II

(Actes non législatifs)

DÉCISIONS

DÉCISION D'EXÉCUTION (UE) 2019/419 DE LA COMMISSION

du 23 janvier 2019

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

[notifiée sous le numéro C(2019) 304]

(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]) (RGPD), et notamment son article 45, paragraphe 3,

après consultation du Contrôleur européen de la protection des données,

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 européenne, vers des pays tiers et à des organisations internationales, dans la mesure où ces transferts relèvent de son champ d'application. Les règles relatives aux transferts internationaux de données à caractère personnel sont définies au chapitre V dudit règlement, plus précisément aux articles 44 à 50. La circulation des données à caractère personnel en provenance ou à destination de pays non membres de l'Union européenne est nécessaire au développement de la coopération internationale et des échanges internationaux, tout en garantissant que le niveau de protection des données à caractère personnel au sein de l'Union européenne n'est pas compromis.

(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 ce pays tiers, ce territoire, ce secteur ou cette organisation internationale 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 du 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. L'évaluation doit déterminer si le pays tiers en question assure un niveau de protection «essentiellement équivalent» à celui qui est garanti dans l'Union [considérant 104 du règlement (UE) 2016/679]. Comme l'a précisé la Cour de justice de l'Union européenne, un niveau de protection identique n'est pas requis ([2]). En particulier, les moyens auxquels ce pays tiers a recours 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 ([3]). Le principe d'adéquation n'exige donc pas que l'on reproduise à l'identique les règles de

([1]) JO L 119 du 4.5.2016, p. 1.
([2]) Affaire C-362/14, Maximillian Schrems/Data Protection Commissioner («Schrems»), ECLI:EU:C:2015:650, point 73.
([3]) Arrêt Schrems, point 74.

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 requis de protection ([4]).

(4) La Commission a soigneusement analysé la législation et les pratiques japonaises. Sur la base des constatations exposées aux considérants 6 à 175, elle conclut que le Japon assure un niveau de protection adéquat des données à caractère personnel transférées aux organisations relevant du champ d'application de la loi sur la protection des informations à caractère personnel ([5]), sous réserve des conditions supplémentaires auxquelles la présente décision renvoie. Ces conditions sont définies dans les règles supplémentaires (annexe I) adoptées par la Commission de protection des informations à caractère personnel (PPC) ([6]) et les déclarations, assurances et engagements officiels formulés par le gouvernement japonais à l'intention de la Commission européenne (annexe II).

(5) La présente décision a pour effet d'autoriser les transferts d'un responsable du traitement ou d'un sous-traitant de l'Espace économique européen (EEE) ([7]) vers de telles organisations au Japon sans qu'il soit nécessaire d'obtenir une autre autorisation. Elle n'a aucune incidence sur l'application directe des dispositions du règlement (UE) 2016/679 à ces organisations lorsque les conditions de son article 3 sont remplies.

2. LES RÈGLES APPLICABLES AU TRAITEMENT DES DONNÉES PAR LES OPÉRATEURS ÉCONOMIQUES

2.1. Le cadre japonais de protection des données

(6) Le régime juridique régissant la protection de la vie privée et la protection des données au Japon trouve son origine dans la Constitution promulguée en 1946.

(7) L'article 13 de la Constitution dispose ce qui suit:

«Tous les citoyens sont respectés en tant qu'individus. Leur droit à la vie et à la liberté ainsi que la poursuite du bonheur sont, dans la mesure où ils n'interfèrent pas avec le bien-être public, la considération suprême dans la législation et dans d'autres affaires gouvernementales.»

(8) Sur la base de cet article, la Cour suprême japonaise a précisé les droits des individus en matière de protection des informations à caractère personnel. Dans une décision de 1969, elle a reconnu le droit au respect de la vie privée et à la protection des données comme un droit constitutionnel ([8]). La Cour a notamment estimé que «chaque individu a la liberté d'empêcher que ses informations à caractère personnel soient divulguées à un tiers ou rendues publiques sans raison valable». En outre, dans un arrêt du 6 mars 2008 («Juki-Net») ([9]), la Cour suprême a considéré que «la liberté des citoyens dans le cadre de leur vie privée doit être protégée contre l'exercice de l'autorité publique et il peut être interprété que chaque individu a, entre autres libertés ayant trait à la vie privée, la liberté d'empêcher que ses informations à caractère personnel soient divulguées à un tiers ou rendues publiques sans raison valable» ([10]).

(9) Le 30 mai 2003, le Japon a adopté une série de lois dans le domaine de la protection des données:

— la loi sur la protection des informations à caractère personnel (APPI),

— la loi sur la protection des informations à caractère personnel détenues par des instances administratives (APPIHAO),

— la loi sur la protection des informations à caractère personnel détenues par des agences administratives intégrées (APPI-IAA).

([4]) Voir la 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.
([5]) Loi sur la protection des informations à caractère personnel (loi n° 57, 2003).
([6]) De plus amples informations sur la PPC sont disponibles à l'adresse suivante: https://www.ppc.go.jp/en/ (coordonnées en cas de questions ou de plaintes: https://www.ppc.go.jp/en/contactus/access/).
([7]) 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.
([8]) Cour suprême, arrêt du Grand Bench du 24 décembre 1969, Keishu vol. 23, n° 12, p. 1625.
([9]) Cour suprême, arrêt du 6 mars 2008, Minshu vol. 62, n° 3, p. 665.
([10]) Cour suprême, arrêt du 6 mars 2008, Minshu vol. 62, n° 3, p. 665.

(10) Les deux dernières lois (modifiées en 2016) contiennent des dispositions applicables à la protection des informations à caractère personnel par les entités du secteur public. Le traitement des données relevant du champ d'application de ces lois ne fait pas l'objet du constat d'adéquation figurant dans la présente décision, qui est limité à la protection des informations à caractère personnel par des «opérateurs économiques traitant des informations à caractère personnel» (OETIP) au sens de l'APPI.

(11) L'APPI a été réformée ces dernières années. L'APPI modifiée a été promulguée le 9 septembre 2015 et est entrée en vigueur le 30 mai 2017. La loi modifiée a introduit un certain nombre de nouvelles garanties et a renforcé les garanties existantes, rapprochant ainsi le système japonais de protection des données du système européen. Cela comprend, par exemple, une série de droits individuels opposables ou la mise en place d'une autorité de contrôle indépendante (PPC) chargée de la supervision et du contrôle de l'application de l'APPI.

(12) Outre l'APPI, le traitement des informations à caractère personnel relevant du champ d'application de la présente décision est soumis à des modalités d'exécution adoptées sur la base de l'APPI. Il s'agit notamment de la modification de l'arrêté ministériel visant à faire appliquer la loi sur la protection des informations à caractère personnel du 5 octobre 2016, ainsi que desdites règles d'[2]application de la loi sur la protection des informations à caractère personnel adoptées par la PPC ([11]). Les deux corpus de règles sont juridiquement contraignants et exécutoires et sont entrés en vigueur en même temps que l'APPI modifiée.

(13) Par ailleurs, le 28 octobre 2016, le cabinet du Japon (composé du Premier ministre et des ministres formant son gouvernement) a adopté une «politique de base» afin de «promouvoir de manière globale et intégrale des mesures relatives à la protection des informations à caractère personnel». Conformément à l'article 7 de l'APPI, la «politique de base» est adoptée sous la forme d'une décision du cabinet et comprend des orientations stratégiques sur l'application de l'APPI, adressées tant au gouvernement central qu'aux autorités locales.

(14) Récemment, par une décision du cabinet adoptée le 12 juin 2018, le gouvernement japonais a modifié la «politique de base». Afin de faciliter les transferts internationaux de données, ladite décision du cabinet délègue à la PPC, en tant qu'autorité compétente en matière de gestion et de mise en œuvre de l'APPI, «le pouvoir de prendre les mesures nécessaires pour combler les divergences entre les systèmes et opérations du Japon et ceux du pays étranger concerné sur la base de l'article 6 de la loi, de manière à garantir le traitement approprié des informations à caractère personnel reçues de ce pays». La décision du cabinet précise qu'il s'agit notamment du pouvoir de mettre en place des protections renforcées au moyen de l'adoption, par la PPC, de règles plus strictes venant compléter les règles établies dans l'APPI et dans l'arrêté ministériel et allant au-delà de celles-ci. Conformément à cette décision, ces règles plus strictes sont contraignantes et exécutoires pour les opérateurs économiques japonais.

(15) Sur la base de l'article 6 de l'APPI et de ladite décision du cabinet, la PPC a adopté, le 15 juin 2018, des règles supplémentaires complétant la loi sur la protection des informations à caractère personnel pour le traitement de données à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation («Supplementary Rules under the Act on the Protection of Personal Information for the Handling of Personal Data Transferred from the EU based on an Adequacy Decision», ci-après les «règles supplémentaires»), afin de renforcer la protection des informations à caractère personnel transférées depuis l'Union européenne vers le Japon sur le fondement de la présente décision d'adéquation. Ces règles supplémentaires sont juridiquement contraignantes pour les opérateurs économiques japonais et peuvent être invoquées, tant par la PPC que par les juridictions, de la même manière que les dispositions de l'APPI que les règles viennent compléter au moyen de règles plus strictes et/ou plus détaillées ([12]). Étant donné que les opérateurs économiques japonais recevant et/ou traitant ultérieurement des données à caractère personnel provenant de l'Union européenne seront soumis à une obligation légale de se conformer aux règles supplémentaires, ils devront faire en sorte [par exemple par des moyens techniques («étiquetage») ou organisationnels (stockage dans une base de données créée à cet effet)] de pouvoir identifier ces données à caractère personnel tout au long de leur «cycle de vie» ([13]). Dans les points suivants, le contenu de chaque règle supplémentaire est analysé dans le cadre de l'évaluation des articles de l'APPI que la règle complète.

(16) Contrairement à la situation antérieure à la loi modifiée de 2015, où cela relevait de la compétence de différents ministères japonais dans des secteurs spécifiques, l'APPI donne à la PPC les moyens d'adopter des «lignes directrices» «en vue de garantir la mise en œuvre adéquate et effective des mesures à prendre par un opérateur économique» conformément aux règles en matière de protection des données. Au moyen de ses lignes directrices, la PPC livre une interprétation de ces règles, en particulier de l'APPI, qui fait autorité. Selon les informations reçues

([11]) Disponibles à l'adresse suivante: https://www.ppc.go.jp/files/pdf/PPC_rules.pdf

([12]) Voir les règles supplémentaires (section introductive).

([13]) Cela n'est pas remis en question par l'exigence générale de tenir des registres (seulement) pendant une certaine période. Bien que l'origine des données figure parmi les informations que l'OETIP acquéreur doit confirmer en vertu de l'article 26, paragraphe 1, de l'APPI, l'exigence prévue à l'article 26, paragraphe 4, de l'APPI, en liaison avec l'article 18 des règles de la PPC, ne concerne qu'une forme particulière de registre (voir article 16 des règles de la PPC) et n'empêche pas un OETIP de garantir l'identification des données pendant des périodes plus longues. Cela a été confirmé par la PPC, selon laquelle «[l]es informations relatives à l'origine des données de l'UE doivent être conservées par l'OETIP aussi longtemps que cela lui est nécessaire pour pouvoir se conformer aux règles supplémentaires».

de la PPC, ces lignes directrices font partie intégrante du cadre juridique, et doivent être lues en combinaison avec le texte de l'APPI, l'arrêté ministériel, les règles de la PPC et une série de questions-réponses ([14]) élaborées par la PPC. Elles sont donc «contraignantes pour les opérateurs économiques». Lorsque les lignes directrices indiquent qu'un opérateur économique «doit» ou «ne devrait pas» agir dans un sens spécifié, la PPC estimera que la non-conformité avec les dispositions concernées constitue une violation de la loi ([15]).

2.2. **Champ d'application matériel et personnel**

(17) Le champ d'application de l'APPI est déterminé par les notions définies que sont les informations à caractère personnel, les données à caractère personnel et les opérateurs économiques traitant des informations à caractère personnel. Dans le même temps, l'APPI prévoit certaines dérogations importantes, surtout pour les données à caractère personnel traitées de manière anonyme et pour des catégories de traitement spécifiques par certains opérateurs. Bien que l'APPI n'utilise pas le terme «processing» dans sa version anglaise, elle s'appuie sur une notion équivalente («handling» dans la version anglaise) qui, selon les informations fournies par la PPC, englobe «toute manipulation de données à caractère personnel», ce qui englobe l'acquisition, la saisie, l'accumulation, l'organisation, le stockage, la modification/le traitement, le renouvellement, l'effacement, l'extraction, l'utilisation ou la fourniture d'informations personnelles.

2.2.1. *Définition des informations à caractère personnel*

(18) Tout d'abord, en ce qui concerne son champ d'application matériel, l'APPI établit une distinction entre les informations à caractère personnel et les données à caractère personnel, seules certaines dispositions de la loi étant applicables à la première catégorie. Conformément à l'article 2, paragraphe 1, de l'APPI, la notion d'«informations à caractère personnel» comprend toute information relative à une personne vivante qui permet l'identification de cette personne. La définition distingue deux catégories d'informations à caractère personnel: i) les codes d'identification individuels et ii) d'autres informations à caractère personnel permettant d'identifier une personne donnée. Cette dernière catégorie comprend également les informations qui ne permettent pas l'identification en soi, mais qui, lorsqu'elles sont «facilement recoupées» avec d'autres informations, permettent d'identifier une personne donnée. Conformément aux lignes directrices de la PPC ([16]), le fait que les informations puissent être considérées comme «facilement recoupées» est apprécié au cas par cas, en prenant en considération la situation réelle («condition») de l'opérateur économique. Ce sera le cas si ce recoupement est (ou peut être) effectué par un opérateur économique moyen («normal») en utilisant les moyens à sa disposition. Par exemple, les informations ne sont pas «facilement recoupées» avec d'autres informations si un opérateur économique doit entreprendre des efforts inhabituels ou commettre des actes illégaux pour obtenir les informations à recouper auprès d'un ou de plusieurs autres opérateurs économiques.

2.2.2. *Définition des données à caractère personnel*

(19) Seules certaines formes d'informations à caractère personnel relèvent de la notion de «données à caractère personnel» au sens de l'APPI. De fait, les «données à caractère personnel» sont définies comme des «informations à caractère personnel constituant une base de données d'informations à caractère personnel», à savoir un «ensemble collectif d'informations» comprenant des informations à caractère personnel «organisées de manière systématique, en vue de permettre la recherche d'informations à caractère personnel particulières au moyen d'un ordinateur» ([17]) ou «définies par arrêté ministériel comme ayant été organisées de manière systématique pour permettre de rechercher facilement des informations à caractère personnel particulières» mais «à l'exclusion de celles définies par arrêté ministériel comme étant peu susceptibles de nuire aux droits et aux intérêts d'une personne compte tenu de leur méthode d'utilisation» ([18]).

(20) Cette exception est spécifiée à l'article 3, paragraphe 1, de l'arrêté ministériel, en vertu duquel les trois conditions cumulatives suivantes doivent être remplies: i) l'ensemble collectif d'informations doit avoir été «élaboré afin d'être vendu à un grand nombre de personnes indéterminées et son élaboration ne peut avoir enfreint les dispositions

([14]) PPC, questions-réponses, 16 février 2017 (modifiées le 30 mai 2017), disponibles à l'adresse suivante: https://www.ppc.go.jp/files/pdf/kojouhouQA.pdf. Les questions-réponses abordent un certain nombre de questions traitées dans les lignes directrices en fournissant des exemples concrets comme ce qui constitue des données à caractère personnel sensibles, l'interprétation du consentement individuel, les transferts à des tiers dans le contexte de l'informatique en nuage ou l'obligation de tenue de registres appliquée aux transferts transfrontières. Elles ne sont disponibles qu'en japonais.

([15]) En réponse à une question précise, la PPC a informé le Comité européen de la protection des données que «les juridictions japonaises fondent l[eur] interprétation sur les lignes directrices lorsqu'elles appliquent l'APPI/les règles de la PPC dans les différents cas qui leur sont soumis et ont ainsi directement renvoyé au texte des lignes directrices de la PPC dans leurs décisions. Les lignes directrices s'imposent donc également aux opérateurs économiques sous cet angle. La PPC n'a connaissance d'aucun cas dans lequel le tribunal se serait écarté des lignes directrices.» À cet égard, la PPC a renvoyé la Commission à un arrêt dans le domaine de la protection des données où le tribunal s'est fondé explicitement sur les lignes directrices pour établir ses conclusions (voir tribunal de district d'Osaka, décision du 19 mai 2006, Hanrei Jiho, vol. 1948, p. 122, où le tribunal a jugé que l'opérateur économique était tenu de prendre des mesures de contrôle de sécurité sur la base de ces lignes directrices).

([16]) Lignes directrices de la PPC (General Rule Edition), p. 6.

([17]) Cela englobe tout système électronique de classement. Les lignes directrices de la PPC (General Edition, p. 17) fournissent des exemples spécifiques à cet égard, par exemple une liste d'adresses électroniques stockées dans le logiciel client du courrier électronique.

([18]) Article 2, paragraphes 4 et 6, de l'APPI.

d'une loi ou d'un arrêté fondé sur celle-ci»; ii) doit pouvoir être «acheté à tout moment par un grand nombre de personnes indéterminées»; et iii) les données à caractère personnel figurant dans l'ensemble doivent être «fournies pour leur finalité initiale, sans ajouter d'autres informations relatives à une personne en vie». Selon les explications fournies par la PPC, cette exception restreinte a été introduite afin d'exclure les annuaires téléphoniques ou des répertoires du même type.

(21) Pour les données collectées au Japon, cette distinction entre les «informations à caractère personnel» et les «données à caractère personnel» est pertinente car ces informations ne font pas toujours partie d'une «base de données d'informations à caractère personnel» (par exemple, un ensemble unique de données collectées et traitées manuellement) et, partant, les dispositions de l'APPI qui ne portent que sur les données à caractère personnel ne s'appliqueront pas ([19]).

(22) Par contre, cette distinction ne sera pas pertinente pour les données à caractère personnel importées de l'Union européenne vers le Japon sur la base d'une décision d'adéquation. Étant donné que ces données seront généralement transmises par voie électronique (sachant qu'à l'ère du numérique, il s'agit du moyen habituel utilisé pour échanger des données, en particulier pour couvrir une distance aussi grande que celle qui sépare l'UE du Japon) et feront donc partie du système électronique de classement de l'importateur de données, ces données de l'UE relèveront de la catégorie des «données à caractère personnel» au sens de l'APPI. Dans le cas exceptionnel où des données à caractère personnel seraient transmises depuis l'UE par d'autres moyens (par exemple, sur support papier), elles resteraient couvertes par l'APPI si, à l'issue de leur transfert, elles font partie d'un «ensemble collectif d'informations» organisé de manière systématique pour permettre de rechercher facilement des informations particulières [article 2, paragraphe 4, point ii), de l'APPI]. En vertu de l'article 3, paragraphe 2, de l'arrêté ministériel, ce sera le cas lorsque les informations sont organisées «selon une certaine règle» et que la base de données comporte des outils tels que, par exemple, une table des matières ou un index facilitant la recherche. Cela correspond à la définition du «fichier» au sens de l'article 2, paragraphe 1, du RGPD.

2.2.3. *Définition des données à caractère personnel conservées*

(23) Certaines dispositions de l'APPI, notamment les articles 27 à 30 relatifs aux droits individuels, ne s'appliquent qu'à une catégorie spécifique de données à caractère personnel, à savoir les «données à caractère personnel conservées». Celles-ci sont définies à l'article 2, paragraphe 7, de l'APPI comme les données à caractère personnel autres que celles qui soit i) «sont définies par arrêté ministériel comme susceptibles de porter atteinte aux intérêts publics ou autres si leur présence ou absence est notifiée», soit ii) «doivent être supprimées dans un délai n'excédant pas un an, défini par arrêté ministériel».

(24) En ce qui concerne la première de ces deux catégories, elle est expliquée à l'article 4 de l'arrêté ministériel et porte sur quatre types de dérogations ([20]). Ces dérogations visent des objectifs similaires à ceux énumérés à l'article 23, paragraphe 1, du règlement (UE) 2016/679, notamment la protection de la personne concernée (appelée «principal» dans la version anglaise de l'APPI) et les libertés d'autrui, la sécurité nationale, la sécurité publique, l'application du droit pénal ou d'autres objectifs importants d'intérêt public général. En outre, il ressort du libellé de l'article 4, paragraphe 1, points i) à iv), de l'arrêté ministériel que leur application suppose toujours un risque spécifique pour un des intérêts importants protégés ([21]).

(25) La deuxième catégorie a été davantage précisée à l'article 5 de l'arrêté ministériel. Lu en liaison avec l'article 2, paragraphe 7, de l'APPI, il exclut du champ d'application de la notion de données à caractère personnel conservées et, par conséquent, des droits individuels garantis par l'APPI, les données à caractère personnel «devant être supprimées» dans un délai de six mois. La PPC a expliqué que cette dérogation vise à encourager les opérateurs économiques à conserver et à traiter les données pour la période la plus brève possible. Toutefois, cela signifierait que les personnes concernées de l'UE ne seraient pas en mesure de bénéficier de droits importants au seul motif de la durée de conservation de leurs données par l'opérateur économique concerné.

(26) Afin de remédier à cette situation, la règle supplémentaire (2) dispose que les données à caractère personnel transférées depuis l'Union européenne doivent être «traitées comme des données à caractère personnel conservées au sens de l'article 2, paragraphe 7, de la loi, quelle que soit la période au terme de laquelle elles doivent être supprimées». Par conséquent, la durée de conservation n'aura aucune incidence sur les droits accordés aux personnes concernées de l'UE.

([19]) Par exemple, l'article 23 de l'APPI sur les conditions de partage des données à caractère personnel avec des tiers.

([20]) À savoir, les données à caractère personnel i) «pour lesquelles si la présence ou l'absence desdites données à caractère personnel est connue, le risque existe que cela porte atteinte à la vie, à l'intégrité physique ou aux biens d'un responsable ou d'un tiers»; ii) les données «pour lesquelles si la présence ou l'absence desdites données à caractère personnel est connue, le risque existe que cela encourage ou provoque un acte illégal ou abusif»; iii) les données «pour lesquelles si la présence ou l'absence desdites données à caractère personnel est connue, le risque existe que cela porte atteinte à la sécurité nationale, détruise une relation de confiance avec un pays étranger ou une organisation internationale, ou cause un préjudice dans les négociations avec un pays étranger ou une organisation internationale»; et iv) les données «pour lesquelles si la présence ou l'absence desdites données à caractère personnel est connue, le risque existe que cela fasse obstacle au maintien de l'ordre public et de la sécurité publique, par exemple pour ce qui est de la prévention des délits ainsi que de la lutte et des enquêtes en la matière».

([21]) Dans ces conditions, il n'est pas nécessaire d'informer la personne concernée, ce qui est conforme aux dispositions de l'article 23, paragraphe 2, point h), du RGPD, qui dispose que les personnes concernées ne doivent pas être informées de la limitation si «cela risque de nuire à la finalité de la limitation».

2.2.4. *Définition des informations à caractère personnel traitées de manière anonyme*

(27) Les exigences applicables aux informations à caractère personnel traitées de manière anonyme, telles que définies à l'article 2, paragraphe 9, de l'APPI, sont énoncées à la section 2 du chapitre 4 de la loi («Tâches d'un opérateur économique traitant des informations traitées de manière anonyme»). Inversement, ces informations ne sont pas régies par les dispositions de la section 1 du chapitre IV de l'APPI, qui comprend les articles énonçant les garanties en matière de protection des données et les droits applicables au traitement de données à caractère personnel relevant du champ d'application de ladite loi. En conséquence, alors que les «informations à caractère personnel traitées de manière anonyme» ne sont pas soumises aux règles «standard» en matière de protection des données (fixées dans la section 1 du chapitre IV et à l'article 42 de l'APPI), elles relèvent bien du champ d'application de l'APPI, notamment de ses articles 36 à 39.

