l'un des éléments suivants est modifié:

1. le destinataire des informations à caractère personnel;
2. la finalité pour laquelle le destinataire des informations à caractère personnel utilise ces informations;
3. les détails des informations à caractère personnel à fournir;
4. la période durant laquelle le destinataire conserve et utilise les informations à caractère personnel;
5. le fait que la personne concernée a le droit de retirer son consentement, et les inconvénients, le cas échéant, résultant du retrait de consentement.

3) Un responsable du traitement d'informations à caractère personnel doit informer une personne concernée des éléments visés au paragraphe 2 et obtenir son consentement pour pouvoir fournir des informations à caractère personnel à un tiers à l'étranger; et il ne doit pas conclure de contrat pour le transfert transfrontière d'informations à caractère personnel en violation de la présente loi.

4) Un responsable du traitement d'informations à caractère personnel peut fournir des informations à caractère personnel sans le consentement d'une personne concernée dans le cadre d'un champ d'application présentant un rapport raisonnable aux finalités pour lesquelles les informations à caractère personnel ont été initialement collectées, conformément aux éléments prescrits par le décret présidentiel, en tenant compte des inconvénients éventuels pour la personne concernée, de l'adoption éventuelle des mesures nécessaires pour garantir la sécurité, telles que le chiffrement, etc.

※ Veuillez vous reporter aux pages 3, 4 et 5 de l'article 18

<Décret d'application de la loi sur la protection des informations à caractère personnel

([Date d'application: 5 février 2021.] [Décret présidentiel n° 30892, 4 août 2020, modifie d'autres lois])>

Article 14-2 (Normes relatives à l'utilisation/la fourniture supplémentaire d'informations à caractère personnel, etc.)

1) Si un responsable du traitement d'informations à caractère personnel utilise ou fournit des informations à caractère personnel (ci-après dénommé «utilisation ou fourniture supplémentaire d'informations à caractère personnel») sans le consentement de la personne concernée conformément à l'article 15, paragraphe 3, ou à l'article 17, paragraphe 4, de la loi, il doit vérifier:

1. si l'utilisation est raisonnablement liée à la finalité initiale pour laquelle les informations à caractère personnel ont été collectées;
2. si une utilisation ou une fourniture supplémentaire des informations à caractère personnel est prévisible à la lumière des circonstances dans lesquelles les informations à caractère personnel ont été collectées et des pratiques de traitement;
3. si l'utilisation ou la fourniture supplémentaire d'informations à caractère personnel ne porte pas atteinte de manière déloyale aux intérêts de la personne concernée; et
4. si les mesures nécessaires pour assurer la sécurité, telles que la pseudonymisation ou le chiffrement, ont été prises.

([4]) Les fournisseurs de services de communication d'informations ne sont soumis qu'à l'article 18, paragraphe 2, points 1 et 2. Les points 5 à 9 ne s'appliquent qu'aux institutions publiques.

2) Le responsable du traitement des informations à caractère personnel divulgue au préalable les critères d'évaluation des éléments visés aux points du paragraphe 1 dans la politique en matière de protection de la vie privée établie en vertu de l'article 30, paragraphe 1, de la loi, et le responsable de la protection de la vie privée nommé en vertu de l'article 31, paragraphe 1, de la loi vérifie que le responsable du traitement des informations à caractère personnel utilise ou fournit des informations à caractère personnel supplémentaires conformément aux normes pertinentes.

i) Si le responsable du traitement des informations à caractère personnel fournit des informations à caractère personnel à un tiers à l'étranger, il doit informer au préalable les personnes concernées de tous les éléments décrits à l'article 17, paragraphe 2, de la loi et obtenir leur consentement, sauf dans les cas relevant des paragraphes 1 ou 2 ci-dessous. Aucun contrat ne doit être conclu concernant la fourniture transfrontière de données à caractère personnel en violation de cette loi.
   (1) Si les informations à caractère personnel sont fournies dans le cadre raisonnablement lié à la finalité initiale de la collecte conformément à l'article 17, paragraphe 4, de la loi. Toutefois, les cas auxquels cette disposition peut être appliquée sont limités aux cas où les normes relatives à l'utilisation et à la fourniture supplémentaires d'informations à caractère personnel, prescrites à l'article 14-2 du décret d'application, sont respectées. En outre, le responsable du traitement des informations à caractère personnel doit examiner si la fourniture d'informations à caractère personnel peut entraîner des inconvénients pour les personnes concernées et s'il a pris les mesures nécessaires pour assurer la sécurité, comme le chiffrement.
   (2) Si les informations à caractère personnel peuvent être fournies à un tiers dans les cas exceptionnels mentionnés à l'article 18, paragraphe 2, de la loi (voir pages 4 à 6). Toutefois, même dans ces cas, si la fourniture de ces informations à caractère personnel est susceptible de porter atteinte de manière déloyale aux intérêts de la personne concernée ou d'un tiers, ces informations ne peuvent être fournies à un tiers. En outre, le fournisseur des informations à caractère personnel doit demander au destinataire de ces informations d'en limiter la finalité ou la méthode d'utilisation ou de prendre les mesures nécessaires pour en assurer la sécurité afin que ces informations puissent être traitées en toute sécurité.

ii) Si les informations à caractère personnel sont fournies à un tiers à l'étranger, il se peut qu'elles ne bénéficient pas du niveau de protection garanti par la loi coréenne sur la protection des informations à caractère personnel en raison des différences entre les systèmes de protection des informations à caractère personnel des différents pays. Par conséquent, ces cas seront considérés comme des «cas où la personne concernée peut subir des inconvénients», mentionnés à l'article 17, paragraphe 4, de la loi, ou des «cas où l'intérêt d'une personne concernée ou d'un tiers est violé de manière déloyale», mentionnés à l'article 18, paragraphe 2, de la loi et à l'article 14-2 du décret d'application de la même loi ([5]). Pour satisfaire aux exigences de ces dispositions, le responsable du traitement des informations à caractère personnel et le tiers doivent donc garantir explicitement un niveau de protection équivalent à celui établi par la loi, y compris en ce qui concerne l'exercice par la personne concernée de ses droits dans des documents juridiquement contraignants tels que des contrats, même après le transfert des informations à caractère personnel à l'étranger.

3. **Notification relative aux données lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée (article 20 de la loi)**

<Loi sur la protection des informations à caractère personnel

(Loi nº 16930, partiellement modifiée le 4 février 2020)>

Article 20 (Notification sur les sources, etc. des informations à caractère personnel collectées auprès de tiers) 1) Lorsqu'un responsable du traitement d'informations à caractère personnel traite des informations à caractère personnel collectées auprès de tiers, il doit immédiatement notifier les éléments suivants à la personne concernée, à la demande de cette dernière:

1. la source des informations à caractère personnel collectées;
2. la finalité du traitement des informations à caractère personnel;
3. le fait que la personne concernée a le droit d'exiger la suspension du traitement des informations à caractère personnel, comme le prévoit l'article 37.

2) Nonobstant le paragraphe 1, lorsqu'un responsable du traitement d'informations à caractère personnel répondant aux critères prescrits par le décret présidentiel, collecte des informations à caractère personnel auprès de tiers, en tenant compte des types et de la quantité d'informations à caractère personnel traitées, du nombre d'employés, du montant des ventes, etc., et les traite conformément à l'article 17, paragraphe 1, point 1, il doit notifier à la personne concernée les éléments visés au paragraphe 1; il est entendu que cette disposition ne s'applique pas lorsque les informations collectées par le responsable du traitement des informations à caractère personnel ne contiennent pas d'informations à caractère personnel, telles que des coordonnées, permettant d'informer la personne concernée.

([5]) Conformément à l'article 18, paragraphe 2, point 2, de la PIPA, cela s'applique également lorsque les informations à caractère personnel sont divulguées à des tiers à l'étranger sur la base des dispositions d'autres lois (par exemple la loi sur les informations en matière de crédit).

3) Les éléments nécessaires relatifs au moment, à la méthode et à la procédure de notification à la personne concernée conformément à la phrase principale du paragraphe 2 sont prescrits par décret présidentiel.

4) Le paragraphe 1 et la disposition principale du paragraphe 2 ne s'appliquent à aucun des cas suivants, à condition que ce soit le cas uniquement lorsqu'elle est manifestement supérieure aux droits des personnes concernées en vertu de la présente loi:

1. lorsque des informations à caractère personnel, qui font l'objet d'une demande de notification, sont incluses dans les fichiers d'informations à caractère personnel visés à l'un des points de l'article 32, paragraphe 2;
2. lorsque cette notification est susceptible de porter atteinte à la vie ou à l'intégrité physique de toute autre personne, ou de porter atteinte de manière déloyale aux biens et autres intérêts de toute autre personne.

i) Si le responsable du traitement des informations à caractère personnel reçoit les données à caractère personnel transférées depuis l'UE sur la base de la décision d'adéquation de cette dernière ([6]), il doit notifier les informations mentionnées aux points 1) à 5) à la personne concernée sans retard excessif, et en tout cas au plus tard un mois après le transfert.

(1) Le nom et les coordonnées des personnes qui transfèrent et reçoivent les informations à caractère personnel.

(2) Les éléments ou catégories d'informations à caractère personnel transférées.

(3) La finalité de la collecte et de l'utilisation des informations à caractère personnel (telle que définie par l'exportateur des données conformément au point 1 de la présente notification).

(4) La période de conservation des informations à caractère personnel.

(5) Les informations sur les droits de la personne concernée en ce qui concerne le traitement des informations à caractère personnel, la méthode et la procédure d'exercice des droits et les inconvénients éventuels si l'exercice de ces droits entraîne des inconvénients.

ii) De même, si le responsable du traitement des informations à caractère personnel fournit les informations à caractère personnel visées au point i) à un tiers en République de Corée ou à l'étranger, il doit notifier les informations mentionnées aux paragraphes 1 à 5 à la personne concernée avant que les informations à caractère personnel ne soient fournies.

(1) Le nom et les coordonnées des personnes qui fournissent et reçoivent les informations à caractère personnel.

(2) Les éléments ou catégories d'informations à caractère personnel fournies.

(3) Le pays auquel les informations à caractère personnel seront fournies, la date envisagée et la méthode de fourniture (limité aux cas où les informations à caractère personnel seront fournies à un tiers à l'étranger).

(4) La finalité et la base juridique de la fourniture des informations à caractère personnel par le fournisseur de ces informations.

(5) Les informations sur les droits de la personne concernée en ce qui concerne le traitement des informations à caractère personnel, la méthode et la procédure d'exercice des droits et les inconvénients éventuels si l'exercice de ces droits entraîne des inconvénients.

iii) Le responsable du traitement des informations à caractère personnel ne peut appliquer les points i) ou ii) dans aucun des cas mentionnés aux paragraphes 1 à 4:

(1) si les informations à caractère personnel qui doivent être notifiées sont incluses dans l'un des fichiers d'informations à caractère personnel mentionnés à l'article 32, paragraphe 2, de la loi, dans la mesure où les intérêts protégés par cette disposition sont manifestement supérieurs aux droits de la personne concernée, et uniquement dans la mesure où la notification menacerait les intérêts en jeu, par exemple en compromettant des enquêtes pénales en cours ou en menaçant la sécurité nationale;

(2) si et aussi longtemps que la notification est susceptible de porter atteinte à la vie ou à l'intégrité physique d'une autre personne, ou de porter atteinte de manière déloyale aux intérêts patrimoniaux d'une autre personne, lorsque ces droits ou intérêts sont manifestement supérieurs aux droits de la personne concernée;

(3) si la personne concernée possède déjà les informations que le responsable du traitement des informations à caractère personnel doit notifier conformément aux points i) ou ii);

(4) si le responsable du traitement des informations à caractère personnel ne dispose pas des coordonnées de la personne concernée ou si des efforts excessifs sont nécessaires pour contacter la personne concernée, y compris dans le cadre d'un traitement dans les conditions énoncées à la section 3 de la PIPA. Pour déterminer s'il est possible ou non de contacter la personne concernée, ou si des efforts excessifs sont nécessaires, il convient de tenir compte de la possibilité de coopérer avec l'exportateur des données dans l'UE.

([6]) Les obligations prévues aux points i), ii) et iii) s'appliquent également lorsque le responsable du traitement qui reçoit des informations à caractère personnel de l'UE sur la base de la décision d'adéquation traite ces informations sur la base d'autres lois, par exemple la loi sur les informations en matière de crédit.

4. **Champ d'application de la dérogation spéciale concernant le traitement d'informations pseudonymisées (articles 28-2, 28-3, 28-4, 28-5, 28-6 et 28-7, article 3 et article 58-2 de la loi)**

<Loi sur la protection des informations à caractère personnel

(Loi n° 16930, partiellement modifiée le 4 février 2020)>

Chapitre III — Traitement des informations à caractère personnel

SECTION 3 — Cas particuliers concernant les données pseudonymes

Article 28-2 (Traitement des données pseudonymes) 1) Le responsable du traitement des informations à caractère personnel peut traiter des informations pseudonymisées sans le consentement des personnes concernées à des fins statistiques, de recherche scientifique, d'archivage dans l'intérêt public, etc.

2) Un responsable du traitement des informations à caractère personnel ne doit pas inclure des informations qui peuvent être utilisées pour identifier une personne en particulier lorsqu'il fournit des informations pseudonymisées à un tiers conformément au paragraphe 1.

Article 28-3 (Restriction de la combinaison de données pseudonymes) 1) Nonobstant l'article 28-2, la combinaison d'informations pseudonymisées traitées par différents responsables du traitement des informations à caractère personnel à des fins statistiques, de recherche scientifique et de conservation d'archives d'intérêt public, etc. doit être effectuée par une institution spécialisée désignée par la Commission de protection ou le chef de l'agence administrative centrale concernée.

2) Le responsable du traitement des informations à caractère personnel qui a l'intention de diffuser les informations combinées en dehors de l'organisation qui les a combinées doit obtenir l'approbation du chef de l'institution spécialisée après avoir transformé les informations en informations pseudonymisées ou sous la forme visée à l'article 58-2.

3) Les éléments nécessaires, y compris les procédures et méthodes de combinaison conformément au paragraphe 1, les normes et procédures pour désigner, ou annuler la désignation d'une institution spécialisée de gestion et de supervision, et les normes et procédures d'exportation et d'approbation conformément au paragraphe 2, sont définis par décret présidentiel.

Article 28-4 (Obligation de prendre des mesures de sécurité pour les données pseudonymes) 1) Lors du traitement des informations pseudonymisées, un responsable du traitement d'informations à caractère personnel doit prendre des mesures techniques, organisationnelles et physiques telles que le stockage et la gestion séparés des informations supplémentaires nécessaires au rétablissement de l'état d'origine, qui peuvent être nécessaires pour assurer la sécurité, conformément au décret présidentiel, afin que les informations à caractère personnel ne puissent être perdues, volées, divulguées, falsifiées, altérées ou endommagées.

2) Le responsable du traitement des informations à caractère personnel qui a l'intention de traiter les informations pseudonymisées doit établir et conserver des registres relatifs aux éléments prescrits par le décret présidentiel, y compris la finalité du traitement des informations pseudonymisées, et un tiers destinataire lorsque des informations pseudonymisées sont fournies, pour gérer le traitement des informations pseudonymisées.

Article 28-5 (Actes interdits pour le traitement des informations pseudonymisées) 1) Nul ne peut traiter les informations pseudonymisées dans le but d'identifier une personne en particulier.

2) Lorsque des informations permettant d'identifier une personne en particulier sont générées pendant le traitement des informations pseudonymisées, le responsable du traitement des informations à caractère personnel doit cesser le traitement de ces informations, les récupérer et les détruire immédiatement.

Article 28-6 (Imposition de surtaxes administratives pour le traitement des informations pseudonymisées) 1) La Commission peut imposer une amende équivalente à moins de trois centièmes du chiffre d'affaires total au responsable du traitement qui a traité des données dans le but d'identifier une personne spécifique en violation de l'article 28-5, paragraphe 1: il est prévu qu'en cas d'absence de ventes ou de difficulté à calculer les recettes des ventes, le responsable du traitement des données peut être soumis à une amende ne dépassant pas 400 millions de wons ou les trois centièmes du montant du capital, le montant le plus élevé étant retenu.

2) L'article 34-2, paragraphes 3 à 5, s'applique mutatis mutandis aux éléments nécessaires à l'imposition et à la perception des surtaxes administratives.

Article 28-7 (Champ d'application) @Les articles 20, 21 et 27, l'article 34, paragraphe 1, et les articles 35 à 37, 39-3, 39-4 et 39-6 à 39-8 ne s'appliquent pas aux informations pseudonymisées.

Chapitre I — Dispositions générales

Article 3 (Principes de protection des informations à caractère personnel) 1) Le responsable du traitement des informations à caractère personnel doit préciser les finalités pour lesquelles les informations à caractère personnel sont traitées; il est également tenu de collecter les informations à caractère personnel de manière licite et loyale et de limiter cette collecte au minimum nécessaire pour atteindre ces finalités.

2) Le responsable du traitement des informations à caractère personnel traite les informations à caractère personnel de la manière appropriée nécessaire aux finalités pour lesquelles les informations à caractère personnel sont traitées, et ne les utilise pas au-delà de ces fins.

3) Le responsable du traitement des informations à caractère personnel veille à ce que les informations à caractère personnel soient exactes, complètes et à jour dans la mesure nécessaire aux finalités pour lesquelles elles sont traitées.

4) Le responsable du traitement des informations à caractère personnel doit gérer les informations à caractère personnel en toute sécurité en fonction des méthodes de traitement, des types, etc. d'informations à caractère personnel, en tenant compte du risque d'atteinte aux droits de la personne concernée et de la gravité des risques pertinents.

5) Le responsable du traitement des informations à caractère personnel doit rendre publics sa politique de protection de la vie privée et d'autres éléments liés au traitement des informations à caractère personnel; il garantit également les droits de la personne concernée, tels que le droit d'accès aux informations à caractère personnel la concernant.

6) Le responsable du traitement des informations à caractère personnel traite les informations à caractère personnel de manière à minimiser le risque d'atteinte à la vie privée d'une personne concernée.

7) S'il est encore possible d'atteindre les finalités de la collecte des informations à caractère personnel en traitant des informations à caractère personnel anonymisées ou pseudonymisées, le responsable du traitement des informations à caractère personnel s'efforce de traiter les informations à caractère personnel par le biais de l'anonymisation, lorsque celle-ci est possible, ou par le biais de la pseudonymisation, s'il est impossible d'atteindre les finalités de la collecte des informations à caractère personnel par le biais de l'anonymisation.

8) Le responsable du traitement des informations à caractère personnel doit s'efforcer d'obtenir la confiance des personnes concernées en respectant et en accomplissant les devoirs et responsabilités prévus par la présente loi et les autres lois connexes.

CHAPITRE IX — Dispositions complémentaires

Article 58-2 (Exemption d'application) La présente loi ne s'applique pas aux informations qui ne permettent plus d'identifier une personne précise lorsqu'elles sont combinées avec d'autres informations, en tenant raisonnablement compte du temps, du coût, de la technologie, etc. <Il s'agit d'un nouvel article inséré par la loi nº 16930 du 4 février 2020>

i) Le chapitre III, section 3, qui traite des cas particuliers concernant les données pseudonymes (articles 28-2 à 28-7), permet le traitement d'informations pseudonymisées sans le consentement de la personne concernée à des fins d'établissement de statistiques, de recherche scientifique, de conservation des archives publiques, etc. (article 28-2), mais dans ces cas, les garanties et interdictions appropriées nécessaires à la protection des droits des personnes concernées sont obligatoires (articles 28-4 et 28-5), des sanctions majorées peuvent être imposées aux contrevenants (article 28-6) et certaines garanties autrement disponibles en vertu de la PIPA ne s'appliquent pas (article 28-7).

ii) Ces dispositions ne s'appliquent pas aux cas où des informations pseudonymisées sont traitées à des fins autres que l'établissement de statistiques, la recherche scientifique, la conservation des archives publiques, etc. Par exemple, si les informations à caractère personnel d'une personne de l'UE qui ont été transférées en Corée conformément à la décision d'adéquation de la Commission européenne sont pseudonymisées à des fins autres que l'établissement de statistiques, la recherche scientifique, la conservation des archives publiques, etc., les dispositions spéciales du chapitre III, section 3, ne s'appliquent pas ([7]).

iii) Lorsqu'un responsable du traitement d'informations à caractère personnel traite des informations pseudonymisées à des fins de compilation de statistiques, de recherche scientifique, de conservation des archives publiques, etc., et si les informations pseudonymisées n'ont pas été détruites une fois que la finalité spécifique du traitement a été atteinte 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 doit rendre les informations anonymes afin de veiller à ce qu'elles ne permettent plus, seules ou combinées à d'autres informations, d'identifier une personne spécifique, en tenant raisonnablement compte du temps, du coût, de la technologie, etc. conformément à l'article 58-2 de la PIPA.