(28) Conformément à l'article 2, paragraphe 9, de l'APPI, les «informations à caractère personnel traitées de manière anonyme» sont des informations relatives à une personne qui ont été «produites à l'issue du traitement d'informations à caractère personnel» au moyen de mesures prescrites dans l'APPI (article 36, paragraphe 1) et précisées dans les règles de la PPC (article 19), d'une façon telle qu'il est devenu impossible d'identifier une personne donnée ou de restaurer les informations à caractère personnel.

(29) Il résulte de ces dispositions, comme l'a également confirmé la PPC, que le processus d'«anonymisation» des informations à caractère personnel ne doit pas être techniquement irréversible. Conformément à l'article 36, paragraphe 2, de l'APPI, les opérateurs économiques traitant des «informations à caractère personnel traitées de manière anonyme» sont uniquement tenus d'empêcher la réidentification en prenant des mesures destinées à garantir la sécurité des «descriptions, etc., et des codes d'identification individuels supprimés des informations à caractère personnel utilisées pour produire les informations traitées de manière anonyme, ainsi que des informations liées à l'application d'une méthode de traitement».

(30) Les «informations à caractère personnel traitées de manière anonyme», telles que définies par l'APPI, comprenant des données pour lesquelles la réidentification de la personne est encore possible, cela pourrait signifier que les données à caractère personnel transférées depuis l'Union européenne pourraient perdre une partie des protections disponibles en raison d'un processus qui, conformément au règlement (UE) 2016/679, serait considéré comme une forme de «pseudonymisation» plutôt que d'«anonymisation» (ce qui ne changerait pas leur nature en tant que données à caractère personnel).

(31) Pour remédier à cette situation, les règles supplémentaires prévoient des exigences supplémentaires applicables uniquement aux données à caractère personnel transférées depuis l'Union européenne sur la base de la présente décision. Conformément à la règle (5) des règles supplémentaires, ces informations à caractère personnel ne sont considérées comme des «informations à caractère personnel traitées de manière anonyme» au sens de l'APPI que «si l'opérateur économique traitant des informations à caractère personnel prend des mesures rendant l'anonymisation de la personne irréversible pour quiconque, notamment en supprimant les informations liées à la méthode de traitement, etc.». Ces dernières sont, conformément à ce qui est précisé dans les règles supplémentaires, des informations relatives aux descriptions et aux codes d'identification individuels qui ont été supprimés des informations à caractère personnel utilisées pour produire des «informations à caractère personnel traitées de manière anonyme», ainsi que des informations relatives à l'application d'une méthode de traitement visant à supprimer ces descriptions et ces codes d'identification individuels. En d'autres termes, les règles supplémentaires requièrent de l'opérateur économique produisant des «informations à caractère personnel traitées de manière anonyme» qu'il détruise la «clé» permettant la réidentification des données. Cela signifie que les données à caractère personnel provenant de l'Union européenne relèveront des dispositions de l'APPI relatives aux «informations à caractère personnel traitées de manière anonyme» seulement dans les cas où elles seraient également considérées comme des informations anonymes au sens du règlement (UE) 2016/679 ([22]).

2.2.5. *Définition de l'opérateur économique traitant des informations à caractère personnel (OETIP)*

(32) Pour ce qui est de son champ d'application personnel, l'APPI s'applique uniquement aux OETIP. Un OETIP est défini à l'article 2, paragraphe 5, de l'APPI comme «une personne fournissant une base de données d'informations à caractère personnel, etc., pour une utilisation dans le cadre d'une activité», à l'exclusion des pouvoirs publics et des agences administratives, aux niveaux tant central que local.

(33) Selon les lignes directrices de la PPC, on entend par «activité», toute «pratique visant à exercer, dans un objectif donné, à des fins lucratives ou non, de manière répétée et continue, une entreprise socialement reconnue». Les organisations dépourvues de personnalité juridique (telles que les associations de fait) ou les particuliers sont considérés comme un OETIP s'ils fournissent (utilisent) une base de données d'informations à caractère personnel, etc., dans le cadre de leur activité ([23]). En conséquence, la notion d'«activité» dans le cadre de l'APPI est très large en ce qu'elle inclut non seulement les activités lucratives, mais également les activités sans but lucratif exercées par tous types d'organisations et de particuliers. Par ailleurs, l'«utilisation dans le cadre d'une activité» couvre également les informations à caractère personnel qui ne sont pas utilisées dans les relations commerciales (extérieures) de l'opérateur, mais en interne, par exemple le traitement des données des salariés.

([22]) Voir le règlement (UE) 2016/679, considérant 26.
([23]) Lignes directrices de la PPC (General Rule Edition), p. 18.

(34) En ce qui concerne les bénéficiaires des protections prévues dans l'APPI, la loi n'établit aucune distinction en fonction de la nationalité, de la résidence ou de la situation géographique de la personne. Il en va de même de la possibilité pour les particuliers de demander réparation, que ce soit auprès de la PPC ou des tribunaux.

2.2.6. *Notions de responsable du traitement et de sous-traitant*

(35) Aucune distinction n'est spécifiquement établie dans l'APPI entre les obligations imposées aux responsables du traitement et celles imposées aux sous-traitants. Cette absence de distinction n'affecte pas le niveau de protection, tous les OETIP étant soumis à l'ensemble des dispositions de la loi. Un OETIP qui confie le traitement de données à caractère personnel à un «mandataire» (l'équivalent d'un sous-traitant au sens du RGPD) reste soumis aux obligations prévues par l'APPI et les règles supplémentaires en ce qui concerne les données confiées. De plus, en vertu de l'article 22 de l'APPI, il est tenu d'«exercer une supervision nécessaire et appropriée» sur le mandataire. Comme la PPC l'a confirmé, le mandataire est à son tour lié par l'ensemble des obligations prévues par l'APPI et les règles supplémentaires.

2.2.7. *Exclusions sectorielles*

(36) L'article 76 de l'APPI exclut certaines catégories de traitement des données du champ d'application du chapitre IV de la loi, qui contient les dispositions principales en matière de protection des données (principes de base, obligations des opérateurs économiques, droits individuels, supervision par la PPC). Le traitement couvert par l'exclusion sectorielle prévue à l'article 76 est également exempté des pouvoirs d'exécution de la PPC, conformément à l'article 43, paragraphe 2, de l'APPI ([24]).

(37) Les catégories relevant de l'exclusion sectorielle prévue à l'article 76 de l'APPI sont définies en utilisant un double critère fondé sur le type d'OETIP traitant les informations à caractère personnel et sur la finalité du traitement. Plus précisément, l'exclusion s'applique: i) aux organismes de radiodiffusion, aux éditeurs de journaux, aux agences de communication ou à d'autres organes de presse (y compris aux particuliers exerçant des activités de presse), dans la mesure où ils traitent des informations à caractère personnel pour la presse; ii) aux personnes exerçant une activité de rédaction professionnelle, dans la mesure où cela implique l'utilisation d'informations à caractère personnel; iii) aux universités et à tout autre groupe ou organisation en rapport avec des études universitaires, et à toute personne appartenant à une organisation de ce type, dans la mesure où ils traitent des informations à caractère personnel dans le cadre desdites études; iv) aux institutions religieuses, dans la mesure où elles traitent des informations à caractère personnel aux fins d'une activité religieuse (y compris toutes les activités connexes); et v) aux organismes politiques, dans la mesure où ils traitent des informations à caractère personnel aux fins de leur activité politique (y compris toutes les activités connexes). Le traitement d'informations à caractère personnel pour une des finalités énumérées à l'article 76 par d'autres types d'OETIP, ainsi que le traitement d'informations à caractère personnel par un des OETIP énumérés à d'autres fins, par exemple dans le cadre du travail, restent couverts par les dispositions du chapitre IV.

(38) Afin de garantir un niveau de protection adéquat des données à caractère personnel transférées depuis l'Union européenne vers les opérateurs économiques au Japon, seul le traitement des informations à caractère personnel relevant du champ d'application du chapitre IV de l'APPI (à savoir, le traitement par un OETIP dans la mesure où il ne relève d'aucune des exclusions sectorielles) devrait être couvert par la présente décision. Il convient donc d'aligner son champ d'application sur celui de l'APPI. Selon les informations fournies par la PPC, dans l'hypothèse où un OETIP couvert par la présente décision modifierait ultérieurement la finalité d'utilisation (dans la mesure où cela est autorisé) et serait dès lors couvert par une des exclusions sectorielles prévues à l'article 76 de l'APPI, cela serait considéré comme un transfert international (étant donné que, dans ce cas, le traitement des informations à caractère personnel ne serait plus couvert par le chapitre IV de l'APPI et sortirait ainsi de son champ d'application). Cela s'appliquerait également dans le cas où un OETIP fournirait des informations à caractère personnel à une entité couverte par l'article 76 de l'APPI en vue d'une utilisation fondée sur une des finalités de traitement indiquées dans cette disposition. Dans le cas des données à caractère personnel transférées depuis l'Union européenne, cela constituerait donc un transfert ultérieur soumis aux garanties applicables (notamment celles spécifiées à l'article 24 de l'APPI et à la règle supplémentaire 4). Lorsque l'OETIP doit obtenir le consentement de la personne concernée ([25]), il devrait lui fournir toutes les informations nécessaires, y compris l'avertir que les informations à caractère personnel ne seront plus protégées par l'APPI.

([24]) En ce qui concerne les autres opérateurs, la PPC, lorsqu'elle exerce ses pouvoirs d'enquête et d'exécution, ne les empêchera pas d'exercer leur droit à la liberté d'expression, à la liberté d'enseignement, à la liberté de religion et à la liberté d'activité politique (article 43, paragraphe 1, de l'APPI).

([25]) Comme indiqué par la PPC, le consentement est interprété dans ses lignes directrices comme «l'expression de l'intention d'une personne concernée d'accepter que ses informations à caractère personnel puissent être traitées selon une méthode indiquée par un opérateur traitant des informations à caractère personnel». Les lignes directrices (General Rule Edition, p. 24) énoncent les modes de consentement considérés comme des «pratiques commerciales courantes au Japon», à savoir le consentement oral, le renvoi de formulaires ou d'autres documents, un accord signifié par courriel, une case cochée sur une page web, un clic sur une page d'accueil, l'utilisation d'un bouton accordant le consentement, une pression sur un écran tactile, etc. Toutes ces méthodes constituent une forme expresse de consentement.

2.3. **Garanties, droits et obligations**

2.3.1. *Limitation de la finalité*

(39) Les données à caractère personnel devraient être traitées dans un but précis et être ensuite utilisées uniquement dans la mesure où cela n'est pas incompatible avec la finalité du traitement. Ce principe de protection des données est garanti par les articles 15 et 16 de l'APPI.

(40) L'APPI repose sur le principe selon lequel un opérateur économique doit spécifier la finalité d'utilisation de la «manière la plus explicite possible» (article 15, paragraphe 1) et sera ensuite lié par cette finalité lorsqu'il traitera les données.

(41) À cet égard, l'article 15, paragraphe 2, de l'APPI dispose que l'OETIP ne peut modifier la finalité initiale «au-delà de la mesure reconnue comme étant raisonnablement en rapport avec la finalité d'utilisation préalable à la modification», que les lignes directrices de la PPC interprètent comme ce qui peut être objectivement anticipé par la personne concernée sur la base de «conventions sociales normales» ([26]).

(42) En outre, l'article 16, paragraphe 1, de l'APPI interdit aux OETIP de traiter des informations à caractère personnel au-delà de la «mesure nécessaire pour atteindre une finalité d'utilisation» spécifiée à l'article 15 sans obtenir au préalable le consentement de la personne concernée, sous réserve de l'application d'une des dérogations prévues à l'article 16, paragraphe 3 ([27]).

(43) Lorsqu'il s'agit d'informations à caractère personnel acquises auprès d'un autre opérateur économique, l'OETIP est en principe libre de fixer une nouvelle finalité d'utilisation ([28]). Pour veiller à ce qu'en cas de transfert à partir de l'Union européenne, un tel destinataire soit lié par la finalité pour laquelle les données ont été transférées, la règle supplémentaire (3) dispose que «lorsqu'un [OETIP] reçoit des données à caractère personnel provenant de l'UE sur la base d'une décision d'adéquation» ou qu'un tel opérateur «reçoit d'un autre [OETIP] des données à caractère personnel transférées précédemment depuis l'UE sur la base d'une décision d'adéquation» (partage ultérieur), le destinataire doit «préciser que les desdites données à caractère personnel seront utilisées dans le cadre de la finalité d'utilisation pour laquelle les données ont été reçues initialement ou ultérieurement». Cette règle garantit donc que dans le contexte d'un transfert, la finalité spécifiée conformément au règlement (UE) 2016/679 continue de déterminer le traitement, et qu'une modification de cette finalité à n'importe quelle étape de la chaîne de traitement au Japon nécessiterait le consentement de la personne concernée dans l'UE. Dès lors que l'obtention de ce consentement impose à l'OETIP de prendre contact avec la personne concernée, dans le cas où une telle démarche n'est pas possible, cela a tout simplement comme conséquence qu'il faut maintenir la finalité initiale.

2.3.2. *Licéité et loyauté du traitement*

(44) La protection supplémentaire mentionnée au considérant 43 est d'autant plus importante que c'est au moyen du principe de limitation de la finalité que le système japonais garantit également un traitement licite et loyal des données à caractère personnel.

(45) Aux termes de l'APPI, lorsqu'un OETIP collecte des informations à caractère personnel, il est tenu de spécifier de manière détaillée la finalité d'utilisation de ces informations ([29]) et d'informer rapidement la personne concernée de cette finalité (ou de la rendre publique) ([30]). En outre, l'article 17 de l'APPI dispose qu'un OETIP ne peut collecter d'informations à caractère personnel à la suite d'une tromperie ou par d'autres moyens inappropriés. Pour ce qui est de certaines catégories de données telles que les informations à caractère personnel nécessitant des précautions particulières, leur acquisition requiert le consentement de la personne concernée (article 17, paragraphe 2, de l'APPI).

([26]) Le «questions-réponses» de la PPC comporte plusieurs exemples illustrant cette notion. L'utilisation d'informations à caractère personnel acquises auprès d'acheteurs de biens ou de services dans le cadre d'une transaction commerciale, qui a pour finalité d'informer ces acheteurs de la disponibilité d'autres biens ou services connexes (par exemple, l'exploitant d'un club de fitness qui enregistre les adresses électroniques des membres afin d'informer ces derniers sur des cours et programmes) figure parmi les exemples de situations dans lesquelles la modification reste dans une mesure qui est raisonnablement en rapport avec la finalité initiale. Le «questions-réponses» fournit également un exemple dans lequel la modification de la finalité d'utilisation n'est pas autorisée, à savoir lorsqu'une entreprise envoie des informations sur ses biens et services aux adresses électroniques qu'elle a collectées afin d'avertir contre l'utilisation frauduleuse ou le vol d'une carte de membre.

([27]) Ces dérogations peuvent résulter d'autres lois et réglementations ou peuvent concerner des situations dans lesquelles le traitement des informations à caractère personnel est nécessaire i) à des fins de «protection de la vie humaine, de l'intégrité physique ou des biens»; ii) pour «améliorer l'hygiène publique ou encourager la croissance d'enfants en bonne santé»; ou iii) pour «coopérer avec des agences ou des organismes gouvernementaux ou avec leurs représentants» dans l'exercice de leurs missions statutaires. En outre, les catégories i) et ii) ne s'appliquent que s'il est difficile d'obtenir le consentement de la personne concernée, et la catégorie iii) ne s'applique que si l'obtention du consentement de la personne concernée risque d'interférer avec l'exercice de ces missions.

([28]) Cela étant, il ressort de l'article 23, paragraphe 1, de l'APPI que la communication des données à un tiers requiert en principe le consentement de la personne concernée. Cette dernière sera ainsi en mesure d'exercer un certain contrôle sur l'utilisation de ses données par un autre opérateur économique.

([29]) Aux termes de l'article 15, paragraphe 1, de l'APPI, cette spécification doit être «aussi explicite que possible».

([30]) Article 18, paragraphe 1, de l'APPI.

(46) Par la suite, et comme indiqué aux considérants 41 et 42, il est interdit à l'OETIP de traiter les informations à caractère personnel pour d'autres finalités, sauf lorsque la personne concernée a donné son consentement à un tel traitement ou lorsque l'une des dérogations prévues à l'article 16, paragraphe 3, de l'APPI s'applique.

(47) Enfin, pour ce qui est de la communication ultérieure d'informations à caractère personnel à un tiers ([31]), l'article 23, paragraphe 1, de l'APPI limite une telle communication à certains cas particuliers, la règle générale voulant que la personne concernée donne son consentement préalable ([32]). L'article 23, paragraphes 2, 3, et 4, de l'APPI prévoit des exceptions à l'exigence d'obtenir le consentement. Toutefois, ces exceptions s'appliquent uniquement aux données non sensibles et exigent de l'opérateur économique qu'il informe au préalable les personnes concernées de son intention de communiquer leurs informations à caractère personnel à un tiers et de la possibilité qui leur est offerte de s'opposer à toute communication ultérieure ([33]).

(48) En ce qui concerne les transferts à partir de l'Union européenne, les données à caractère personnel devront nécessairement avoir été d'abord collectées et traitées dans l'UE conformément au règlement (UE) 2016/679. Cela impliquera toujours, d'une part, la collecte et le traitement de données, y compris pour le transfert de l'Union européenne vers le Japon, sur la base d'un des motifs légaux énumérés à l'article 6, paragraphe 1, du règlement et, d'autre part, la collecte de données pour une finalité déterminée, explicite et légitime, ainsi que l'interdiction d'un traitement ultérieur, y compris au moyen d'un transfert, d'une manière qui serait incompatible avec cette finalité, conformément à l'article 5, paragraphe 1, point b), et à l'article 6, paragraphe 4, du règlement.

(49) Selon la règle supplémentaire (3), à la suite du transfert, l'OETIP qui recevra les données devra «confirmer» la ou les finalités spécifique(s) fondant le transfert [la finalité spécifiée conformément au règlement (UE) 2016/679] et traiter ultérieurement ces données conformément à cette/ces finalité(s) ([34]). Cela signifie que non seulement le premier acquéreur de ces données à caractère personnel au Japon, mais également leur destinataire futur (y compris un mandataire) sont liés par la ou les finalité(s) spécifiée(s) conformément au règlement.

(50) En outre, dans le cas où un OETIP souhaiterait modifier la finalité spécifiée précédemment conformément au règlement (UE) 2016/679, l'article 16, paragraphe 1, de l'APPI dispose qu'il devrait obtenir en principe le consentement de la personne concernée. Sans ce consentement, tout traitement de données allant au-delà de ce qui est nécessaire pour atteindre cette finalité d'utilisation constituerait une violation de l'article 16, paragraphe 1, lequel pourrait être invoqué par la PPC et les juridictions compétentes.

(51) Étant donné qu'en vertu du règlement (UE) 2016/679, un transfert requiert une base juridique valide et une finalité déterminée, lesquelles figurent dans la finalité d'utilisation «confirmée» aux termes de l'APPI, la combinaison des dispositions applicables de l'APPI et de la règle supplémentaire (3) garantit donc que le traitement des données de l'UE au Japon restera licite.

2.3.3. *Exactitude et minimisation des données*

(52) Les données à caractère personnel doivent être exactes et, au besoin, actualisées. Elles doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

(53) Ces principes sont garantis dans le droit japonais par l'article 16, paragraphe 1, de l'APPI, qui interdit le traitement d'informations à caractère personnel au-delà de la «mesure nécessaire pour atteindre une finalité d'utilisation». Comme l'explique la PPC, cette interdiction exclut non seulement l'utilisation de données qui ne serait pas adéquate et l'utilisation excessive de données (au-delà de ce qui est nécessaire pour atteindre la finalité d'utilisation), mais englobe également l'interdiction de traiter des données non pertinentes pour atteindre la finalité d'utilisation.

([31]) Bien que les mandataires soient exclus de la notion de «tiers» aux fins de l'application de l'article 23 (voir paragraphe 5), cette exclusion s'applique uniquement dans la mesure où le mandataire traite les données à caractère personnel dans les limites du mandat conféré («dans la mesure nécessaire pour atteindre une finalité d'utilisation»), c'est-à-dire dans la mesure où il agit en qualité de sous-traitant.

([32]) Les autres motifs d'exception sont les suivants: i) la communication d'informations à caractère personnel «sur la base de dispositions législatives et réglementaires»; ii) les cas «dans lesquels il est nécessaire de protéger la vie, l'intégrité physique ou les biens d'une personne ou dans lesquels il est difficile d'obtenir le consentement de la personne concernée»; iii) les cas «dans lesquels il est spécifiquement nécessaire d'améliorer l'hygiène publique ou de favoriser la bonne santé des enfants ou dans lesquels il est difficile d'obtenir le consentement de la personne concernée»; et iv) les cas «dans lesquels il est nécessaire de coopérer avec un organisme de l'administration centrale ou une administration locale ou avec une personne chargée par ces dernières d'exercer des missions établies par la loi ou la réglementation, et lorsque l'obtention du consentement de la personne concernée risque d'interférer avec l'exercice desdites missions».

([33]) Les informations à fournir comprennent notamment les catégories de données à caractère personnel à partager avec un tiers et la méthode utilisée pour les transmettre. En outre, l'OETIP doit informer la personne concernée sur la possibilité dont elle dispose de s'opposer à la transmission et les moyens d'introduire une telle demande.

([34]) En vertu de l'article 26, paragraphe 1, point ii), de l'APPI, un OETIP est tenu, lorsqu'il reçoit des données à caractère personnel de la part d'un tiers, de «confirmer» (vérifier) les «détails relatifs à l'acquisition des données à caractère personnel par le tiers», y compris la finalité de cette acquisition. Si l'article 26 ne spécifie pas expressément que l'OETIP doit dans ce cas respecter cette finalité, la règle supplémentaire (3) l'exige explicitement.

(54) En ce qui concerne l'obligation de faire en sorte que les données restent exactes et à jour, l'article 19 de l'APPI impose à l'OETIP de «veiller à ce que les données à caractère personnel restent exactes et à jour dans la mesure nécessaire pour atteindre une finalité d'utilisation». Cette disposition doit être lue en liaison avec l'article 16, paragraphe 1, de l'APPI: selon les explications données par la PPC, si un OETIP ne respecte pas les normes d'exactitude fixées, le traitement des informations à caractère personnel ne sera pas considéré comme conforme à la finalité d'utilisation et deviendra dès lors illicite en vertu de l'article 16, paragraphe 1.

2.3.4. *Limitation de la conservation*

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

(56) Aux termes de l'article 19 de l'APPI, les OETIP doivent «s'efforcer […] de supprimer les données à caractère personnel sans délai lorsqu'une telle utilisation n'est plus nécessaire». Cette disposition doit être lue en liaison avec l'article 16, paragraphe 1, de l'APPI, qui interdit le traitement d'informations à caractère personnel au-delà de «la mesure nécessaire pour atteindre une finalité d'utilisation». Dès que la finalité d'utilisation a été atteinte, le traitement des informations à caractère personnel ne peut plus être considéré comme nécessaire et ne peut donc plus se poursuivre (à moins que l'OETIP n'obtienne le consentement de la personne concernée à cette fin).