5. **Mesures correctives, etc. (paragraphes 1, 2 et 4 de l'article 64 de la loi)**

<Loi sur la protection des informations à caractère personnel (Loi nº 16930, partiellement modifiée le 4 février 2020)>

Article 64 (Mesures correctives) 1) Lorsque la Commission de protection estime qu'il y a des raisons sérieuses de penser qu'il y a eu violation des informations à caractère personnel, et que l'absence de mesures est susceptible de causer des dommages difficilement réparables, elle peut ordonner au contrevenant à la présente loi (à l'exclusion des agences administratives centrales, des gouvernements locaux, de l'Assemblée nationale, de la Cour, de la Cour constitutionnelle et de la Commission électorale nationale) de prendre l'une des mesures suivantes:

1. suspendre l'infraction en matière d'informations à caractère personnel;
2. suspendre temporairement le traitement des informations à caractère personnel;

([7]) De même, l'exception visée à l'article 40-3 de la loi sur les informations en matière de crédit ne s'applique qu'au traitement d'informations de crédit pseudonymisées à des fins de compilation de statistiques, de recherche scientifique et de conservation des archives publiques.

3. prendre d'autres mesures nécessaires à la protection des informations à caractère personnel et à la prévention de toute violation de ces informations.

2) Lorsque le responsable d'une agence administrative centrale apparentée estime qu'il existe des raisons sérieuses de penser qu'il y a eu une violation des données à caractère personnel et que l'absence d'action est susceptible de causer des dommages difficilement réparables, il peut ordonner au responsable du traitement des données à caractère personnel de prendre l'une des mesures prévues au paragraphe 1 conformément aux lois relevant de la compétence de cette agence administrative centrale apparentée.

4) Lorsqu'un organisme administratif central, un gouvernement local, l'Assemblée nationale, la Cour, la Cour constitutionnelle ou la Commission électorale nationale enfreint la présente loi, la Commission de protection peut recommander au chef de l'organisme concerné de prendre l'une des mesures prévues au paragraphe 1. Dans ce cas, dès réception de la recommandation, l'organisme s'y conforme, sauf circonstances extraordinaires.

i) Premièrement, la jurisprudence ([8]) ([9]) interprète les «dommages difficilement réparables» comme un cas susceptible de porter atteinte aux droits personnels ou à la vie privée d'un individu.

ii) Par conséquent, les «raisons sérieuses de considérer qu'il y a eu une violation concernant les informations à caractère personnel et que l'absence d'action est susceptible de causer un dommage difficilement réparable», mentionnées à l'article 64, paragraphes 1 et 2, se réfèrent aux cas où une violation de la loi est considérée comme étant susceptible de porter atteinte aux droits et à la liberté des individus en ce qui concerne les informations à caractère personnel. Cela s'appliquera chaque fois que l'un des principes, droits et devoirs inclus dans la loi pour protéger les informations à caractère personnel sera violé ([10]).

iii) Selon le paragraphe 4 de l'article 64 de la loi sur la protection des informations à caractère personnel, il s'agit d'une mesure concernant «une violation de cette loi», c'est-à-dire une action contre une violation de la PIPA.

Une agence administrative centrale, etc., en tant qu'autorité publique liée par l'état de droit, ne peut violer aucune loi et est obligée de prendre une mesure corrective, y compris de cesser immédiatement l'action, et de réparer les préjudices dans le cas exceptionnel où un acte illégal a néanmoins été commis.

Par conséquent, même sans intervention de la Commission de protection conformément à l'article 64, paragraphe 4, de la PIPA, une agence administrative centrale, etc. doit prendre une mesure corrective contre les violations si elle a connaissance d'une violation de la loi.

En particulier, lorsque la Commission de protection a recommandé une mesure corrective, il sera normalement objectivement clair pour l'agence administrative centrale, etc. qu'elle a violé la loi. Ainsi, afin de justifier pourquoi elle considère qu'une recommandation de la Commission de protection ne doit pas être suivie, une agence administrative centrale, etc. doit présenter des motifs clairs qui peuvent prouver qu'elle n'a pas violé la loi. La recommandation doit être suivie, à moins que la Commission de protection ne détermine que ce n'est effectivement pas le cas.

En conséquence, les «circonstances extraordinaires» visées à l'article 64, paragraphe 4, de la loi sur la protection des informations à caractère personnel doivent être strictement limitées aux circonstances extraordinaires dans lesquelles il existe des raisons claires permettant aux agences administratives centrales, etc. de prouver que «cette loi n'a en fait pas été violée», comme dans les «cas où il existe des circonstances extraordinaires (factuelles ou juridiques)» que la Commission de protection ne connaissait pas lorsqu'elle a formulé sa recommandation initiale et que la Commission de protection détermine qu'il n'y a pas eu de violation.

6. **Application de la PIPA au traitement des données à caractère personnel à des fins de sécurité nationale, y compris les enquêtes sur les infractions et l'exécution conformément à la PIPA (article 7-8, article 7-9, article 58, article 3, article 4 et article 62 de la PIPA)**

<Loi sur la protection des informations à caractère personnel

(Loi nº 16930, partiellement modifiée le 4 février 2020)>

Article 7-8 (Travail de la Commission de protection) 1) La Commission de protection est chargée: […]

3. des questions concernant l'enquête sur la violation du droit des personnes concernées et les dispositions qui en découlent;

4. du traitement des plaintes ou des procédures de recours relatives au traitement des informations à caractère personnel et à la médiation des litiges concernant les informations à caractère personnel;

[…]

([8]) (Arrêt 97Da10215,10222 de la Cour suprême du 26 janvier 1999) Si les faits délictueux de l'accusé sont divulgués par les médias, cela est susceptible de causer des dommages psychologiques et physiques irréparables non seulement à la victime, c'est-à-dire le plaignant, mais aussi aux personnes de son entourage, y compris les familles.

([9]) (Arrêt 2006Na92006 de la Haute Cour de Séoul du 16 janvier 2008) Si un article diffamatoire est publié, il est susceptible de causer un préjudice grave et irréparable à la personne concernée.

([10]) Les mêmes principes que ceux énoncés au point ii) s'appliquent à l'article 45-4 de la loi sur les informations en matière de crédit.

Article 7-9 (Questions soumises à la délibération et à la résolution de la Commission de protection) 1) La Commission de protection délibère et prend des décisions sur les questions suivantes: […]

5. les questions concernant l'interprétation et le fonctionnement de la loi relative à la protection des informations à caractère personnel;

[…]

Article 58 (Exclusion partielle de l'application) 1) Les chapitres III à VII ne s'appliquent à aucune des informations à caractère personnel suivantes:

1. les informations à caractère personnel collectées en vertu de la loi sur les statistiques et destinées à être traitées par des institutions publiques;
2. les informations à caractère personnel collectées ou dont la communication est demandée pour l'analyse d'informations liées à la sécurité nationale;
3. les informations à caractère personnel traitées temporairement lorsqu'elles sont nécessaires pour une urgence en matière de sûreté et de sécurité publiques, de santé publique, etc.;
4. les informations à caractère personnel collectées ou utilisées à des fins propres de reportage par la presse, d'activités missionnaires par les organisations religieuses et de nomination de candidats par les partis politiques, respectivement.

[Paragraphes 2 et 3 omis]

4) Dans le cas du traitement d'informations à caractère personnel conformément au paragraphe 1, le responsable du traitement des informations à caractère personnel limite le traitement des informations à caractère personnel à la portée et à la durée minimales nécessaires pour atteindre la finalité visée; il prend également les dispositions nécessaires, telles que les mesures techniques, organisationnelles et physiques, le traitement des griefs individuels et les autres mesures nécessaires au traitement approprié de ces informations à caractère personnel et à leur gestion en toute sécurité.

Article 3 (Principes de protection des informations à caractère personnel) 1) Le responsable du traitement des informations à caractère personnel doit préciser explicitement les finalités pour lesquelles les informations à caractère personnel sont traitées; il est également tenu de collecter les informations à caractère personnel de manière licite et loyale et de limiter cette collecte au minimum nécessaire pour atteindre ces finalités.

2) Le responsable du traitement des informations à caractère personnel traite les informations à caractère personnel de la manière appropriée nécessaire aux finalités pour lesquelles les informations à caractère personnel sont traitées, et ne les utilise pas au-delà de ces fins.

3) Le responsable du traitement des informations à caractère personnel veille à ce que les informations à caractère personnel soient exactes, complètes et à jour dans la mesure nécessaire aux finalités pour lesquelles elles sont traitées.

4) Le responsable du traitement des informations à caractère personnel doit gérer les informations à caractère personnel en toute sécurité en fonction des méthodes de traitement, des types, etc. d'informations à caractère personnel, en tenant compte du risque d'atteinte aux droits de la personne concernée et de la gravité des risques pertinents.

5) Le responsable du traitement des informations à caractère personnel doit rendre publics sa politique de protection de la vie privée et d'autres éléments liés au traitement des informations à caractère personnel; il garantit également les droits de la personne concernée, tels que le droit d'accès aux informations à caractère personnel la concernant.

6) Le responsable du traitement des informations à caractère personnel traite les informations à caractère personnel de manière à minimiser le risque d'atteinte à la vie privée d'une personne concernée.

7) S'il est encore possible d'atteindre les finalités de la collecte des informations à caractère personnel en traitant des informations à caractère personnel anonymisées ou pseudonymisées, le responsable du traitement des informations à caractère personnel s'efforce de traiter les informations à caractère personnel par le biais de l'anonymisation, lorsque celle-ci est possible, ou par le biais de la pseudonymisation, s'il est impossible d'atteindre les finalités de la collecte des informations à caractère personnel par le biais de l'anonymisation.

8) Le responsable du traitement des informations à caractère personnel doit s'efforcer d'obtenir la confiance des personnes concernées en respectant et en accomplissant les devoirs et responsabilités prévus par la présente loi et les autres lois connexes.

Article 4 (Droits des personnes concernées) Une personne concernée a les droits suivants en ce qui concerne le traitement de ses propres informations à caractère personnel:

1. le droit d'être informée du traitement de ces informations à caractère personnel;
2. le droit de donner ou non son consentement et de déterminer la portée de celui-ci en ce qui concerne le traitement de ces informations à caractère personnel;
3. le droit de confirmer si des informations à caractère personnel sont traitées ou non et de demander l'accès (y compris la fourniture de copies; ci-après, la même disposition s'applique) à ces informations à caractère personnel;
4. le droit de suspendre le traitement de ces informations à caractère personnel et d'en demander la correction, l'effacement et la destruction;
5. le droit à une réparation appropriée de tout dommage résultant du traitement de ces informations à caractère personnel par le biais d'une procédure rapide et équitable.

Article 62 (Signalement des violations) 1) Toute personne qui subit une violation des droits ou des intérêts relatifs à ses informations à caractère personnel dans le cadre du traitement des informations à caractère personnel par un responsable du traitement des informations à caractère personnel peut signaler cette violation à la Commission de protection.
2) La Commission de protection peut désigner une institution spécialisée afin de recevoir et de traiter efficacement les rapports de réclamation en vertu du paragraphe 1), comme le prévoit le décret présidentiel. Dans ce cas, cette institution spécialisée met en place et gère un centre d'appel destiné à prendre en charge les violations des données à caractère personnel (ci-après dénommé «centre d'appel consacré à la protection de la vie privée»).
3) Le centre d'appel consacré à la protection de la vie privée remplit les fonctions suivantes:
1. il reçoit des rapports de réclamation et assure des consultations en rapport avec le traitement des informations à caractère personnel;
2. il enquête et confirme les incidents et procède à l'audition des parties concernées;
3. il assure les fonctions découlant des points 1 et 2.

4) La Commission de protection peut, si nécessaire, envoyer son agent public dans l'institution spécialisée désignée au paragraphe 2 conformément à l'article 32-4 de la loi sur les agents publics de l'État afin d'enquêter efficacement et de confirmer les incidents conformément au paragraphe 3, point 2.

i) La collecte d'informations à caractère personnel à des fins de sécurité nationale est réglementée par des lois spécifiques qui habilitent les autorités compétentes (p. ex., le Service national de renseignement) à intercepter des communications ou à demander leur divulgation sous certaines conditions et moyennant certaines garanties (ci-après: les «lois sur la sécurité nationale»). Ces lois sur la sécurité nationale comprennent, par exemple, la loi sur la protection de la confidentialité des communications, la loi antiterroriste pour la protection des citoyens et la sécurité publique ou la loi sur les entreprises de télécommunications. En outre, la collecte et le traitement ultérieur des informations à caractère personnel doivent être conformes aux exigences de la PIPA. À cet égard, l'article 58, paragraphe 1, point 2, de la PIPA prévoit que les chapitres III à VII ne s'appliquent pas aux informations à caractère personnel collectées ou dont la communication est demandée pour l'analyse d'informations liées à la sécurité nationale. Cette exception partielle s'applique donc au traitement des informations à caractère personnel à des fins de sécurité nationale.
Parallèlement, le chapitre I (Dispositions générales), le chapitre II (Établissement de politiques de protection des informations à caractère personnel, etc.), le chapitre VIII (Recours collectif en cas de violation des données), le chapitre IX (Dispositions complémentaires) et le chapitre X (Dispositions pénales) de la PIPA s'appliquent au traitement de ces informations à caractère personnel. Cela inclut les principes généraux de protection des données énoncés à l'article 3 (Principes de protection des informations à caractère personnel) et les droits individuels garantis par l'article 4 de la PIPA (Droits des personnes concernées).
En outre, l'article 58, paragraphe 4, de la PIPA prévoit que le traitement de ces informations doit être limité à la portée et à la durée minimales nécessaires pour atteindre la finalité visée; par ailleurs, il exige du responsable du traitement des informations à caractère personnel qu'il mette en place les mesures nécessaires pour garantir une gestion des données en toute sécurité et un traitement approprié de celles-ci, telles que des mesures techniques, organisationnelles et physiques, ainsi que des mesures pour le traitement approprié des griefs individuels.
Enfin, les dispositions régissant les tâches et les pouvoirs de la Commission de protection des informations à caractère personnel [PIPC] (notamment les articles 60 à 65 de la PIPA sur le traitement des plaintes et l'adoption de recommandations et de mesures correctives) ainsi que les dispositions relatives aux sanctions administratives et pénales (articles 70 et suivants de la PIPA) sont applicables. Selon l'article 7-8, paragraphe 1, points 3 et 4, et l'article 7-9, paragraphe 1, point 5, de la PIPA, ces pouvoirs d'enquête et de correction, y compris lorsqu'ils sont exercés dans le cadre du traitement des plaintes, couvrent également les éventuelles infractions aux règles contenues dans des lois spécifiques fixant les limites et les garanties en matière de collecte d'informations à caractère personnel, telles que les lois sur la sécurité nationale. Étant donné les exigences de l'article 3, paragraphe 1, de la PIPA concernant la collecte licite et loyale des informations à caractère personnel, et que cette infraction constitue une violation de la «présente loi» au sens des articles 63 et 64, cela permet à la PIPC de mener une enquête et de prendre des mesures correctives ([11]). L'exercice de ces pouvoirs par la PIPC complète, mais ne remplace pas, les pouvoirs de la Commission nationale des droits de l'homme en vertu de la loi sur la Commission des droits de l'homme. L'application des principes, droits et obligations fondamentaux de la PIPA au traitement des informations à caractère personnel à des fins de sécurité nationale tient compte des garanties inscrites dans la Constitution pour la protection du droit de la personne à contrôler ses propres informations à caractère personnel. Comme l'a reconnu la Cour constitutionnelle, cela inclut le droit d'un individu ([12]) «de décider personnellement quand, à qui ou par qui et dans quelle mesure ses informations seront divulguées ou utilisées. Il s'agit d'un droit fondamental ([13]), […], qui vise à protéger la liberté de décision personnelle contre les risques liés à l'élargissement des fonctions de l'État et aux technologies de l'information et de la communication». Toute restriction à ce droit, par exemple lorsqu'elle est nécessaire à la protection de la sécurité nationale, nécessite une mise en balance des droits et intérêts de l'individu avec l'intérêt public pertinent et ne peut porter atteinte à l'essence de ce droit (article 37, paragraphe 2, de la Constitution).

([11]) En ce qui concerne les mesures correctives en vertu de l'article 64, voir également section 5 ci-dessus.
([12]) Arrêt 99HunMa513, 2004HunMa190, de la Cour constitutionnelle du 26 mai 2005.
([13]) Arrêt 2003HunMa282 de la Cour constitutionnelle du 21 juillet 2005.

Par conséquent, lorsqu'il traite des informations à caractère personnel à des fins de sécurité nationale, le responsable du traitement (p. ex., le NIS) doit, entre autres:

1) préciser explicitement les finalités pour lesquelles les informations à caractère personnel sont traitées et collecter les informations à caractère personnel de manière licite et loyale et limiter cette collecte au minimum nécessaire pour atteindre ces finalités (article 3, paragraphe 1 de la PIPA); en particulier, il ne recueille et ne traite les informations à caractère personnel que dans le but d'accomplir les tâches prévues par les lois pertinentes, telles que la loi sur le Service national de renseignement;

2) limiter le traitement des informations à caractère personnel à la portée et à la durée minimales nécessaires pour atteindre la finalité visée (article 58, paragraphe 4, de la PIPA); lorsque la finalité du traitement est atteinte, le responsable du traitement détruit de manière irréversible les informations à caractère personnel, à moins qu'une conservation supplémentaire ne soit spécifiquement prescrite par la loi, auquel cas les informations à caractère personnel pertinentes sont stockées et gérées séparément des autres informations à caractère personnel, ne sont pas utilisées à d'autres fins que celles spécifiées dans la loi et sont détruites à la fin de la période de conservation;

3) traiter les informations à caractère personnel de la manière appropriée nécessaire aux finalités pour lesquelles les informations à caractère personnel sont traitées, et ne pas les utiliser au-delà de ces finalités (article 3, paragraphe 2, de la PIPA);

4) veiller à ce que les informations à caractère personnel soient exactes, complètes et à jour dans la mesure nécessaire aux finalités pour lesquelles les informations à caractère personnel sont traitées (article 3, paragraphe 3, de la PIPA);

5) gérer les informations à caractère personnel en toute sécurité en fonction des méthodes de traitement, des types, etc. d'informations à caractère personnel, en tenant compte du risque d'atteintes aux droits de la personne concernée et de la gravité des risques pertinents (article 3, paragraphe 4, de la PIPA);

6) rendre publics sa politique de confidentialité et d'autres éléments relatifs au traitement des informations à caractère personnel (article 3, paragraphe 5, de la PIPA);

7) traiter les informations à caractère personnel de manière à réduire au minimum le risque de porter atteinte à la vie privée d'une personne concernée (article 3, paragraphe 6, de la PIPA).

ii) Conformément à l'article 58, paragraphe 4, de la PIPA, le responsable du traitement (p. ex. les autorités compétentes en matière de sécurité nationale telles que le NIS) prend les dispositions nécessaires, telles que la mise en place de mesures techniques, organisationnelles et physiques, pour garantir le respect de ces principes et le traitement approprié des informations à caractère personnel. Il peut s'agir, par exemple, de mesures spécifiques visant à garantir la sécurité des informations à caractère personnel, telles que des restrictions d'accès aux informations à caractère personnel, des contrôles de l'accès, de la tenue de journaux, de la fourniture aux employés d'une formation spécifique sur le traitement des informations à caractère personnel, etc.

En outre, conformément à l'article 3, paragraphe 5, et à l'article 4 de la PIPA, les personnes concernées ont, entre autres, les droits suivants en ce qui concerne les informations à caractère personnel traitées à des fins de sécurité nationale:

1) le droit d'obtenir la confirmation que des informations à caractère personnel les concernant sont traitées ou non, ainsi que des informations sur le traitement, et le droit d'accéder à ces informations, y compris d'en obtenir des copies (article 4, paragraphes 1 et 3, de la PIPA);

2) le droit de faire suspendre le traitement, ainsi que d'obtenir la correction, l'effacement et la destruction des informations à caractère personnel (article 4, paragraphe 4, de la PIPA).

iii) Une personne concernée peut introduire une demande dans le cadre de l'exercice de ces droits directement auprès du responsable du traitement ou indirectement par l'intermédiaire de la Commission de protection, et peut autoriser son représentant à le faire. Lorsque la personne concernée dépose une demande, le responsable du traitement accorde ce droit sans tarder, à condition, toutefois, qu'il puisse retarder, limiter ou refuser le droit si cela est spécifiquement prévu ou inévitable pour se conformer à d'autres lois, dans la mesure et pour la durée nécessaires et proportionnées à la protection d'un objectif important d'intérêt public (p. ex., dans la mesure et pour la durée où l'octroi du droit compromettrait une enquête en cours ou menacerait la sécurité nationale), ou lorsque l'octroi du droit peut porter atteinte à la vie ou à l'intégrité physique d'un tiers, ou porter une atteinte injustifiée aux biens et à d'autres intérêts d'un tiers. En cas de refus ou de limitation de la demande, il en notifie sans tarder les motifs à la personne concernée. Le responsable du traitement établit la méthode et la procédure permettant aux personnes concernées de déposer des demandes et les annonce publiquement afin que les personnes concernées puissent en prendre connaissance.

En outre, conformément à l'article 58, paragraphe 4, de la PIPA (obligation d'assurer un traitement approprié des griefs individuels) et à l'article 4, paragraphe 5, de la PIPA (droit à une réparation appropriée de tout préjudice résultant du traitement d'informations à caractère personnel, au moyen d'une procédure rapide et équitable), les personnes concernées ont le droit d'obtenir réparation. Cela inclut le droit de signaler une violation présumée au centre de signalement des violations d'informations à caractère personnel (conformément à l'article 62, paragraphe 3, de la PIPA), de déposer une plainte auprès de la PIPC conformément à l'article 62 de la PIPA concernant toute violation des droits ou intérêts liés aux informations à caractère personnel d'une personne et de former un recours en justice contre les décisions ou l'inaction de la PIPC en vertu de la loi sur le contentieux administratif. En outre, les personnes concernées peuvent former un recours en justice en vertu de la loi sur le contentieux administratif s'il y a eu atteinte à leurs droits ou intérêts en raison d'une disposition ou d'une omission du responsable du traitement (p. ex., la collecte illicite de données à caractère personnel), ou obtenir une réparation des préjudices subis conformément à la loi sur l'indemnisation publique. Ces voies de recours sont disponibles tant en cas d'éventuelles violations des règles contenues dans les lois spécifiques fixant les limites et les garanties en matière de collecte d'informations à caractère personnel, telles que les lois sur la sécurité nationale, que dans la PIPA.

Une personne de l'UE peut déposer une plainte auprès de la PIPC par l'intermédiaire de son autorité nationale de protection des données et la PIPC informera la personne par l'intermédiaire de l'autorité nationale de protection des données, une fois que l'enquête et la mesure corrective (le cas échéant) ont pris fin.

ANNEXE II

18 mai 2021

Son Excellence M. Didier Reynders, commissaire à la justice de la Commission européenne

Votre Excellence,

Je me félicite des discussions constructives menées entre la Corée et la Commission européenne visant à mettre en place le cadre pour le transfert de données à caractère personnel de l'UE vers la Corée.

À la demande de la Commission européenne adressée au gouvernement de la Corée, j'ai l'honneur de vous transmettre ci-joint un document qui donne un aperçu du cadre juridique relatif à l'accès à l'information par le gouvernement coréen.

Ce document concerne de nombreux ministères et agences du gouvernement coréen. En ce qui concerne le contenu du document, les ministères et agences concernés (Commission de protection des informations à caractère personnel, ministère de la justice, Service national de renseignement, Commission nationale des droits de l'homme de Corée, Centre national de lutte contre le terrorisme, cellule de renseignement financier de Corée) sont responsables des passages relevant de leurs compétences respectives. Vous trouverez ci-dessous les ministères et agences concernés ainsi que les signatures correspondantes.

La Commission de protection des informations à caractère personnel accepte toutes les questions relatives à ce document et coordonnera les réponses nécessaires entre les ministères et les agences concernés.

J'espère que ce document sera utile pour la prise de décisions à la Commission européenne.

J'apprécie votre précieuse contribution à ce sujet.

Veuillez agréer, Excellence, l'expression de ma haute considération,

윤 종 인

Yoon Jong In
Président de la Commission de protection des informations à caractère personnel

Ce document a été élaboré par la Commission de protection des informations à caractère personnel et les ministères et agences concernés suivants.

박 지 원

Park Jie Won
Président (directeur), Service national de renseignement

이 정 수

Lee Jung Soo
Directeur général, ministère de la justice

Choi Young Ae
Président de la Commission nationale des droits de l'homme de Corée

Kim Hyuck Soo
Directeur, Centre national de lutte contre le terrorisme

Kim Jeong Kag
Commissaire, cellule de renseignement financier de Corée

Cadre juridique relatif à la collecte et à l'utilisation d'informations à caractère personnel par les autorités publiques coréennes à des fins répressives et de sécurité nationale

Le document suivant donne un aperçu du cadre juridique relatif à la collecte et à l'utilisation d'informations à caractère personnel par les autorités publiques coréennes à des fins répressives et de sécurité nationale (ci-après dénommé «*accès des pouvoirs publics*»), notamment en ce qui concerne les bases juridiques disponibles, les conditions applicables (limitations) et les garanties, ainsi que la surveillance indépendante et les possibilités de recours individuels.

1. PRINCIPES JURIDIQUES GÉNÉRAUX APPLICABLES À L'ACCÈS DES POUVOIRS PUBLICS

1.1. Cadre constitutionnel

La Constitution de la République de Corée établit le droit à la vie privée en général (article 17) et le droit au secret de la correspondance en particulier (article 18). Il est du devoir de l'État de garantir ces droits fondamentaux ([1]). La Constitution prévoit en outre que les droits et libertés des citoyens ne peuvent être restreints que par la loi et lorsque cela est nécessaire pour la sécurité nationale, ou le maintien de l'ordre public pour le bien-être de la population ([2]). Même lorsque de telles restrictions sont imposées, elles ne peuvent porter atteinte à l'essence de la liberté ou du droit en jeu ([3]). Les juridictions coréennes ont appliqué ces dispositions dans des cas d'ingérence du gouvernement dans la vie privée. La Cour suprême a estimé, par exemple, que la surveillance des civils violait le droit fondamental à la vie privée, soulignant que les citoyens ont «*le droit à l'autodétermination des informations à caractère personnel*» ([4]). Dans une autre affaire, la Cour constitutionnelle a estimé que la vie privée est un droit fondamental qui confère une protection contre l'intervention et l'observation de l'État dans la vie privée des citoyens ([5]).

La Constitution coréenne garantit en outre que nul ne peut être arrêté, détenu, fouillé, interrogé ou voir ses biens saisis, sauf dans les cas prévus par la loi ([6]). En outre, les perquisitions et les saisies ne peuvent être effectuées que sur la base d'un mandat délivré par un juge, à la demande d'un procureur, et dans le respect d'une procédure régulière ([7]). Dans des circonstances exceptionnelles, c'est-à-dire lorsqu'un suspect est appréhendé alors qu'il est en train de commettre une infraction (flagrant délit), ou lorsqu'il existe un risque qu'une personne soupçonnée d'avoir commis une infraction passible d'une peine d'emprisonnement de trois ans ou plus s'échappe ou détruise des preuves, les autorités chargées de l'enquête peuvent procéder à une perquisition ou à une saisie sans mandat, auquel cas elles doivent demander un mandat a posteriori ([8]). Ces principes généraux sont développés dans des lois spécifiques traitant de la procédure pénale et de la protection des communications (voir ci-dessous pour un aperçu détaillé).

En ce qui concerne les ressortissants étrangers, la Constitution prévoit que leur statut est garanti comme le prescrivent le droit et les traités internationaux ([9]). Plusieurs accords internationaux auxquels la Corée est partie garantissent le droit à 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, si la Constitution fait en principe référence aux droits des «*citoyens*», la Cour constitutionnelle a jugé que les ressortissants étrangers jouissaient eux aussi de droits fondamentaux ([10]). En particulier, la Cour a estimé que la protection de la dignité et de la valeur d'une personne en tant qu'être humain ainsi que le droit à la recherche du bonheur sont des droits

([1]) Article 10 de la Constitution de la République de Corée, promulguée le 17 juillet 1948 (ci-après «la Constitution»).
([2]) Article 37, paragraphe 2, de la Constitution.
([3]) Article 37, paragraphe 2, de la Constitution.
([4]) Décision 96DA42789 de la Cour suprême de Corée du 24 juillet 1998.
([5]) Décision 2002Hun-Ma51 de la Cour constitutionnelle du 30 octobre 2003. De même, dans les décisions 99Hun-Ma513 et 2004Hun-Ma190 (consolidées) du 26 mai 2005, la Cour constitutionnelle a précisé que «*le droit de contrôler ses propres informations à caractère personnel signifie que la personne concernée par les informations a le droit de décider personnellement quand, à qui ou par qui, et dans quelle mesure ses informations seront divulguées ou utilisées. Il s'agit d'un droit fondamental, bien qu'il ne soit pas spécifié dans la Constitution, qui vise à protéger la liberté de décision personnelle contre les risques liés à l'élargissement des fonctions de l'État et des technologies de l'information et de la communication*».
([6]) Article 12, paragraphe 1, première phrase, de la Constitution.
([7]) Article 16 et article 12, paragraphe 3, de la Constitution.
([8]) Article 12, paragraphe 3, de la Constitution.
([9]) Article 6, paragraphe 2, de la Constitution.
([10]) Décision 93Hun-MA120 de la Cour constitutionnelle du 29 décembre 1994. Voir aussi, par exemple, décision 2014Hun-Ma346 de la Cour constitutionnelle (31 mai 2018), dans laquelle la Cour a estimé que le droit constitutionnel d'un ressortissant soudanais retenu à l'aéroport de bénéficier de l'assistance d'un avocat avait été violé. Dans une autre affaire, la Cour constitutionnelle a estimé que la liberté de choisir son lieu de travail légal est étroitement liée au droit à la recherche du bonheur ainsi qu'à la dignité et à la valeur de l'homme, et qu'elle n'est donc pas réservée aux seuls citoyens, mais peut également être garantie aux étrangers qui sont employés légalement en République de Corée (décision 2007Hun-Ma1083 de la Cour constitutionnelle du 29 septembre 2011).

de tout être humain, et pas seulement des citoyens ([11]). La Cour a également précisé que le droit de contrôler ses informations est considéré comme un droit fondamental, fondé sur le droit à la dignité et à la recherche du bonheur et le droit à la vie privée ([12]). Bien que la jurisprudence n'ait jusqu'à présent pas traité spécifiquement du droit à la vie privée des ressortissants non coréens, il est donc largement admis parmi les spécialistes que les articles 12 à 22 de la Constitution (qui comprennent le droit à la vie privée ainsi que la liberté individuelle) énoncent les «*droits des êtres humains*».

Enfin, la Constitution prévoit également le droit de réclamer une juste réparation aux autorités publiques ([13]). En outre, sur la base de la loi sur la Cour constitutionnelle, toute personne dont les droits fondamentaux garantis par la Constitution sont violés par l'exercice du pouvoir gouvernemental (à l'exclusion des jugements des juridictions) peut déposer une plainte constitutionnelle auprès de la Cour constitutionnelle ([14]).

1.2. **Règles générales relatives à la protection des données**

La loi générale relative à la protection des données en République de Corée, à savoir la loi sur la protection des informations à caractère personnel (ci-après la «*PIPA*»), s'applique à la fois au secteur privé et au secteur public. En ce qui concerne les autorités publiques, la PIPA mentionne spécifiquement l'obligation d'élaborer des politiques visant à prévenir l'«*utilisation abusive et détournée des informations à caractère personnel, la surveillance et le suivi indiscrets, etc., et à renforcer la dignité des êtres humains et la vie privée des individus*» ([15]).

Le traitement des données à caractère personnel à des fins répressives est soumis à l'ensemble des exigences de la PIPA. Cela signifie, par exemple, que les autorités chargées de l'application des lois pénales doivent se conformer aux obligations de traitement licite, à savoir se fonder sur l'un des fondements juridiques énumérés dans la PIPA pour la collecte, l'utilisation ou la fourniture d'informations à caractère personnel (articles 15 à 18 de la PIPA), ainsi que sur les principes de limitation des finalités (article 3, paragraphes 1 et 2, de la PIPA), de la proportionnalité et de la minimisation des données (article 3, paragraphes 1 et 6, de la PIPA), de la conservation limitée des données (article 21 de la PIPA), de la sécurité des données, y compris la notification des violations de données (article 3, paragraphe 4, et articles 29 et 34 de la PIPA), et de la transparence (article 3, paragraphes 1 et 5, et articles 20, 30 et 32 de la PIPA). Des garanties spécifiques s'appliquent aux informations sensibles (article 23 de la PIPA). En outre, conformément à l'article 3, paragraphe 5, et à l'article 4 de la PIPA, ainsi qu'aux articles 35 à 39-2 de la PIPA, les personnes peuvent exercer leurs droits d'accès, de rectification, de suppression et de suspension vis-à-vis des autorités chargées de l'application des lois.

Si la PIPA s'applique donc pleinement au traitement des données à caractère personnel à des fins d'application du droit pénal, elle contient une exception lorsque les données à caractère personnel sont traitées à des fins de sécurité nationale. Selon l'article 58, paragraphe 1, point 2, de la PIPA, les articles 15 à 50 de cette loi ne s'appliquent pas aux informations à caractère personnel collectées ou demandées pour l'analyse d'informations liées à la sécurité nationale ([16]). En revanche, le chapitre I (Dispositions générales), le chapitre II (Établissement de politiques de protection des informations à caractère personnel, etc.), le chapitre VIII (Recours collectif en cas de violation des données), le chapitre IX (Dispositions complémentaires) et le chapitre X (Dispositions pénales) de la PIPA restent applicables. Cela inclut les principes généraux de protection des données énoncés à l'article 3 (Principes de protection des informations à caractère personnel) et les droits individuels garantis par l'article 4 de la PIPA (Droits des personnes concernées). Cela signifie que les principes et les droits essentiels sont garantis également dans ce domaine. En outre, l'article 58, paragraphe 4, de la PIPA prévoit que le traitement de ces informations doit être limité à la portée et à la durée minimales nécessaires pour atteindre la finalité visée; elle exige également du responsable du traitement des informations à caractère personnel qu'il mette en place les mesures nécessaires pour assurer une gestion sûre des données et un traitement approprié, telles que des mesures de protection techniques, administratives et physiques, ainsi que des mesures pour le traitement approprié des griefs individuels.

Dans la notification 2021-1 sur les règles supplémentaires pour l'interprétation et l'application de la loi sur la protection des informations à caractère personnel, la Commission de protection des informations à caractère personnel (ci-après la «*PIPC*») a précisé la manière dont la PIPA s'applique au traitement des données à caractère personnel à des fins de sécurité nationale, à la lumière de cette exemption partielle ([17]). Cela comprend notamment les droits des personnes (accès, rectification, suspension et suppression) ainsi que les motifs et les limites d'éventuelles restrictions de ces droits. Selon la notification, l'application des principes, droits et obligations fondamentaux de la PIPA au traitement des données à caractère personnel à des fins de sécurité nationale reflète les garanties fournies par la Constitution pour

([11]) Décision 99HeonMa494 de la Cour constitutionnelle du 29 novembre 2001.
([12]) Voir par exemple décision 99HunMa513 de la Cour constitutionnelle.
([13]) Article 29, paragraphe 1, de la Constitution.
([14]) Article 68, paragraphe 1, de la loi sur la Cour constitutionnelle.
([15]) Article 5, paragraphe 1, de la PIPA.
([16]) Article 58, paragraphe 1, point 2, de la PIPA.
([17]) Notification 2021-1 de la PIPC sur les règles supplémentaires pour l'interprétation et l'application de la loi sur la protection des informations à caractère personnel, section III, point 6.

la protection du droit de la personne à contrôler ses propres informations à caractère personnel. Toute restriction à ce droit, par exemple lorsqu'elle est nécessaire à la protection de la sécurité nationale, nécessite une mise en balance des droits et intérêts de l'individu avec l'intérêt public pertinent et ne peut porter atteinte à l'essence du droit (article 37, paragraphe 2, de la Constitution).

2. ACCÈS DES AUTORITÉS PUBLIQUES À DES FINS RÉPRESSIVES

2.1. Autorités publiques compétentes en matière d'application de la loi

Sur la base du code de procédure pénale (ci-après le «*CPP*»), de la loi sur la protection de la confidentialité des communications (ci-après dénommée «*CPPA*») et de la loi sur les activités de télécommunications (ci-après la «*TBA*»), la police, les procureurs et les juridictions peuvent collecter des données à caractère personnel à des fins d'application de la loi pénale. Dans la mesure où la loi sur le Service national de renseignement confère également ce pouvoir au Service national de renseignement (ci-après le «*NIS*»), celui-ci doit se conformer aux lois susmentionnées ([18]). Enfin, la loi sur la communication et l'utilisation de certaines informations en matière d'opérations financières (ci-après l'«ARUSFTI») fournit une base juridique permettant aux institutions financières de divulguer des informations à la cellule de renseignement financier de Corée (ci-après la «CRFCO») dans le but de prévenir le blanchiment de capitaux et le financement du terrorisme. Cette agence spécialisée peut à son tour fournir ces informations aux autorités chargées de l'application de la loi. Toutefois, ces obligations de divulgation ne s'appliquent qu'aux responsables du traitement qui traitent des informations personnelles en matière de crédit en vertu de la loi sur les informations en matière de crédit et qui sont soumis à la surveillance de la Commission des services financiers. Étant donné que le traitement d'informations personnelles en matière de crédit par ces responsables est exclu du champ d'application de la décision d'adéquation, les limitations et les garanties qui s'appliquent dans le cadre de l'ARUSFTI ne sont pas décrites plus en détail dans le présent document.

2.2. Bases juridiques et limitations

Le CPP (voir section 2.2.1), la CPPA (voir section 2.2.2) et la loi sur les activités de télécommunications (voir section 2.2.3) fournissent des bases juridiques pour la collecte d'informations à caractère personnel à des fins répressives et définissent les limitations et garanties applicables.

2.2.1. *Perquisitions et saisies*

2.2.1.1. Fondement juridique

Les procureurs et les hauts responsables de la police judiciaire ne peuvent inspecter des objets, procéder à des fouilles corporelles ou saisir des objets que 1) si une personne est soupçonnée d'avoir commis une infraction (un suspect); 2) si cela est nécessaire pour l'enquête; et 3) si les objets à inspecter, les personnes à fouiller et les objets éventuellement saisis sont réputés avoir un lien avec l'affaire ([19]). De même, les juridictions peuvent effectuer des perquisitions et saisir tout objet devant servir de preuve ou susceptible d'être confisqué, pour autant que ces objets ou ces personnes soient considérés comme liés à une affaire spécifique ([20]).

2.2.1.2. Limitations et garanties

À titre d'obligation générale, les procureurs et les agents de la police judiciaire doivent respecter les droits de l'homme du suspect ainsi que ceux de toute autre personne concernée ([21]). En outre, les mesures obligatoires pour atteindre le but de l'enquête ne peuvent être prises que si elles sont explicitement prévues par la CPP et doivent être limitées au strict nécessaire ([22]).

Les perquisitions, inspections ou saisies effectuées par des agents de police ou des procureurs dans le cadre d'une enquête pénale ne peuvent avoir lieu que sur la base d'un mandat délivré par une juridiction ([23]). L'autorité qui formule une demande de mandat doit présenter des documents exposant les raisons pour lesquelles un individu est soupçonné d'avoir commis une infraction, et démontrant que la perquisition, l'inspection ou la saisie est nécessaire et que les objets pertinents à saisir existent ([24]). Quant au mandat, il doit, entre autres éléments, contenir les noms du suspect et la qualification de l'infraction, le lieu, la personne ou les objets à fouiller, ou les objets à saisir, la date de délivrance et la période effective d'application ([25]). De même, lorsque, dans le cadre d'une procédure judiciaire en cours, des perquisitions et des saisies sont effectuées ailleurs qu'en audience publique, un mandat délivré par une juridiction doit être obtenu au préalable ([26]). La personne concernée et l'avocat qui la défend sont informés à l'avance de la perquisition ou de la saisie et peuvent être présents lors de l'exécution du mandat ([27]).

([18]) Voir article 3 de la loi sur le NIS (loi n° 12948), qui fait référence aux enquêtes pénales concernant certaines infractions, telles que l'insurrection, la rébellion et les infractions à la sécurité nationale (p. ex., l'espionnage). Les procédures du CPP concernant les perquisitions et les saisies s'appliqueraient dans un tel contexte, tandis que la CPPA régirait la collecte des données de communication (voir partie 3 sur les dispositions relatives à l'accès aux communications à des fins de sécurité nationale).
([19]) Article 215, paragraphes 1 et 2, du CPP.
([20]) Article 106, paragraphe 1, et articles 107 et 109 du CPP.
([21]) Article 198, paragraphe 2, du CPP.
([22]) Article 199, paragraphe 1, du CPP.
([23]) Article 215, paragraphes 1 et 2, du CPP.
([24]) Article 108, paragraphe 1, du règlement sur la procédure pénale.
([25]) Article 114, paragraphe 1, du CPP, en liaison avec l'article 219 du CPP.
([26]) Article 113 du CPP.
([27]) Articles 121 et 122 du CPP.

Lors de perquisitions ou de saisies et lorsque l'objet à perquisitionner est un disque d'ordinateur ou un autre support de stockage de données, en principe seules les données elles-mêmes (copiées ou imprimées) seront saisies plutôt que le support entier ([28]). Le support de données lui-même ne peut être saisi que lorsqu'il est considéré comme fondamentalement impossible d'imprimer ou de copier séparément les données requises, ou lorsqu'il est considéré comme fondamentalement irréaliste d'atteindre autrement le but de la perquisition ([29]). La personne concernée doit être informée de la saisie sans tarder ([30]). Le CPP ne prévoit aucune exception à cette obligation de notification.

Les perquisitions, inspections et saisies sans mandat ne peuvent avoir lieu que dans des cas limités. Tout d'abord, c'est le cas lorsqu'il est impossible d'obtenir un mandat en raison de l'urgence sur les lieux d'une infraction ([31]). Toutefois, un mandat doit ensuite être obtenu sans tarder ([32]). Les perquisitions et inspections sans mandat peuvent également avoir lieu sur place lorsqu'un suspect est arrêté ou détenu ([33]). Enfin, un procureur ou un haut responsable de la police judiciaire peut saisir un objet sans mandat lorsque l'objet a été jeté par un suspect ou une tierce personne, ou a été présenté volontairement ([34]).