2.3.5. *Sécurité des données*

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

(58) Ce principe est mis en œuvre dans le droit japonais par l'article 20 de l'APPI, qui dispose qu'un OETIP «prend les mesures nécessaires appropriées pour contrôler la sécurité des données à caractère personnel, y compris pour prévenir la fuite, la perte ou la détérioration des données à caractère personnel qu'il traite.» Les lignes directrices de la PPC décrivent les mesures à prendre, y compris les méthodes à suivre pour établir des dispositions de base, des règles relatives au traitement des données et diverses «actions de contrôle» (concernant la sécurité organisationnelle, ainsi que la sécurité humaine, physique et technologique) ([35]). En outre, les lignes directrices de la PPC et une communication spécifique (appendice 8 sur le contenu des mesures de gestion de la sécurité à prendre) publiée par la PPC fournissent de plus amples détails sur les mesures concernant les incidents de sécurité impliquant par exemple la fuite d'informations à caractère personnel, dans le cadre des mesures de gestion de la sécurité à adopter par les OETIP ([36]).

(59) En outre, chaque fois que des informations à caractère personnel sont traitées par des employés ou des sous-traitants, les articles 20 et 21 de l'APPI disposent qu'il convient d'assurer une «supervision nécessaire et appropriée» à des fins de contrôle de la sécurité. Enfin, aux termes de l'article 83 de l'APPI, la fuite intentionnelle ou le vol d'informations à caractère personnel est passible d'une sanction pouvant aller jusqu'à un an d'emprisonnement.

2.3.6. *Transparence*

(60) Les personnes concernées devraient être informées des principales caractéristiques du traitement de leurs données à caractère personnel.

(61) L'article 18, paragraphe 1, de l'APPI impose à l'OETIP de mettre des informations sur la finalité d'utilisation des informations à caractère personnel acquises à la disposition de la personne concernée, excepté dans les «cas où une finalité d'utilisation a été communiquée préalablement au public». La même obligation s'applique en cas de modification licite de la finalité (article 18, paragraphe 3). La personne concernée est ainsi aussi informée du fait que ses données ont été collectées. Bien que l'APPI n'impose généralement pas à l'OETIP d'informer la personne concernée sur les destinataires prévus des informations à caractère personnel au stade de la collecte, une telle information est une condition nécessaire à toute communication ultérieure des informations à un tiers (destinataire) sur la base de l'article 23, paragraphe 2, c'est-à-dire lorsque cette transmission se fait sans le consentement préalable de la personne concernée.

([35]) Lignes directrices de la PPC (General Rule Edition), p. 41 et pp. 86-98.

([36]) Selon la section 3-3-2 des lignes directrices de la PPC, en cas de fuite, de détérioration ou de perte, l'OETIP est tenu de procéder aux investigations nécessaires et, en particulier, d'évaluer l'ampleur de l'atteinte aux droits et intérêts de la personne concernée, ainsi que la nature et le volume des informations à caractère personnel concernées.

(62) En ce qui concerne les «données à caractère personnel conservées», l'article 27 de l'APPI dispose que l'OETIP informe la personne concernée de son identité (ses coordonnées), de la finalité d'utilisation et des procédures prévues pour donner suite à toute demande concernant les droits individuels de la personne concernée formulée au titre des articles 28, 29 et 30 de l'APPI.

(63) Étant donné qu'en vertu des règles supplémentaires, les données à caractère personnel transférées à partir de l'Union européenne seront considérées comme des «données à caractère personnel conservées» indépendamment de leur durée de conservation (sauf si elles sont couvertes par une dérogation), elles seront toujours soumises aux exigences de transparence sur la base des deux dispositions susmentionnées.

(64) Tant les exigences de l'article 18 que l'obligation d'information sur la finalité d'utilisation prévue à l'article 27 de l'APPI sont soumises au même ensemble d'exceptions, fondées pour la plupart sur des considérations d'intérêt public et la protection des droits et intérêts de la personne concernée, des tiers et du responsable du traitement ([37]). Selon l'interprétation des lignes directrices de la PPC, ces exceptions s'appliquent dans des situations très particulières, par exemple lorsque les informations sur la finalité d'utilisation risquent d'affaiblir les mesures légitimes prises par l'opérateur économique pour protéger certains intérêts (par exemple, la lutte contre la fraude, l'espionnage industriel, le sabotage).

2.3.7. *Catégories particulières de données*

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

(66) Les «informations à caractère personnel nécessitant des précautions particulières» sont définies à l'article 2, paragraphe 3, de l'APPI. Cette disposition porte sur les «informations à caractère personnel concernant notamment la race, les convictions religieuses, le statut social, les antécédents médicaux, le casier judiciaire, le fait d'avoir subi un préjudice résultant d'un acte criminel, ou d'autres descriptions fixées par arrêté ministériel, telles que celles dont le traitement requiert des précautions particulières afin d'éviter à la personne concernée toute discrimination injuste, tout préjudice ou tout autre dommage». Ces catégories correspondent en grande partie à la liste des données sensibles établie aux articles 9 et 10 du règlement (UE) 2016/679. Les «antécédents médicaux», en particulier, correspondent aux données concernant la santé, tandis que le «casier judiciaire et le fait d'avoir subi un préjudice résultant d'un acte criminel» sont fondamentalement identiques aux catégories figurant à l'article 10 du règlement (UE) 2016/679. Les catégories visées à l'article 2, paragraphe 3, de l'APPI font l'objet d'une interprétation plus détaillée dans l'arrêté ministériel et les lignes directrices de la PPC. En vertu de la section 2.3, point (8), des lignes directrices de la PPC, les sous-catégories des «antécédents médicaux» détaillées à l'article 2, points ii) et iii), de l'arrêté ministériel sont interprétées comme englobant les données génétiques et biométriques. En outre, bien que la liste n'englobe pas expressément les termes «origine ethnique» et «opinion politique», elle comporte des références à la «race» et aux «convictions religieuses». Comme expliqué dans la section 2.3, points (1) et (2), des lignes directrices de la PPC, la référence à la «race» englobe «les liens ethniques ou les liens avec une partie donnée du monde», tandis que les «convictions religieuses» s'entendent comme englobant les opinions tant religieuses que politiques.

(67) Il ressort clairement du libellé de cette disposition que cette liste n'est pas fermée; d'autres catégories de données pourraient y être ajoutées dans la mesure où leur traitement engendrerait un risque de «discrimination injuste, de préjudice ou de tout autre dommage pour la personne concernée».

(68) Si la notion de données «sensibles» est en soi une construction sociale en ce qu'elle est ancrée dans les traditions culturelles et juridiques, les considérations morales, les choix politiques, etc., d'une société donnée, compte tenu de l'importance d'offrir des garanties adéquates pour les données sensibles transférées à des opérateurs économiques au Japon, la Commission a obtenu que les protections particulières accordées aux «informations à caractère personnel nécessitant des précautions particulières» en vertu du droit japonais soient étendues à l'ensemble des catégories reconnues comme des «données sensibles» dans le règlement (UE) 2016/679. À cette fin, la règle supplémentaire (1) dispose que les données transférées à partir de l'Union européenne et concernant la vie sexuelle, l'orientation sexuelle ou l'appartenance syndicale d'une personne sont traitées par les OETIP «de la même manière que les informations à caractère personnel nécessitant des précautions particulières au sens de l'article 2, paragraphe 3, de l'APPI».

([37]) Il s'agit i) des cas dans lesquels le fait d'informer la personne concernée de la finalité d'utilisation ou de rendre celle-ci publique risque de porte atteinte à la vie, à l'intégrité physique, aux biens ou à d'autres droits et intérêts de la personne concernée ou d'un tiers ou «aux droits ou intérêts légitimes de l'[…]OETIP»; ii) des cas dans lesquels «il est nécessaire de coopérer avec un organisme de l'administration centrale ou une administration locale» dans l'exercice de leurs missions statutaires et si une telle information ou une telle communication au public interfère avec ces «missions»; iii) des cas dans lesquels la finalité d'utilisation est claire sur la base de la situation dans laquelle les données ont été collectées.

(69) En ce qui concerne les garanties substantielles supplémentaires applicables aux informations à caractère personnel nécessitant des précautions particulières, l'article 17, paragraphe 2, de l'APPI n'autorise pas les OETIP à acquérir ce type de données sans le consentement préalable de la personne concernée, sous réserve de quelques exceptions limitées ([38]). En outre, cette catégorie d'informations à caractère personnel est exclue de la possibilité d'une communication à des tiers sur la base de la procédure prévue à l'article 23, paragraphe 2, de l'APPI (autorisant la transmission de données à des tiers sans le consentement préalable de la personne concernée).

2.3.8. *Responsabilité*

(70) 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.

(71) Comme mentionné à la note de bas de page n° 34 (considérant 49), les OETIP sont tenus, en vertu de l'article 26, paragraphe 1, de l'APPI, de vérifier l'identité du tiers leur fournissant des données à caractère personnel et les «circonstances» dans lesquelles ce tiers a acquis ces données [s'il s'agit de données à caractère personnel auxquelles s'applique la présente décision, l'APPI et la règle supplémentaire (3) disposent que ces circonstances incluent le fait que les données proviennent de l'Union européenne, ainsi que la finalité du transfert initial des données]. Cette mesure vise notamment à garantir la licéité du traitement des données tout au long de la chaîne de traitement des données à caractère personnel par les OETIP. En outre, en vertu de l'article 26, paragraphe 3, de l'APPI, les OETIP sont tenus de conserver une trace de la date de réception et les informations (obligatoires) fournies par le tiers en application du paragraphe 1, ainsi que le nom de la personne concernée, les catégories des données traitées et, dans la mesure où cela est pertinent, le fait que la personne concernée a consenti au partage de ses données à caractère personnel. Comme indiqué à l'article 18 des règles de la PPC, il convient de conserver ces éléments d'information pendant une période d'au moins un à trois ans, selon les circonstances. Dans l'exercice de ses missions, la PPC peut exiger la présentation de ces éléments d'information ([39]).

(72) Les OETIP doivent traiter rapidement et de manière appropriée les plaintes des personnes concernées relatives au traitement de leurs informations à caractère personnel. Pour faciliter le traitement des plaintes, ils doivent établir un «système nécessaire pour atteindre [cette] finalité», ce qui implique qu'ils mettent en place les procédures appropriées au sein de leur organisation (par exemple assigner des responsabilités ou fournir un point de contact).

(73) Enfin, l'APPI crée un cadre visant à associer des organisations sectorielles aux efforts déployés pour assurer un niveau élevé de conformité (voir chapitre IV, section 4). Le rôle de ces organisations agréées dans le domaine de la protection des informations à caractère personnel ([40]) consiste à promouvoir la protection des informations à caractère personnel en offrant leur expertise à des entreprises, mais aussi à contribuer à la mise en œuvre de garanties, consistant notamment à traiter les plaintes de particuliers et à contribuer au règlement des différends. À cette fin, elles peuvent demander aux OETIP participants d'adopter les mesures nécessaires, s'il y a lieu ([41]). En outre, en cas de violation de données ou d'autres incidents de sécurité, les OETIP informent en principe la PPC ainsi que la personne concernée (ou le public) et prennent les mesures nécessaires, notamment pour réduire au minimum tout préjudice subi et éviter que de tels incidents ne se reproduisent ([42]). Bien que ces dispositifs soient établis sur une base volontaire, le 10 août 2017, la PPC avait recensé 44 organisations, dont la plus grande, le

([38]) Ces exceptions sont les suivantes: i) les «cas fondés sur des dispositions législatives et réglementaires»; ii) les «cas dans lesquels il convient de protéger la vie humaine, l'intégrité physique ou les biens de la personne concernée ou dans lesquels il est difficile d'obtenir le consentement de cette dernière»; iii) les «cas dans lesquels il est spécifiquement nécessaire d'améliorer l'hygiène publique ou de promouvoir la bonne santé des enfants ou dans lesquels il est difficile d'obtenir le consentement de la personne concernée»; iv) les «cas dans lesquels il est nécessaire de coopérer avec un organisme de l'administration centrale ou une administration locale ou avec une personne chargée par ces dernières d'exercer des missions prescrites par la loi ou la réglementation, et dans lesquels l'obtention du consentement de la personne concernée risque d'interférer avec l'exercice desdites missions»; et v) les cas dans lesquels les informations à caractère personnel en question nécessitant des précautions particulières sont communiquées au public par la personne concernée, un organisme gouvernemental, une autorité locale, une personne appartenant à l'une des catégories visées à l'article 76, paragraphe 1, ou d'autres personnes décrites par les règles de la PPC. Une autre catégorie concerne les «autres cas définis par arrêté ministériel comme étant équivalents aux cas énoncés à chaque point précédent» et englobe notamment, en vertu de l'arrêt ministériel en vigueur, des caractéristiques manifestes d'une personne (telles qu'un problème de santé visible) si les données sensibles ont été acquises (de manière non intentionnelle) en observant, en filmant ou en photographiant la personne concernée, par exemple au moyen de caméras de surveillance.

([39]) En vertu de l'article 40, paragraphe 1), de l'APPI, la PPC peut, dans la mesure nécessaire à la mise en œuvre des dispositions de l'APPI, imposer à un OETIP de fournir les informations ou éléments requis relatifs au traitement des informations à caractère personnel.

([40]) L'APPI prévoit notamment des règles régissant l'agrément de ces organisations; voir les articles 47-50 de l'APPI.

([41]) Article 52 de l'APPI.

([42]) Notification n° 1/2017 de la PPC «Concernant les mesures à prendre en cas de violation des données à caractère personnel ou d'autres incidents».

Centre japonais de traitement et de développement de l'information (JIPDEC), qui représente à elle seule 15 436 opérateurs économiques participants ([43]). Ces dispositifs agréés incluent des associations sectorielles telles que l'association japonaise des opérateurs sur titres, l'association japonaise des écoles de conduite automobile ou l'association des organisateurs de mariages ([44]).

(74) Les organisations agréées de protection des informations à caractère personnel présentent des rapports annuels sur leurs activités. Selon le «Bilan de l'état de mise en œuvre [de] l'APPI au cours de l'exercice 2015» publié par la PPC, les organisations agréées de protection des informations à caractère personnel ont reçu au total 442 plaintes, demandé à 123 reprises à des opérateurs économiques relevant de leur compétence de leur fournir des explications, demandé à ces opérateurs de leur soumettre des documents dans 41 cas, formulé 181 instructions et émis deux recommandations ([45]).

2.3.9. *Limitations concernant les transferts ultérieurs*

(75) Le niveau de protection conféré aux données à caractère personnel qui sont transférées depuis l'Union européenne vers des opérateurs économiques au Japon ne doit pas être compromis par le tranfert ultérieur de ces mêmes données vers des bénéficiaires se trouvant dans un pays tiers autre que le Japon. De tels «transferts ultérieurs», qui constituent, du point de vue de l'opérateur économique japonais, des transferts internationaux à partir du Japon, ne devraient être autorisés que si le destinataire ultérieur hors du Japon est lui-même soumis à des règles assurant un niveau de protection similaire à celui garanti par l'ordre juridique japonais.

(76) Une première protection est inscrite à l'article 24 de l'APPI, qui interdit d'une manière générale le transfert de données à caractère personnel vers un tiers en dehors du territoire japonais en l'absence de consentement préalable de la personne concernée. La règle supplémentaire (4) garantit qu'en cas de transferts de données depuis l'Union européenne, un tel consentement sera donné en pleine connaissance de cause, puisqu'elle prévoit que la personne concernée «reçoit des informations sur les circonstances entourant le transfert, informations qui sont nécessaires pour permettre à la personne concernée de prendre une décision quant à son consentement». Sur cette base, la personne concernée est informée du fait que les données vont être transférées à l'étranger (en dehors du champ d'application de l'APPI), ainsi que du pays de destination spécifique. Elle pourra ainsi apprécier le risque lié au transfert en termes de respect de la vie privée. De même, comme on peut le déduire de l'article 23 de l'APPI (voir le considérant 47), les informations communiquées à la personne concernée devraient porter sur les éléments obligatoires visés au paragraphe 2 dudit article, à savoir les catégories de données à caractère personnel communiquées à un tiers et le mode de communication de celles-ci.

(77) L'article 24 de l'APPI, appliqué conjointement avec l'article 11-2 des règles de la PPC, prévoit plusieurs exceptions à cette règle fondée sur le consentement. En outre, conformément à l'article 24, les mêmes dérogations que celles applicables en vertu de l'article 23, paragraphe 1, de l'APPI s'appliquent également aux transferts internationaux de données ([46]).

(78) Afin de garantir la continuité de la protection en cas de transfert de données à caractère personnel de l'Union européenne vers le Japon sur la base de la présente décision, la règle supplémentaire (4) accroît le niveau de protection applicable aux transferts ultérieurs de ces données effectués par l'OETIP vers un destinataire se trouvant dans un pays tiers. À cet effet, elle pose des limites et établit un cadre que l'OETIP peut appliquer pour les transferts internationaux, comme solution de remplacement au consentement. Plus spécifiquement, et sans préjudice des dérogations prévues à l'article 23, paragraphe 1, de l'APPI, les données à caractère personnel transférées sur la base de la présente décision peuvent faire l'objet de transferts (ultérieurs) en l'absence de consentement dans deux cas uniquement, à savoir i) lorsque les données sont transférées vers un pays tiers qui a été reconnu par la PPC, conformément à l'article 24 de l'APPI, comme garantissant un niveau de protection équivalent à celui garanti au Japon ([47]), ou ii) lorsque l'OETIP et le destinataire tiers ont mis en œuvre conjointement des mesures offrant un niveau de protection équivalent à celui de l'APPI, lue en combinaison avec les règles supplémentaires, au moyen d'une convention, d'autres types d'accords contraignants ou encore, d'accords contraignants au sein d'un groupe d'entreprises. La deuxième catégorie correspond aux instruments utilisés en application du règlement (UE) 2016/679 à des fins de garanties appropriées (clauses contractuelles et règles d'entreprise contraignantes, notamment). En outre, ainsi que l'a confirmé la PPC, le transfert reste, même dans ces cas, soumis aux règles générales applicables à toute fourniture de données à caractère personnel à un tiers en application de l'APPI (obligation d'obtenir le consentement en vertu de l'article 23, paragraphe 1, ou obligation d'information assortie d'une possibilité de renonciation en vertu de l'article 23, paragraphe 2, de l'APPI). Lorsqu'il n'est pas possible de faire

([43]) Selon les chiffres publiés sur le site internet PrivacyMark du JIPDEC, en date du 2 octobre 2017.

([44]) PPC, Liste des organisations agréées de protection des données à caractère personnel, disponible à l'adresse suivante: https://www.ppc.go.jp/personal/nintei/list/ ou https://www.ppc.go.jp/files/pdf/nintei_list.pdf

([45]) PPC, Bilan de l'état de mise en œuvre de l'APPI au cours de l'exercice 2015 (octobre 2016), disponible (uniquement en japonais) sur l'internet à l'adresse suivante: https://www.ppc.go.jp/files/pdf/personal_sekougaiyou_27ppc.pdf

([46]) Voir la note de bas de page nº 32.

([47]) Conformément à l'article 11 des règles de la PPC, cela nécessite non seulement un contrôle effectif des normes matérielles équivalentes à l'APPI par une autorité indépendante chargée de les faire respecter, mais également la garantie de la mise en œuvre des règles correspondantes dans le pays tiers.

parvenir à la personne concernée une demande de consentement ou une demande de communication des informations préalables requises conformément à l'article 23, paragraphe 2, de l'APPI, le transfert ne peut avoir lieu.

(79) En conséquence, en dehors des cas dans lesquels la PPC a constaté que le pays tiers en question garantissait un niveau de protection équivalent à celui garanti par l'APPI ([48]), les exigences énoncées dans la règle supplémentaire (4) excluent le recours à des instruments de transfert qui ne conduisent pas à la mise en place d'une relation contraignante entre l'exportateur de données japonais et l'importateur de données du pays tiers et qui ne garantissent pas le niveau de protection requis. Tel sera le cas, par exemple, du système de règles transfrontalières de protection de la vie privée de l'APEC («APEC Cross Border Privacy Rules» ou les «CBPR»), dont le Japon est une économie participante ([49]): dans ce système, en effet, les protections ne résultent pas d'un accord contraignant pour la personne qui exporte les données et pour celle qui les importe dans le cadre de leur relation bilatérale, et leur niveau est clairement inférieur à celui garanti par la combinaison de l'APPI et des règles supplémentaires ([50]).

(80) Enfin, les articles 20 et 22 de l'APPI offrent également une garantie supplémentaire en cas de transferts (ultérieurs). En vertu de ces dispositions, lorsqu'un opérateur d'un pays tiers (soit la personne qui importe les données) agit au nom de l'OETIP (soit la personne qui exporte les données), c'est-à-dire en tant que sous-traitant, ce dernier doit assurer la surveillance du premier pour ce qui est de la sécurité du traitement des données.

2.3.10. *Droits individuels*

(81) À l'instar du droit de l'UE en matière de protection des données, l'APPI confère aux particuliers plusieurs droits opposables, parmi lesquels le droit d'accès («divulgation»), le droit de rectification et le droit à l'effacement des données, ainsi que le droit d'opposition («cessation d'utilisation»).

(82) Premièrement, en vertu de l'article 28, paragraphes 1 et 2, de l'APPI, la personne concernée a le droit de demander à un OETIP de «lui divulguer des données à caractère personnel conservées permettant de l'identifier»; après avoir reçu une telle demande, l'OETIP «[…] divulgue les données à caractère personnel conservées» à la personne concernée. L'article 29 (droit de rectification) et l'article 30 (droit à la cessation d'utilisation) ont la même structure que l'article 28.

(83) L'article 9 de l'arrêté ministériel précise que la divulgation de données à caractère personnel, au sens de l'article 28, paragraphe 2, de l'APPI, doit s'effectuer par écrit, sauf si l'OEITP et la personne concernée en ont convenu autrement.

(84) Ces droits font l'objet de trois types de limitations, qui ont trait aux droits et intérêts de la personne concernée elle-même ou aux droits et intérêts de tiers ([51]), à une atteinte grave aux opérations économiques de l'OETIP ([52]), ainsi qu'aux cas dans lesquels une divulgation serait contraire à d'autres lois ou réglementations ([53]). Les situations dans lesquelles ces limitations s'appliqueraient sont similaires à certaines des exceptions applicables en vertu de l'article 23, paragraphe 1, du règlement (UE) 2016/679, qui autorise des limitations en ce qui concerne les droits des

([48]) À ce jour, la PPC n'a pas encore adopté de décision en vertu de l'article 24 de l'APPI reconnaissant qu'un pays tiers offre un niveau de protection équivalent à celui garanti au Japon. La seule décision qu'elle envisage actuellement d'adopter porte sur l'EEE. En ce qui concerne d'autres décisions futures éventuelles, la Commission suivra la situation de près et prendra, le cas échéant, les mesures appropriées pour remédier aux éventuelles conséquences négatives pour la continuité de la protection (voir ci-après les considérants 176, 177 et 184, ainsi que l'article 3, paragraphe 1).

([49]) Bien que deux entreprises japonaises seulement soient certifiées conformément au système de CBPR de l'APEC (voir https://english.jipdec.or.jp/sp/protection_org/cbpr/list.html). En dehors du Japon, les seuls autres opérateurs économiques certifiés dans le cadre de ce système sont quelques entreprises américaines (au nombre, peu élevé, de 23) (voir https://www.trustarc.com/consumer-resources/trusted-directory/#apec-list).

([50]) Ainsi, par exemple, il n'existe pas de définition ni de protection spécifique pour les données sensibles, ni d'obligation de conserver les données durant une période limitée. Voir également l'avis 02/2014 du groupe de travail «article 29» concernant des critères de référence pour les exigences applicables aux règles d'entreprise contraignantes à l'intention des autorités nationales compétentes en matière de protection des données dans l'UE, et concernant les règles transfrontalières de protection de la vie privée de l'APEC soumises aux «Accountability Agents» du système CBPR de l'APEC, 6 mars 2014.