Les preuves qui ont été obtenues en violation du CPP seront considérées comme irrecevables ([35]). En outre, le code pénal dispose que les fouilles corporelles illégales ou les perquisitions illégales du lieu de résidence d'une personne, d'un bâtiment gardé, d'une structure, d'un véhicule, d'un navire, d'un aéronef ou d'une pièce occupée sont passibles d'une peine d'emprisonnement de trois ans maximum ([36]). Cette disposition s'applique donc également lorsque des objets, tels que des dispositifs de stockage de données, sont saisis lors d'une perquisition illégale.

2.2.2. *Collecte d'informations sur les communications*

2.2.2.1. Fondement juridique

La collecte d'informations sur les communications est régie par une loi spécifique, la CPPA. En particulier, la CPPA prévoit l'interdiction pour quiconque de censurer tout courrier, de mettre sur écoute toute télécommunication, de fournir des données de confirmation des communications, ou d'enregistrer ou d'écouter toute conversation entre d'autres personnes qui ne sont pas rendues publiques, sauf sur la base du CPP, de la CPPA ou de la loi sur les tribunaux militaires ([37]). Le terme «*communications*» au sens de la CPPA couvre à la fois les courriers ordinaires et les télécommunications ([38]). À cet égard, la CPPA établit une distinction entre les «*mesures de restriction des communications*» ([39]) et la collecte des «*données de confirmation des communications*».

La notion de mesures restrictives des communications couvre la «*censure*», c'est-à-dire la collecte du contenu du courrier postal traditionnel, ainsi que les «*écoutes*», c'est-à-dire l'interception directe (acquisition ou enregistrement) du contenu des télécommunications ([40]). La notion de données de confirmation des communications couvre les «*données sur les enregistrements des télécommunications*», qui comprennent la date des télécommunications, leur heure de début et de fin, le nombre d'appels sortants et entrants ainsi que le numéro d'abonné de l'autre partie, la fréquence d'utilisation, les fichiers journaux sur l'utilisation des services de télécommunications et les informations de localisation (p. ex., à partir des pylônes de transmission où les signaux sont reçus) ([41]).

([28]) Article 106, paragraphe 3, du CPP.
([29]) Article 106, paragraphe 3, du CPP.
([30]) Article 219 du CPP, en liaison avec l'article 106, paragraphe 4, du CPP.
([31]) Article 216, paragraphe 3, du CPP.
([32]) Article 216, paragraphe 3, du CPP.
([33]) Article 216, paragraphes 1 et 2, du CPP.
([34]) Article 218 du CPP. En ce qui concerne les informations à caractère personnel, cela ne couvre que la présentation volontaire par la personne concernée elle-même, et non par un responsable du traitement des informations à caractère personnel détenant ces informations (ce qui nécessiterait une base juridique spécifique en vertu de la loi sur la protection des informations à caractère personnel). Les objets présentés volontairement ne sont admis comme preuves dans une procédure judiciaire que s'il n'y a pas de doute raisonnable quant au caractère volontaire de la divulgation, ce qu'il appartient au procureur de démontrer. Voir décision 2013Do11233 de la Cour suprême du 10 mars 2016.
([35]) Article 308-2 du CPP.
([36]) Article 321 du code pénal.
([37]) Article 3 de la CPPA. La loi sur les tribunaux militaires régit en principe la collecte d'informations sur le personnel militaire et ne peut s'appliquer aux civils que dans un nombre limité de cas (p. ex., si des militaires et des civils commettent ensemble une infraction, ou si un individu commet une infraction contre des militaires, une procédure peut être engagée devant un tribunal militaire, voir article 2 de la loi sur les tribunaux militaires). Les dispositions générales régissant les perquisitions et les saisies sont similaires à celles du CPP, voir par exemple articles 146 à 149 et 153 à 156 de la loi sur les tribunaux militaires. Par exemple, le courrier postal ne peut être collecté que lorsque cela est nécessaire pour une enquête et sur la base d'un mandat du tribunal militaire. Dans la mesure où des communications électroniques seraient collectées, les limitations et les garanties de la CPPA s'appliquent.
([38]) Article 2, paragraphe 1, de la CPPA, c'est-à-dire «*la transmission ou la réception de tous types de sons, de mots, de symboles ou d'images par branchement filaire, sans fil, câble de fibres ou autre système électromagnétique, y compris le téléphone, le courrier électronique, le service d'information des membres, la télécopie et la radiomessagerie*».
([39]) Article 2, paragraphe 7, et article 3, paragraphe 2, de la CPPA.
([40]) La «censure» est définie comme «*l'ouverture du courrier sans le consentement de la partie concernée, ou la prise de connaissance, l'enregistrement ou la rétention de son contenu par d'autres moyens*» (article 2, paragraphe 6, de la CPPA). L'«écoute» signifie «*l'acquisition ou l'enregistrement du contenu de télécommunications par l'écoute ou la lecture commune des sons, mots, symboles ou images des communications au moyen de dispositifs électroniques et mécaniques sans le consentement de la partie concernée, ou l'interférence avec leur transmission et leur réception*» (article 2, paragraphe 7, de la CPPA).
([41]) Article 2, paragraphe 11, de la CPPA.

La CPPA définit les limites et les garanties relatives à la collecte de ces deux types de données, et le non-respect de plusieurs de ces exigences est passible de sanctions pénales ([42]).

2.2.2.2. Limitations et garanties applicables à la collecte du contenu des communications (mesures de restriction des communications)

La collecte du contenu des communications ne peut avoir lieu que comme moyen supplémentaire de faciliter une enquête pénale (c'est-à-dire comme mesure de dernier recours) et il importe de réduire au minimum toute atteinte au secret des communications entre personnes ([43]). Conformément à ce principe général, les mesures de restriction des communications ne peuvent être déployées que lorsqu'il est difficile d'empêcher autrement la commission d'une infraction, d'arrêter l'auteur de celle-ci ou de recueillir des preuves ([44]). Les services répressifs qui collectent le contenu des communications doivent cesser immédiatement de le faire dès que l'accès continu n'est plus jugé nécessaire, ce qui permet de limiter autant que possible l'atteinte à la confidentialité des communications ([45]).

En outre, les mesures de restriction des communications ne peuvent être utilisées que lorsqu'il existe des raisons sérieuses de soupçonner que certaines infractions graves spécifiquement énumérées dans la CPPA sont en train d'être planifiées ou commises ou ont été commises. Il s'agit d'infractions telles que l'insurrection, les infractions liées à la drogue ou aux explosifs, ainsi que les infractions liées à la sécurité nationale, aux relations diplomatiques ou aux bases et installations militaires ([46]). Une mesure de restriction des communications doit cibler des envois postaux ou des télécommunications spécifiques envoyés ou reçus par le suspect, ou des envois postaux ou des télécommunications envoyés ou reçus par le suspect pendant une période déterminée ([47]).

Même lorsque ces conditions sont remplies, la collecte de données relatives au contenu ne peut avoir lieu que sur la base d'un mandat délivré par une juridiction. En particulier, un procureur peut demander à la juridiction d'autoriser la collecte de données relatives au contenu concernant le suspect ou la personne faisant l'objet d'une enquête ([48]). De même, un agent de la police judiciaire peut demander une autorisation à un procureur, qui à son tour peut demander un mandat à la juridiction ([49]). Une demande de mandat doit être faite par écrit et doit contenir des éléments spécifiques. Elle doit notamment exposer 1) les raisons sérieuses qui conduisent à penser qu'une des infractions énumérées est planifiée, en train d'être commise ou a été commise, ainsi que tous les éléments permettant d'établir une preuve à première vue de la suspicion; 2) les mesures de restriction des communications ainsi que leur cible, leur portée, leur objectif et leur période d'effet; et 3) le lieu où les mesures seraient exécutées et la manière dont elles seraient exécutées ([50]).

Lorsque les exigences légales sont remplies, la juridiction peut accorder l'autorisation écrite de mettre en œuvre des mesures de restriction des communications à l'égard du suspect ou de la personne faisant l'objet de l'enquête ([51]). Ce mandat précise les types de mesures ainsi que leur objectif, leur portée, leur période d'effet, leur lieu d'exécution et leurs modalités d'exécution ([52]).

Les mesures de restriction des communications ne peuvent être exécutées que pendant une période de deux mois ([53]). Si l'objectif des mesures est atteint plus tôt au cours de cette période, les mesures doivent être abandonnées immédiatement. À l'inverse, si les conditions requises sont toujours réunies, une demande de prolongation de la période effective des mesures de restriction des communications peut être déposée dans le délai de deux mois. Cette demande doit comporter des éléments justifiant à première vue la prolongation des mesures ([54]). La période prolongée ne peut pas dépasser un an au total, ou trois ans pour certaines infractions particulièrement graves (p. ex., les infractions liées à l'insurrection, à l'agression étrangère, à la sécurité nationale, etc.) ([55]).

Les autorités chargées de l'application de la loi peuvent contraindre les opérateurs de communications à leur prêter assistance en leur fournissant l'autorisation écrite d'une juridiction ([56]). Les opérateurs de communications sont tenus de coopérer et de conserver l'autorisation reçue dans leurs dossiers ([57]). Ils peuvent refuser de coopérer lorsque les informations sur la personne ciblée, telles qu'indiquées dans l'autorisation écrite de la juridiction (par exemple le numéro de téléphone de la personne), sont incorrectes. En outre, il leur est interdit en toutes circonstances de divulguer les mots de passe utilisés pour les télécommunications ([58]).

([42]) Articles 16 et 17 de la CPPA. Cela s'applique par exemple à la collecte sans mandat, à l'absence de conservation de registres, à l'absence d'interruption de la collecte lorsque l'urgence cesse d'exister ou à l'absence de notification à la personne concernée.
([43]) Article 3, paragraphe 2, de la CPPA.
([44]) Article 5, paragraphe 1, de la CPPA.
([45]) Article 2 du décret d'application de la CPPA.
([46]) Article 5, paragraphe 1, de la CPPA.
([47]) Article 5, paragraphe 2, de la CPPA.
([48]) Article 6, paragraphe 1, de la CPPA.
([49]) Article 6, paragraphe 2, de la CPPA.
([50]) Article 6, paragraphe 4, de la CPPA et article 4, paragraphe 1, du décret d'application de la CPPA.
([51]) Article 6, paragraphe 5, et article 6, paragraphe 8, de la CPPA.
([52]) Article 6, paragraphe 6, de la CPPA.
([53]) Article 6, paragraphe 7, de la CPPA.
([54]) Article 6, paragraphe 7, de la CPPA.
([55]) Article 6, paragraphe 8, de la CPPA.
([56]) Article 9, paragraphe 2, de la CPPA.
([57]) Article 15-2 de la CPPA et article 12 du décret d'application de la CPPA.
([58]) Article 9, paragraphe 4, de la CPPA.

Toute personne qui exécute des mesures de restriction des communications ou à qui il est demandé de coopérer doit tenir un registre précisant les objectifs des mesures, leur exécution, la date à laquelle la coopération a été fournie et la cible ([59]). Les autorités chargées de l'application de la loi qui mettent en œuvre des mesures de restriction des communications doivent également tenir des registres indiquant les détails et les résultats obtenus ([60]). Les agents de la police judiciaire doivent fournir ces informations par le biais d'un rapport adressé au procureur lorsqu'ils clôturent une enquête ([61]).

Lorsqu'un procureur émet un acte d'accusation concernant une affaire dans laquelle des mesures de restriction des communications ont été utilisées, ou adopte une décision de ne pas inculper ou arrêter la personne concernée (c'est-à-dire pas seulement un arrêt des poursuites), il doit notifier à la personne faisant l'objet des mesures de restriction des communications le fait que des mesures de restriction des communications ont été exécutées, en précisant quelle agence d'exécution s'en est chargée ainsi que la période d'exécution. Cet avis doit être fourni par écrit dans les 30 jours suivant la décision ([62]). La notification peut être différée lorsqu'elle est susceptible de porter gravement atteinte à la sécurité nationale ou de perturber la sécurité et l'ordre publics, ou lorsqu'elle est susceptible d'entraîner un préjudice important pour la vie et l'intégrité physique d'autrui ([63]). Lorsqu'il a l'intention de différer la notification, le procureur ou l'agent de la police judiciaire doit obtenir l'approbation du parquet de district ([64]). Lorsque les motifs de report cessent d'exister, la notification à ce propos doit être transmise dans les 30 jours à compter de ce moment ([65]).

La CPPA prévoit également une procédure spécifique pour la collecte du contenu des communications dans les situations d'urgence. En particulier, les autorités chargées de l'application de la loi peuvent collecter le contenu des communications en cas d'imminence de la planification ou de l'exécution d'un crime organisé ou d'une autre infraction grave susceptible de causer directement la mort ou des blessures graves, et en cas d'urgence rendant impossible le recours à la procédure normale (comme indiqué ci-dessus) ([66]). Dans une telle situation d'urgence, un agent de police ou un procureur peut prendre des mesures de restriction des communications sans l'autorisation préalable d'une juridiction, mais il doit déposer une demande d'autorisation auprès de la juridiction immédiatement après l'exécution de la mesure. Si l'autorité chargée de l'application de la loi ne parvient pas à obtenir l'autorisation de la juridiction dans un délai de 36 heures à compter du moment où les mesures d'urgence ont été prises, la collecte doit être interrompue immédiatement, et les informations collectées sont généralement détruites ([67]). Les policiers effectuant une surveillance d'urgence le font sous le contrôle d'un procureur ou, dans le cas où il est impossible de recevoir les instructions du procureur à l'avance en raison de la nécessité d'agir en urgence, la police doit obtenir l'approbation d'un procureur dès le début de l'exécution ([68]). Les règles relatives à la notification de l'individu telles que décrites ci-dessus s'appliquent également à la collecte du contenu des communications dans les situations d'urgence.

La collecte d'informations dans des situations d'urgence doit toujours se faire conformément à une «*déclaration de censure/d'écoute d'urgence*» et l'autorité qui procède à la collecte doit tenir un registre de toute mesure d'urgence ([69]). La demande d'autorisation de mesures d'urgence adressée à une juridiction doit être accompagnée d'un document écrit indiquant les mesures de restriction des communications nécessaires, la cible, le sujet, la portée, la période, le lieu d'exécution, la méthode, et une explication de la manière dont les mesures de restriction des communications pertinentes répondent à l'article 5, paragraphe 1, de la CPPA ([70]), ainsi que des documents justificatifs.

Dans les cas où les mesures d'urgence sont réalisées dans un court laps de temps, ce qui exclut l'autorisation d'une juridiction (p. ex., si le suspect est arrêté immédiatement après le déclenchement de l'interception, qui s'arrête donc), le chef du bureau du procureur compétent signifie un avis de mesure d'urgence à la juridiction compétente ([71]). L'avis doit indiquer l'objectif, la cible, la portée, la période, le lieu d'exécution et la méthode de collecte ainsi que les motifs pour lesquels une demande d'autorisation n'a pas été déposée auprès d'une juridiction ([72]). Cet avis permet à la juridiction destinataire d'examiner la légalité de la collecte et doit être inscrit dans un registre des avis de mesures d'urgence.

([59]) Article 9, paragraphe 3, de la CPPA.
([60]) Article 18, paragraphe 1, du décret d'application de la CPPA.
([61]) Article 18, paragraphe 2, du décret d'application de la CPPA.
([62]) Article 9-2, paragraphe 1, de la CPPA.
([63]) Article 9-2, paragraphe 4, de la CPPA.
([64]) Article 9-2, paragraphe 5, de la CPPA.
([65]) Article 9-2, paragraphe 6, de la CPPA.
([66]) Article 8, paragraphe 1, de la CPPA.
([67]) Article 8, paragraphe 2, de la CPPA.
([68]) Article 8, paragraphe 3, de la CPPA et article 16, paragraphe 3, du décret d'application de la CPPA.
([69]) Article 8, paragraphe 4, de la CPPA.
([70]) C'est-à-dire qu'il existe une raison sérieuse de soupçonner que certaines infractions graves sont en train d'être planifiées ou commises, ou ont été commises, et qu'il est impossible d'empêcher autrement la commission d'un crime, d'arrêter le responsable de l'infraction ou de recueillir des preuves.
([71]) Article 8, paragraphe 5, de la CPPA.
([72]) Article 8, paragraphes 6 et 7, de la CPPA.

D'une manière générale, le contenu des communications obtenues par l'exécution de mesures de restriction des communications sur la base de la CPPA ne peut être utilisé que pour enquêter sur les infractions spécifiques énumérées ci-dessus, les poursuivre ou les prévenir, ou dans le cadre de procédures disciplinaires engagées pour les mêmes infractions, d'une demande de dommages et intérêts présentée par une partie aux communications ou lorsque cela est autorisé par d'autres lois ([73]).

Des garanties spécifiques s'appliquent lorsque des télécommunications transmises par l'internet sont collectées ([74]). Ces informations ne peuvent être utilisées que pour enquêter sur les infractions graves énumérées à l'article 5, paragraphe 1, de la CPPA. Pour conserver les informations, il faut obtenir l'approbation de la juridiction qui a autorisé les mesures de restriction des communications ([75]). Une demande de conservation doit contenir des informations sur les mesures de restriction des communications, un résumé des résultats des mesures, les raisons de la conservation (avec les documents justificatifs) et les télécommunications à conserver ([76]). En l'absence d'une telle demande, les télécommunications acquises doivent être supprimées dans les 14 jours suivant la fin des mesures de restriction des communications ([77]). Si une demande est rejetée, les télécommunications doivent être détruites dans les sept jours ([78]). Lorsque les télécommunications sont supprimées, un rapport exposant les raisons de la suppression, ainsi que les détails et le calendrier de celle-ci, doit être déposé dans un délai de sept jours auprès de la juridiction qui a autorisé les mesures de restriction des communications.

Plus généralement, si des informations ont été obtenues illégalement au moyen de mesures de restriction des communications, elles ne seront pas admises comme preuves dans le cadre de procédures judiciaires ou disciplinaires ([79]). En outre, la CPPA interdit à toute personne prenant des mesures de restriction des communications de divulguer les informations confidentielles obtenues dans le cadre de la mise en œuvre de ces mesures, et d'utiliser les informations obtenues pour porter atteinte à la réputation des personnes faisant l'objet de ces mesures ([80]).

2.2.2.3. Limitations et garanties applicables à la collecte d'informations de confirmation des communications

Sur la base de la CPPA, les autorités chargées de l'application des lois peuvent demander aux opérateurs de télécommunications de fournir des données de confirmation des communications lorsque cela est nécessaire pour mener une enquête ou exécuter une peine ([81]). Contrairement à la collecte de données de contenu, la possibilité de collecter des données de confirmation des communications n'est pas limitée à certaines infractions spécifiques. Toutefois, comme c'est le cas pour les données de contenu, la collecte de données de confirmation de communication nécessite l'autorisation écrite préalable d'une juridiction et est soumise aux mêmes conditions que celles décrites précédemment ([82]). Lorsque l'obtention d'une autorisation judiciaire est impossible pour des raisons d'urgence, les données de confirmation des communications peuvent être collectées sans mandat. Dans ce cas, l'autorisation doit être obtenue immédiatement après la demande des données et doit être communiquée au prestataire des services de télécommunications ([83]). Si aucune autorisation ultérieure n'est obtenue, les informations collectées doivent être détruites ([84]).

Les procureurs, les agents de la police judiciaire et les tribunaux doivent tenir un registre des demandes de données de confirmation des communications ([85]). En outre, les fournisseurs de télécommunications doivent rendre compte deux fois par an de la divulgation des données de confirmation des communications au ministre des sciences et des technologies de l'information et de la communication, et doivent conserver ces données pendant sept ans à compter de la date à laquelle elles ont été divulguées ([86]).

Les personnes concernées sont en principe informées du fait que des données de confirmation des communications ont été collectées ([87]). Le moment de cette notification dépend des circonstances de l'enquête ([88]). Une fois que la décision est prise de (ne pas) engager de poursuites, une notification doit être faite dans les 30 jours. Inversement, si la mise en

([73]) Article 12 de la CPPA.
([74]) Article 12-2 de la CPPA.
([75]) Le procureur ou l'agent de police qui exécute les mesures de restriction des communications doit sélectionner les télécommunications à conserver dans les 14 jours suivant la fin des mesures et demander l'approbation de la juridiction (dans le cas d'une affaire de police, la demande doit être faite à un procureur, qui à son tour soumet la demande à la juridiction), voir article 12-2, paragraphes 1 et 2, de la CPPA.
([76]) Article 12-2, paragraphe 3, de la CPPA.
([77]) Article 12-2, paragraphe 5, de la CPPA.
([78]) Article 12-2, paragraphe 5, de la CPPA.
([79]) Article 4 de la CPPA.
([80]) Article 11, paragraphe 2, du décret d'application de la CPPA.
([81]) Article 13, paragraphe 1, de la CPPA.
([82]) Articles 13 et 6 de la CPPA.
([83]) Article 13, paragraphe 2, de la CPPA. Comme pour les mesures urgentes de restriction des communications, un document exposant les détails de l'affaire (le suspect, les mesures à prendre, l'infraction suspectée ainsi que l'urgence) doit être établi. Voir article 37, paragraphe 5, du décret d'application de la CPPA.
([84]) Article 13, paragraphe 3, de la CPPA.
([85]) Article 13, paragraphes 5 et 6, de la CPPA.
([86]) Article 13, paragraphe 7, de la CPPA.
([87]) Voir article 13-3, paragraphe 7, en liaison avec l'article 9-2 de la CPPA.
([88]) Article 13-3, paragraphe 1, de la CPPA.

accusation est suspendue, la notification doit être faite dans un délai de 30 jours un an après la décision de suspension. En tout état de cause, la notification doit être effectuée dans un délai de 30 jours un an après la collecte des informations.

La notification peut être différée si elle est susceptible 1) de mettre en danger la sécurité nationale ou la sécurité et l'ordre publics; 2) de causer la mort ou des blessures corporelles; 3) d'entraver une procédure judiciaire équitable (p. ex. en entraînant la destruction de preuves ou en mettant en danger des témoins); ou 4) de diffamer le suspect, les victimes ou d'autres personnes concernées par l'affaire, ou de porter atteinte à leur vie privée ([89]). La notification pour l'un des motifs susmentionnés requiert l'autorisation du responsable d'un parquet de district compétent ([90]). Lorsque les motifs d'ajournement cessent d'exister, l'avis doit être donné dans un délai de 30 jours à compter de ce moment ([91]).

Les personnes notifiées peuvent présenter une demande écrite au procureur ou à l'agent de la police judiciaire concernant les raisons de la collecte des données de confirmation des communications ([92]). Dans ce cas, le procureur ou l'agent de la police judiciaire doit fournir les motifs par écrit dans les 30 jours suivant la réception de la demande, sauf si l'un des motifs susmentionnés (exceptions au report de la notification) s'applique ([93]).

2.2.3. *Divulgation volontaire par les opérateurs de télécommunications*

L'article 83, paragraphe 3, de la TBA permet aux opérateurs de télécommunications de se conformer volontairement à une demande (faite à l'appui d'un procès pénal, d'une enquête ou de l'exécution d'une peine) d'une juridiction, d'un procureur ou du chef d'un service d'enquête, de divulguer des «*données relatives aux communications*». Dans le contexte de la TBA, les «*données relatives aux communications*» couvrent le nom, le numéro d'enregistrement du résident, l'adresse et le numéro de téléphone des utilisateurs, les dates auxquelles les utilisateurs s'abonnent ou résilient leur abonnement ainsi que les codes d'identification des utilisateurs (c'est-à-dire les codes utilisés pour identifier l'utilisateur légitime des systèmes informatiques ou des réseaux de communication) ([94]). Aux fins de la TBA, seuls les individus qui contractent directement des services auprès d'un fournisseur de télécommunications coréen sont considérés comme des utilisateurs ([95]). Par conséquent, les situations dans lesquelles les personnes de l'UE dont les données ont été transférées en République de Corée seraient considérées comme des utilisateurs au titre de la TBA sont vraisemblablement très limitées, car ces personnes ne sont en principe pas amenées à conclure directement un contrat avec un opérateur de télécommunications coréen.

Les demandes d'obtention de données de communication sur la base de la TBA doivent être faites par écrit et indiquer les raisons de la demande, le lien avec l'utilisateur concerné et la portée des données demandées ([96]). Lorsqu'il est impossible de fournir une demande écrite pour des raisons d'urgence, la demande écrite doit être fournie dès que la raison de l'urgence disparaît ([97]). Les opérateurs de télécommunications qui se conforment aux demandes de divulgation de données de communication doivent conserver des registres contenant des fichiers indiquant que les données de communication ont été fournies, ainsi que les documents connexes, tels que la demande écrite ([98]). En outre, les opérateurs de télécommunications doivent rendre compte de la fourniture de données de communication au ministre des sciences et des TIC deux fois par an ([99]).

Les opérateurs de télécommunications ne sont pas tenus de répondre aux demandes de divulgation de données de communication sur la base de la TBA. Chaque demande doit donc être évaluée par l'opérateur à la lumière des exigences applicables en matière de protection des données en vertu de la PIPA. Un opérateur de télécommunications doit, en particulier, tenir compte des intérêts de la personne concernée et n'est pas autorisé à divulguer les informations si cela est susceptible de porter atteinte de manière déloyale aux intérêts de la personne ou d'un tiers ([100]). En outre, conformément à la notification 2021-1 sur les règles supplémentaires pour l'interprétation et l'application de la loi sur la protection des informations à caractère personnel, il convient de communiquer cette divulgation à la personne concernée. Dans des situations exceptionnelles, cette communication peut être retardée, notamment si et aussi longtemps que la notification risque de compromettre une enquête pénale en cours ou de porter atteinte à la vie ou à l'intégrité physique d'une autre personne, lorsque ces droits ou intérêts sont manifestement supérieurs aux droits de la personne concernée ([101]).

En 2016, la Cour suprême a confirmé que la fourniture volontaire de données de communication par les opérateurs de télécommunications sans mandat sur la base de la TBA ne viole pas en tant que telle le droit à l'autodétermination informationnelle de l'utilisateur du service de télécommunications. Dans le même temps, la Cour a précisé qu'il y aurait violation s'il était manifeste que l'agence requérante avait abusé de son autorité pour demander la divulgation de données de communication, portant ainsi atteinte aux intérêts de l'individu concerné ou d'un tiers ([102]). Plus généralement, toute demande de divulgation volontaire par une autorité répressive doit respecter les principes de licéité, de nécessité et de proportionnalité découlant de la Constitution coréenne (article 12, paragraphe 1, et article 37, paragraphe 2).

([89]) Article 13-3, paragraphe 2, de la CPPA.
([90]) Article 13-3, paragraphe 3, de la CPPA.
([91]) Article 13-3, paragraphe 4, de la CPPA.
([92]) Article 13-3, paragraphe 5, de la CPPA.
([93]) Article 13-3, paragraphe 6, de la CPPA.
([94]) Article 83, paragraphe 3, de la TBA.
([95]) Article 2, paragraphe 9, de la TBA.
([96]) Article 83, paragraphe 4, de la TBA.
([97]) Article 83, paragraphe 4, de la TBA.
([98]) Article 83, paragraphe 5, de la TBA.
([99]) Article 83, paragraphe 6, de la TBA.
([100]) Article 18, paragraphe 2, de la PIPA.
([101]) Notification 2021-1 de la PIPC sur les règles supplémentaires pour l'interprétation et l'application de la loi sur la protection des informations à caractère personnel, section III, paragraphe 2, point iii).
([102]) Décision 2012Da105482 de la Cour suprême du 10 mars 2016.

2.3. **Surveillance**

La surveillance des autorités chargées de l'application du droit pénal s'effectue par le biais de différents mécanismes, tant internes qu'externes.

2.3.1. *Autocontrôle*

Conformément à la loi sur les audits dans le secteur public, les autorités publiques sont encouragées à mettre en place un organe interne d'autocontrôle, chargé, entre autres, d'effectuer un contrôle de la légalité ([103]). L'indépendance des responsables de ces organes de contrôle doit être garantie dans toute la mesure du possible ([104]). Plus précisément, ces responsables sont nommés en dehors de l'autorité compétente (p. ex. anciens juges, professeurs) pour une période de deux à cinq ans et ne peuvent être licenciés que pour des raisons justifiées (p. ex., lorsqu'ils sont incapables de remplir leurs fonctions en raison d'un trouble mental ou physique, lorsqu'ils font l'objet d'une action disciplinaire) ([105]). De même, les auditeurs sont nommés sur la base de conditions spécifiques prévues par la loi ([106]). Les rapports d'audit peuvent inclure des recommandations ou des demandes de compensation ou de correction, ainsi que des réprimandes et des recommandations ou des demandes de mesures disciplinaires ([107]). Ils sont notifiés au chef de l'autorité publique faisant l'objet de l'audit, ainsi qu'au comité d'audit et d'inspection (voir section 2.3.2) dans les 60 jours suivant la fin de l'audit ([108]). L'autorité concernée doit mettre en œuvre les mesures requises et rendre compte des résultats au comité d'audit et d'inspection ([109]). En outre, les résultats des audits sont généralement mis à la disposition du public ([110]). Le refus d'un autocontrôle ou l'entrave à la réalisation de celui-ci est passible d'amendes administratives ([111]). Dans le domaine de l'application de la loi pénale, pour se conformer à la législation susmentionnée, l'Agence nationale de police gère un système d'inspection générale pour traiter les audits internes, notamment en ce qui concerne les éventuelles violations des droits de l'homme ([112]).

2.3.2. *Le comité d'audit et d'inspection*

Le comité d'audit et d'inspection (ci-après le «*BAI*») peut inspecter les activités des autorités publiques et, sur la base de ces inspections, émettre des recommandations, demander des mesures disciplinaires ou déposer une plainte pénale ([113]). Le BAI est placé sous l'autorité du président de la République de Corée, mais conserve un statut indépendant en ce qui concerne ses fonctions ([114]). En outre, la loi instituant le BAI exige que celui-ci bénéficie d'une indépendance maximale en ce qui concerne la nomination, le licenciement et l'organisation de son personnel, ainsi que l'établissement de son budget ([115]). Le président du BAI est nommé par le président de la République, avec le consentement de l'Assemblée nationale ([116]). Les six autres commissaires sont nommés par le président de la République, sur recommandation du président du BAI, pour un mandat de quatre ans ([117]). Les commissaires (y compris le président) doivent posséder des qualifications spécifiques définies par la loi ([118]) et ne peuvent être révoqués qu'en cas de mise en accusation, de condamnation à une peine d'emprisonnement ou d'incapacité à exercer leurs fonctions en raison d'une déficience mentale ou physique durable ([119]). En outre, il est interdit aux commissaires de participer à des activités politiques et d'exercer simultanément des fonctions au sein de l'Assemblée nationale, des agences administratives, des organisations soumises à l'audit et à l'inspection du BAI ou toute autre fonction ou tout autre poste rémunéré(e) ([120]).

Le BAI réalise un audit général tous les ans, mais il peut également mener des audits spécifiques concernant des questions revêtant un intérêt particulier. Le BAI peut demander la présentation de documents au cours d'une inspection et demander la présence de certaines personnes ([121]). Dans le cadre d'un audit, le BAI examine les recettes et les dépenses

([103]) Articles 3 et 5 de la loi sur les audits du secteur public.
([104]) Article 7 de la loi sur les audits du secteur public.
([105]) Articles 8 à 11 de la loi sur les audits du secteur public.
([106]) Articles 16 et suivants de la loi sur les audits du secteur public.
([107]) Article 23, paragraphe 2, de la loi sur les audits du secteur public.
([108]) Article 23, paragraphe 1, de la loi sur les audits du secteur public.
([109]) Article 23, paragraphe 3, de la loi sur les audits du secteur public.
([110]) Article 26 de la loi sur les audits du secteur public.
([111]) Article 41 de la loi sur les audits du secteur public.
([112]) Voir en particulier les divisions relevant du directeur général de l'audit et de l'inspection: https://www.police.go.kr/eng/knpa/org/org01.jsp
([113]) Articles 24 et 31 à 35 de la loi sur le comité d'audit et d'inspection (ci-après la «*loi sur le BAI*»).
([114]) Article 2, paragraphe 1, de la loi sur le BAI.
([115]) Article 2, paragraphe 2, de la loi sur le BAI.
([116]) Article 4, paragraphe 1, de la loi sur le BAI.
([117]) Article 5, paragraphe 1, et article 6 de la loi sur le BAI.
([118]) Par exemple, avoir assumé les fonctions de juge, de procureur ou d'avocat pendant au moins dix ans, avoir été fonctionnaire, avoir exercé la fonction de professeur ou occupé un poste de niveau supérieur dans une université pendant au moins huit ans, ou avoir travaillé pendant au moins dix ans dans une entreprise cotée en bourse ou dans une institution financée par le gouvernement (dont cinq ans au moins en qualité de directeur), voir article 7 de la loi sur le BAI.
([119]) Article 8 de la loi sur le BAI.
([120]) Article 9 de la loi sur le BAI.
([121]) Voir p. ex. article 27 de la loi sur le BAI.

de l'État, mais vérifie également si les autorités et les agents publics se conforment aux obligations qui sont les leurs en vue d'améliorer le fonctionnement de l'administration publique ([122]). Sa surveillance s'étend donc au-delà des aspects budgétaires et comprend également un contrôle de la légalité.

2.3.3. *L'Assemblée nationale*

L'Assemblée nationale peut enquêter sur les autorités publiques et mener des inspections au sein de celles-ci ([123]). Au cours d'une enquête ou d'une inspection, l'Assemblée nationale peut demander la divulgation de documents et exiger la comparution de témoins ([124]). Toute personne commettant un parjure au cours d'une enquête de l'Assemblée nationale est passible de sanctions pénales (emprisonnement jusqu'à dix ans) ([125]). Le processus et les résultats des inspections peuvent être rendus publics ([126]). Si l'Assemblée nationale constate une activité illégale ou répréhensible, elle peut demander que l'autorité publique concernée prenne des mesures correctives, notamment en accordant une réparation, en prenant des mesures disciplinaires et en améliorant ses procédures internes ([127]). À la suite d'une telle demande, l'autorité doit agir sans tarder et rendre compte du résultat à l'Assemblée nationale ([128]).

2.3.4. *La Commission de protection des informations à caractère personnel*

La Commission de protection des informations à caractère personnel (ci-après la «*PIPC*») exerce un contrôle sur le traitement des informations à caractère personnel par les autorités chargées de l'application des lois pénales, conformément à la PIPA. En outre, conformément à l'article 7-8, paragraphes 3 et 4, et à l'article 7-9, paragraphe 5, de la PIPA, la surveillance de la PIPC couvre également les éventuelles infractions aux règles fixant les limites et les garanties en matière de collecte d'informations à caractère personnel, y compris celles contenues dans les lois spécifiques régissant la collecte de preuves (électroniques) aux fins de l'application du droit pénal (voir section 2.2). Étant donné les exigences de l'article 3, paragraphe 1, de la PIPA concernant la collecte licite et loyale des informations à caractère personnel, toute infraction de ce type constitue également une violation de la PIPA, ce qui permet à la PIPC de mener une enquête et de prendre des mesures correctives ([129]).

Dans l'exercice de sa fonction de surveillance, la PIPC a accès à toutes les informations pertinentes ([130]). La PIPC peut conseiller les autorités chargées de l'application de la loi afin d'améliorer le niveau de protection des informations à caractère personnel de leurs activités de traitement, imposer des mesures correctives (p. ex., suspendre le traitement des données ou prendre les mesures nécessaires pour protéger les informations à caractère personnel) ou conseiller à l'autorité de prendre des mesures disciplinaires ([131]). Enfin, des sanctions pénales sont prévues pour certaines violations de la PIPA, telles que l'utilisation ou la divulgation illicites d'informations à caractère personnel à des tiers ou le traitement illicite d'informations sensibles ([132]). À cet égard, la PIPC peut renvoyer l'affaire à l'organisme d'enquête compétent (y compris un procureur) ([133]).

2.3.5. *La Commission nationale des droits de l'homme*

La Commission nationale des droits de l'homme (ci-après la «*CNDH*») — un organe indépendant chargé de protéger et de promouvoir les droits fondamentaux ([134]) — a le pouvoir d'enquêter sur les violations des articles 10 à 22 de la Constitution, qui incluent le droit à la vie privée et le secret de la correspondance, et d'y remédier. La CNDH est composée de 11 commissaires, nommés sur proposition de l'Assemblée nationale (quatre), du président de la République (quatre) et du président de la Cour suprême (trois) ([135]). Pour être nommé, un commissaire doit 1) avoir exercé au moins la fonction de professeur associé pendant au moins dix ans dans une université ou un institut de recherche agréé; 2) avoir assumé les fonctions de juge, de procureur ou d'avocat pendant au moins dix ans; 3) avoir participé à des activités liées aux droits de l'homme pendant au moins dix ans (par exemple, pour une organisation à but non lucratif, une organisation non gouvernementale ou une organisation internationale); ou 4) avoir été recommandé par des groupes de la société civile ([136]). Le président est nommé par le président de la République parmi les commissaires et cette

([122]) Articles 20 et 24 de la loi sur le BAI.
([123]) Article 128 de la loi sur l'Assemblée nationale et articles 2, 3 et 15 de la loi sur les inspections et les enquêtes relatives à l'administration de l'État. Cela comprend des inspections annuelles des affaires gouvernementales dans leur ensemble et des enquêtes sur des questions spécifiques.
([124]) Article 10, paragraphe 1, de la loi sur les inspections et les enquêtes relatives à l'administration de l'État. Voir également les articles 128 et 129 de la loi sur l'Assemblée nationale.
([125]) Article 14 de la loi sur le témoignage, l'évaluation, etc. devant l'Assemblée nationale.
([126]) Article 12-2 de la loi sur les inspections et les enquêtes relatives à l'administration de l'État.
([127]) Article 16, paragraphe 2, de la loi sur les inspections et les enquêtes relatives à l'administration de l'État.
([128]) Article 16, paragraphe 3, de la loi sur les inspections et les enquêtes relatives à l'administration de l'État.
([129]) Voir la notification 2021-1 de la PIPC sur les règles supplémentaires pour l'interprétation et l'application de la loi sur la protection des informations à caractère personnel.
([130]) Article 63 de la PIPA.
([131]) Article 61, paragraphe 2, article 65, paragraphes 1 et 2, et article 64, paragraphe 4, de la PIPA.
([132]) Articles 70 à 74 de la PIPA
([133]) Article 65, paragraphe 1, de la PIPA.
([134]) Article 1er de la loi sur la Commission des droits de l'homme (ci-après la «*loi sur la CNDH*»).
([135]) Article 5, paragraphes 1 et 2, de la loi sur la CNDH.
([136]) Article 5, paragraphe 3, de la loi sur la CNDH.

nomination doit être confirmée par l'Assemblée nationale ([137]). Les commissaires (y compris le président) sont nommés pour un mandat renouvelable d'une durée de trois ans et ne peuvent être révoqués que s'ils sont condamnés à une peine de prison ou ne sont plus en mesure d'exercer leurs fonctions en raison d'une déficience physique ou mentale prolongée (auquel cas les deux tiers des commissaires doivent approuver la révocation) ([138]). Les commissaires de la CNDH ont l'interdiction d'exercer simultanément un mandat à l'Assemblée nationale, dans des conseils locaux ou dans toute administration de l'État ou locale (en qualité de fonctionnaire) ([139]).

La CNDH peut ouvrir une enquête de sa propre initiative ou sur la base d'une requête présentée par un particulier. Dans le cadre de son enquête, la CNDH peut demander la présentation de documents pertinents, effectuer des inspections et citer des personnes à comparaître en qualité de témoins ([140]). À la suite d'une enquête, la CNDH peut émettre des recommandations visant à améliorer ou à corriger des politiques et des pratiques spécifiques, et peut les rendre publiques ([141]). Les autorités publiques doivent informer la CNDH d'un plan de mise en œuvre de ces recommandations dans les 90 jours suivant leur réception ([142]). En outre, en cas de non-application des recommandations, l'autorité concernée doit en informer la Commission ([143]). La CNDH peut à son tour divulguer ce manquement à l'Assemblée nationale et/ou le rendre public. Les autorités publiques se conforment généralement aux recommandations de la CNDH et sont fortement incitées à le faire, car la mise en œuvre de celle-ci a été évaluée dans le cadre de l'évaluation générale menée par le Bureau de coordination des politiques gouvernementales, sous l'autorité du cabinet du Premier ministre.

2.4. **Recours individuel**

2.4.1. *Mécanismes de recours disponibles en vertu de la PIPA*

Les particuliers peuvent exercer leurs droits d'accès, de correction, de suppression et de suspension en vertu de la PIPA en ce qui concerne les informations à caractère personnel traitées par les autorités chargées de l'application des lois pénales. L'accès peut être demandé directement à l'autorité compétente ou indirectement via la PIPC ([144]). L'autorité compétente ne peut limiter ou refuser l'accès que si cela est prévu par la loi, si cela risque de porter atteinte à la vie ou à l'intégrité physique d'un tiers, ou si cela risque d'entraîner une atteinte injustifiée aux intérêts patrimoniaux et autres d'une autre personne (c'est-à-dire si les intérêts de l'autre personne l'emportent sur ceux du particulier qui fait la demande) ([145]). Si une demande d'accès est refusée, la personne doit être informée des raisons de ce refus et de la manière de former un recours ([146]). De même, une demande de rectification ou d'effacement peut être rejetée lorsque cela est prévu par d'autres lois, auquel cas la personne doit être informée des raisons sous-jacentes et de la possibilité de former un recours ([147]).

En ce qui concerne les recours, les particuliers peuvent déposer une plainte auprès de la PIPC, notamment par l'intermédiaire du centre d'appel consacré à la protection de la vie privée géré par l'agence coréenne de l'internet et de la sécurité ([148]). En outre, une personne peut obtenir une médiation par le Comité de médiation des litiges relatifs aux informations à caractère personnel ([149]). Ces voies de recours sont disponibles tant en cas d'éventuelles violations des règles contenues dans les lois spécifiques fixant les limites et les garanties en matière de collecte d'informations à caractère personnel (section 2.2) que de la PIPA. En outre, les particuliers peuvent contester les décisions ou l'inaction de la PIPC en vertu de la loi sur le contentieux administratif (voir section 2.4.3).