([51]) Selon la PPC, seuls des intérêts «devant être protégés juridiquement» peuvent justifier une limitation. Cette appréciation doit être effectuée au cas par cas «en tenant compte de l'interférence avec le droit fondamental au respect de la vie privée, y compris à la protection des données, tel que reconnu par la Constitution et les précédents jurisprudentiels». Parmi les intérêts protégés, on peut citer, par exemple, les secrets d'affaires ou autres secrets commerciaux.

([52]) La notion d'«atteinte grave à la bonne exécution des activités de l'opérateur» est illustrée, dans les lignes directrices de la PPC, par différents exemples, comme des demandes complexes répétées et identiques émanant de la même personne dès lors que de telles demandes impliquent une charge substantielle pour un opérateur économique qui compromettrait sa capacité de répondre à d'autres demandes [lignes directrices de la PPC (General Rule Edition), p. 62]. D'une manière plus générale, la PPC a confirmé que cette catégorie était limitée à des cas exceptionnels allant au-delà de simples désagréments. Plus spécifiquement, un OETIP ne peut refuser que des informations soient communiquées au seul motif que le volume de données réclamées est élevé.

([53]) Ainsi que l'a confirmé la PPC, de telles lois doivent respecter le droit au respect de la vie privée tel qu'il est garanti par la Constitution et, partant, «refléter une limitation nécessaire et raisonnable».

personnes pour des raisons liées à «la protection de la personne concernée ou des droits et libertés d'autrui» ou à d'«autres objectifs importants d'intérêt public général». Si la catégorie des cas dans lesquels la divulgation violerait d'«autres lois ou réglementations» peut sembler étendue, les lois et réglementations prévoyant des limitations en la matière doivent toutefois respecter le droit à la vie privée inscrit dans la Constitution et ne peuvent imposer des limitations que dans la mesure où l'exercice de ce droit «porterait atteinte au bien-être public» ([54]). Il convient à cet effet de trouver un équilibre entre les intérêts en jeu.

(85) En vertu de l'article 28, paragraphe 3, de l'APPI, si les données demandées n'existent pas, ou si l'OETIP concerné décide de ne pas donner accès aux données conservées, l'OETIP est tenu d'en informer la personne sans tarder.

(86) Deuxièmement, en vertu de l'article 29, paragraphes 1 et 2, de l'APPI, une personne concernée dispose du droit de faire rectifier, compléter ou supprimer ses données à caractère personnel conservées lorsque ces données sont inexactes. Lorsqu'il reçoit une telle demande, l'OEITP «procède […] à une enquête nécessaire» et, en fonction des résultats de cette enquête, «rectifie, etc., le contenu des données conservées».

(87) Troisièmement, en vertu de l'article 30, paragraphes 1 et 2, de l'APPI, une personne concernée a le droit de demander à un OETIP de cesser d'utiliser des données à caractère personnel, ou de supprimer de telles données, lorsque celles-ci font l'objet d'un traitement contraire à l'article 16 (qui traite de la limitation de la finalité) ou ont été obtenues de manière abusive en violation de l'article 17 de l'APPI (qui traite de l'acquisition à la suite d'une tromperie, par d'autres moyens inappropriés ou, dans le cas des données sensibles, sans consentement). De même, en vertu de l'article 30, paragraphes 3 et 4, de l'APPI, la personne a le droit de demander à l'OETIP de cesser de fournir les données à un tiers dès lors que cela serait contraire aux dispositions de l'article 23, paragraphe 1, ou de l'article 24 de l'APPI (concernant la fourniture à un tiers, y compris les transferts internationaux).

(88) Lorsque la demande est fondée, l'OETIP met fin sans tarder à l'utilisation des données ou à la fourniture de données à un tiers, dans la mesure nécessaire pour remédier à la violation. Dans les cas relevant d'une exception (notamment si la cessation de l'utilisation est susceptible d'entraîner des coûts particulièrement élevés) ([55]), l'OETIP met en place d'autres mesures nécessaires pour protéger les droits et intérêts de la personne concernée.

(89) Contrairement au droit de l'UE, l'APPI et les règles de niveau inférieur pertinentes ne comportent pas de dispositions juridiques traitant spécifiquement de la possibilité de s'opposer à un traitement à des fins de prospection. Un tel traitement s'inscrira toutefois, conformément à la présente décision, dans le cadre d'un transfert de données à caractère personnel ayant été précédemment collectées dans l'Union européenne. En vertu de l'article 21, paragraphe 2, du règlement (UE) 2016/679, la personne concernée aura toujours la possibilité de s'opposer à un transfert de données à des fins de prospection. En outre, ainsi que cela est expliqué au considérant 43, en vertu de la règle supplémentaire (3), un OETIP est tenu de traiter les données reçues sur la base de la décision aux mêmes fins que celles pour lesquelles elles ont été transférées depuis l'Union européenne, sauf si la personne concernée consent à une modification de la finalité de l'utilisation.En conséquence, si le transfert a été effectué à d'autres fins que des fins de prospection, il sera interdit à un OETIP japonais de traiter les données à des fins de prospection en l'absence de consentement de la personne concernée dans l'UE.

(90) Dans tous les cas mentionnés aux articles 28 et 29 de l'APPI, l'OETIP est tenu de communiquer sans tarder à la personne les suites données à sa demande et doit en outre expliquer tout refus (partiel) fondé sur les exceptions statuaires prévues aux articles 27 à 30 (article 31 de l'APPI).

([54]) L'article 13 de la Constitution a été interprété par la Cour suprême comme conférant un droit à la protection de la vie privée (voir les considérants 7 et 8 ci-dessus). Bien que ce droit puisse être limité dès lors qu'il «interfère avec le bien-être public», la Cour suprême, dans son arrêt du 6 mars 2008 (voir le considérant 8), a précisé que toute limitation (soit, en l'espèce, l'autorisation pour une autorité publique de collecter et de traiter des données à caractère personnel) doit être mise en balance avec le droit au respect de la vie privée en tenant compte d'éléments tels que la nature des données concernées, les risques engendrés par le traitement de ces données pour les personnes, les protections applicables, ainsi que les avantages du traitement pour l'intérêt public. Cela est très semblable au type de mise en balance requis en application du droit de l'UE, fondé sur les principes de nécessité et de proportionnalité, aux fins de l'autorisation de toute limitation des droits et garanties en matière de protection des données.

([55]) Pour plus de précisions concernant ces exceptions, voir Professeur Katsuya Uga, «Article by Article Commentary of the revised Act on the Protection of Personal Information» (commentaires, article par article, sur la loi révisée sur la protection des données à caractères personnel), 2015, p. 217. À titre d'exemple de demande entraînant «des dépenses élevées», on peut citer une situation dans laquelle seuls certains noms figurant sur une longue liste (comme un répertoire, par exemple) font l'objet d'un traitement contraire au principe de limitation de la finalité alors que ce répertoire est déjà en vente. Le rappel des exemplaires dudit répertoire et leur remplacement par de nouveaux exemplaires entraînerait des coûts élevés. Dans ce même exemple, lorsque des exemplaires de ce répertoire ont déjà été vendus à de nombreuses personnes et qu'il est impossible de tous les réunir, il serait également «difficile de respecter une injonction de cessation d'utilisation». Dans ces scénarios, une «autre action nécessaire» pourrait consister, par exemple, à publier ou à distribuer un rectificatif. Une telle action n'exclut pas d'autres formes de recours (judiciaire), que ce soit pour atteinte à la vie privée, atteinte à l'image (diffamation) causée par la publication ou encore, violation d'autres intérêts.

(91) En ce qui concerne les conditions d'introduction d'une demande, l'article 32 de l'APPI (lu en combinaison avec l'arrêté ministériel) autorise l'OETIP à définir des procédures raisonnables, y compris en ce qui concerne les informations nécessaires pour identifier les données à caractère personnel qui sont conservées. Conformément à l'article 32, paragraphe 4, toutefois, l'OETIP ne doit pas imposer «une charge excessive à une personne concernée». Dans certains cas, il peut également imposer des frais tant que le montant de ceux-ci demeure «dans les limites considérées comme raisonnables compte tenu des coûts effectifs» (article 33 de l'APPI).

(92) Enfin, la personne peut s'opposer à la communication de ses données à caractère personnel à un tiers sur le fondement de l'article 23, paragraphe 2, de l'APPI, ou ne pas donner son consentement sur la base de l'article 23, paragraphe 1 (et, de la sorte, empêcher la divulgation s'il n'existe aucune autre base légale). De même, la personne peut mettre un terme au traitement de données effectué à des fins différentes en refusant de donner son consentement sur la base de l'article 16, paragraphe 1, de l'APPI.

(93) Contrairement au droit de l'UE, l'APPI et les règles de niveau inférieur pertinentes ne comportent pas de dispositions générales traitant de la question des décisions affectant la personne concernée et reposant uniquement sur le traitement automatisé de données à caractère personnel. Toutefois, cette question est abordée dans certaines règles sectorielles applicables au Japon qui sont particulièrement pertinentes pour ce type de traitement. Les secteurs en question sont notamment ceux dans lesquels les entreprises sont les plus susceptibles de recourir au traitement automatisé de données à caractère personnel pour prendre des décisions affectant des personnes (comme, par exemple, le secteur financier). Ainsi, les orientations exhaustives relatives à la supervision des grands établissements bancaires, telles que révisées en juin 2017, prévoient que la personne concernée doit obtenir des explications spécifiques quant aux motifs du rejet d'une demande de conclusion d'une convention de prêt. Ces règles offrent donc des protections dans un nombre vraisemblablement assez limité de cas dans lesquels des décisions automatisées seraient prises par l'opérateur économique japonais «important» les données (plutôt que par le responsable du traitement des données dans l'UE «exportant» les données).

(94) En tout état de cause, pour ce qui est des données à caractère personnel qui ont été collectées dans l'Union européenne, toute décision fondée sur un traitement automatisé sera généralement prise par le responsable du traitement des données de l'Union (qui est en relation directe avec la personne concernée) et relève par conséquent du règlement (UE) 2016/679 ([56]). Cela inclut les cas de transfert dans lesquels le traitement est effectué par un opérateur économique étranger (japonais, par exemple) en tant qu'agent (sous-traitant) agissant au nom du responsable du traitement des données de l'UE (ou en tant que sous-traitant agissant au nom du sous-traitant de l'UE ayant obtenu les données auprès d'un responsable du traitement des données de l'UE 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 l'APPI affecte le niveau de protection des données à caractère personnel transférées sur la base de la présente décision.

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

2.4.1. *Supervision indépendante*

(95) Pour garantir un niveau adéquat de protection des données également 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.

(96) Au Japon, l'autorité chargée de surveiller l'application de l'APPI et de la faire respecter est la PPC. Cette dernière compte un président et huit commissaires nommés par le premier ministre avec l'accord des deux chambres de la Diète. Le mandat du président et de chaque commissaire a une durée de cinq ans et peut être reconduit (article 64 de l'APPI). Les commissaires ne peuvent être démis de leurs fonctions que pour une bonne raison, dans un nombre limité de circonstances exceptionnelles ([57]), et ne peuvent pas exercer activement des activités politiques. En outre, en vertu de l'APPI, les commissaires qui travaillent à temps plein doivent s'abstenir d'exercer toute autre activité rémunérée ou activité commerciale. Tous les commissaires sont également soumis à des règles internes leur interdisant de prendre part aux délibérations en cas de possible conflit d'intérêts. La PPC est assistée par un secrétariat, dirigé par un secrétaire général et mis en place aux fins de l'exécution des tâches confiées à la PPC (article 70 de l'APPI). Tant les commissaires que l'ensemble des fonctionnaires du secrétariat sont liés par des règles strictes en matière de secret (articles 72 et 82 de l'APPI).

([56]) Inversement, il peut exister exceptionnellement un lien direct entre l'opérateur japonais 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 japonais 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.

([57]) En vertu de l'article 65 de l'APPI, un commissaire ne peut être démis de ses fonctions contre son gré que pour l'une des raisons suivantes: i) ouverture d'une procédure de faillite; ii) condamnation pour violation de l'APPI ou de la loi sur l'utilisation de numéros d'identification; iii) condamnation à une peine d'emprisonnement non assortie d'une peine de travail ou à une peine encore plus sévère; iv) incapacité d'exécuter ses fonctions en raison de troubles mentaux ou physiques ou d'un comportement répréhensible.

(97) Les compétences de la PPC, exercées en toute indépendance ([58]), sont essentiellement énoncées aux articles 40, 41 et 42 de l'APPI. En vertu de l'article 40, la PPC peut demander aux OETIP de faire rapport ou de fournir des documents sur les opérations de traitement et peut également procéder à des inspections sur place ou au contrôle de livres ou autres documents. Dans la mesure où cela est nécessaire aux fins de la mise en œuvre de l'APPI, elle peut également fournir aux OETIP des orientations ou des conseils concernant le traitement des données à caractère personnel. La PPC a déjà fait usage de cette compétence en application de l'article 41 de l'APPI en adressant des orientations à Facebook à la suite des révélations concernant Facebook/Cambridge Analytica.

(98) Qui plus est, la PPC a le pouvoir - agissant à la suite d'une plainte ou de sa propre initiative - d'émettre des recommandations et de prononcer des injonctions pour faire respecter l'APPI et d'autres règles contraignantes (y compris les règles supplémentaires) dans des cas individuels. Ces compétences sont énoncées à l'article 42 de l'APPI. Alors que les paragraphes 1 et 2 de celui-ci prévoient un mécanisme en deux phases selon lequel la PPC peut prononcer une injonction (uniquement) à la suite d'une recommandation préalable, le paragraphe 3 permet l'adoption directe d'une injonction dans les cas d'urgence.

(99) Toutes les dispositions du chapitre IV, section 1, de l'APPI ne sont pas reprises à l'article 42, paragraphe 1 — qui définit également le champ d'application de l'article 42, paragraphe 2 —, ce qui peut toutefois s'expliquer par le fait que certaines de ces dispositions ne concernent pas les obligations de l'OETIP ([59]) et que toutes les protections essentielles sont déjà fournies par d'autres dispositions qui figurent sur cette liste. Ainsi, bien que l'article 15 (qui exige de l'OETIP qu'il détermine la finalité de l'utilisation et traite les données à caractère personnel correspondantes exclusivement dans ce cadre) ne soit pas mentionné, le non-respect de cette exigence peut donner lieu à une recommandation basée sur une violation de l'article 16, paragraphe 1 (qui interdit à l'OETIP de traiter des données à caractère personnel au-delà de ce qui est nécessaire pour réaliser la finalité de l'utilisation, à moins d'obtenir le consentement de la personne concernée) ([60]). Une autre disposition qui n'est pas mentionnée à l'article 42, paragraphe 1, est l'article 19 de l'APPI relatif à l'exactitude et à la conservation des données. Le non-respect de cette disposition peut consister en une violation de l'article 16, paragraphe 1, ou découler d'une violation de l'article 29, paragraphe 2, si la personne concernée demande la rectification ou la suppression de données erronées ou excédentaires et que l'OETIP refuse de satisfaire cette demande. Pour ce qui est des droits de la personne concernée en vertu de l'article 28, paragraphe 1, de l'article 29, paragraphe 1, et de l'article 30, paragraphe 1, la surveillance par la PPC est garantie par les pouvoirs d'exécution conférés à celle-ci pour ce qui est des obligations correspondantes de l'OETIP énoncées dans lesdits articles.

(100) En vertu de l'article 42, paragraphe 1, de l'APPI, la PPC peut, si elle reconnaît qu'il est «nécessaire de protéger les droits et intérêts d'un individu dans les cas où un [OETIP] a enfreint» des dispositions spécifiques de l'APPI, émettre une recommandation en vue de la «suspension de l'acte de violation ou de l'adoption d'autres mesures nécessaires pour remédier à cette violation». Une telle recommandation n'est pas contraignante, mais ouvre la voie à l'adoption d'une injonction contraignante en vertu de l'article 42, paragraphe 2, de l'APPI. Sur la base de cette disposition, lorsque la recommandation n'est pas suivie «sans raisons légitimes» et que la PPC «reconnaît le caractère imminent d'une violation grave des droits et intérêts d'un individu», elle peut enjoindre à l'OETIP de prendre des mesures conformément à cette recommandation.

(101) Les règles supplémentaires précisent encore et renforcent les pouvoirs d'exécution de la PPC. Plus spécifiquement, dans les cas concernant des données importées depuis l'Union européenne, la PPC considérera toujours le fait que l'OETIP n'ait pas, sans raison légitime, adopté de mesures en application d'une recommandation émise par l'APPI conformément à l'article 42, paragraphe 1, comme une violation grave des droits et intérêts d'un individu présentant un caractère imminent au sens de l'article 42, paragraphe 2, et partant une infraction justifiant l'émission d'une injonction contraignante. En outre, comme «raison légitime» de ne pas se conformer à une recommandation, la PPC n'acceptera qu'un «événement de nature extraordinaire [empêchant de s'y conformer], échappant au contrôle de l'[OETIP], et qui ne peut raisonnablement pas être prévu (comme, par exemple, des catastrophes naturelles)» ou les cas dans lesquels la nécessité de prendre des mesures concernant une recommandation «a disparu, car l'[OETIP] a pris une autre mesure qui remédie pleinement à la violation».

([58]) Voir l'article 62 de l'APPI.

([59]) Ainsi, certaines dispositions concernent les actions facultatives de l'OETIP (articles 32 et 33 de l'APPI, ou les obligations de moyens qui sont, en tant que telles, non exécutoires (article 31, article 35, article 36, paragraphe 6, et article 39 de l'APPI). Certaines obligations ne s'adressent pas à l'OETIP, mais à d'autres acteurs. Tel est le cas, par exemple, de l'article 23, paragraphe 4, de l'article 26, paragraphe 2, et de l'article 34 de l'APPI [bien que le respect de l'article 26, paragraphe 2, de l'APPI soit garanti par la possibilité de sanctions pénales au sens de l'article 88, point i), de l'APPI].

([60]) En outre, ainsi que cela a été expliqué ci-dessus au considérant (48), dans le cas d'un transfert, la «finalité de l'utilisation» sera précisée par la personne qui exporte les données à partir de l'UE, personne qui est liée, à cet égard, par l'obligation énoncée à l'article 5, paragraphe 1, point b), du règlement (UE) 2016/679. Cette obligation doit être respectée par l'autorité de protection des données (APD) de l'Union européenne.

(102) Le non-respect d'une injonction de la PPC est considéré comme une infraction pénale en vertu de l'article 84 de l'APPI, et un OETIP jugé coupable peut être condamné à une peine d'emprisonnement assortie d'une peine de travail d'une durée maximale de six mois ou se voir infliger une amende d'un montant maximal de 300 000 yens. De plus, conformément à l'article 85, point i), de l'APPI, l'absence de coopération avec la PPC ou une obstruction à l'enquête sont punissables d'une amende d'un montant maximal de 300 000 yens. Ces sanctions pénales viennent s'ajouter à celles qui peuvent être infligées pour des violations de l'APPI sur le fond (voir le considérant 108).

2.4.2. *Recours juridictionnel*

(103) 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.

(104) Préalablement à l'introduction d'un recours administratif ou juridictionnel, ou en lieu et place de l'introduction d'un tel recours, une personne peut décider de déposer une plainte concernant le traitement de ses données à caractère personnel auprès du responsable du traitement des données lui-même. En vertu de l'article 35 de l'APPI, les OETIP s'efforcent de traiter ces plaintes «rapidement et de manière appropriée» et mettent en place à cet effet des systèmes internes de traitement des plaintes. En outre, en vertu de l'article 61, point ii), de l'APPI, la PPC est chargée d'assurer la «médiation nécessaire pour ce qui est de la plainte qui a été déposée et de la coopération proposée à un opérateur économique traitant cette plainte», ce qui, dans les deux cas, inclus les plaintes déposées par des étrangers. À cet égard, le législateur japonais a également chargé l'administration centrale de prendre les «mesures nécessaires» pour permettre et faciliter le règlement de plaintes par les OETIP (article 9), tandis que les administrations locales doivent, en pareils cas, favoriser la médiation (article 13). De même, les personnes peuvent introduire une plainte auprès de l'un des centres de consommateurs, dont le nombre est supérieur à 1 700, mis en place par les administrations locales conformément à la loi sur la sécurité des consommateurs ([61]), outre la possibilité qui leur est donnée de déposer plainte auprès du centre national des consommateurs du Japon. De telles plaintes peuvent également avoir trait à une violation de l'APPI. En vertu de l'article 19 de la loi fondamentale sur les consommateurs ([62]), les administrations locales s'efforcent de rechercher des solutions de médiation en ce qui concerne les plaintes et apportent l'expertise nécessaire aux parties. Ces mécanismes de résolution des litiges semblent assez efficaces, le taux de résolution étant de 91,2 % pour plus de 75 000 plaintes en 2015.

(105) Les violations des dispositions de l'APPI par un OETIP peuvent donner lieu à des actions civiles, ainsi qu'à des procédures et à des sanctions pénales. Premièrement, si une personne considère que les droits dont elle jouit en vertu des articles 28, 29 et 30 de l'APPI ont été violés, elle peut réclamer une mesure injonctive, en demandant au tribunal d'enjoindre à un OETIP de satisfaire à la demande qu'elle a formulée sur le fondement de l'une de ces dispositions, en lui divulguant les données à caractère personnel conservées (article 28), en rectifiant les données à caractère personnel conservées qui sont incorrectes (article 29), ou encore en mettant un terme au traitement illicite ou à la fourniture de données à un tiers (article 30). Une telle action peut être menée sans devoir se fonder sur l'article 709 du code civil ([63]) ou, d'une autre façon, sur le droit de la responsabilité civile ([64]). Cela signifie notamment que la personne n'a pas à démontrer l'existence d'un préjudice.

(106) Deuxièmement, lorsqu'une infraction présumée ne concerne pas des droits individuels conférés par les articles 28, 29 et 30, mais des principes ou obligations généraux en matière de protection des données à caractère personnel applicables à l'OETIP, la personne concernée peut se constituer partie civile contre l'opérateur économique sur le fondement des dispositions du code civil japonais en matière de responsabilité délictuelle, et plus particulièrement de l'article 709 de celui-ci. Alors qu'une action en justice engagée sur le fondement de l'article 709 requiert, outre l'existence d'une faute (intentionnelle ou commise par négligence), la démonstration d'un préjudice, un tel préjudice peut, en vertu de l'article 710 du code civil, être tant matériel qu'immatériel. Aucune limite n'est imposée quant au montant de l'indemnisation.

(107) En ce qui concerne les voies de recours disponibles, l'article 709 du code civil japonais prévoit une indemnisation monétaire. Toutefois, la jurisprudence japonaise a interprété cet article comme conférant également le droit d'obtenir une injonction ([65]). En conséquence, si une personne concernée intente une action sur le fondement de l'article 709 du code civil et fait valoir qu'il a été porté atteinte à ses droits ou intérêts du fait d'une violation d'une disposition de l'APPI par la partie défenderesse, cette réclamation peut inclure, outre l'indemnisation du préjudice subi, une demande de mesure injonctive, visant notamment à mettre fin au traitement illicite.

([61]) Loi n° 50 du 5 juin 2009.
([62]) Loi n° 60 du 22 août 2012.
([63]) L'article 709 du code civil constitue le principal fondement des procédures civiles en matière de dommages et intérêts. En vertu de cette disposition, «une personne qui a violé, intentionnellement ou par négligence, des droits d'autres personnes ou des intérêts d'autres personnes protégés par la loi, est tenue de réparer le préjudice qui en résulte».
([64]) Haute cour de Tokyo, arrêt du 20 mai 2015 (non publié); Tribunal de district de Tokyo, arrêt du 8 septembre 2014, Westlaw Japon 2014WLJPCA09088002. Voir également l'article 34, paragraphes 1 et 3, de l'APPI.
([65]) Voir Cour suprême, arrêt du 24 septembre 2002 (Hanrei Times vol. 1106, p. 72).