([137]) Article 5, paragraphe 5, de la loi sur la CNDH.
([138]) Article 7, paragraphe 1, et article 8 de la loi sur la CNDH.
([139]) Article 10 de la loi sur la CNDH.
([140]) Article 36 de la loi sur la CNDH. En vertu de l'article 36, paragraphe 7, de la loi, la présentation d'éléments ou d'objets peut être refusée si cela risque de porter atteinte à un secret d'État susceptible d'avoir un effet notable sur la sécurité nationale ou les relations diplomatiques ou de constituer un obstacle sérieux à une enquête pénale ou à un procès en cours. Dans de tels cas, la Commission peut demander des informations complémentaires au directeur de l'agence concernée (qui doit satisfaire à cette demande de bonne foi) lorsque cela est nécessaire pour examiner si le refus de fournir les informations est justifié.
([141]) Article 25, paragraphe 1, de la loi sur la CNDH.
([142]) Article 25, paragraphe 3, de la loi sur la CNDH.
([143]) Article 25, paragraphe 4, de la loi sur la CNDH.
([144]) Article 35, paragraphe 2, de la PIPA.
([145]) Article 35, paragraphe 4, de la PIPA.
([146]) Article 42, paragraphe 2, du décret d'application de la PIPA.
([147]) Article 36, paragraphes 1 et 2, de la PIPA et article 43, paragraphe 3, du décret d'application de la PIPA.
([148]) Article 62 de la PIPA.
([149]) Articles 40 à 50 de la PIPA et articles 48-2 à 57 du décret d'application de la PIPA.

2.4.2. *Recours devant la Commission nationale des droits de l'homme*

La CNDH traite les plaintes des particuliers (coréens et étrangers) concernant les violations des droits de l'homme commises par les autorités publiques ([150]). Un particulier n'a pas à prouver sa qualité pour agir pour pouvoir déposer plainte auprès de la CNDH ([151]). En conséquence, une plainte sera traitée par la CNDH même si la personne concernée ne peut pas démontrer un préjudice de fait au stade de l'examen de la recevabilité. Dans le contexte de la collecte de données à caractère personnel à des fins d'application de la loi pénale, une personne ne serait donc pas tenue de démontrer que ses informations à caractère personnel ont effectivement été consultées par les autorités publiques coréennes pour que la plainte soit recevable devant la CNDH. Une personne peut également demander que sa plainte soit traitée par la médiation ([152]).

Pour enquêter sur une plainte, la CNDH peut faire usage de ses pouvoirs d'enquête, notamment en demandant la présentation de documents pertinents, en effectuant des inspections et en citant des personnes à comparaître en qualité de témoins ([153]). Si l'enquête révèle qu'une violation des lois applicables a eu lieu, la CNDH peut recommander la mise en œuvre de mesures correctives ou la rectification ou l'amélioration de toute loi, institution, politique ou pratique pertinente ([154]). Les réparations proposées peuvent inclure la médiation, la cessation de la violation des droits de l'homme, la réparation des préjudices et des mesures pour éviter que de telles violences ne se reproduisent ([155]). En cas de collecte illicite d'informations à caractère personnel en vertu des règles applicables, les mesures correctives peuvent inclure la suppression des informations à caractère personnel collectées. S'il est jugé hautement probable que l'infraction se poursuive et qu'il est probable que, si rien n'est fait, des dommages difficilement réparables seront causés, la CNDH peut adopter des mesures de secours urgentes ([156]).

Bien que la CNDH n'ait pas de pouvoir de contrainte, ses décisions (p. ex., la décision de ne pas poursuivre l'enquête sur une plainte) ([157]) et ses recommandations peuvent être contestées devant les juridictions coréennes en vertu de la loi sur le contentieux administratif (voir section 2.4.3 ci-dessous) ([158]). En outre, si les conclusions de la CNDH révèlent que des données à caractère personnel ont été collectées de manière illicite par une autorité publique, une personne peut demander réparation devant les juridictions coréennes contre cette autorité publique, par exemple en contestant la collecte en vertu de la loi sur le contentieux administratif, en déposant une plainte constitutionnelle en vertu de la loi sur la Cour constitutionnelle ou en demandant une réparation des préjudices en vertu de la loi sur l'indemnisation publique (voir section 2.4.3 ci-dessous).

2.4.3. *Recours juridictionnel*

Les particuliers peuvent invoquer les limitations et les garanties décrites dans les sections précédentes pour obtenir réparation devant les juridictions coréennes par différents moyens.

Premièrement, conformément au CPP, la personne concernée et son conseil peuvent être présents lors de l'exécution d'un mandat de perquisition ou de saisie, et peuvent donc soulever une objection au moment de l'exécution du mandat ([159]). En outre, le CPP prévoit un mécanisme appelé de «quasi-plainte», qui permet aux personnes de saisir la juridiction compétente pour demander l'annulation ou la modification d'une décision prise par un procureur ou un agent de police concernant une saisie ([160]). Cela permet aux particuliers de contester les mesures prises pour exécuter un mandat de saisie.

([150]) Bien que l'article 4 de la loi sur la CNDH fasse référence aux citoyens et aux étrangers résidant en République de Corée, le terme «résidant» renvoie à la notion de juridiction plutôt qu'à celle de territoire. Par conséquent, si les droits fondamentaux d'un étranger résidant hors de Corée sont violés par des institutions nationales en Corée, cette personne peut déposer une plainte auprès de la CNDH. Voir par exemple la question correspondante sur la page des questions fréquemment posées de la CNDH, disponible à l'adresse suivante: https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Tel serait le cas si les données à caractère personnel d'un étranger transférées vers la Corée étaient consultées de manière illicite par des autorités publiques coréennes.

([151]) Une plainte doit en principe être introduite dans un délai d'un an à partir de la violation, mais la CNDH peut néanmoins décider d'enquêter sur une plainte introduite après cette période pour autant que le délai de prescription prévu par le droit pénal ou civil n'ait pas expiré (article 32, paragraphe 1, point 4, de la loi sur la CNDH).

([152]) Articles 42 et suivants de la loi sur la CNDH.

([153]) Articles 36 et 37 de la loi sur la CNDH.

([154]) Article 44 de la loi sur la CNDH.

([155]) Article 42, paragraphe 4, de la loi sur la CNDH.

([156]) Article 48 de la loi sur la CNDH.

([157]) Par exemple, si la CNDH n'est exceptionnellement pas en mesure d'inspecter certains éléments ou équipements, car ces derniers concernent ou contiennent des secrets d'État susceptibles d'avoir un effet notable sur la sécurité nationale ou les relations diplomatiques, ou lorsque l'inspection risque de constituer un obstacle sérieux à une enquête pénale ou un procès en cours (voir note de bas de page 166) et que cela l'empêche de conduire l'enquête nécessaire pour évaluer le bien-fondé de la demande reçue, elle informera la personne des raisons pour lesquelles la plainte a été rejetée, conformément à l'article 39 de la loi sur la CNDH. Dans ce cas, la personne pourrait contester la décision de la CNDH sur la base de la loi sur le contentieux administratif.

([158]) Voir, par exemple, décision 2007Nu27259 de la Haute Cour de Séoul du 18 avril 2008, confirmée par la décision 2008Du7854 de la Cour suprême du 9 octobre 2008; et décision 2017Nu69382 de la Haute Cour de Séoul du 2 février 2018.

([159]) Article 121 et 219 du CPP.

([160]) Article 417 du CPP, en liaison avec l'article 414, paragraphe 2, du CPP. Voir également décision 97Mo66 de la Cour suprême du 29 septembre 1997.

Par ailleurs, les personnes peuvent obtenir une indemnisation devant les juridictions coréennes. En se fondant sur la loi sur l'indemnisation publique, les particuliers peuvent demander réparation des préjudices causés par des agents publics dans l'exercice de leurs fonctions officielles en violation de la loi ([161]). Une demande au titre de la loi sur l'indemnisation publique peut être introduite auprès d'un «conseil de l'indemnisation» spécialisé ou directement auprès des juridictions coréennes ([162]). Si la victime est un ressortissant étranger, la loi sur l'indemnisation publique s'applique pour autant que son pays d'origine garantisse l'indemnisation publique des ressortissants coréens ([163]). Selon la jurisprudence, cette condition est remplie si les exigences pour demander une indemnisation dans l'autre pays «*ne sont pas nettement déséquilibrées entre la Corée et l'autre pays*» et «*ne sont pas généralement plus strictes que celles déterminées par la Corée, n'ayant aucune différence matérielle et substantielle*» ([164]). Le code civil régit la responsabilité de l'État en matière d'indemnisation et, par conséquent, la responsabilité de l'État porte également sur les préjudices non matériels (p. ex., la souffrance morale) ([165]).

En cas de violation des règles de protection des données, un recours juridique supplémentaire est prévu par la PIPA. Selon l'article 39 de la PIPA, toute personne subissant un préjudice du fait d'une violation de la PIPA ou d'une perte, d'un vol, d'une divulgation, d'une falsification, d'une altération ou d'un endommagement de ses informations à caractère personnel peut obtenir une indemnisation devant les juridictions. Il n'y a pas d'exigence de réciprocité similaire à celle de la loi sur l'indemnisation publique.

Outre la réparation des préjudices, un recours administratif peut être introduit contre les actions ou omissions des agences administratives en vertu de la loi sur le contentieux administratif. Tout individu peut contester une disposition (c'est-à-dire l'exercice ou le refus d'exercer la puissance publique dans un cas spécifique) ou une omission (le fait qu'une agence administrative ne prenne pas une certaine disposition pendant une période prolongée contrairement à une obligation légale en la matière), ce qui peut conduire à la révocation/modification d'une disposition illégale, à une constatation de nullité (c'est-à-dire une constatation que la disposition n'a pas d'effet juridique ou son inexistence dans l'ordre juridique) ou à la constatation de l'illégalité d'une omission ([166]). Pour pouvoir contester une disposition administrative, celle-ci doit avoir un impact direct sur les droits et devoirs civils ([167]). Cela inclut les mesures visant à collecter des données à caractère personnel, que ce soit directement (p. ex. en interceptant des communications) ou par le biais d'une demande de divulgation (p. ex. à un prestataire de services).

Les réclamations susmentionnées peuvent d'abord être portées devant les commissions de recours administratif placées sous l'autorité de certaines autorités publiques (p. ex., le NIS, la CNDH) ou devant la Commission centrale de recours administratif, placée sous l'autorité de la Commission pour la lutte contre la corruption et les droits civils ([168]). Un tel recours administratif constitue une autre voie, plus informelle, pour contester une disposition ou une omission d'une autorité publique. Toutefois, une demande peut également être directement introduite devant les juridictions coréennes sur la base de la loi sur le contentieux administratif.

Une demande de révocation/modification d'une disposition en vertu de la loi sur le contentieux administratif peut être déposée par toute personne ayant un intérêt juridique à demander la révocation/modification, ou à être rétablie dans ses droits par la révocation/modification si la disposition ne produit plus d'effets ([169]). De même, une action en nullité peut être intentée par une personne ayant un intérêt juridique à une reconnaissance de nullité, tandis qu'une action visant à faire reconnaître l'illégalité d'une omission peut être introduite par toute personne ayant fait une demande de disposition et ayant un intérêt juridique à demander que l'illégalité de l'omission soit reconnue ([170]). Conformément à la jurisprudence de la Cour suprême, un «intérêt juridique» est interprété comme un «intérêt protégé par le droit», à savoir un intérêt direct et spécifique protégé par les lois et réglementations sur lesquelles les dispositions administratives sont fondées (par opposition aux intérêts généraux, indirects et abstraits du public) ([171]). Les personnes ont donc un intérêt juridique en cas de violation des limitations et des garanties relatives à la collecte de leurs données à caractère personnel à des fins de répression pénale (en vertu de lois spécifiques ou de la PIPA). Un jugement définitif rendu au titre de la loi sur le contentieux administratif est contraignant pour les parties ([172]).

Une demande d'annulation/de modification d'une disposition et une demande de confirmation de l'illégalité d'une omission doivent être introduites dans un délai de 90 jours à compter de la date à laquelle la personne a eu connaissance de la disposition/l'omission et, en principe, au plus tard un an à partir de la date de publication de la disposition

([161]) Article 2, paragraphe 1, de la loi sur l'indemnisation publique.

([162]) Articles 9 et 12 de la loi sur l'indemnisation publique. La loi crée des conseils de district (présidés par le procureur adjoint du bureau du procureur correspondant), un conseil central (présidé par le vice-ministre de la justice) et un conseil spécial (présidé par le vice-ministre de la défense nationale et chargé des demandes de réparation des préjudices infligés par des militaires ou des employés civils de l'armée). Les demandes d'indemnisation sont en principe traitées par les conseils de district, qui, dans certaines circonstances, doivent transmettre l'affaire au conseil central/spécial, par exemple si l'indemnisation dépasse un certain montant ou si une personne demande une nouvelle délibération. Tous les conseils sont composés de membres nommés par le ministre de la Justice (par exemple, parmi les fonctionnaires du ministère de la Justice, des officiers ministériels, des avocats et des personnes possédant une expertise en matière d'indemnisation publique) et sont soumis à des règles spécifiques en matière de conflit d'intérêts (voir l'article 7 du décret d'application de la loi sur l'indemnisation publique).

([163]) Article 7 de la loi sur l'indemnisation publique.

([164]) Décision 2013Da208388 de la Cour suprême du 11 juin 2015.

([165]) Voir l'article 8 de la loi sur l'indemnisation publique, et l'article 751 du code civil.

([166]) Articles 2 et 4 de la loi sur le contentieux administratif.

([167]) Décision 98Du18435 de la Cour suprême du 22 octobre 1999; décision 99Du1113 de la Cour suprême du 8 septembre 2000; et décision 2010Du3541 de la Cour suprême du 27 septembre 2012.

([168]) Article 6 de la loi sur les recours administratifs et article 18, paragraphe 1, de la loi sur le contentieux administratif.

([169]) Article 12 de la loi sur le contentieux administratif.

([170]) Articles 35 et 36 de la loi sur le contentieux administratif.

([171]) Décision 2006Du330 de la Cour suprême du 26 mars 2006.

([172]) Article 30, paragraphe 1, de la loi sur le contentieux administratif.

ou de survenance de l'omission, sauf s'il existe des raisons justifiables ([173]). Selon la jurisprudence de la Cour suprême, la notion de «raisons justifiables» doit être interprétée de manière large et nécessite d'évaluer s'il est socialement acceptable d'autoriser une plainte tardive, à la lumière de toutes les circonstances de l'affaire ([174]). Par exemple, cette notion inclut (entre autres) des motifs de retard pour lesquels la partie concernée ne saurait être tenue pour responsable (c'est-à-dire, une situation échappant au contrôle du plaignant, par exemple lorsqu'il n'a pas été informé de la collecte de ses informations à caractère personnel) ou un cas de force majeure (par exemple, une catastrophe naturelle, une guerre, etc.).

Enfin, les particuliers peuvent également déposer une plainte constitutionnelle auprès de la Cour constitutionnelle ([175]). En vertu de la loi sur la Cour constitutionnelle, toute personne dont les droits fondamentaux garantis par la Constitution sont violés en raison de l'exercice ou du non-exercice du pouvoir gouvernemental (à l'exclusion des jugements des juridictions) peut introduire une plainte constitutionnelle. Si d'autres voies de recours sont disponibles, celles-ci doivent être épuisées en premier lieu. Conformément à la jurisprudence de la Cour constitutionnelle, les ressortissants étrangers peuvent déposer une plainte constitutionnelle dans la mesure où leurs droits fondamentaux sont reconnus par la Constitution coréenne (voir explications figurant à la section 1.1) ([176]). Les plaintes constitutionnelles doivent être introduites dans un délai de 90 jours à compter de la date à laquelle la personne a eu connaissance de la violation, et dans un délai d'un an après sa survenance. Étant donné que la procédure de la loi sur le contentieux administratif est appliquée aux procédures judiciaires relevant de la loi sur la Cour constitutionnelle ([177]), une plainte sera toujours recevable s'il existe des «raisons justifiables» au sens de la jurisprudence de la Cour suprême décrite ci-dessus.

Si d'autres voies de recours doivent être épuisées en premier lieu, une plainte constitutionnelle doit être introduite dans un délai de 30 jours à compter de la décision définitive rendue au terme de ladite voie de recours ([178]). La Cour constitutionnelle peut invalider l'exercice du pouvoir gouvernemental ayant entraîné la violation ou confirmer le caractère inconstitutionnel d'un défaut d'action particulier ([179]). Dans ce cas, l'autorité concernée doit prendre des mesures en vue de se conformer à la décision de la Cour.

3. ACCÈS DES POUVOIRS PUBLICS À DES FINS DE SÉCURITÉ NATIONALE

3.1. Autorités publiques compétentes en matière de sécurité nationale

La République de Corée dispose de deux agences de renseignement spécialisées: le NIS et le commandement du soutien de la défense et de la sécurité. En outre, la police et le ministère public peuvent également recueillir des informations à caractère personnel à des fins de sécurité nationale.

Le NIS, qui a été institué par la loi sur le Service national de renseignement (ci-après la «*loi sur le NIS*»), est placé directement sous l'autorité et la surveillance du président de la République ([180]). En particulier, le NIS collecte, compile et distribue des informations sur les pays étrangers (et la Corée du Nord) ([181]), des renseignements liés à la lutte contre l'espionnage (y compris l'espionnage militaire et industriel), le terrorisme et les activités des organisations criminelles internationales, des renseignements sur certains types d'infractions à la sécurité publique et nationale (p. ex., insurrection intérieure, agression étrangère) et des renseignements liés à la tâche d'assurer la cybersécurité et de prévenir ou de contrer les cyberattaques et les cybermenaces ([182]). La loi sur le NIS, qui institue le NIS et définit ses tâches, fournit également des principes généraux qui encadrent toutes ses activités. En règle générale, le NIS doit respecter la neutralité politique et protéger les libertés et les droits des personnes ([183]). Le président du NIS est chargé d'élaborer des directives générales qui définissent les principes, le champ d'application et les procédures d'exécution des tâches du NIS en matière de collecte et d'utilisation des informations, et doit en faire rapport à l'Assemblée nationale ([184]). L'Assemblée nationale (par l'intermédiaire de sa commission du renseignement) peut exiger que les lignes directrices soient corrigées ou complétées si elle estime qu'elles sont illégales ou injustes. Plus généralement, dans l'exercice de leurs fonctions, le directeur et le personnel du NIS ne peuvent contraindre une institution, une organisation ou une personne à accomplir une action sans qu'elle y soit obligée, ni entraver l'exercice des droits d'un individu, en abusant de leur autorité officielle ([185]). En outre, toute censure de courrier, interception de télécommunications,

([173]) Article 20 de la loi sur le contentieux administratif. Ce délai s'applique également à une demande visant à affirmer l'illégalité d'une omission, voir l'article 38, paragraphe 2, de la loi sur le contentieux administratif.
([174]) Décision 90Nu6521 de la Cour suprême du 28 juin 1991.
([175]) Article 68, paragraphe 1, de la loi sur la Cour constitutionnelle.
([176]) Décision 99HeonMa194 de la Cour constitutionnelle du 29 novembre 2001.
([177]) Article 40 de la loi sur la Cour constitutionnelle.
([178]) Article 69 de la loi sur la Cour constitutionnelle.
([179]) Article 75, paragraphe 3, de la loi sur la Cour constitutionnelle.
([180]) Article 2 et article 4, paragraphe 2, de la loi sur le NIS.
([181]) Cette notion ne couvre pas les informations sur les individus, mais les informations générales sur les pays étrangers (tendances, évolutions) et sur les activités des acteurs étatiques des pays tiers.
([182]) Article 3, paragraphe 1, de la loi sur le NIS.
([183]) Article 3, paragraphe 1, article 6, paragraphe 2, article 11 et article 21. Voir également règles relatives aux conflits d'intérêts, en particulier les articles 10 et 12.
([184]) Article 4, paragraphe 2, de la loi sur le NIS.
([185]) Article 13 de la loi sur le NIS.

collecte d'informations de localisation, collecte de données de confirmation des communications ou enregistrement ou écoute de communications privées par le NIS doit être conforme à la CPPA, à la loi sur les informations de localisation ou au CPP ([186]). Tout abus de pouvoir ou toute collecte d'informations en violation de ces lois est passible de sanctions pénales ([187]).

Le commandement du soutien de la défense et de la sécurité est une agence de renseignement militaire, établie sous la tutelle du ministère de la défense. Il est responsable des questions de sécurité au sein de l'armée, des enquêtes pénales militaires (soumises à la loi sur les tribunaux militaires) et du renseignement militaire. En général, le commandement du soutien de la défense et de la sécurité ne surveille pas les civils, à moins que cela ne soit nécessaire à l'exercice de ses fonctions militaires. Les personnes qui peuvent faire l'objet d'une enquête sont le personnel militaire, les employés civils de l'armée, les personnes en formation militaire, les réservistes et les recrues, ainsi que les prisonniers de guerre ([188]). Lorsqu'il collecte des informations sur les communications à des fins de sécurité nationale, le commandement du soutien de la défense et de la sécurité est soumis aux limitations et aux garanties prévues par la CPPA et son décret d'application.

3.2. **Bases juridiques et limitations**

La CPPA, la loi antiterroriste pour la protection des citoyens et la sécurité publique (ci-après «*loi antiterroriste*») et la TBA fournissent des bases juridiques pour la collecte d'informations à caractère personnel à des fins de sécurité nationale et définissent les limitations et garanties applicables ([189]). Ces limitations et garanties, décrites dans les sections suivantes, garantissent que la collecte et le traitement des informations sont limités à ce qui est strictement nécessaire pour atteindre un objectif légitime. Cela exclut la collecte massive et indifférenciée d'informations à caractère personnel à des fins de sécurité nationale.

3.2.1. *Collecte d'informations sur les communications*

3.2.1.1. Collecte d'informations sur les communications par les agences de renseignement

3.2.1.1.1. Fondement juridique

La CPPA habilite les agences de renseignement à collecter des données de communication et exige des fournisseurs de communications qu'ils coopèrent avec les demandes de ces agences ([190]). Comme décrit à la section 2.2.2.1, la CPPA fait la distinction entre la collecte du contenu des communications [c'est-à-dire les «*mesures de restriction des communications*» telles que les mesures d'«*écoute*» ou de «*censure*» ([191])], et la collecte des «*données de confirmation des communications*» ([192]).

Le seuil de collecte de ces deux types d'informations diffère, mais les procédures et garanties applicables sont dans une large mesure identiques ([193]). La collecte de données de confirmation des communications (ou métadonnées) peut avoir lieu dans le but de lutter contre les menaces à sécurité nationale ([194]). Un seuil plus élevé s'applique à l'exécution des mesures de restriction des communications (c'est-à-dire à la collecte du contenu des communications), qui ne peuvent être prises que lorsque la sécurité nationale risque d'être gravement menacée et que la collecte de renseignements est nécessaire pour lutter contre ce danger (c'est-à-dire s'il existe un risque grave pour la sécurité nationale et que la collecte est nécessaire pour l'éviter) ([195]). En outre, le contenu des communications ne peut être consulté qu'en dernier recours pour garantir la sécurité nationale, et il faut tout mettre en œuvre pour réduire au minimum la violation de la confidentialité des communications ([196]). Même lorsque l'approbation/autorisation appropriée a été obtenue, ces mesures doivent être arrêtées immédiatement dès qu'elles ne sont plus nécessaires, ce qui garantit que toute atteinte aux secrets des communications de l'individu est limitée au minimum ([197]).

3.2.1.1.2. Limitations et garanties applicables à la collecte d'informations sur les communications concernant au moins un ressortissant coréen

La collecte d'informations sur les communications (contenu et métadonnées) lorsque l'une des personnes concernées par la communication ou les deux sont des ressortissants coréens ne peut avoir lieu qu'avec l'autorisation d'un haut

([186]) Article 14 de la loi sur le NIS.
([187]) Articles 22 et 23 de la loi sur le NIS.
([188]) Article 1er de la loi sur les tribunaux militaires.
([189]) Lorsqu'ils enquêtent sur des infractions à la sécurité nationale, la police et le NIS agissent sur la base du CPP, tandis que le commandement du soutien de la défense et de la sécurité est soumis à la loi sur les tribunaux militaires.
([190]) Article 15-2 de la CPPA.
([191]) Article 2, paragraphes 6 et 7, de la CPPA.
([192]) Article 2, paragraphe 11, de la CPPA.
([193]) Voir également l'article 13-4, paragraphe 2, de la CPPA et l'article 37, paragraphe 4, du décret d'application de la CPPA, en vertu desquels les procédures applicables à la collecte du contenu des communications s'appliquent mutatis mutandis à la collecte des données de confirmation des communications.
([194]) Article 13-4 de la CPPA.
([195]) Article 7, paragraphe 1, de la CPPA.
([196]) Article 3, paragraphe 2, de la CPPA.
([197]) Article 2 du décret d'application de la CPPA.

magistrat de la Haute Cour ([198]). La demande de l'agence de renseignement doit être adressée par écrit à un procureur ou à un bureau du procureur général ([199]). Elle doit indiquer les raisons de la collecte (c'est-à-dire que la sécurité nationale risque d'être gravement menacée ou que la collecte est nécessaire pour prévenir les menaces à la sécurité nationale), ainsi que les éléments étayant ces raisons et établissant une preuve à première vue, ainsi que les détails de la demande (c'est-à-dire les objectifs, la ou les personnes visées, la portée, la période effective de la collecte, ainsi que la méthode et le lieu de la collecte) ([200]). Le procureur/bureau du procureur général demande à son tour l'autorisation d'un haut magistrat de la Haute Cour ([201]). Le haut magistrat ne peut accorder une autorisation écrite que s'il estime que la demande est justifiée et rejette la demande s'il la considère sans fondement ([202]). Le mandat précise le type, l'objectif, la cible, la portée et la période effective de la collecte, ainsi que le lieu et la manière dont elle peut avoir lieu ([203]).

Des règles spécifiques s'appliquent dans le cas où la mesure vise à enquêter sur un acte de conspiration qui menace la sécurité nationale et qu'il existe une urgence qui rend impossible de passer par les procédures susmentionnées ([204]). Lorsque ces conditions sont remplies, les agences de renseignement peuvent exécuter des mesures de surveillance sans l'approbation préalable d'une juridiction ([205]). Toutefois, immédiatement après l'exécution des mesures d'urgence, l'agence de renseignement doit demander l'autorisation de la juridiction. Si l'autorisation n'est pas obtenue dans un délai de 36 heures à partir du moment où les mesures sont prises, elles doivent être interrompues immédiatement ([206]). La collecte d'informations dans des situations d'urgence doit toujours se faire conformément à une «déclaration de censure/d'écoute d'urgence» et l'agence de renseignement qui effectue la collecte doit tenir un registre de toutes les mesures d'urgence ([207]).

Si la mesure de surveillance est mise en œuvre sur une courte période, ce qui exclut l'autorisation de la juridiction, le chef du bureau du procureur général compétent doit transmettre un avis de mesure d'urgence préparé par l'agence de renseignement au président de la juridiction compétente, qui conserve le registre des mesures d'urgence ([208]). Cela permet à la juridiction d'examiner la légalité de la collecte.

3.2.1.1.3. Limitations et garanties applicables à la collecte d'informations sur les communications impliquant uniquement des ressortissants non coréens

Pour collecter des informations sur des communications échangées exclusivement entre des ressortissants non coréens, les agences de renseignement doivent obtenir au préalable l'approbation écrite du président de la République ([209]). Ces communications ne seront collectées à des fins de sécurité nationale que si elles entrent dans l'une des catégories énumérées, à savoir les communications entre des responsables gouvernementaux ou d'autres individus de pays hostiles à la République de Corée, des agences, groupes ou ressortissants étrangers soupçonnés de se livrer à des activités anticoréennes ([210]), ou des membres de groupes situés dans la péninsule coréenne et échappant effectivement à la souveraineté de la République de Corée et leurs groupes de tutelle basés dans des pays étrangers ([211]). Inversement, si l'une des parties à une communication est un ressortissant coréen et l'autre un ressortissant non coréen, l'approbation de la juridiction sera requise conformément à la procédure décrite à la section 3.2.1.1.2.

Le chef d'une agence de renseignement doit soumettre au directeur du NIS un plan relatif aux mesures qu'il entend prendre ([212]). Le directeur du NIS examine si le plan est approprié et, si c'est le cas, le soumet à l'approbation du président de la République ([213]). Les informations qui doivent être incluses dans le plan sont les mêmes que celles requises pour une demande d'autorisation judiciaire de collecte d'informations sur des ressortissants coréens (comme décrit ci-dessus) ([214]). Il doit notamment indiquer les raisons de la collecte (c'est-à-dire que la sécurité nationale risque d'être gravement menacée ou que la collecte est nécessaire pour lutter contre les menaces à la sécurité nationale), les principaux motifs de suspicion, ainsi que les éléments étayant ces motifs et établissant une preuve à première vue, ainsi

([198]) Article 7, paragraphe 1, point 1, de la CPPA. La juridiction compétente est la Haute Cour du lieu du domicile ou du siège de l'une ou des deux parties soumises à la surveillance.
([199]) Article 7, paragraphe 3, du décret d'application de la CPPA.
([200]) Article 7, paragraphe 3, et article 6, paragraphe 4, de la CPPA.
([201]) Article 7, paragraphe 4, du décret d'application de la CPPA. La demande du procureur au tribunal doit exposer les principaux motifs de suspicion et, dans la mesure où plusieurs autorisations sont demandées en même temps, leur justification (voir article 4 du décret d'application de la CPPA).
([202]) Article 7, paragraphe 3, article 6, paragraphe 5, et article 6, paragraphe 9, de la CPPA.
([203]) Article 7, paragraphe 3, et article 6, paragraphe 6, de la CPPA.
([204]) Article 8 de la CPPA.
([205]) Article 8, paragraphe 1, de la CPPA.
([206]) Article 8, paragraphe 2, de la CPPA.
([207]) Article 8, paragraphe 4, de la CPPA. Voir ci-dessus section 2.2.2.2 pour les mesures d'urgence dans le cadre de l'application de la loi.
([208]) Article 8, paragraphes 5 et 7, de la CPPA. Cet avis doit indiquer l'objectif, la cible, la portée, la période, le lieu d'exécution de la surveillance et la méthode de surveillance, ainsi que les motifs justifiant l'absence de demande avant l'adoption de la mesure (article 8, paragraphe 6, de la CPPA).
([209]) Article 7, paragraphe 1, point 2, de la CPPA.
([210]) Il s'agit d'activités qui menacent l'existence et la sécurité de la nation, l'ordre démocratique ou la survie et la liberté de la population.
([211]) En outre, si l'une des parties est une personne décrite à l'article 7, paragraphe 1, point 2, de la CPPA et que l'autre est inconnue ou ne peut être spécifiée, la procédure prescrite par l'article 7, paragraphe 1, point 2, s'appliquera.
([212]) Article 8, paragraphe 1, du décret d'application de la CPPA. Le directeur du NIS est nommé par le président de la République après confirmation par le Parlement (article 7 de la loi sur le NIS).
([213]) Article 8, paragraphe 2, du décret d'application de la CPPA.
([214]) Article 8, paragraphe 3, du décret d'application de la CPPA, en liaison avec l'article 6, paragraphe 4, de la CPPA.

que les détails de la demande (c'est-à-dire les objectifs, la ou les personnes visées, la portée, la période effective de collecte, ainsi que la méthode et le lieu de la collecte). Lorsque plusieurs autorisations sont demandées en même temps, il indique leur objet et leurs motifs ([215]).

Dans les situations d'urgence ([216]), il faut obtenir l'autorisation préalable du ministre dont dépend l'agence de renseignement concernée. Toutefois, dans ce cas, l'agence de renseignement doit demander l'approbation du président de la République immédiatement après que les mesures d'urgence ont été prises. Si une agence de renseignement n'obtient pas d'approbation dans les 36 heures suivant la demande, la collecte doit être interrompue immédiatement ([217]). Dans ce cas, les informations collectées seront toujours détruites.

3.2.1.1.4. Limitations générales et garanties

Lorsqu'elles demandent la coopération d'entités privées, les agences de renseignement doivent leur fournir le mandat de la juridiction/l'autorisation présidentielle ou une copie de la couverture d'une déclaration de censure d'urgence, que l'entité contrainte doit conserver dans ses dossiers ([218]). Les entités auxquelles il est demandé de divulguer des informations aux agences de renseignement sur la base de la CPPA peuvent refuser de le faire lorsque l'autorisation ou la déclaration de censure d'urgence fait référence à un identifiant erroné (p. ex., un numéro de téléphone appartenant à une personne différente de celle identifiée). En outre, dans aucun cas, les mots de passe utilisés pour les communications ne peuvent être divulgués ([219]).

Les services de renseignement peuvent confier la mise en œuvre de mesures de restriction des communications ou la collecte d'informations de confirmation des communications à un bureau de poste ou à un fournisseur de services de télécommunications (tel que défini par la loi sur les entreprises de télécommunications) ([220]). Tant l'agence de renseignement compétent que le fournisseur recevant une demande de coopération doivent conserver pendant trois ans des registres indiquant l'objet de la demande de mesures, la date d'exécution ou de coopération et l'objet des mesures (p. ex., courrier, communications téléphoniques, courrier électronique) ([221]). Les fournisseurs de services de télécommunications qui fournissent des données de confirmation des communications doivent conserver les informations sur la fréquence de la collecte dans leurs dossiers pendant sept ans et faire rapport deux fois par an au ministre des sciences et des TIC ([222]).

Les agences de renseignement doivent rendre compte au directeur du NIS des informations qu'elles ont recueillies et du résultat de l'activité de surveillance ([223]). En ce qui concerne la collecte des données de confirmation des communications, elles doivent conserver les documents attestant qu'une demande de ces données a été faite, ainsi que la demande écrite elle-même et le nom de l'institution qui s'en est servie ([224]).

La collecte tant du contenu des communications que des données de confirmation des communications ne peut avoir lieu que pendant une période maximale de quatre mois et, si l'objectif poursuivi est atteint entre-temps, elle doit être immédiatement interrompue ([225]). Si les conditions de l'autorisation demeurent, le délai peut être prolongé de quatre mois au maximum, avec l'autorisation de la juridiction ou l'approbation du président de la République. La demande d'approbation de l'extension des mesures de surveillance doit être faite par écrit, en indiquant les raisons pour lesquelles l'extension est demandée et en fournissant des pièces justificatives ([226]).

En fonction de la base juridique de la collecte, les personnes sont généralement informées lorsque leurs communications sont collectées. En particulier, indépendamment du fait que les informations recueillies concernent le contenu des communications ou les données de confirmation des communications et qu'elles aient été obtenues selon la procédure ordinaire ou dans une situation d'urgence, le chef de l'agence de renseignement doit notifier par écrit la mesure de surveillance à la personne concernée dans les 30 jours suivant la date à laquelle la surveillance a pris fin ([227]). La notification doit mentionner 1) le fait que les informations ont été collectées, 2) l'agence d'exécution et 3) la période

([215]) Article 8, paragraphe 3, et article 4 du décret d'application de la CPPA.
([216]) C'est-à-dire des situations dans lesquelles, lorsque la mesure vise une entente qui menace la sécurité nationale, il n'y a pas suffisamment de temps pour obtenir l'approbation du président de la République et la non-adoption des mesures d'urgence peut porter atteinte à la sécurité nationale (article 8, paragraphe 8, de la CPPA).
([217]) Article 8, paragraphe 9, de la CPPA.
([218]) Article 9, paragraphe 2, de la CPPA et article 12 du décret d'application de la CPPA.
([219]) Article 9, paragraphe 4, de la CPPA.
([220]) Article 13 du décret d'application de la CPPA.
([221]) Article 9, paragraphe 3, de la CPPA et article 17, paragraphe 2, du décret d'application de la CPPA. Cette durée ne s'applique pas aux données de confirmation des communications (voir article 39 du décret d'application de la CPPA).
([222]) Article 13, paragraphe 7, de la CPPA et article 39 du décret d'application de la CPPA.
([223]) Article 18, paragraphe 3, du décret d'application de la CPPA.
([224]) Article 13, paragraphes 5, et article 13-4, paragraphe 3, de la CPPA.
([225]) Article 7, paragraphe 2, de la CPPA.
([226]) Article 7, paragraphe 2, de la CPPA et article 5 du décret d'application de la CPPA.
([227]) Article 9-2, paragraphe 3, de la CPPA. Conformément à l'article 13-4 de la CPPA, cela s'applique tant à la collecte du contenu des communications qu'à celle des données de confirmation des communications.

d'exécution. Toutefois, s'il est probable que la notification mettrait en danger la sécurité nationale ou porterait atteinte à la vie et à la sécurité physique des personnes, la notification peut être différée ([228]). La notification doit être effectuée dans un délai de 30 jours à partir du moment où les motifs du report cessent d'exister ([229]).

Cette obligation de notification ne s'applique toutefois qu'à la collecte d'informations lorsqu'au moins une des parties est un ressortissant coréen. En conséquence, les ressortissants non coréens ne seront avertis que lorsque leurs communications avec des ressortissants coréens seront collectées. Il n'y a donc pas d'obligation de notification lorsque des communications intervenant exclusivement entre des ressortissants non coréens sont collectées.

Le contenu de toute communication ainsi que les données de confirmation des communications acquises par la surveillance sur la base de la CPPA ne peuvent être utilisés que 1) pour l'enquête, la poursuite ou la prévention de certaines infractions; 2) pour des procédures disciplinaires; 3) pour des procédures judiciaires lorsqu'une partie liée à la communication les invoque dans une demande de dommages et intérêts; ou 4) sur la base d'autres lois ([230]).

3.2.1.2. Collecte d'informations sur les communications par la police/les procureurs à des fins de sécurité nationale

La police/le procureur peut recueillir des informations sur les communications (tant le contenu des communications que les données de confirmation des communications) à des fins de sécurité nationale dans les mêmes conditions que celles décrites à la section 3.2.1.1. Lorsqu'il convient d'agir dans des situations d'urgence ([231]), la procédure applicable est celle qui a été décrite précédemment en ce qui concerne la collecte du contenu des communications à des fins répressives dans des situations d'urgence (c'est-à-dire l'article 8 de la CPPA).

3.2.2. *Collecte d'informations sur les individus soupçonnés d'activités terroristes*

3.2.2.1. Fondement juridique

La loi antiterroriste habilite le directeur du NIS à recueillir des informations sur les individus soupçonnés d'activités terroristes ([232]). Un «*individu soupçonné d'activités terroristes*» est défini comme un membre d'un groupe terroriste ([233]), une personne qui a fait la propagande d'un groupe terroriste (en promouvant et en diffusant les idées ou les tactiques d'un groupe terroriste), a collecté ou contribué à des fonds pour le terrorisme ([234]), ou s'est engagée dans d'autres activités de préparation, de conspiration, de propagande ou d'instigation du terrorisme, ou une personne pour laquelle il existe de bonnes raisons de soupçonner qu'elle s'est livrée à de telles activités ([235]). En règle générale, tout agent public chargé d'appliquer la loi antiterroriste doit respecter les droits fondamentaux inscrits dans la Constitution coréenne ([236]).

La loi antiterroriste n'établit pas en soi de pouvoirs, de limites et de garanties spécifiques pour la collecte d'informations sur les individus soupçonnés d'activités terroristes, mais renvoie plutôt aux procédures prévues par d'autres lois. Premièrement, sur la base de la loi antiterroriste, le directeur du NIS peut recueillir 1) des informations sur l'entrée et la sortie de la République de Corée, 2) des informations sur les transactions financières et 3) des informations sur les communications. Selon le type d'information recherché, les exigences procédurales pertinentes sont prévues respectivement dans la loi sur l'immigration et la loi sur les douanes, l'ARUSFTI ou la CPPA ([237]). Pour la collecte d'informations sur l'entrée et la sortie de Corée, la loi antiterroriste renvoie aux procédures définies dans la loi sur l'immigration et la loi sur les douanes. Toutefois, ces lois ne prévoient pas actuellement de tels pouvoirs. En ce qui concerne la collecte

([228]) Article 9-2, paragraphe 4, de la CPPA.
([229]) Article 13-4, paragraphe 2, et article 9-2, paragraphe 6, de la CPPA.
([230]) Article 5, paragraphes 1 et 2, article 12 et article 13-5, de la CPPA.
([231]) C'est-à-dire lorsque la mesure vise un acte de conspiration qui menace la sécurité nationale et qu'il existe une urgence qui rend impossible le recours à la procédure d'approbation ordinaire (article 8, paragraphe 1, de la CPPA).
([232]) Article 9 de la loi antiterroriste.
([233]) Un «*groupe terroriste*» est défini comme un groupe de terroristes désignés par les Nations unies (article 2, paragraphe 2, de la loi antiterroriste).
([234]) Le «*terrorisme*» est défini par l'article 2, paragraphe 1, de la loi antiterroriste comme un comportement visant à entraver l'exercice de l'autorité de l'État, d'un gouvernement local ou d'un gouvernement étranger (y compris les gouvernements locaux et les organisations internationales), à obliger celui-ci à prendre des mesures sans qu'il y soit légalement tenu ou à menacer le public. Cela comprend a) le fait de tuer une personne ou de mettre sa vie en danger en lui infligeant des blessures corporelles ou en arrêtant, séquestrant, enlevant ou prenant en otage une personne; b) certains types de comportements visant un aéronef (p. ex., un accident, un détournement ou l'endommagement d'un aéronef en vol); c) certains types de comportements liés à un navire (p. ex., s'emparer d'un navire ou d'une structure marine en service, détruire un navire ou une structure marine en service ou leur infliger des dommages d'une ampleur telle que leur sécurité est compromise, y compris la détérioration de la cargaison chargée sur un navire ou une structure marine en service); d) le fait de placer, de faire exploser ou d'utiliser de toute autre manière une arme ou un dispositif biochimique, explosif ou incendiaire dans l'intention de causer la mort, des blessures graves ou des dégâts matériels importants, ou d'avoir un tel effet sur certains types de véhicules ou d'installations (p. ex., trains, tramways, véhicules à moteur, parcs publics et gares, installations d'approvisionnement en électricité, gaz et télécommunications, etc.); e) certains types de comportements liés aux matières nucléaires, aux matières radioactives ou aux installations nucléaires (p. ex., porter atteinte à des vies humaines, à l'intégrité physique ou à des biens, ou perturber de toute autre manière la sécurité publique en détruisant un réacteur nucléaire ou en manipulant de manière illégale des matières radioactives, etc.).
([235]) Article 2, paragraphe 3, de la loi antiterroriste.
([236]) Article 3, paragraphe 3, de la loi antiterroriste.
([237]) Article 9, paragraphe 1, de la loi antiterroriste.

d'informations sur les communications et les transactions financières, la loi antiterroriste renvoie aux limitations et aux garanties prévues par la CPPA (qui sont expliquées plus en détail ci-dessous) et l'ARUSFTI (qui, comme expliqué à la section 2.1, n'est pas pertinente aux fins de l'évaluation de la décision d'adéquation).