(108) Troisièmement, outre les voies de recours en responsabilité délictuelle, une personne concernée a la possibilité d'introduire une plainte auprès du parquet ou d'un fonctionnaire de la police judiciaire en cas de violations de l'APPI, qui peut déboucher sur des sanctions pénales. Le chapitre VII de l'APPI contient plusieurs dispositions pénales. La plus importante (article 84) a trait au non-respect, par l'OETIP, des injonctions de la PPC émises en vertu de l'article 42, paragraphes 2 et 3. Si un opérateur économique ne respecte pas une injonction émise par la PPC, le président de celle-ci (de même que tout autre fonctionnaire de l'administration) ([66]) peut transmettre le dossier au parquet ou au fonctionnaire de la police judiciaire et, ce faisant, déclencher l'ouverture d'une procédure pénale. La violation d'une injonction de la PPC est sanctionnée par une peine d'emprisonnement accompagnée d'une peine de travail d'une durée maximale de six ans ou d'une amende d'un montant maximal de 300 000 yens. D'autres dispositions de l'APPI prévoient des sanctions en cas de violations de l'APPI affectant les droits et intérêts des personnes concernées, parmi lesquelles l'article 83 de l'APPI (qui concerne «la fourniture ou l'utilisation détournée» d'une base de données à caractère personnel «aux fins de la recherche de […] profits illégaux») et l'article 88, point i), de l'APPI (qui concerne le fait, pour un tiers, de ne pas informer dûment l'OEITP lorsque ce dernier reçoit des données à caractère personnel conformément à l'article 26, paragraphe 1, de l'APPI, en particulier des précisions sur l'acquisition préalable de ces données par un tiers). Les sanctions applicables à de telles violations de l'APPI sont, respectivement, une peine d'emprisonnement accompagnée d'une peine de travail d'une durée maximale d'un an ou une amende d'un montant maximal de 500 000 yens (dans le cas de l'article 83), ou une amende administrative d'un montant maximal de 100 000 yens [dans le cas de l'article 88, point i)]. Bien que la menace d'une sanction pénale soit déjà, en soi, susceptible d'avoir un effet fortement dissuasif sur les gestionnaires d'une entreprise qui dirigent les opérations de traitement de l'OETIP ainsi que sur les personnes qui procèdent au traitement des données, l'article 87 de l'APPI précise que lorsqu'un représentant, un salarié ou tout autre travailleur d'une personne morale a commis une des infractions prévues aux articles 83 à 85 de l'APPI, «ce représentant, salarié ou travailleur est sanctionné, et une amende, fixée par les articles respectifs, est infligée à ladite personne morale». En pareil cas, tant le salarié que la société peuvent se voir infliger des sanctions jusqu'à concurrence du montant total maximum.

(109) Enfin, les personnes peuvent également former un recours contre toute action ou tout défaut d'action de la PPC. À cet égard, la loi japonaise prévoit plusieurs voies de recours administratif ou judiciaire.

(110) Lorsqu'une personne n'est pas satisfaite de l'intervention de la PPC, elle peut introduire un recours administratif en vertu de la loi sur l'examen des recours administratifs ([67]). Inversement, lorsqu'une personne considère que la PPC aurait dû agir mais ne l'a pas fait, elle peut demander à cette autorité, conformément à l'article 36-3 de la loi précitée, d'arrêter une disposition ou de fournir des orientations administratives si elle estime «qu'une disposition n'a pas été arrêtée ou que des orientations administratives n'ont pas été imposées aux fins de la correction de la violation, en dépit de leur nécessité».

(111) En ce qui concerne le recours juridictionnel, une personne qui n'est pas satisfaite d'une disposition administrative prise par la PPC peut, en vertu de la loi sur les contentieux administratifs, introduire une demande de *mandamus* ([68]) pour que le tribunal enjoigne à la PPC de prendre d'autres mesures ([69]). Dans certains cas, le tribunal peut aussi émettre une injonction de *mandamus* provisoire afin de prévenir un préjudice irréversible ([70]). En outre, en vertu de cette même loi, une personne peut demander la révocation d'une décision de la PPC ([71]).

(112) Enfin, une personne peut également introduire une action en dommages et intérêts auprès de l'État contre la PPC en vertu de l'article 1er, paragraphe 1, de la loi sur les recours auprès de l'État si elle a subi un préjudice du fait du caractère illicite d'une injonction rendue par cette dernière à l'égard d'un opérateur économique ou si la PPC n'a pas exercé ses compétences.

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

(113) La Commission a également évalué les limitations et les garanties prévues, y compris les mécanismes de surveillance et de recours prévus par le droit japonais en ce qui concerne la collecte et l'utilisation ultérieure des données à caractère personnel transférées à des opérateurs économiques au Japon par les autorités publiques pour des motifs d'intérêt public, en particulier à des fins répressives et à des fins de sécurité nationale («accès des pouvoirs publics»). À cet égard, le gouvernement japonais 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.

([66]) Article 239, paragraphe 2, du code de procédure pénale.
([67]) Loi n° 160 de 2014.
([68]) Article 37-2 de la loi sur les contentieux administratifs.
([69]) En vertu de l'article 3, paragraphe 6, de la loi sur les contentieux administratifs, les termes «procédure de mandamus» désignent une action tendant à obtenir une injonction du tribunal contre une agence administrative en vue de l'adoption d'une disposition administrative originale que cette dernière aurait «dû» prendre mais qu'elle n'a pas prise.
([70]) Article 37-5 de la loi sur les contentieux administratifs.
([71]) Chapitre II, section 1, de la loi sur les contentieux administratifs.

3.1. **Cadre juridique général**

(114) En tant qu'exercice de l'autorité publique, l'accès des pouvoirs publics aux données au Japon doit intervenir dans le respect total de la loi (principe de légalité). À cet égard, la Constitution du Japon prévoit des dispositions qui limitent et encadrent la collecte de données à caractère personnel par les autorités publiques. Comme cela a déjà été mentionné au sujet du traitement des données par les opérateurs économiques, en se fondant sur l'article 13 de la Constitution, qui, notamment, protège le droit à la liberté, la Cour suprême du Japon a reconnu le droit au respect de la vie privée et à la protection des données ([72]). Un aspect important de ce droit est la liberté pour une personne d'empêcher que ses informations à caractère personnel soient divulguées à un tiers sans son autorisation ([73]), ce qui implique un droit à la protection effective des données à caractère personnel contre les abus et (en particulier) les accès non autorisés. Une protection supplémentaire est assurée par l'article 35 de la Constitution sur le droit de toutes les personnes d'être en sécurité dans leurs domicile, papiers et effets, qui exige des pouvoirs publics qu'ils obtiennent un mandat délivré par un tribunal pour «cause adéquate» ([74]) dans tous les cas de «perquisitions et saisies». Dans son arrêt du 15 mars 2017 (affaire GPS), la Cour suprême a précisé que cette obligation de mandat s'applique dès que le gouvernement envahit («entre dans») la sphère privée de sorte que la volonté de la personne est supprimée et donc, lorsqu'il procède à une «enquête coercitive». Un juge ne peut délivrer ce mandat que sur la base d'une suspicion concrète d'infraction, c'est-à-dire lorsque lui ont été fournies des preuves documentaires sur la base desquelles la personne concernée par l'enquête peut être considérée comme ayant commis une infraction pénale ([75]). Par conséquent, les autorités japonaises ne sont pas habilités à collecter des informations à caractère personnel par des moyens de contrainte lorsqu'aucune violation de la loi n'a encore eu lieu ([76]), en vue par exemple de prévenir une infraction ou une autre menace pour la sécurité (comme c'est le cas pour les enquêtes pour des raisons de sécurité nationale).

(115) Selon le principe de la réserve de la loi, toute collecte de données dans le cadre d'une enquête coercitive doit être expressément autorisée par la loi [ainsi qu'illustré par exemple par l'article 197, paragraphe 1, du code de procédure pénale («CCP») en ce qui concerne la collecte d'informations par voie de contrainte aux fins d'une enquête pénale]. Cette exigence s'applique également à l'accès aux informations électroniques.

(116) Qui plus est, l'article 21, paragraphe 2, de la Constitution garantit le secret de tous les moyens de communication, des limitations n'étant autorisées par voie législative que pour des raisons d'intérêt public. L'article 4 de la loi sur les activités de télécommunications, selon laquelle le secret des communications traitées par une entreprise de télécommunications ne peut être violé, met en œuvre cette obligation de confidentialité au niveau de la loi. Cette disposition a été interprétée comme interdisant la divulgation des données des communications, sauf si les utilisateurs donnent leur consentement ou si elle se fonde sur l'une des dérogations explicites découlant de la responsabilité pénale en vertu du code pénal ([77]).

(117) Par ailleurs, la Constitution garantit le droit d'accès à la justice (article 32) et le droit d'intenter une action en justice contre l'État pour obtenir réparation dans le cas où une personne a subi des dommages en raison d'un acte illégal d'un fonctionnaire public (article 17).

(118) En ce qui concerne spécifiquement le droit à la protection des données, le chapitre III, sections 1, 2 et 3, de l'APPI établit des principes généraux communs à tous les secteurs, y compris le secteur public. En particulier, l'article 3 de l'APPI dispose que toutes les informations à caractère personnel doivent être traitées conformément au principe de respect de la personnalité des individus. Une fois que des informations à caractère personnel ont été collectées («obtenues») par des autorités publiques ([78]), y compris dans le cadre d'enregistrements électroniques, leur

([72]) Voir, par exemple, l'arrêt de la Cour suprême du 12 septembre 2003, dans l'affaire n° 1656 [2002 (Ju)]. En particulier, la Cour suprême a estimé que «chaque personne a la liberté d'empêcher que ses informations à caractère personnel soient divulguées à un tiers ou rendues publiques sans raison valable».

([73]) Cour suprême, arrêt du 6 mars 2008 (Juki-net).

([74]) La «cause adéquate» n'existe que lorsque la personne concernée (suspect ou accusé) est considérée comme ayant commis une infraction et que la perquisition et la saisie sont nécessaires pour l'enquête pénale. Voir l'arrêt de la Cour suprême du 18 mars 1969, dans l'affaire n° 100 [1968 (Shi)].

([75]) Voir l'article 156, paragraphe 1, du code de procédure pénale.

([76]) Il convient de noter, toutefois, que la loi sur la répression de la criminalité organisée et le contrôle des produits du crime, du 15 juin 2017, crée une nouvelle infraction qui criminalise la préparation d'actes de terrorisme et de certaines autres formes de criminalité organisée. Des enquêtes ne peuvent être engagées qu'en cas de suspicion concrète, fondée sur la preuve que les trois conditions nécessaires pour constituer l'infraction sont toutes remplies (implication d'un groupe criminel organisé, «acte de planification» et «acte de préparation à la mise en œuvre» de l'infraction). Voir aussi, par exemple, les articles 38 à 40 de la loi sur la prévention des activités subversives (loi n° 240 du 21 juillet 1952).

([77]) Article 15, paragraphe 8, des lignes directrices sur la protection des informations à caractère personnel dans le secteur des télécommunications.

([78]) Les instances administratives telles que définies à l'article 2, paragraphe 1, de l'APPIHAO. D'après les informations communiquées par le gouvernement japonais, toutes les autorités publiques, à l'exception de la police préfectorale, relèvent de la définition des «instances administratives». Dans le même temps, la police préfectorale opère dans le cadre juridique fixé par les ordonnances préfectorales sur la protection des informations à caractère personnel (voir l'article 11 de l'APPI et la politique de base), qui prévoient des dispositions relatives à la protection des informations à caractère personnel équivalentes à celles de l'APPIHAO. Voir l'annexe II, point I.B. Comme l'explique la PPC, conformément à la «politique de base», ces ordonnances doivent être adoptées sur la base du contenu de l'APPIHAO, et le MIC émet des notes afin de fournir aux administrations locales les orientations nécessaires à cet égard. Comme elle le souligne, «[d]ans le respect de ces limites, l'ordonnance relative à la protection des données à caractère personnel dans chaque préfecture doit être établie […] sur la base de la politique de base et du contenu des notes».

traitement est régi par la loi sur la protection des informations à caractère personnel détenues par des instances administratives («APPIHAO») ([79]). Cette disposition s'applique en principe ([80]) également au traitement des informations à caractère personnel à des fins répressives ou à des fins de sécurité nationale. L'APPIHAO prévoit notamment que les autorités publiques: i) ne peuvent conserver des informations à caractère personnel que dans la mesure où cela est nécessaire à l'exercice de leurs fonctions; ii) ne peuvent utiliser ces informations à des fins «inappropriées» ou les divulguer à un tiers sans justification; iii) doivent spécifier la finalité et ne pas en changer au-delà de ce qui peut raisonnablement être considéré comme pertinent pour la finalité initiale (limitation de la finalité); iv) ne peuvent, en principe, pas utiliser ni transmettre à un tiers les informations à caractère personnel conservées à d'autres fins et, si elles l'estiment nécessaire, doivent imposer des restrictions à la finalité ou à la méthode d'utilisation par des tiers; v) doivent s'efforcer de garantir l'exactitude des informations (qualité des données); vi) doivent prendre les mesures nécessaires en vue d'assurer une gestion correcte des informations et de prévenir toute fuite, toute perte ou tout dommage (sécurité des données); et vii) doivent s'efforcer de traiter correctement et rapidement toute plainte relative au traitement des informations ([81]).

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

(119) Le droit japonais prévoit plusieurs limitations de l'accès aux données à caractère personnel et de l'utilisation de ces données à des fins répressives, ainsi que des mécanismes de surveillance et de recours qui offrent des garanties suffisantes pour que lesdites données soient protégées de manière efficace contre les interventions illicites et le risque d'abus.

3.2.1. *Base juridique et limitations/garanties applicables*

(120) Dans le cadre juridique japonais, la collecte d'informations électroniques à des fins répressives est autorisée sur la base d'un mandat (collecte par voie de contrainte) ou d'une demande de divulgation volontaire.

3.2.1.1. Enquête coercitive sur la base d'un mandat délivré par un tribunal

(121) Comme indiqué au considérant 115, toute collecte de données dans le cadre d'une enquête coercitive doit être spécifiquement autorisée par la loi et ne peut être effectuée que sur la base d'un mandat délivré par un tribunal pour «cause adéquate» (article 35 de la Constitution). En ce qui concerne les enquêtes en matière d'infractions pénales, cette exigence est reflétée dans les dispositions du code de procédure pénale («CPP»). Aux termes de l'article 197, paragraphe 1, du CPP, les mesures de contrainte «ne doivent pas s'appliquer à moins que des dispositions spéciales aient été prévues dans le présent code». En ce qui concerne la collecte d'informations électroniques, les seules bases juridiques pertinentes ([82]) à cet égard sont l'article 218 du CPP (perquisition et saisie) et l'article 222-2 du CPP, selon lequel les mesures de contrainte pour l'interception de communications électroniques sans le consentement de l'une ou l'autre partie doivent être exécutées sur la base d'autres actes, à savoir la loi sur les écoutes téléphoniques pour les enquêtes pénales («loi sur les écoutes»). Dans les deux cas, l'exigence de mandat s'applique.

(122) Plus spécifiquement, en vertu de l'article 218, paragraphe 1, du CPP, un procureur, un assistant du procureur ou un officier de police judiciaire peut, si cela est nécessaire à l'enquête sur une infraction, procéder à une perquisition ou une saisie (y compris en ordonnant des enregistrements) sur la base d'un mandat émis au préalable par un juge ([83]). Un tel mandat doit notamment contenir le nom du suspect ou de l'accusé, l'infraction retenue ([84]), les enregistrements électromagnétiques à saisir, et «le lieu ou les articles» à perquisitionner (article 219, paragraphe 1, du CPP).

([79]) Les informations à caractère personnel obtenues par les agents d'une instance administrative dans l'exercice de leurs fonctions et détenues par ladite instance administrative pour un usage organisationnel relèvent de la définition des «informations à caractère personnel conservées» au sens de l'article 2, paragraphe 3, de l'APPIHAO pour autant qu'elles soient consignées dans des «documents administratifs». Cela inclut les informations électroniques collectées puis traitées par ces instances, étant donné que la définition des «documents administratifs» employée à l'article 2, paragraphe 2, de la loi sur l'accès aux informations détenues par des instances administratives (loi n° 42 de 1999) englobe les enregistrements électromagnétiques.

([80]) Toutefois, selon l'article 53-2 du code de procédure pénale, le chapitre IV de l'APPIHAO est exclu pour les «documents relatifs à des procès», y compris, selon les informations reçues, les informations électroniques obtenues sur la base d'un mandat ou d'une demande de coopération volontaire dans le cadre d'une enquête pénale. De même, en ce qui concerne les informations recueillies dans le domaine de la sécurité nationale, les particuliers ne pourront faire valoir leurs droits en vertu de l'APPIHAO si le directeur de l'autorité publique a un «motif raisonnable» de considérer que la divulgation «est susceptible de porter atteinte à la sécurité nationale» [voir l'article 14, point iv)]. Cela étant dit, les autorités publiques sont tenues d'accorder au moins la divulgation partielle chaque fois que cela est possible (article 15).

([81]) Voir les références spécifiques à l'APPIHAO dans l'annexe II, point II.A.1) b) 2).

([82]) Alors que l'article 220 du CPP autorise une perquisition et une saisie «sur le terrain» sans mandat lorsqu'un procureur, un assistant du procureur ou un fonctionnaire de police judiciaire arrête un suspect/contrevenant en flagrant délit, cela n'est pas pertinent dans un contexte de transfert et, par conséquent, aux fins de la présente décision.

([83]) Conformément à l'article 222, paragraphe 1, en liaison avec l'article 110, du CPP, le mandat de perquisition/saisie pour les enregistrements doit être présenté à la personne qui va subir la mesure.

([84]) Voir aussi l'article 189, paragraphe 2, du CPP, selon lequel un officier de police judiciaire doit enquêter sur le contrevenant et les preuves le concernant «lorsqu'il estime qu'une infraction a été commise». De même, l'article 155, paragraphe 1, du CPP exige qu'une demande écrite de mandat contienne, notamment, «l'infraction retenue» et un «résumé des faits infractionnels».

(123) En ce qui concerne l'interception des communications, l'article 3 de la loi sur les écoutes n'autorise de telles mesures qu'à des conditions strictes. En particulier, les autorités publiques doivent obtenir un mandat judiciaire préalable qui ne peut être délivré que pour les enquêtes relatives à certains crimes graves (énumérés dans l'annexe de la loi) ([85]) et lorsqu'il est «extrêmement difficile d'identifier le criminel ou de clarifier les circonstances/détails de la commission par d'autres moyens quelconques» ([86]). En vertu de l'article 5 de la loi sur les écoutes, la garantie est émise pour une durée limitée et des conditions supplémentaires peuvent être imposées par le juge. En outre, la loi sur les écoutes prévoit plusieurs garanties supplémentaires, telles que, par exemple, la présence nécessaire des témoins (articles 12 et 20), l'interdiction de placer sur écoute certains groupes privilégiés (médecins, avocats, par exemple) (article 15), l'obligation de mettre fin à l'écoute si elle n'est plus justifiée, même durant la période de validité de la garantie (article 18), ou encore l'obligation générale d'informer la personne concernée et d'autoriser l'accès aux enregistrements dans les 30 jours suivant la fin de l'écoute (articles 23 et 24).

(124) Pour toutes les mesures de contrainte fondées sur un mandat, seul un tel examen «limité à ce qui est nécessaire pour atteindre son objectif» peut être réalisé (c'est-à-dire lorsque les objectifs poursuivis par l'enquête ne peuvent pas être atteints d'une autre manière) (article 197, paragraphe 1, du CCP). Bien que les critères pour déterminer cette nécessité ne soient pas davantage précisés dans la loi, la Cour suprême japonaise a statué que le juge qui délivre un mandat doit procéder à une appréciation globale prenant en considération en particulier i) la gravité de l'infraction et la manière dont elle a été commise; ii) la valeur et l'importance des éléments qui seront saisis en tant que preuves; iii) la probabilité (le risque) que ces preuves puissent être dissimulées ou détruites; et iv) la mesure dans laquelle la saisie peut causer un préjudice à la personne concernée ([87]).

3.2.1.2. Demande de divulgation volontaire sur la base d'une «demande de renseignements»

(125) Dans les limites de leurs compétences, les autorités publiques peuvent également collecter des informations électroniques sur la base de demandes de divulgation volontaire. Il s'agit d'une forme de coopération non contraignante, où l'on ne peut forcer le respect de la demande ([88]), qui dispense ainsi les autorités publiques de l'obligation d'obtenir un mandat délivré par un tribunal.

(126) Dans la mesure où une telle demande est adressée à un opérateur économique et porte sur des informations à caractère personnel, cet opérateur doit se conformer aux exigences de l'APPI. Conformément à l'article 23, paragraphe 1, de l'APPI, les opérateurs économiques ne peuvent divulguer des informations à caractère personnel à des tiers sans le consentement de la personne concernée que dans certains cas, et notamment lorsque la divulgation est fondée «sur des dispositions législatives et réglementaires» ([89]). Dans le domaine répressif, la base juridique pour de telles demandes est fournie par l'article 197, paragraphe 2, du CPP, selon lequel «il peut être demandé aux organisations privées de rendre des comptes sur des questions nécessaires à l'enquête». Une «demande de renseignements» n'étant autorisée que dans le cadre d'une enquête pénale, elle présuppose toujours une suspicion concrète d'infraction déjà commise ([90]). En outre, étant donné que ces enquêtes sont généralement réalisées par la police préfectorale, les limitations prévues à l'article 2, paragraphe 2, de la loi sur la police ([91]) s'appliquent. Conformément à cette disposition, les activités de la police sont «strictement limitées» à l'exercice de ses responsabilités et fonctions (c'est-à-dire à la prévention et à la répression des infractions, ainsi qu'aux enquêtes en la matière). En outre, dans l'exercice de ses fonctions, la police est tenue d'agir de manière impartiale, sans parti pris et avec équité, et ne doit jamais abuser de ses pouvoirs «d'une manière qui interfère avec les droits et libertés d'une personne garantis par la Constitution du Japon» (ce qui inclut, comme signalé plus haut, le droit au respect de la vie privée et à la protection des données) ([92]).

(127) En ce qui concerne spécifiquement l'article 197, paragraphe 2, du CPP, la police nationale, en tant qu'autorité fédérale chargée, entre autres, de toutes les questions concernant la police criminelle, a émis des instructions à

([85]) L'annexe fait référence à 9 types de crimes, comme les crimes liés à la drogue et aux armes à feu, la traite des êtres humains et les assassinats. Il convient de noter que l'infraction introduite récemment de «préparation d'actes de terrorisme et d'autres formes de criminalité organisée» (voir la note de bas de page 76) ne figure pas dans cette liste limitative.

([86]) En outre, conformément à l'article 23 de la loi sur les écoutes, l'autorité chargée de l'enquête doit informer par écrit la personne concernée que ses communications ont été interceptées (et qu'elles figurent donc dans le registre d'interception).

([87]) Voir l'annexe II, point II.A.1) b) 1).

([88]) Selon les informations reçues, les opérateurs économiques qui ne coopèrent pas ne subissent de conséquences négatives (et notamment de sanctions) en vertu d'aucune loi. Voir l'annexe II, point II.A.2) a).

([89]) Conformément aux lignes directrices de la PPC (General Rule Edition), l'article 23, paragraphe 1, point i), constitue la base juridique pour la divulgation d'informations à caractère personnel pour répondre à la fois à un mandat (article 218 du CPP) et à une «demande de renseignements» (article 197, paragraphe 2, du CPP).

([90]) Cela signifie que la «demande de renseignements» peut être utilisée dans le seul but de collecter des informations dans des cas individuels et non en vue d'une collecte massive de données à caractère personnel. Voir également l'annexe II, point I.A.2) b) 1).

([91]) Ainsi que les règlements de la commission préfectorale de sûreté publique, voir l'article 189, paragraphe 1, du CPP.

([92]) Voir également l'article 3 de la loi sur la police, selon lequel tous les agents de police prêtent serment d'«être fidèles à l'obligation de défendre et de respecter la Constitution et les lois du Japon, et de s'acquitter de leurs fonctions de manière impartiale et équitable et sans préjugés».

l'intention de la police préfectorale ([93]) sur la «bonne utilisation des demandes écrites de renseignements sur des matières relevant de l'enquête». Selon cette notification, les demandes doivent être introduites à l'aide d'un formulaire préétabli (le «formulaire n° 49» ou «la demande de renseignements») ([94]) et doivent porter sur des enregistrements «relatifs à une enquête spécifique», et les renseignements demandés doivent être «nécessaires à cette enquête». Dans chaque cas, l'enquêteur en chef doit «examiner de manière approfondie la nécessité, le contenu, etc. de la demande en question» et doit obtenir l'approbation interne d'un fonctionnaire de haut rang.

(128) En outre, dans deux arrêts de 1969 et 2008 ([95]), la Cour suprême du Japon a prévu des limitations à l'obligation de respecter des mesures non contraignantes qui interfèrent avec le droit au respect de la vie privée ([96]). En particulier, la Cour a estimé que ces mesures doivent être «raisonnables» et rester dans «les limites généralement admises», c'est-à-dire qu'elles doivent être nécessaires pour l'enquête sur un suspect (pour récolter des preuves) et doivent être accomplies «par des méthodes appropriées à la réalisation de l'objectif de l'enquête» ([97]). Ces arrêts montrent que cela implique un contrôle de la proportionnalité qui tienne compte de toutes les circonstances de l'affaire (le niveau d'interférence avec le droit à la vie privée, y compris l'attente quant au respect de la vie privée, la gravité de l'infraction, la probabilité d'obtenir des preuves utiles, l'importance de ces preuves, les autres moyens d'enquête possibles, etc.) ([98]).

(129) Outre ces limitations à l'exercice de l'autorité publique, les opérateurs économiques eux-mêmes sont tenus de vérifier («confirmer») la nécessité et la «rationalité» de la fourniture à un tiers ([99]). Il s'agit notamment de savoir s'ils sont empêchés, par la loi, de coopérer. De telles obligations légales conflictuelles peuvent en particulier résulter d'obligations de confidentialité telles que celles prévues à l'article 134 du code pénal (concernant la relation entre un médecin et son patient, entre un avocat et son client, un prêtre et un fidèle, etc.). De même, «toute personne qui exerce une activité de télécommunications maintiendra comme tels, pendant la durée de ses fonctions, les secrets de tiers dont il aurait eu connaissance en ce qui concerne les communications traitées par son entreprise de télécommunications» (article 4, paragraphe 2, de la loi sur les activités de télécommunications). Cette obligation est complétée par la sanction prévue à l'article 179 de la loi sur les activités de télécommunications, en vertu duquel toute personne qui a violé le secret des communications traitées par une entreprise de télécommunications se rend coupable d'une infraction pénale et est passible d'une peine d'emprisonnement accompagnée d'une peine de travail d'une durée maximale de deux ans ou d'une amende n'excédant pas un million de yens ([100]). Si cette exigence n'est pas absolue et autorise, en particulier, des mesures portant atteinte au secret des communications qui constituent des «actes justifiables» au sens de l'article 35 du code pénal ([101]), cette exception ne couvre pas la réponse aux demandes non contraignantes d'autorités publiques concernant la divulgation d'informations électroniques formulées en vertu de l'article 197, paragraphe 2, du CPP.

3.2.1.3. Utilisation ultérieure des informations recueillies

(130) Lors de la collecte des données par les autorités publiques japonaises, les informations à caractère personnel relèvent du champ d'application de l'APPIHAO. Cette loi régit le traitement des «informations à caractère personnel

([93]) En vertu de l'article 30, paragraphe 1, et de l'article 31, paragraphe 2, de la loi sur la police, le directeur général des bureaux de police régionaux (antennes locales de la police régionale) «dirige et supervise» la police préfectorale.

([94]) La demande de renseignements doit également indiquer les coordonnées du «gestionnaire» (intitulé de la section, fonction, nom du gestionnaire, numéro de téléphone du bureau, numéro d'extension, etc.).

([95]) Cour suprême, arrêt du 24 décembre 1969 [1965(A) 1187]; arrêt du 15 avril 2008 [2007(A) 839].

([96]) Même si ces arrêts ne concernaient pas la collecte d'informations électroniques, le gouvernement japonais a précisé que l'application des critères élaborés par la Cour suprême s'étend à toute interférence des autorités publiques avec le droit à la protection de la vie privée, y compris à l'ensemble des «enquêtes sur la base d'une action volontaire», et que ces critères lient par conséquent les autorités japonaises également lorsqu'elles présentent des demandes de divulgation volontaire d'informations. Voir l'annexe II, point II.A.2) b) 1).

([97]) Selon les informations reçues, ces facteurs doivent être considérés comme «raisonnables au regard des conventions socialement acceptées». Voir l'annexe II, point II.A.2) b) 1).

([98]) Pour des considérations similaires dans le contexte des enquêtes coercitives (écoutes), voir également l'arrêt de la Cour suprême du 16 décembre 1999, 1997(A) 636.

([99]) À cet égard, les autorités japonaises ont attiré l'attention sur les lignes directrices de la PPC (General Rule Edition) et sur le point 5/14 des questions-réponses préparées par la PPC pour l'application de l'APPI. Selon les autorités japonaises, «compte tenu de la prise de conscience croissante par les individus de leur droit à la vie privée, ainsi que de la charge de travail causée par ces demandes, les opérateurs économiques sont de plus en plus prudents dans leurs réponses à ces demandes». Voir l'annexe II, point II.A.2), en référence également à la notification de la police nationale de 1999. Selon les informations reçues, dans certains cas, des opérateurs économiques ont effectivement refusé de coopérer. Par exemple, dans son rapport sur la transparence de 2017, LINE (l'application de messagerie la plus populaire au Japon) déclare: «Lorsque nous recevons des demandes d'instances d'investigation etc., nous vérifions qu'elles sont appropriées du point de vue de la légalité, de la protection des utilisateurs, etc. À l'issue de cette vérification, nous rejetons la demande dès qu'une lacune juridique est constatée. Si la portée de la demande est trop large à des fins d'enquête, nous demandons à l'instance d'investigation qu'elle nous fournisse des explications. Si ces explications ne sont pas motivées, nous ne répondons pas à la demande.» Disponible sur l'internet à l'adresse suivante: https://linecorp.com/en/security/transparency/top

([100]) Les sanctions sont une peine d'emprisonnement assortie d'une peine de travail d'une durée de trois ans ou une amende n'excédant pas deux millions de yens pour toute personne qui «exerce une activité de télécommunications».

([101]) Les «actes justifiables» au regard du code pénal désignent en particulier les actes d'une entreprise de télécommunications par lesquels cette dernière se conforme aux mesures de l'État ayant force légale (mesures de contrainte), par exemple lorsque les autorités d'enquête prennent des mesures sur la base d'un mandat émis par un juge. Voir l'annexe II, point II.A.2) b) 2), qui renvoie aux lignes directrices sur la protection des informations à caractère personnel dans le secteur des télécommunications.

conservées» et impose à ce titre un certain nombre de limitations et de garanties (voir le considérant 118) ([102]). En outre, le fait qu'une instance administrative ne puisse conserver des informations à caractère personnel «que lorsque la conservation est nécessaire pour mener à bien les affaires relevant de sa juridiction en vertu de dispositions législatives ou réglementaires» (article 3, paragraphe 1, de l'APPIHAO) impose également des restrictions, au moins indirectement, à la collecte initiale.

3.2.2. *Surveillance indépendante*

(131) Au Japon, la collecte d'informations électroniques dans le domaine répressif relève avant tout ([103]) de la compétence de la police préfectorale ([104]), qui est soumise à cet égard à plusieurs niveaux de surveillance.

(132) Premièrement, dans tous les cas où des informations électroniques sont collectées par des moyens de contrainte (perquisitions et saisies), la police doit obtenir un mandat judiciaire préalable (voir considérant 121). Par conséquent, dans ces cas, la collecte sera vérifiée ex ante par un juge, sur la base d'une norme stricte de «cause adéquate».

(133) Même s'il n'existe pas de contrôle ex ante par un juge dans le cas de demandes de divulgation volontaire, les opérateurs économiques auxquels de telles demandes sont adressées peuvent s'y opposer sans risquer de conséquences négatives (et ils devront prendre en compte l'impact sur la vie privée de toute divulgation). En outre, conformément à l'article 192, paragraphe 1, du CPP, les fonctionnaires de police devront toujours coopérer et coordonner leurs actions avec le procureur (et avec la commission préfectorale de sûreté publique) ([105]). À son tour, le procureur peut donner les instructions générales nécessaires fixant des normes pour une enquête équitable et/ou émettre des injonctions spécifiques en ce qui concerne une enquête particulière (article 193 du CPP). Lorsque ces instructions et/ou injonctions ne sont pas suivies, le ministère public peut introduire une procédure pour mesures disciplinaires (article 194 du CPP). Par conséquent, la police préfectorale est placée sous le contrôle du procureur.

(134) Deuxièmement, selon l'article 62 de la Constitution, chacune des chambres du parlement japonais (la Diète) peut mener des enquêtes à l'égard de l'État, y compris en ce qui concerne la légalité de la collecte d'informations par la police. À cette fin, elle peut exiger la présence et l'audition de témoins, et/ou la production d'enregistrements. Ces pouvoirs d'enquête sont précisés dans le règlement de la Diète, en particulier son chapitre XII. Plus spécifiquement, l'article 104 du règlement de la Diète dispose que le gouvernement, les services et les autres instances publiques «doivent donner suite aux demandes, introduites par l'une des chambres ou l'une de leurs commissions, de production de rapports et d'enregistrements à des fins d'enquête». Le refus de s'y conformer n'est autorisé que si les pouvoirs publics fournissent une raison plausible acceptable par la Diète, ou en cas de déclaration officielle que la production des rapports ou enregistrements «porterait gravement atteinte à l'intérêt national» ([106]). En outre, les membres de la Diète peuvent poser des questions écrites au gouvernement (articles 74 et 75 du règlement de la Diète), et par le passé, certaines de ces «questions écrites» ont également abordé le traitement des informations à caractère personnel par l'administration ([107]). Le rôle de la Diète dans la supervision de l'exécutif est renforcé par les obligations de rendre des comptes, en vertu par exemple de l'article 29 de la loi sur les écoutes.

(135) Troisièmement, toujours au sein du pouvoir exécutif, la police préfectorale est soumise à une surveillance indépendante. Cette surveillance est exercée en particulier par les commissions préfectorales de sûreté publique, établies au niveau préfectoral afin de garantir une administration démocratique et la neutralité politique de la police ([108]). Ces commissions sont composées de membres nommés par le gouverneur préfectoral avec le consentement de l'assemblée préfectorale (qui compte des citoyens n'ayant pas été fonctionnaires de police au cours des cinq dernières années) et leur mandat est garanti (en particulier, les révocations ne sont possibles que pour un motif valable) ([109]). Selon les informations reçues, elles ne reçoivent pas d'instructions et peuvent donc être considérées comme totalement indépendantes ([110]). En ce qui concerne les tâches et compétences de ces commissions, celles-ci sont chargées, conformément à l'article 38, paragraphe 3, en liaison avec l'article 2 et l'article 36, paragraphe 2, de loi sur la police, de «la protection des droits et liberté d'une personne». À cet effet, elles sont habilitées à

([102]) En ce qui concerne les droits des personnes concernées, voir la section 3.1.
([103]) En principe, un procureur (ou un assistant du procureur sous ses ordres) peut, s'il l'estime nécessaire, enquêter sur une infraction (article 191, paragraphe 1, du CPP).
([104]) D'après les informations reçues, la police nationale ne mène pas d'enquêtes pénales individuelles. Voir l'annexe II, point II.A.1) a).
([105]) Voir également l'article 246 du CPP, selon lequel la police judiciaire a l'obligation de transmettre le dossier au procureur une fois qu'elle a procédé à une enquête portant sur une infraction pénale («principe de transmission dans tous les cas»).
([106]) La Diète peut aussi demander que le conseil de surveillance et d'examen des secrets spécifiquement désignés mène une enquête sur le refus de répondre. Voir l'article 104-II du règlement de la Diète.
([107]) Voir l'annexe II, point II.B.4).
([108]) En outre, conformément aux dispositions de l'article 100 de la loi sur l'autonomie locale, l'assemblée locale est habilitée à enquêter sur les activités des autorités chargées de l'application de la loi établies au niveau préfectoral, y compris la police préfectorale.
([109]) Voir les articles 39 à 41 de la loi sur la police. En ce qui concerne la neutralité politique, voir aussi l'article 42 de la loi sur la police.
([110]) Voir l'annexe II, point II.B.3) («système de conseil indépendant»).

«superviser» ([111]) toutes les activités d'enquête de la police préfectorale, y compris la collecte de données à caractère personnel. En particulier, les commissions «peuvent instruire la police préfectorale en détail ou dans un cas particulier d'inspection d'une faute commise par le personnel de la police, si nécessaire» ([112]). Lorsque le chef de la police préfectorale ([113]) reçoit une telle instruction ou prend par lui-même connaissance d'un cas de faute possible (y compris la violation de lois ou d'autres négligences), il doit promptement procéder à l'inspection du cas et transmettre le résultat de son inspection à la commission préfectorale de sûreté publique (article 56, paragraphe 3, de la loi sur la police). Si cette dernière l'estime nécessaire, elle peut également désigner un de ses membres pour examiner l'état d'avancement de la mise en œuvre. Ce processus se poursuit jusqu'à ce que la commission préfectorale de sûreté publique estime que l'incident a été résolu de manière appropriée.

(136) En outre, en ce qui concerne l'application correcte de l'APPIHAO, le ministre ou le chef d'agence compétent (à savoir, par exemple, le commissaire général de la police nationale) dispose de la compétence d'application, sous la surveillance du ministère des affaires intérieures et des communications (MIC). Conformément à l'article 49 de l'APPIHAO, le MIC «peut collecter des rapports sur l'état d'avancement de l'application de la présente loi» auprès des chefs des instances administratives (ministre). Cette fonction de surveillance est exercée avec l'appui des 51 «centres d'informations complètes» (un dans chaque préfecture du Japon) relevant du MIC, qui traitent chaque année des milliers de demandes émanant de particuliers ([114]) (et qui peuvent, à leur tour, révéler d'éventuelles violations de la loi). Lorsqu'il estime que cela est nécessaire pour garantir le respect de la loi, le MIC peut demander que lui soient communiqués des explications et des éléments, et émettre des avis sur le traitement des informations à caractère personnel par l'instance administrative en cause (articles 50 et 51 de l'APPIHAO).

3.2.3. *Recours individuel*

(137) Outre la surveillance de droit, il existe plusieurs possibilités pour obtenir réparation à titre individuel, tant par l'intermédiaire d'autorités indépendantes (comme les Commissions préfectorales de sûreté publique ou la PPC) qu'auprès des juridictions japonaises.

(138) Premièrement, en ce qui concerne les informations à caractère personnel collectées par des instances administratives, ces dernières sont tenues de «s'efforcer de traiter les plaintes de manière appropriée et sans délai» afférentes à leur traitement ultérieur (article 48 de l'APPIHAO). Alors que le chapitre IV de l'APPIHAO relatif aux droits individuels ne s'applique pas aux informations à caractère personnel figurant dans des «documents relatifs à des procès et à des biens saisis» (article 53, paragraphe 2, 2e alinéa, du CPP), qui couvre les informations à caractère personnel collectées dans le cadre d'enquêtes pénales, les personnes peuvent porter plainte en invoquant les principes généraux de protection des données comme, par exemple, l'obligation de ne conserver des données à caractère personnel que «si cela est nécessaire pour l'exercice [de fonctions répressives]» (article 3, paragraphe 1, de l'APPIHAO).

(139) En outre, l'article 79 de la loi sur la police garantit aux personnes ayant exprimé des inquiétudes quant à l'«exercice de ses fonctions» par le personnel de police le droit de déposer plainte auprès de la Commission préfectorale de sûreté publique indépendante (qui est compétente). La Commission traitera ces plaintes «loyalement», dans le respect des lois et des arrêtés municipaux, et informera le plaignant par écrit des résultats de la procédure. Compte tenu de l'autorité qui lui incombe de surveiller la police préfectorale et de lui «donner des instructions» en ce qui concerne les fautes commises par le personnel (article 38, paragraphe 3, et article 43, paragraphe 2, 1er alinéa, de la loi sur la police), elle peut demander à la police préfectorale d'instruire les faits, de prendre des mesures appropriées sur la base des résultats de l'instruction et de rendre compte des résultats. Si elle estime que l'enquête menée par la police n'est pas satisfaisante, la Commission peut aussi fournir des instructions sur le traitement de la plainte.

(140) Pour faciliter le traitement des plaintes, la police nationale a publié une «note» à l'intention de la Commission de police et de la Commission préfectorale de sûreté publique sur la marche à suivre pour le traitement des plaintes

([111]) Voir l'article 5, paragraphe 3, et l'article 38, paragraphe 3, de la loi sur la police.

([112]) Voir l'article 38, paragraphe 3, et l'article 43-2, paragraphe 1, de la loi sur la police. Dans le cas où elle «donne une instruction» au sens de l'article 43-2, paragraphe 1,) la commission préfectorale de sûreté publique peut ordonner à un comité désigné par la commission d'assurer le suivi de sa mise en œuvre (paragraphe 2). En outre, la commission peut recommander des mesures disciplinaires ou la révocation du chef de la police préfectorale (article 50, paragraphe 2), ainsi que celle d'autres officiers de police (article 55, paragraphe 4, de la loi sur la police).

([113]) Il en va de même pour le superintendant général dans le cas de la police métropolitaine de Tokyo (voir l'article 48, paragraphe 1, de la loi sur la police).

([114]) D'après les informations reçues, au cours de l'exercice 2017 (d'avril 2017 à mars 2018), 5 186 demandes émanant de particuliers ont été traitées par les «centres d'informations complètes».

relatives à l'exercice des fonctions des agents de police. La police nationale y énonce des normes pour l'interprétation et l'application de l'article 79 de la loi sur la police. Elle demande entre autres à la police préfectorale de mettre en place un «système de traitement des plaintes», de traiter toutes les plaintes et de les notifier «rapidement» à la Commission préfectorale de sûreté publique. Dans sa note, elle définit les plaintes comme des demandes tendant à obtenir la correction de «tout désavantage spécifique résultant d'un comportement illégal ou inapproprié» ([115]) ou de «l'absence d'adoption d'une mesure nécessaire par un officier de police dans l'exercice de ses fonctions» ([116]) et comme tout «grief/mécontentement quant à l'exercice inapproprié des fonctions d'un officier de police». En conséquence, l'objet concret d'une plainte est défini au sens large, couvrant toute plainte relative à la collecte illégale de données. Il n'est pas non plus nécessaire qu'une plainte démontre un quelconque préjudice résultant des actes d'un officier de police. Il convient de préciser que la note précise que les étrangers (notamment) doivent recevoir une assistance aux fins de la formulation d'une plainte. À la suite d'une plainte, les commissions préfectorales de sûreté publique sont chargées de veiller à ce que la police préfectorale examine les faits, mette en œuvre des mesures «en fonction du résultat de l'examen» et rende compte des résultats. Lorsque la Commission estime que l'examen est insuffisant, elle enjoint à la police préfectorale de suivre ses instructions sur le traitement de la plainte. Sur la base des rapports reçus et des mesures prises, la Commission informe le plaignant en indiquant, entre autres, les mesures prises pour répondre à la plainte. La note de la police nationale insiste sur le fait que les plaintes devraient être traitées de «manière sincère» et que le résultat devrait être communiqué «dans un délai […] jugé opportun compte tenu des normes sociales et du bon sens».

(141) Deuxièmement, étant donné que le recours devra de toute évidence être exercé à l'étranger, dans un système étranger et une langue étrangère, le gouvernement japonais a fait usage de son pouvoir pour créer un mécanisme spécifique, géré et contrôlé par la PPC, chargé du traitement des plaintes et du règlement des litiges dans ce domaine afin de faciliter les recours pour les citoyens de l'UE dont les données à caractère personnel sont transférées à des opérateurs économiques au Japon puis consultées par les autorités publiques. Ce mécanisme repose sur l'obligation de coopération imposée aux autorités publiques japonaises par l'APPI et sur le rôle particulier que joue la PPC en ce qui concerne les transferts internationaux de données à partir de pays tiers en vertu de l'article 6 de l'APPI et de la politique de base (établie par arrêté ministériel du gouvernement japonais). Les modalités détaillées de ce mécanisme sont exposées dans les déclarations, garanties et engagements officiels fournis par le gouvernement japonais et jointes en annexe II à la présente décision. Le recours au mécanisme ne nécessite pas de qualité pour agir, ce dernier étant ouvert à toute personne, qu'elle soit ou non soupçonnée ou accusée d'avoir commis une infraction pénale.

(142) Dans le cadre de ce mécanisme, une personne peut déposer plainte auprès de la PPC (à titre individuel ou par l'intermédiaire de l'autorité de protection des données de son pays au sens de l'article 51 du RGPD) si elle suspecte que des données la concernant, transférées depuis l'Union européenne, ont été collectées ou utilisées par les autorités publiques japonaises (y compris les autorités répressives) en violation des règles applicables. La PPC sera dans l'obligation de traiter la plainte et, en premier lieu, d'en informer les autorités publiques compétentes, y compris les organes de contrôle compétents. Ces autorités sont tenues de coopérer avec la PPC «notamment en fournissant les informations nécessaires et les éléments utiles pour permettre à la PPC de déterminer si la collecte ou l'utilisation ultérieure des données à caractère personnel a eu lieu dans le respect des règles applicables» ([117]). Cette obligation, qui découle de l'article 80 de l'APPI (en vertu duquel les autorités publiques japonaises sont tenues de coopérer avec la PPC), s'applique d'une manière générale et s'étend par conséquent à l'examen de toute mesure d'enquête prise par ces autorités, lesquelles se sont en outre engagées à faire preuve d'une telle coopération au moyen d'assurances fournies par écrit par les ministres et chefs des agences compétents, ainsi que cela ressort de l'annexe II.

(143) Si l'évaluation montre que les règles applicables n'ont pas été respectées, «la coopération entre les autorités publiques concernées et la PPC suppose l'obligation de mettre fin à l'infraction», ce qui inclut la suppression des données à caractère personnel collectées de manière illicite. Il est important de noter que cette obligation est exécutée sous le contrôle de la PPC qui «confirmera, avant de conclure l'évaluation, que des mesures ont été prises pour remédier intégralement à l'infraction».

(144) Après la conclusion de l'évaluation, la PPC informe la personne, dans un délai raisonnable, du résultat de l'évaluation, y compris des éventuelles mesures correctives. Dans le même temps, elle l'informe également de la possibilité de demander confirmation du résultat auprès de l'autorité publique compétente et la renseigne sur

([115]) La condition relative à un «désavantage spécifique» donne simplement à penser que le plaignant doit être concerné à titre individuel par le comportement (ou l'inaction) de la police, et non qu'il doit démontrer un quelconque préjudice.