En outre, l'article 9, paragraphe 3, de la loi antiterroriste précise que le directeur du NIS peut demander des informations à caractère personnel ou des informations de localisation d'un individu soupçonné d'activités terroristes à un responsable du traitement d'informations à caractère personnel ([238]) ou à un fournisseur d'informations de localisation ([239]). Cette possibilité est limitée aux demandes de divulgation volontaire, auxquelles les responsables du traitement des informations à caractère personnel et les fournisseurs d'informations de localisation ne sont pas tenus de répondre et, en tout état de cause, auxquelles ils ne peuvent répondre que conformément à la PIPA et à la loi sur les informations de localisation (voir section 3.2.2.2 ci-dessous).

3.2.2.2. Limitations et garanties s'appliquant à la divulgation volontaire en vertu de la PIPA et de la loi sur les informations de localisation

Les demandes de coopération volontaire au titre de la loi antiterroriste doivent être limitées aux informations sur les individus soupçonnés d'activités terroristes (voir ci-dessus section 3.2.2.1). Toute demande de ce type émanant du NIS doit être conforme aux principes de licéité, de nécessité et de proportionnalité découlant de la Constitution coréenne (article 12, paragraphe 1, et article 37, paragraphe 2) ([240]) ainsi qu'aux exigences de la PIPA en matière de collecte d'informations à caractère personnel (article 3, paragraphe 1, de la PIPA, voir section 1.2 ci-dessus). La loi sur le NIS précise en outre que le NIS ne peut contraindre une institution, une organisation ou une personne à accomplir une action sans qu'elle y soit obligée, ni faire obstacle à l'exercice des droits d'un individu, en abusant de son autorité officielle ([241]). Une violation de cette interdiction peut faire l'objet de sanctions pénales ([242]).

Les responsables du traitement d'informations à caractère personnel et les fournisseurs d'informations de localisation qui reçoivent des demandes du NIS sur la base de la loi antiterroriste ne sont pas tenus de s'y conformer. Ils peuvent s'y conformer sur une base volontaire, mais ne sont autorisés à le faire que conformément à la PIPA et à la loi sur les informations de localisation. En ce qui concerne le respect de la PIPA, le responsable du traitement doit, en particulier, tenir compte des intérêts de la personne concernée et n'est pas autorisé à divulguer les informations si cela est susceptible de porter atteinte de manière déloyale aux intérêts de la personne ou d'un tiers ([243]). En outre, conformément à la notification 2021-1 sur les règles supplémentaires pour l'interprétation et l'application de la loi sur la protection des informations à caractère personnel, il convient de communiquer cette divulgation à la personne concernée. Dans des situations exceptionnelles, cette communication peut être retardée, notamment si et aussi longtemps que la notification risque de compromettre une enquête pénale en cours ou de porter atteinte à la vie ou à l'intégrité physique d'une autre personne, lorsque ces droits ou intérêts sont manifestement supérieurs aux droits de la personne concernée ([244]).

3.2.2.3. Limitations et garanties en vertu de la CPPA

Sur la base de la loi antiterroriste, les agences de renseignement ne peuvent collecter des informations sur les communications (tant le contenu des communications que les données de confirmation des communications) que lorsque cela est nécessaire pour des activités de lutte contre le terrorisme, c'est-à-dire des activités liées à la prévention du terrorisme et aux contre-mesures en la matière. Les procédures de la CPPA décrites à la section 3.2.1 s'appliquent à la collecte d'informations de communication à des fins de lutte contre le terrorisme.

3.2.3. *Divulgation volontaire par les opérateurs de télécommunications*

Sur la base de la TBA, les opérateurs de télécommunications peuvent se conformer à une demande de divulgation de «données de communication» émanant d'une agence de renseignement qui a l'intention de collecter ces informations pour contrer une menace à la sécurité nationale ([245]). Toute demande de ce type doit être conforme aux principes de licéité, de nécessité et de proportionnalité découlant de la Constitution coréenne (article 12, paragraphe 1, et article 37, paragraphe 2) ([246]) ainsi qu'aux exigences de la PIPA en matière de collecte d'informations à caractère personnel (article 3, paragraphe 1, de la PIPA, voir section 1.2 ci-dessus). En outre, les mêmes limitations et garanties que pour les divulgations volontaires à des fins d'application de la loi s'appliquent (voir section 2.2.3) ([247]).

([238]) Comme défini à l'article 2 de la PIPA, c'est-à-dire une institution publique, une personne morale, une organisation, un individu, etc. qui traite des informations à caractère personnel directement ou indirectement pour exploiter des fichiers d'informations à caractère personnel à des fins officielles ou commerciales.

([239]) Comme défini à l'article 5 de la loi sur la protection, l'utilisation, etc. des informations de localisation (ci-après la «loi sur les informations de localisation»), c'est-à-dire toute personne ayant obtenu l'autorisation de la Commission coréenne des communications d'exercer une activité liée aux informations de localisation.

([240]) Voir également article 3; paragraphes 2 et 3, de la loi antiterroriste.

([241]) Article 11, paragraphe 1, de la loi sur le NIS.

([242]) Article 19 de la loi sur le NIS.

([243]) Article 18, paragraphe 2, de la PIPA.

([244]) Notification 2021-1 de la PIPC sur les règles supplémentaires pour l'interprétation et l'application de la loi sur la protection des informations à caractère personnel, section III, paragraphe 2, point iii).

([245]) Article 83, paragraphe 3, de la TBA.

([246]) Voir également article 3; paragraphes 2 et 3, de la loi antiterroriste.

([247]) En particulier, la demande doit être formulée par écrit et indiquer les raisons de la demande, ainsi que le lien avec l'utilisateur concerné et la portée des informations demandées, et le fournisseur de services de télécommunications doit tenir des registres et faire rapport au ministre des sciences et des TIC deux fois par an.

Les opérateurs de télécommunications ne sont pas tenus de satisfaire ces demandes, mais peuvent le faire sur une base volontaire et uniquement dans le respect de la PIPA. À cet égard, les mêmes obligations, y compris en ce qui concerne la notification de la personne, s'appliquent aux opérateurs du secteur des télécommunications que lorsqu'ils reçoivent des demandes des services répressifs, comme expliqué plus en détail à la section 2.2.3.

3.3. **Surveillance**

Différents organes supervisent les activités des agences de renseignement coréennes. La surveillance du commandement du soutien de la défense et de la sécurité est assurée par le ministère de la défense nationale, conformément à la directive du ministère sur la mise en œuvre de l'audit interne. Le NIS est soumis au contrôle du pouvoir exécutif, de l'Assemblée nationale et d'autres organes indépendants, comme expliqué plus en détail ci-dessous.

3.3.1. *Le délégué à la protection des droits de l'homme*

Lorsque les agences de renseignement recueillent des informations sur des individus soupçonnés d'activités terroristes, la loi antiterroriste prévoit une surveillance par la Commission de lutte contre le terrorisme et le délégué à la protection des droits de l'homme (ci-après le «HRPO») ([248]).

La Commission de lutte contre le terrorisme élabore notamment des politiques concernant les activités de lutte contre le terrorisme et supervise la mise en œuvre des mesures de lutte en la matière ainsi que les activités des différentes autorités compétentes dans ce domaine ([249]). La Commission est présidée par le Premier ministre et composée de plusieurs ministres et directeurs d'agences gouvernementales, dont le ministre des affaires étrangères, le ministre de la justice, le ministre de la défense nationale, le ministre de l'intérieur et de la sécurité, le directeur du NIS, le commissaire général de l'Agence nationale de police et le président de la Commission des services financiers ([250]). Lorsqu'il mène des enquêtes antiterroristes et qu'il recherche des individus soupçonnés d'activités terroristes afin de recueillir des informations ou des éléments nécessaires aux activités de lutte en la matière, le directeur du NIS doit faire rapport au président de la Commission de lutte contre le terrorisme (c'est-à-dire le Premier ministre) ([251]).

La loi antiterroriste institue en outre le HRPO afin de protéger les droits fondamentaux des personnes contre les atteintes causées par les activités de lutte contre le terrorisme ([252]). Le HRPO est nommé par le président de la Commission de lutte contre le terrorisme parmi les personnes qui répondent aux qualifications énumérées dans le décret d'application de la loi antiterroriste [c'est-à-dire toute personne qualifiée en tant qu'avocat ayant au moins dix ans d'expérience professionnelle, ou ayant des connaissances spécialisées dans le domaine des droits de l'homme et exerçant ou ayant exercé (au moins) la fonction de professeur associé pendant au moins dix ans, ou ayant exercé la fonction de haut fonctionnaire dans des agences d'État ou des gouvernements locaux, ou ayant au moins dix ans d'expérience professionnelle dans le domaine des droits de l'homme, par exemple dans une organisation non gouvernementale] ([253]). Le HRPO est nommé pour deux ans (avec possibilité de renouvellement du mandat) et ne peut être démis de ses fonctions que pour des motifs spécifiques et limités et pour une raison valable, par exemple en cas d'inculpation dans une affaire pénale liée à ses fonctions, en cas de divulgation d'informations confidentielles ou en raison d'une incapacité mentale ou physique de longue durée ([254]).

Dans le cas de ses attributions, le HRPO peut émettre des recommandations pour améliorer la protection des droits de l'homme par les agences impliquées dans les activités de lutte contre le terrorisme, et traiter les demandes au civil (voir section 3.4.3) ([255]). Lorsque l'existence d'une violation des droits de l'homme par un agent public dans l'exercice de ses fonctions officielles peut être raisonnablement établie, le HRPO peut recommander au chef de l'agence responsable de corriger cette violation ([256]). À son tour, l'agence responsable doit notifier au HRPO les actions entreprises pour mettre en œuvre cette recommandation ([257]). Si une agence ne met pas en œuvre une recommandation du HRPO, l'affaire est portée devant la Commission, y compris son président, le Premier ministre. Jusqu'à présent, il n'y a pas eu de cas où les recommandations du HRPO n'ont pas été mises en œuvre.

3.3.2. *L'Assemblée nationale*

Comme décrit dans la section 2.3.2, l'Assemblée nationale peut enquêter sur les autorités publiques et mener des inspections au sein de celles-ci, et, dans ce contexte, demander la divulgation de documents et imposer la comparution de témoins. En ce qui concerne les questions relevant de la compétence du NIS, ce contrôle parlementaire est assuré par la Commission du renseignement de l'Assemblée nationale ([258]). Le directeur du NIS, qui supervise l'exécution des tâches

([248]) Article 7 de la loi antiterroriste.
([249]) Article 5, paragraphe 3, de la loi antiterroriste.
([250]) Article 3, paragraphe 1, du décret d'application de la loi antiterroriste.
([251]) Article 9, paragraphe 4, de la loi antiterroriste.
([252]) Article 7 de la loi antiterroriste.
([253]) Article 7, paragraphe 1, du décret d'application de la loi antiterroriste.
([254]) Article 7, paragraphe 3, du décret d'application de la loi antiterroriste.
([255]) Article 8, paragraphe 1, du décret d'application de la loi antiterroriste.
([256]) Article 9, paragraphe 1, du décret d'application de la loi antiterroriste. Le HRPO décide de manière autonome de l'adoption des recommandations, mais il doit rendre compte de ces recommandations au président de la Commission de lutte contre le terrorisme.
([257]) Article 9, paragraphe 2, du décret d'application de la loi antiterroriste.
([258]) Article 36 et article 37, paragraphe 1, point 16, de la loi sur l'Assemblée nationale.

de l'agence, rend compte à la Commission du renseignement (ainsi qu'au président de la République) ([259]). Cette commission elle-même peut également demander un rapport sur une question spécifique, et le directeur du NIS est tenu de répondre sans tarder ([260]). Le directeur ne peut refuser de répondre ou de témoigner devant la Commission du renseignement qu'en ce qui concerne les secrets d'État relatifs à des questions militaires, diplomatiques ou liées à la Corée du Nord, lorsque leur divulgation peut avoir une incidence grave sur le destin national ([261]). Dans ce cas, la Commission du renseignement peut demander une explication au Premier ministre. Si cette explication n'est pas fournie dans les sept jours suivant la demande, la réponse ou le témoignage ne peut plus être refusé(e).

Si l'Assemblée nationale constate qu'il y a eu une activité illégale ou répréhensible, elle peut demander que l'autorité publique concernée prenne des mesures correctives, par exemple, l'octroi d'une indemnisation, l'adoption de mesures disciplinaires ou l'amélioration de procédures internes ([262]). À la suite d'une telle demande, l'autorité doit agir sans tarder et rendre compte du résultat à l'Assemblée nationale. Des règles spécifiques concernant le contrôle parlementaire existent en ce qui concerne l'utilisation de mesures de restriction des communications (c'est-à-dire la collecte du contenu des communications) dans le cadre de la CCPA ([263]). En ce qui concerne ce dernier point, l'Assemblée nationale peut demander aux directeurs des agences de renseignement un rapport sur toute mesure spécifique de restriction des communications. En outre, elle peut procéder à des inspections sur place du matériel d'écoute. Enfin, les agences de renseignement qui ont collecté et les opérateurs qui ont divulgué des informations sur le contenu à des fins de sécurité nationale doivent rendre compte de cette divulgation sur demande de l'Assemblée nationale.

3.3.3. *Le comité d'audit et d'inspection*

Le BAI exerce les mêmes fonctions de contrôle à l'égard des agences de renseignement que dans le domaine de l'application des lois pénales (voir section 2.3.2) ([264]).

3.3.4. *La Commission de protection des informations à caractère personnel*

En ce qui concerne le traitement des données à des fins de sécurité nationale, y compris la phase de collecte, un contrôle supplémentaire est effectué par la PIPC. Comme expliqué plus en détail à la section 1.2, cela inclut les principes et obligations généraux énoncés à l'article 3 et à l'article 58, paragraphe 4, de la PIPA ainsi que l'exercice des droits individuels garantis par l'article 4 de la PIPA. En outre, conformément à l'article 7-8, paragraphes 3 et 4, et à l'article 7-9, paragraphe 5, de la PIPA, la surveillance de la PIPC couvre également les éventuelles infractions aux règles contenues dans des lois spécifiques fixant les limites et les garanties en matière de collecte d'informations à caractère personnel, telles que la CPPA, la loi antiterroriste et la TBA. Étant donné les exigences de l'article 3, paragraphe 1, de la PIPA concernant la collecte licite et loyale des informations à caractère personnel, toute violation de ces lois constitue une violation de la PIPA. La PIPC a donc le pouvoir d'enquêter ([265]) sur les violations des lois régissant l'accès aux données à des fins de sécurité nationale ainsi que des règles de traitement de la PIPA, et de donner des conseils pour améliorer la situation, d'imposer des mesures correctives, de recommander des actions disciplinaires et de soumettre les infractions potentielles aux autorités d'enquête compétentes ([266]).

3.3.5. *La Commission nationale des droits de l'homme*

La surveillance exercée par la CNDH s'applique de la même manière aux agences de renseignement qu'aux autres autorités gouvernementales (voir section 2.3.2).

3.4. **Recours individuel**

3.4.1. *Recours devant le délégué à la protection des droits de l'homme*

En ce qui concerne la collecte d'informations à caractère personnel dans le cadre des activités antiterroristes, une voie de recours spécifique est offerte par le HRPO, placée sous l'autorité de la Commission de lutte contre le terrorisme. Le HRPO traite les demandes au civil liées à la violation des droits de l'homme en conséquence des activités de lutte contre le terrorisme ([267]). Il peut recommander une action corrective et l'agence concernée doit rendre compte au délégué de toute mesure prise pour mettre en œuvre cette recommandation. Un particulier n'a pas à prouver sa qualité pour agir pour pouvoir déposer plainte auprès de la CNDH. En conséquence, une plainte sera traitée par le HRPO même si la personne concernée ne peut pas démontrer un préjudice de fait au stade de la recevabilité.

([259]) Article 18 de la loi sur le NIS.
([260]) Article 15, paragraphe 2, de la loi sur le NIS.
([261]) Article 17, paragraphe 2, de la loi sur le NIS. Les «secrets d'État» sont définis comme «*des faits, des biens ou des connaissances (classés comme tels) qui ne doivent pas être divulgués à un autre pays ou une autre organisation, afin d'éviter tout préjudice grave pour la sécurité nationale, et dont l'accès n'est autorisé qu'à un nombre limité de personnes*», voir article 13, paragraphe 4, de la loi sur le NIS.
([262]) Article 16, paragraphe 2, de la loi sur les inspections et les enquêtes relatives à l'administration de l'État.
([263]) Article 15 de la CPPA.
([264]) Comme c'est le cas pour la Commission du renseignement de l'Assemblée nationale, le directeur du NIS ne peut refuser de répondre au BAI que sur des questions qui constituent des secrets d'État et si leur divulgation risquait d'avoir de graves conséquences pour la sécurité nationale (article 13, paragraphe 1, de la loi sur le NIS).
([265]) Article 63 de la PIPA.
([266]) Article 61, paragraphe 2, article 65, paragraphes 1 et 2, et article 64, paragraphe 4, de la PIPA.
([267]) Article 8, paragraphe 1, point 2, du décret d'application de la loi antiterroriste.

3.4.2. *Mécanismes de recours disponibles en vertu de la PIPA*

Les personnes peuvent exercer leurs droits d'accès, de correction, de suppression et de suspension en vertu de la PIPA en ce qui concerne les informations à caractère personnel traitées à des fins de sécurité nationale ([268]). Les demandes d'exercice de ces droits peuvent être déposées directement auprès de l'agence de renseignement, ou indirectement via la PIPC. L'agence de renseignement peut retarder, limiter ou refuser l'exercice du droit dans la mesure et aussi longtemps que nécessaire et proportionné pour protéger un objectif important d'intérêt public (p. ex., dans la mesure et aussi longtemps que l'octroi du droit compromettrait une enquête en cours ou menacerait la sécurité nationale), ou lorsque l'octroi du droit peut porter atteinte à la vie ou à l'intégrité physique d'un tiers. Lorsque la demande est refusée ou restreinte, la personne doit être informée sans tarder des raisons.

En outre, conformément à l'article 58, paragraphe 4, de la PIPA (obligation d'assurer un traitement approprié des griefs individuels) et à l'article 4, paragraphe 5, de la même loi (droit à une réparation appropriée de tout préjudice résultant du traitement d'informations à caractère personnel, au moyen d'une procédure rapide et équitable), les personnes ont le droit d'obtenir réparation. Cela inclut le droit de signaler une violation présumée au centre d'appel consacré à la protection de la vie privée géré par l'agence coréenne de l'internet et de la sécurité et de déposer plainte auprès de la PIPC ([269]). Ces voies de recours sont disponibles à la fois en cas d'éventuelles violations des règles contenues dans les lois spécifiques fixant les limitations et les garanties en matière de collecte d'informations à caractère personnel à des fins de sécurité nationale et de la PIPA. Comme expliqué dans la notification 2021-1, une personne de l'Union européenne peut déposer une plainte auprès de la PIPC par l'intermédiaire de son autorité nationale de protection des données. Dans ce cas, la PIPC informera la personne concernée par l'entremise de l'autorité nationale de la protection des données une fois l'enquête terminée (y compris, le cas échéant, avec des informations sur les mesures correctives imposées). Les décisions ou l'inaction de la PIPC peuvent faire l'objet d'un recours devant les juridictions coréennes en vertu de la loi sur le contentieux administratif.

3.4.3. *Recoursdevant la Commission nationale des droits de l'homme*

La possibilité d'introduire un recours individuel devant le CNDH s'applique de la même manière aux agences de renseignement qu'aux autres autorités gouvernementales (voir section 2.4.2).

3.4.4. *Recours juridictionnel*

Comme c'est le cas pour les activités des autorités chargées de l'application des lois pénales, les particuliers peuvent introduire une procédure judiciaire contre les agences de renseignement en ce qui concerne les violations des limitations et des garanties susmentionnées au moyen de différentes voies de recours.

Tout d'abord, les particuliers peuvent obtenir une indemnisation pour les préjudices subis en vertu de la loi sur l'indemnisation publique. Par exemple, dans une affaire, une indemnisation a été accordée pour une surveillance illicite par le commandement du soutien de la défense (le prédécesseur du commandement du soutien de la défense et de la sécurité) ([270]).

Deuxièmement, la loi sur le contentieux administratif permet aux individus de contester les dispositions et omissions des agences administratives, y compris les agences de renseignement ([271]).

Enfin, les individus peuvent déposer une plainte constitutionnelle auprès de la Cour constitutionnelle contre les mesures prises par les agences de renseignement sur la base de la loi sur la Cour constitutionnelle.

([268]) Article 3, paragraphe 5, et article 4, paragraphes 1, 3 et 4, de la PIPA.
([269]) Article 62 et article 63, paragraphe 2, de la PIPA.
([270]) Décision 96Da42789 de la Cour suprême du 24 juillet 1998.
([271]) Articles 3 et 4 de la loi sur le contentieux administratif.