([116]) Le respect de la loi, y compris des exigences légales en matière de collecte et d'utilisation des données à caractère personnel, fait partie de ces fonctions. Voir l'article 2, paragraphe 2, point 3, de la loi sur la police.

([117]) Pour réaliser son évaluation, la PPC coopérera avec le ministère des affaires intérieures et de la communication qui, comme expliqué au considérant 136, peut demander que des explications et des éléments lui soient communiqués, et émettre un avis sur le traitement des informations à caractère personnel par l'instance administrative en cause (articles 50 et 51 de l'APPIHAO).

l'identité de l'autorité à laquelle il convient d'adresser une telle demande de confirmation. La possibilité de recevoir une telle confirmation, y compris de prendre connaissance des raisons sur lesquelles repose la décision de l'autorité compétente, peut aider la personne à prendre d'autres mesures, notamment à former un recours en justice. L'accès aux résultats détaillés de l'évaluation peut être limité s'il existe des motifs raisonnables de penser que la communication de ces informations est de nature à porter préjudice à l'enquête en cours.

(145) Troisièmement, une personne qui n'est pas d'accord avec la décision de saisie (mandat) ([118]) rendue par un juge pour les données à caractère personnel qui la concernent, ou avec les mesures prises par la police ou l'autorité exécutant une telle décision, peut demander l'annulation ou la modification de cette décision ou de ces mesures (article 429, paragraphe 1, article 430, paragraphes 1 et 2, du CPP et article 26 de la loi sur les écoutes) ([119]). Lorsque l'instance révisionnelle considère que le mandat même ou son exécution («procédure de saisie») est illicite, elle accédera à la demande et ordonnera la restitution des articles saisis ([120]).

(146) Quatrièmement, toute personne qui considère que la collecte de données à caractère personnel la concernant dans le cadre d'une enquête pénale était illicite peut opter pour une forme plus indirecte de contrôle juridictionnel et invoquer ce caractère illicite lorsqu'elle est jugée au pénal. Si la juridiction reconnaît ce caractère illicite, les preuves seront exclues pour cause d'irrecevabilité.

(147) Enfin, en vertu de l'article 1er, paragraphe 1, de la loi sur les recours auprès de l'État, une juridiction peut accorder une indemnisation lorsqu'un fonctionnaire exerçant l'autorité publique de l'État a, dans l'exercice de ses fonctions, porté préjudice à la personne concernée, en agissant illicitement et fautivement (intentionnellement ou par négligence). En vertu de l'article 4 de la loi sur les recours auprès de l'État, la responsabilité de l'État en dommages-intérêts est fondée sur les dispositions du code civil. À cet égard, l'article 710 du code civil dispose que cette responsabilité couvre également les dommages autres que ceux causés aux biens, et partant le préjudice moral (par exemple, sous la forme de «souffrance morale»). Cela inclut les cas dans lesquels une personne a été victime, dans sa vie privée, d'activités de surveillance illégale et/ou de la collecte de données à caractère personnel la concernant (par exemple, exécution illégale d'un mandat) ([121]).

(148) Outre une indemnisation monétaire, la personne peut, dans certaines conditions, également bénéficier de mesures injonctives (par exemple, suppression des données à caractère personnel collectées par les autorités publiques) fondées sur son droit à la vie privée consacré par l'article 13 de la Constitution ([122]).

(149) En ce qui concerne toutes ces voies de recours, le mécanisme de règlement des litiges créé par le gouvernement japonais permet à une personne qui demeure insatisfaite du résultat de la procédure de s'adresser à la PPC «qui informe la personne des différentes possibilités et procédures détaillées pour obtenir réparation en vertu des lois et règlementations japonaises.» En outre, la PPC «viendra en aide à la personne, notamment en lui prodiguant conseil et assistance, pour engager une éventuelle action supplémentaire auprès de l'instance administrative ou judiciaire compétente».

(150) Cela inclut de faire usage des droits procéduraux prévus par le CPP. Ainsi, «lorsque l'évaluation révèle qu'une personne est suspectée dans une affaire pénale, la PPC l'en informera» ([123]); en vertu de l'article 259 du CPP, la personne peut également demander au ministère public d'être informée lorsque celui-ci décide de ne pas engager de procédure pénale. De la même manière, si l'évaluation révèle que des informations à caractère personnel concernant la personne ont été utilisées dans le cadre d'une affaire et que cette affaire est close, la PPC informera la personne que le dossier peut être consulté en vertu de l'article 53 du CPP (et de l'article 4 de la loi sur les dossiers des affaires pénales closes). Il est important qu'une personne ait accès à son dossier car cela l'aidera à mieux

([118]) Cela inclut un mandat autorisant les écoutes téléphoniques, pour lesquelles la loi correspondante prévoit une obligation de notification spécifique (article 23). Conformément à cette disposition, l'autorité chargée de l'enquête doit informer les personnes concernées par écrit que leurs communications ont été interceptées (et figurent donc dans le registre correspondant). Autre exemple: en vertu de l'article 100, paragraphe 3, du CPP, lorsqu'une juridiction saisit des envois postaux ou des télégrammes envoyés ou reçus par l'accusé, elle en informe l'expéditeur ou le destinataire sauf s'il existe un risque que cette notification fasse obstruction à la procédure juridictionnelle. L'article 222, paragraphe 1, du CPP renvoie à cette disposition pour les perquisitions et les saisies effectuées par l'autorité chargée de l'enquête.

([119]) Si une telle demande n'a pas pour effet automatique de suspendre l'exécution de la décision de saisie, l'instance révisionnelle peut ordonner la suspension jusqu'à ce qu'elle se prononce sur le fond. Voir l'article 429, paragraphe 2, et l'article 432 en liaison avec l'article 424 du CPP.

([120]) Voir l'annexe II, point II.C.1).

([121]) Voir l'annexe II, point II.C.2).

([122]) Voir, par exemple, l'arrêt (no 2925) rendu le 24 mars 1988 par le tribunal de district de Tokyo et l'arrêt (no 2925) rendu le 26 avril 2007 par le tribunal de district d'Osaka. D'après le tribunal de district d'Osaka, un équilibre devra être trouvé entre plusieurs facteurs, comme par exemple: i) la nature et le contenu des informations à caractère personnel en cause; ii) le mode de collecte; iii) les inconvénients pour la personne concernée au cas où les informations ne seraient pas supprimées; et iv) l'intérêt public, y compris les inconvénients pour l'autorité publique en cas de suppression des informations.

([123]) En tout état de cause, après l'ouverture de la procédure pénale, le ministère public donne à l'accusé la possibilité d'examiner ces éléments (voir les articles 298 et 299 du CPP). En ce qui concerne les victimes d'infractions pénales, voir les articles 316 à 333 du CPP.

comprendre l'enquête menée contre elle et donc à préparer une éventuelle action en justice (par exemple, action en indemnisation) si elle estime que les données la concernant ont été collectées ou utilisées de manière illicite.

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

(151) D'après les autorités japonaises, aucune loi au Japon n'autorise les demandes d'informations contraignantes ou les «écoutes administratives» en dehors du cadre des enquêtes pénales. Par conséquent, des informations ne peuvent être obtenues, pour des raisons de sécurité nationale, qu'auprès d'une source d'information librement accessible à tous ou par divulgation volontaire. Les acteurs économiques qui reçoivent une demande de coopération volontaire (sous forme de divulgation d'informations électroniques) n'ont aucune obligation légale de fournir ces informations ([124]).

(152) Par ailleurs, d'après les informations reçues, quatre organismes publics seulement sont habilités à recueillir des informations électroniques auprès des acteurs économiques japonais pour des raisons de sécurité nationale, à savoir: i) le bureau d'analyse et de renseignement du gouvernement (Cabinet Intelligence & Research Office — CIRO); ii) le ministère de la défense; iii) la police (tant la police nationale ([125]) que la police préfectorale); et iv) l'agence de renseignement en matière de sécurité publique (Public Security Intelligence Agency — PSIA). Cependant, le CIRO ne recueille jamais d'informations directement auprès des acteurs économiques, y compris en interceptant des communications. Lorsqu'il reçoit des informations d'autres autorités publiques en vue de la communication d'une analyse au Cabinet, ces autres autorités doivent à leur tour se conformer à la loi, y compris aux limitations et protections analysées dans la présente décision. Ses activités ne sont donc pas pertinentes dans le cadre d'un transfert.

3.3.1. *Base juridique et limitations/garanties applicables*

(153) D'après les informations reçues, le ministère de la défense collecte des informations (électroniques) sur le fondement de l'acte portant sa création. Aux termes de l'article 3 de cet acte, le ministère de la défense a pour mission de gérer et de commander les forces militaires et de «conduire les affaires y afférentes afin d'assurer l'indépendance et la paix nationale ainsi que la sécurité de la nation.» Son article 4, paragraphe 4, dispose que «la défense et la protection», les mesures à prendre par les forces d'autodéfense et le déploiement des forces militaires, y compris la collecte des informations nécessaires à la réalisation de ces activités, relèvent de la compétence du ministère de la défense. Il a seulement le pouvoir de recueillir des informations (électroniques) auprès des opérateurs économiques dans le cadre d'une coopération volontaire.

(154) La police préfectorale est, quant à elle, chargée de «veiller au maintien de l'ordre et d'assurer la sécurité publique» (article 35, paragraphe 2, en liaison avec l'article 2, paragraphe 1, de la loi sur la police). Dans le cadre de ces compétences, la police peut collecter des informations, mais seulement sur une base volontaire, sans valeur juridique. En outre, les activités de la police sont «strictement limitées» aux activités nécessaires à l'accomplissement de sa mission. La police agit de plus «avec impartialité, avec neutralité, sans préjugé et avec équité» et n'abuse jamais de ses pouvoirs «d'aucune manière susceptible, par exemple, de porter atteinte aux droits et libertés d'un individu garantis par la Constitution japonaise» (article 2 de la loi sur la police).

(155) Enfin, la PSIA peut mener des enquêtes en vertu de la loi sur la prévention des activités subversives (SAPA) et de la loi sur le contrôle des organisations ayant commis des massacres collectifs aveugles (ACO), lorsque ces enquêtes sont nécessaires en vue de l'adoption de mesures permettant de contrôler certaines organisations ([126]). En vertu de ces deux lois, à la demande du directeur général de la PSIA, la Commission d'examen de la sécurité publique peut prévoir certaines «dispositions» [surveillance/interdictions dans le cas de l'ACO ([127]); dissolution/interdiction dans le cas de la SAPA ([128])]. La PSIA peut mener des enquêtes ([129]) dans ce contexte. Selon les informations reçues, ces

([124]) Les acteurs économiques peuvent donc décider librement de ne pas coopérer, sans risque de sanctions ou d'autres conséquences négatives. Voir l'annexe II, point III.A.1).

([125]) Toutefois, d'après les informations reçues, le rôle principal de la police nationale consiste à coordonner les enquêtes menées par les différents départements de la police préfectorale et à échanger des informations avec des autorités étrangères. Même dans l'exercice de cette fonction, la police nationale est soumise au contrôle de la commission préfectorale de sûreté publique, chargée notamment de la protection des droits et des libertés des individus (article 5, paragraphe 1, de la loi sur la police).

([126]) Voir l'annexe II, point III.A.1) 3). Le champ d'application respectif de ces deux lois est limité: la SAPA fait référence à des «activités subversives terroristes» et l'ACO fait référence à la notion d'«acte de massacre collectif aveugle» (ce qui signifie qu'une «activité subversive terroriste» en vertu de la SAPA est un acte «par lequel un grand nombre de personnes sont assassinées sans distinction»).

([127]) Voir les articles 5 et 8 de l'ACO. Une disposition de surveillance implique également une obligation de déclaration de la part de l'organisation concernée par la mesure. Voir les articles 12 et 13 ainsi que les articles 15 à 27 de l'ACO pour les garanties procédurales, en particulier les exigences en matière de transparence et l'autorisation préalable de la Commission d'examen de la sécurité publique.

([128]) Voir les articles 5 et 7 de la SAPA ainsi que ses articles 11 à 25 pour les garanties procédurales, en particulier les exigences en matière de transparence et l'autorisation préalable de la Commission d'examen de la sécurité publique.

([129]) Voir l'article 27 de la SAPA et les articles 29 et 30 de l'ACO.

enquêtes sont toujours menées sur une base volontaire c'est-à-dire que la PSIA ne peut pas contraindre les personnes possédant des informations à caractère personnel à fournir ces informations ([130]). Dans chaque cas, les contrôles et les enquêtes se limitent au strict nécessaire pour parvenir à l'objectif de contrôle et, en aucune manière, ne restreignent «abusivement» les droits et les libertés garantis par la Constitution japonaise (article 3, paragraphe 1, de la SAPA et de l'ACO). En outre, conformément à l'article 3, paragraphe 2, de la SAPA et de l'ACO, la PSIA ne doit, en aucune circonstance, effectuer abusivement de tels contrôles ou des enquêtes préparatoires à ces contrôles. Si un agent de la PSIA abuse de l'autorité que lui confère la loi concernée et force une personne à faire ce qu'elle n'est pas tenue de faire ou empiète sur l'exercice des droits d'une personne, il peut faire l'objet de sanctions pénales conformément à l'article 45 de la SAPA ou à l'article 42 de l'ACO. Enfin, ces deux lois imposent expressément que leurs dispositions, y comprrésultant is les pouvoirs qu'elles octroient, ne fassent «en aucun cas l'objet d'une interprétation au sens large» (article 2 de la SAPA et de l'ACO).

(156) Dans tous les cas concernant l'accès des autorités publiques aux données pour des raisons de sécurité nationale décrits dans la présente section, les limitations prévues par la Cour suprême japonaise pour les enquêtes basées sur une action volontaire s'appliquent, c'est-à-dire que la collecte d'informations (électroniques) doit être réalisée en conformité avec les principes de nécessité et de proportionnalité («méthode appropriée») ([131]). Ainsi que l'ont confirmé explicitement les autorités japonaises, «la collecte et le traitement des informations se font uniquement dans la mesure nécessaire à l'exécution des tâches spécifiques de l'autorité publique compétente et en fonction des menaces spécifiques». En conséquence, «cela exclut la collecte massive et indifférenciée ou l'accès à des données à caractère personnel pour des raisons de sécurité nationale» ([132]).

(157) En outre, une fois collectées, les informations à caractère personnel conservées par les autorités publiques à des fins de sécurité nationale seront soumises aux mesures de protection prévues par l'APPIHAO, qui s'appliqueront à leur stockage, leur utilisation et leur divulgation ultérieurs (voir le considérant 118).

3.3.2. *Surveillance indépendante*

(158) La collecte d'informations à caractère personnel à des fins de sécurité nationale est soumise à plusieurs niveaux de surveillance exercée par les trois branches du pouvoir.

(159) Premièrement, la Diète japonaise, par l'intermédiaire de ses commissions spécialisées, peut examiner la légalité des enquêtes en vertu de ses fonctions de contrôle parlementaire (article 62 de la Constitution, article 104 du règlement de la Diète; Voir le considérant 134). Cette fonction de surveillance s'appuie sur des obligations spécifiques de déclaration concernant les activités réalisées sur le fondement de certaines des bases juridiques précitées ([133]).

(160) Deuxièmement, plusieurs mécanismes de surveillance existent au sein du pouvoir exécutif.

(161) En ce qui concerne le ministère de la défense, la surveillance est exercée par le bureau de l'inspecteur général chargé du respect de la législation ([134]); il a été institué en vertu de l'article 29 de l'acte portant création du ministère et est placé, au sein du ministère de la défense, sous le contrôle du ministre de la défense (auquel il rend compte); il est toutefois indépendant des services opérationnels de ce ministère. Le bureau de l'inspecteur général est chargé de veiller au respect des lois et réglementations ainsi qu'à la bonne exécution des tâches incombant aux fonctionnaires du ministère de la défense. Il est notamment habilité à réaliser des «inspections dans le domaine de la défense», tant à intervalles réguliers («inspections régulières dans le domaine de la défense») que dans des circonstances ponctuelles («inspections spéciales dans le domaine de la défense») qui, par le passé, ont également porté sur le traitement approprié des informations à caractère personnel ([135]). Dans le cadre de telles inspections, le bureau de l'inspecteur général peut avoir accès à des sites (bureaux) et demander qu'on lui fournisse des documents ou des

([130]) Voir l'annexe II, point III.A.1) 3).

([131]) Voir l'annexe II, point III.A.2) b). «Il découle de la jurisprudence de la Cour suprême que, pour pouvoir être adressée à un opérateur économique, une demande de coopération volontaire doit être nécessaire à l'enquête sur un délit présumé et être raisonnable aux fins de l'enquête. Bien que la base juridique et la finalité des enquêtes effectuées par les services d'enquête en matière de sécurité nationale et celles réalisées par les services d'enquête en ce qui concerne l'application des lois soient différentes, les principes fondamentaux afférents à la "nécessité de l'enquête" et au "caractère adapté de la méthode utilisée" s'appliquent de la même manière dans le domaine de la sécurité nationale et doivent être respectés en tenant dûment compte des circonstances spécifiques de chaque cas».

([132]) Voir l'annexe II, point III.A.2) b).

([133]) Voir, par exemple, l'article 36 de la SAPA et l'article 31 de l'ACO (pour la PSIA).

([134]) Le responsable du bureau de l'inspecteur général est un ancien procureur. Voir l'annexe II, point III.B.3).

([135]) Voir l'annexe II, point III.B.3). D'après l'exemple cité, l'inspection régulière menée en 2016 dans le domaine de la défense au sujet de la «sensibilisation/préparation au respect de la législation», entre autres, portait sur «la situation en matière de protection des informations à caractère personnel» (gestion, stockage, etc.). Le rapport élaboré à la suite de cette inspection a constaté des cas de gestion inadaptée des données et a demandé que des améliorations soient apportées en la matière. Le ministère de la défense a publié le rapport sur son site internet.

informations, y compris des explications de la part du vice-ministre adjoint du ministère de la défense. Au terme de l'inspection, un rapport est remis au ministre de la défense, énonçant les conclusions et les mesures à prendre pour améliorer la situation (la mise en œuvre de ces mesures peut également faire l'objet de nouvelles inspections). Le ministre de la défense s'appuie sur ce rapport pour ordonner la mise en œuvre des mesures nécessaires pour remédier à la situation; le vice-ministre adjoint est chargé d'appliquer ces mesures et doit faire rapport sur leur suivi.

(162) En ce qui concerne la police préfectorale, la surveillance est assurée par les commissions préfectorales de sûreté publique, indépendantes, comme expliqué au considérant 135 relatif au domaine répressif.

(163) Enfin, comme indiqué, la PSIA ne peut mener des enquêtes que dans la mesure où elles sont nécessaires pour l'adoption d'une interdiction, une dissolution ou une mesure de surveillance en vertu de la SAPA et de l'ACO; pour ces dispositions, la Commission d'examen de la sécurité publique indépendante ([136]) exerce un contrôle ex ante. En outre, des inspections régulières/périodiques (au cours desquelles les activités de la PSIA sont examinées dans le détail) ([137]) et des inspections internes spéciales ([138]) sur les activités de chaque service/bureau, etc. sont effectuées par des inspecteurs désignés à cet effet; à l'issue de ces inspections, des instructions peuvent être données aux chefs des départements concernés, etc. pour prendre des mesures correctrices ou apporter des améliorations.

(164) Ces mécanismes de surveillance, encore renforcés par la possibilité offerte aux personnes de demander l'intervention de la PPC en sa qualité d'autorité de contrôle indépendante (voir le considérant 168 ci-après), fournissent des garanties adéquates contre les risques d'abus de pouvoir de la part des autorités japonaises dans le domaine de la sécurité nationale et contre toute collecte illicite d'informations électroniques.

3.3.3. *Recours individuel*

(165) S'agissant du recours individuel, en ce qui concerne les informations à caractère personnel collectées et par conséquent «conservées» par des instances administratives, ces dernières sont tenues de «s'efforcer de traiter les plaintes de manière appropriée et sans délai» (article 48 de l'APPIHAO).

(166) En outre, contrairement à ce qui est prévu pour les enquêtes pénales, les personnes (y compris les ressortissants étrangers vivant à l'étranger) disposent en principe du droit à la divulgation ([139]), du droit de rectification (y compris du droit à l'effacement) et du droit à la suspension de l'utilisation/de la fourniture en vertu de l'APPIHAO. Cela étant dit, le responsable de l'instance administrative peut refuser la divulgation des informations «pour lesquelles il existe des motifs raisonnables […] de penser que leur divulgation est susceptible de porter atteinte à la sécurité nationale» [article 14, point iv), de l'APPIHAO] sans être obligé de révéler l'existence de telles informations (article 17 de l'APPIHAO). De la même manière, alors qu'une personne peut demander, en vertu de l'article 36, paragraphe 1, point i), de l'APPIHAO, la suspension de l'utilisation ou la suppression des informations obtenues de manière illicite ou conservées/utilisées par l'instance administrative au-delà de ce qui est nécessaire pour atteindre la finalité spécifiée, l'autorité peut rejeter la demande si elle estime que la suspension de l'utilisation «est susceptible de faire obstacle à la bonne exécution des affaires relevant de la finalité pour laquelle les informations à caractère personnel sont utilisées du fait de la nature des affaires en cause» (article 38 de l'APPIHAO). Cependant, lorsqu'il est possible de distinguer facilement et d'exclure les parties d'informations faisant l'objet d'une exception, les instances administratives sont tenues d'accorder au moins une divulgation partielle (voir, par exemple, l'article 15, paragraphe 1, de l'APPIHAO) ([140]).

([136]) Conformément à la loi sur l'établissement de la Commission d'examen de la sécurité publique, le président et les membres de la Commission «exercent leurs compétences en toute indépendance» (article 3). Ils sont nommés par le premier ministre avec l'accord des deux chambres de la Diète et ne peuvent être démis de leurs fonctions que «pour une raison donnée» (comme, par exemple, une peine d'emprisonnement, un comportement répréhensible, des troubles mentaux ou physiques ou l'ouverture d'une procédure de faillite).

([137]) Règlement relatif aux inspections périodiques de l'Agence de renseignement en matière de sécurité publique (direction générale de la PSIA, instruction n° 4, 1986).

([138]) Règlement relatif aux inspections spéciales de l'Agence de renseignement en matière de sécurité publique (direction générale de la PSIA, instruction n° 11, 2008). Des inspections spéciales auront lieu lorsque le directeur général de la PSIA estimera qu'elles sont nécessaires.

([139]) Ce droit correspond au droit de recevoir une copie des «informations à caractère personnel conservées».

([140]) Voir également la possibilité d'une «divulgation discrétionnaire» même lorsque les «informations dont la divulgation est interdite» font partie des «informations à caractère personnel conservées» dont la divulgation est demandée (article 16 de l'APPIHAO).

(167) En tout état de cause, l'instance administrative doit prendre une décision par écrit dans un délai déterminé (soit un délai de 30 jours, qui peut être prolongé d'une nouvelle période de 30 jours dans certaines conditions). Si la demande est rejetée ou accordée seulement en partie ou si la personne, pour d'autres raisons, considère le comportement de l'instance administrative comme étant «illégal ou injuste», cette personne peut demander un réexamen administratif sur la base de la loi sur les recours administratifs ([141]). Dans un tel cas, le chef de l'instance administrative chargé de prendre une décision sur l'appel consulte le comité d'examen de la protection des informations à caractère personnel et de la divulgation des informations (articles 42 et 43 de l'APPIHAO), un comité spécialisé et indépendant dont les membres sont nommés par le premier ministre avec l'accord des deux chambres de la Diète. D'après les informations reçues, le comité peut procéder à un examen ([142]) et, à cet égard, demander à l'instance administrative de fournir les informations à caractère personnel conservées, y compris tout contenu classifié, ainsi que d'autres informations et documents. Alors que le rapport final adressé au plaignant ainsi qu'à l'instance administrative et rendu public n'est pas juridiquement contraignant, ses recommandations sont suivies dans presque tous les cas ([143]). La personne a en outre la possibilité de contester la décision d'appel en justice sur la base de la loi sur les contentieux administratifs. Cette démarche ouvre la voie au contrôle juridictionnel de l'utilisation de dérogation(s) pour raison de sécurité nationale, qui visera notamment à déterminer si cette dérogation a été utilisée de manière abusive ou est toujours justifiée.

(168) Pour faciliter l'exercice des droits susmentionnés dans le cadre de l'APPIHAO, le ministère des affaires intérieures et de la communication a mis en place 51 «centres d'information globale» qui fournissent des informations de synthèse sur ces droits, les procédures applicables pour introduire une demande et les voies de recours possibles ([144]). Les instances administratives sont, quant à elles, tenues de fournir les «informations qui contribuent à préciser les informations à caractère personnel conservées» ([145]) et à prendre «d'autres mesures appropriées en tenant compte de la commodité de la personne qui a l'intention de formuler la demande» (article 47, paragraphe 1, de l'APPIHAO).

(169) Comme pour les enquêtes dans le domaine répressif, les personnes peuvent obtenir réparation à titre individuel dans le domaine de la sécurité nationale en contactant directement la PPC. Cette démarche déclenchera la procédure spécifique de règlement des litiges créée par le gouvernement japonais pour les citoyens de l'UE dont les données à caractère personnel sont transférées sur la base de la présente décision (voir les explications détaillées aux considérants 141 à 144 et 149).

(170) En outre, les individus peuvent former un recours juridictionnel sous la forme d'un recours en indemnisation en vertu de la loi sur les recours auprès de l'État, qui couvre également les dommages moraux, et demander, dans certaines conditions, la suppression des données collectées (voir le considérant 147).

4. CONCLUSION: NIVEAU DE PROTECTION ADÉQUAT DES DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES DE L'UNION EUROPÉENNE VERS DES OPÉRATEURS ÉCONOMIQUES AU JAPON

(171) La Commission considère que l'APPI, tel que complétée par les règles supplémentaires figurant à l'annexe I, conjointement avec les déclarations, assurances et engagements officiels contenus dans l'annexe II, garantit un niveau de protection des données à caractère personnel transférées de l'Union européenne qui est essentiellement équivalent à celui garanti par le règlement (UE) 2016/679.

(172) De plus, la Commission estime que, pris dans leur ensemble, les mécanismes de surveillance et les voies de recours prévus dans le droit japonais permettent d'identifier et de sanctionner en pratique les infractions commises par des OETIP destinataires 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.

([141]) Loi sur le réexamen des recours administratifs (loi n° 160 de 2014), et notamment son article 1er, paragraphe 1.

([142]) Voir l'article 9 de la loi instaurant le comité d'examen de la protection des informations à caractère personnel et de la divulgation des informations (loi n° 60 de 2003).

([143]) D'après les informations reçues, en l'espace de 13 ans depuis 2005 (date d'entrée en vigueur de l'APPIHAO), l'instance administrative n'a pas suivi le rapport dans deux cas seulement sur plus de 2000 bien que les décisions administratives aient été contredites à plusieurs reprises par le comité d'examen. En outre, lorsque l'instance administrative prend une décision qui s'écarte des conclusions du rapport, elle doit en indiquer clairement les raisons. Voir l'annexe II, point III.C, avec référence à l'article 50, paragraphe 1, point iv), de la loi sur le réexamen des recours administratifs.

([144]) Les centres d'information globale — un par préfecture — fournissent aux citoyens des explications sur les informations à caractère personnel collectées par les autorités publiques (comme les bases de données existantes, par exemple) et les règles applicables en matière de protection des données (APPIHAO), y compris sur les modalités de l'exercice du droit à la divulgation, du droit de rectification ou du droit à la suspension de l'utilisation. Les centres servent par ailleurs de point de contact pour les demandes de renseignements/plaintes émanant des citoyens. Voir l'annexe II, point II.C.4) a).

([145]) Voir également les articles 10 et 11 de l'APPIHAO sur le «registre des fichiers d'informations à caractère personnel» qui contient toutefois des exceptions majeures lorsqu'il s'agit des «fichiers d'informations à caractère personnel» préparés ou obtenus en vue d'enquêtes pénales ou qui contiennent des questions ayant trait à la sécurité et à d'autres intérêts importants de l'État [voir l'article 10, paragraphe 2, points i) et ii), de l'APPIHAO].

(173) Enfin, sur la base des informations disponibles concernant l'ordre juridique du Japon, y compris les déclarations, assurances et engagements du gouvernement japonais 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 le Japon par des autorités publiques japonaises 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.

(174) Par conséquent, à la lumière des constatations contenues dans la présente décision, la Commission considère que le Japon assure un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne vers des OETIP situés au Japon et soumis à l'APPI, hormis dans les cas où le destinataire relève de l'une des catégories énumérées à l'article 76, paragraphe 1, de l'APPI, et où les finalités du traitement correspondent en tout ou partie à l'une des finalités définies dans cette disposition.

(175) Compte tenu de ces éléments, la Commission conclut au respect de la norme en matière d'adéquation prévue à l'article 45 du règlement (UE) 2016/679, interprétée à la lumière de la charte des droits fondamentaux de l'Union européenne, en particulier dans l'arrêt Schrems ([146]).

5. ACTION DES AUTORITÉS DE PROTECTION DES DONNÉES ET INFORMATION DE LA COMMISSION

(176) Conformément à la jurisprudence de la Cour de justice ([147]), 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 Japon continue de garantir un niveau de protection essentiellement équivalent. Une telle vérification s'impose, en tout état de cause, lorsque la Commission reçoit des informations faisant naître un doute justifié à cet égard.

(177) Par conséquent, la Commission devrait surveiller de manière permanente la situation 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 japonaises, des déclarations, assurances et engagements contenus dans l'annexe II. Pour faciliter ce processus, il est attendu des autorités japonaises qu'elles informent la Commission de toute évolution importante en rapport avec la présente décision, concernant tant le traitement des données à caractère personnel par les opérateurs économiques que les limitations et garanties applicables à l'accès des autorités aux données à caractère personnel. Ceci devrait inclure toute décision adoptée par la PPC en vertu de l'article 24 de l'APPI reconnaissant qu'un pays tiers fournit un niveau de protection équivalent à celui garanti au Japon.

(178) En outre, afin de permettre à la Commission d'accomplir efficacement sa mission de contrôle, les États membres devraient l'informer de toute mesure pertinente prise par les autorités nationales de protection des données («APD»), en particulier en ce qui concerne les questions ou les plaintes des personnes concernées de l'UE au sujet du transfert de données à caractère personnel de l'Union européenne vers des opérateurs économiques situés au Japon. La Commission devrait également être informée de tout élément indiquant que les actions des autorités japonaises 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.

(179) 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. 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. Parallèlement, ainsi que la Cour de justice l'a expliqué dans l'arrêt Schrems ([148]) et comme prévu à l'article 58, paragraphe 5, du règlement, lorsqu'une APD 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 ([149]).

([146]) Voir la note de bas de page 3 ci-dessus.
([147]) Arrêt Schrems, point 76.
([148]) Arrêt Schrems, point 65.
([149]) 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.»

6. EXAMEN PÉRIODIQUE DU CONSTAT D'ADÉQUATION

(180) En application de l'article 45, paragraphe 3, du règlement (UE) 2016/679 ([150]), et au regard du fait que le niveau de protection assuré par l'ordre juridique du Japon est susceptible d'évoluer, la Commission, après l'adoption de la présente décision, devrait vérifier de manière périodique si les conclusions relatives au niveau adéquat de la protection assurée par le Japon sont toujours justifiées en fait et en droit.

(181) À cette fin, la présente décision devrait faire l'objet d'un premier examen dans un délai de deux 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 RGPD, sur l'opportunité de maintenir, ou non, le cycle de deux ans. En tous les cas, les examens ultérieurs devraient avoir lieu au moins une fois tous les quatre ans ([151]). L'examen devrait couvrir tous les aspects du fonctionnement de la présente décision, notamment l'application des règles supplémentaires (en accordant une attention particulière aux protections accordées en cas de transferts ultérieurs), l'application des règles relatives au consentement, notamment en cas de retrait, le caractère effectif de l'exercice des droits individuels, ainsi que les limitations et garanties en ce qui concerne l'accès des pouvoirs publics aux données, y compris le mécanisme de recours tel qu'exposé à l'annexe II de la présente décision. Il devrait également englober l'efficacité de la surveillance et du contrôle du respect des règles applicables, aussi bien aux OETIP que dans les domaines des procédures pénales et de la sécurité nationale.

(182) En vue de la réalisation de cet examen, la Commission devrait rencontrer la PPC, accompagnée, le cas échéant, d'autres autorités japonaises 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 du réexamen conjoint, la Commission devrait demander à la PPC 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 ([152]). 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 japonaises ou d'autres parties prenantes au Japon, par le Comité européen de la protection des données, par diverses APD, par des groupes de la société civile, ainsi que des informations relayées par les médias ou toute autre source d'informations disponible.

(183) Sur la base du réexamen conjoint, la Commission devrait élaborer un rapport public qui sera présenté au Parlement européen et au Conseil.

7. SUSPENSION DE LA DÉCISION D'ADÉQUATION

(184) Lorsque, sur la base des vérifications ad hoc régulières ou de toute autre information disponible, la Commission parvient à la conclusion que le niveau de protection assuré par l'ordre juridique japonais ne peut plus être considéré comme essentiellement équivalent à celui qui est garanti dans l'Union européenne, elle devrait en informer les autorités japonaises compétentes et demander que des mesures appropriées soient prises dans un délai raisonnable bien défini. Sont incluses à cet égard les règles applicables tant aux opérateurs économiques qu'aux autorités japonaises responsables de l'application du droit pénal ou de la sécurité nationale. Une telle procédure serait par exemple déclenchée dans les cas où les transferts ultérieurs, notamment sur la base des décisions adoptées par la PPC en vertu de l'article 24 de l'APPI reconnaissant qu'un pays tiers fournit un niveau de protection équivalent à celui garanti au Japon, ne seront plus effectués en bénéficiant des garanties assurant la continuité de la protection au sens de l'article 44 du RGPD.

(185) Si, à l'expiration de la période précisée, les autorités japonaises compétentes échouent à démontrer de manière satisfaisante que la présente décision reste fondée sur un niveau de protection adéquat, la Commission devrait, en application de l'article 45, paragraphe 5, du règlement (UE) 2016/679, lancer la procédure conduisant à la suspension partielle ou complète ou à l'abrogation de la présente décision. À défaut, la Commission devrait lancer la procédure de modification de 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 la continuité de la protection est assurée au sens de l'article 44 du RGPD.

([150]) 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».

([151]) 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 rev. 01.

([152]) Voir également l'annexe II, point IV: «Dans le cadre de l'examen périodique de la décision d'adéquation, la PPC et la Commission européenne échangeront des informations sur le traitement des données dans les conditions définies dans le constat d'adéquation, y compris celles énumérées dans la présente déclaration.»

(186) Plus particulièrement, la Commission devrait lancer la procédure de suspension ou d'abrogation en présence d'éléments indiquant que les règles 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 japonaises ne respectent pas les déclarations, assurances et engagements contenus dans l'annexe II de la présente décision.

(187) 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 du réexamen conjoint, les autorités japonaises compétentes ne fournissent pas les informations ou les clarifications nécessaires pour apprécier le niveau de protection conféré aux données à caractère personnel transférées de l'Union européenne vers le Japon ou 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.

(188) Pour des raisons d'urgence dûment justifiée, telle qu'un risque de violation grave des droits des personnes concernées, la Commission devrait envisager l'adoption d'une décision suspendant ou abrogeant la présente décision, qui serait immédiatement applicable, conformément aux dispositions combinées de l'article 93, paragraphe 3, du règlement (UE) 2016/679 et de l'article 8 du règlement (UE) n° 182/2011 du Parlement européen et du Conseil ([153]).

8. **CONSIDÉRATIONS FINALES**

(189) Le Comité européen de la protection des données a publié son avis ([154]), dont il a été tenu compte dans l'élaboration de la présente décision.

(190) Le Parlement européen a adopté une résolution sur une stratégie pour le commerce numérique, dans laquelle il invite la Commission à élever au rang de priorité et à accélérer l'adoption de décisions d'adéquation avec ses principaux partenaires commerciaux dans le respect des conditions définies dans le règlement (UE) 2016/679, et ce comme mécanisme important pour sécuriser les transferts de données à caractère personnel depuis l'Union vers un pays tiers ([155]). Le Parlement européen a également adopté une résolution sur l'adéquation de la protection des données à caractère personnel assurée par le Japon ([156]).

(191) Les mesures prévues par la présente décision sont conformes à l'avis du comité institué en vertu de l'article 93, paragraphe 1, du RGPD.

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

1. Aux fins de l'article 45 du règlement (UE) 2016/679, le Japon assure un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne à des opérateurs économiques traitant des informations à caractère personnel au Japon et soumis à la loi sur la protection des informations à caractère personnel, telle que complétée par les règles supplémentaires figurant à l'annexe I, ainsi que par les déclarations, les assurances et les engagements officiels contenus dans l'annexe II.

([153]) Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

([154]) Opinion 28/2018 regarding the European Commission Draft Implementing Decision on the adequate protection of personal data in Japan [avis 28/2018 relatif au projet de décision d'exécution de la Commission européenne constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon], adopté le 5 décembre 2018.

([155]) Résolution du Parlement européen du 12 décembre 2017 intitulée «Vers une stratégie pour le commerce numérique» [2017/2065(INI)]. Voir, en particulier, le point 8 [(…) rappelle que les données à caractère personnel peuvent être transférées vers des pays tiers sans recourir aux disciplines générales lorsque sont remplies les exigences — actuelles et futures — consacrées (…) par le chapitre V du règlement (UE) 2016/679; reconnaît que les décisions relatives à l'adéquation du niveau de protection des données, y compris partielles ou spécifiques à un secteur, représentent un mécanisme indispensable pour sécuriser les transferts de données depuis l'Union vers un pays tiers; relève que l'Union n'a adopté de telles décisions qu'à l'égard de quatre de ses vingt principaux partenaires commerciaux (…)], ainsi que le point 9 [«invite la Commission à élever au rang de priorité et à accélérer l'adoption de décisions d'adéquation, à condition que les pays tiers garantissent, au titre de leur droit interne ou de leurs engagements internationaux, un niveau de protection «essentiellement équivalent» à celui garanti par l'Union (…)].

([156]) Résolution du Parlement européen du 13 décembre 2018 sur l'adéquation de la protection des données à caractère personnel assurée par le Japon [2018/2979(RSP)].

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 organismes de radiodiffusion, les éditeurs de journaux, les agences de communication ou d'autres organes de presse (y compris les particuliers exerçant des activités de presse), dans la mesure où ils traitent des données à caractère personnel à des fins de presse;

b) les personnes exerçant une activité de rédaction professionnelle, dans la mesure où cela implique des données à caractère personnel;

c) les universités et tout autre groupe ou toute autre organisation en rapport avec des études universitaires, et toute personne appartenant à une organisation ou à un groupe de ce type, dans la mesure où ils traitent des données à caractère personnel aux fins desdites études;

d) les institutions religieuses, dans la mesure où elles traitent des données à caractère personnel aux fins d'une activité religieuse (y compris toutes les activités connexes); et

e) les organismes politiques, dans la mesure où ils traitent des données à caractère personnel aux fins de leur activité politique (y compris toutes les activités connexes).

Article 2

Lorsque, afin de protéger des personnes à l'égard du traitement de leurs données à caractère personnel, les autorités compétentes des États membres exercent leurs pouvoirs en vertu de l'article 58 du règlement (UE) 2016/679 pour suspendre ou interdire définitivement les flux de données vers un opérateur économique spécifique au Japon dans le cadre du champ d'application de l'article 1er, les États membres concernés en informent la Commission sans délai.

Article 3

1. La Commission surveille de manière continue l'application du cadre juridique sur lequel se fonde la présente décision, notamment les conditions dans lesquelles sont effectués les transferts ultérieurs, dans le but de déterminer si le Japon continue d'assurer un niveau de protection adéquat au sens de l'article 1er.

2. Les États membres et la Commission s'informent mutuellement des cas dans lesquels la Commission de protection des informations à caractère personnel, ou toute autre autorité japonaise 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 japonaises 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 deux 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 du réexamen conjoint réalisé avec les autorités japonaises 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 japonaises compétentes. Si nécessaire, elle peut décider de suspendre, de modifier ou d'abroger la présente décision, ou d'en restreindre le champ d'application, notamment en présence d'éléments indiquant:

a) que les opérateurs économiques au Japon 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 prévues par les règles supplémentaires figurant à l'annexe I à la présente décision, ou que la surveillance et le contrôle du respect des règles sont insuffisants à cet égard;

b) que les autorités japonaises ne respectent pas les déclarations, assurances et engagements contenus dans l'annexe II à la présente décision, 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 et à l'accès des autorités japonaises à ces données, à des fins répressives ou à des fins de sécurité nationale.

La Commission peut également présenter un projet des mesures à prendre si le défaut de coopération de la part des autorités japonaises l'empêche de déterminer si le constat établi à l'article 1er, paragraphe 1, de la présente décision est affecté.

Article 4

Les États membres sont destinataires de la présente décision.

Fait à Bruxelles, le 23 janvier 2019.

Par la Commission
Věra JOUROVÁ
Membre de la Commission

ANNEXE 1

RÈGLES SUPPLÉMENTAIRES COMPLÉTANT LA LOI SUR LA PROTECTION DES INFORMATIONS À CARACTÈRE PERSONNEL POUR LE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL TRANSFÉRÉES DEPUIS L'UE SUR LA BASE D'UNE DÉCISION D'ADÉQUATION

Table des matières

[Termes utilisés]

«Loi»	Loi sur la protection des informations à caractère personnel (loi n° 57 de 2003)
«Arrêté ministériel»	Arrêté ministériel visant à faire appliquer la loi sur la protection des informations à caractère personnel (arrêté ministériel n° 507 de 2003)
«Règles»	Règles d'application de la loi sur la protection des informations à caractère personnel (règles n° 3 de 2016 adoptées par la Commission de protection des données à caractère personnel)
«Lignes directrices (règles générales)»	Lignes directrices relatives à la loi sur la protection des informations à caractère personnel (volume sur les règles générales) (note n° 65 de 2015 de la Commission de protection des données à caractère personnel)
«UE»	Union européenne, y compris ses États membres, ainsi que, à la lumière de l'accord EEE, l'Islande, le Liechtenstein et la Norvège
«RGPD»	Règlement du Parlement européen et du Conseil 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)
Décision d'adéquation	Décision de la Commission par laquelle la Commission constate qu'un pays tiers ou un territoire de ce pays tiers, etc., assure un niveau de protection des données à caractère personnel adéquat conformément à l'article 45 du RGPD.

La Commission de protection des données à caractère personnel, aux fins d'un transfert mutuel et harmonieux des données à caractère personnel entre le Japon et l'UE, a désigné l'UE en tant que pays étranger établissant un système de protection des informations à caractère personnel reconnu comme appliquant des normes équivalentes à celles du Japon en ce qui concerne la protection des droits et intérêts des personnes sur le fondement de l'article 24 de la loi. La Commission européenne, de son côté, a constaté que le Japon garantissait un niveau de protection des données à caractère personnel adéquat conformément à l'article 45 du RGPD.

En conséquence, le transfert mutuel et harmonieux des données à caractère personnel entre le Japon et l'UE sera effectué selon des modalités garantissant un niveau de protection élevé des droits et intérêts des personnes. Afin de garantir un tel niveau de protection élevé en ce qui concerne les informations à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation, et compte tenu de l'existence de plusieurs différences pertinentes en dépit du degré élevé de convergence entre les deux systèmes, la Commission de protection des données à caractère personnel a adopté les présentes règles supplémentaires, qui s'appuient sur les dispositions de la loi concernant la mise en œuvre, etc., de la coopération avec les administrations d'autres pays, l'objectif étant également de garantir un traitement approprié des informations à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation par un opérateur économique traitant des informations à caractère personnel, ainsi que la mise en œuvre adéquate et efficace des obligations énoncées dans lesdites règles ([1]).

([1]) Articles 4, 6, 8, 24, 60 et 78 de la loi et article 11 des règles.

Plus spécifiquement, l'article 6 de la loi confère le pouvoir de prendre les mesures, législatives et autres, nécessaires pour garantir une protection accrue des informations à caractère personnel et bâtir un système relatif aux informations à caractère personnel qui soit compatible avec les normes internationales, au moyen de règles plus strictes complétant et dépassant celles définies dans la loi et l'arrêté ministériel. En conséquence, la Commission de protection des données à caractère personnel, en sa qualité d'autorité chargée de l'application générale de la loi, est habilitée à établir, conformément à l'article 6 de la loi, des réglementations plus strictes, en formulant les présentes règles supplémentaires garantissant un niveau accru de protection des droits et intérêts des personnes en ce qui concerne le traitement des données à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation, y compris pour ce qui est de la définition des informations à caractère personnel nécessitant des précautions particulières au sens de l'article 2, paragraphe 3, de la loi et des informations à caractère personnel conservées au sens de l'article 2, paragraphe 7, de la loi (y compris en ce qui concerne la durée de conservation pertinente).

Sur cette base, les règles supplémentaires revêtent un caractère contraignant à l'égard des opérateurs économiques traitant des informations à caractère personnel qui reçoivent des données à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation, qui sont donc tenus de s'y conformer. Tous les droits et obligations, quels qu'ils soient, constituant des règles juridiquement contraignantes, ils peuvent être invoqués par la Commission de protection des données à caractère personnel, à l'instar des dispositions de la loi qu'ils viennent compléter par des règles plus strictes et/ou plus détaillées. En cas de violation des droits et obligations découlant des règles supplémentaires, les personnes peuvent également obtenir réparation auprès d'un tribunal de la même manière que pour les dispositions de la loi qu'ils viennent compléter par des règles plus strictes et/ou plus détaillées.

Pour ce qui est de l'application par la Commission de protection des données à caractère personnel, lorsqu'un opérateur économique traitant des informations à caractère personnel ne se conforme pas à une ou à plusieurs des obligations fixées par les règles supplémentaires, la Commission de protection des données à caractère personnel est habilitée à adopter des mesures en vertu de l'article 42 de la loi. En ce qui concerne, d'une manière générale, les informations à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation, le fait, pour un opérateur économique traitant des informations à caractère personnel, de ne pas prendre de mesures conformément à une recommandation émise en vertu de l'article 42, paragraphe 1, de la loi, sans raison légitime ([2]), est considéré comme une violation grave des droits et intérêts d'une personne, présentant un caractère imminent au sens de l'article 42, paragraphe 2, de ladite loi.

(1) Informations à caractère personnel nécessitant des précautions particulières (article 2, paragraphe 3, de la loi)

Article 2 (paragraphe 3) de la loi

3. Au sens de la présente loi, on entend par «informations à caractère personnel nécessitant des précautions particulières» les informations à caractère personnel concernant la race, les convictions religieuses, le statut social, les antécédents médicaux, le casier judiciaire, le fait d'avoir subi un préjudice résultant d'un acte criminel, ou d'autres descriptions, etc., fixées par arrêté ministériel, dont le traitement requiert des précautions particulières afin d'éviter à la personne concernée toute discrimination injuste, tout préjudice ou tout autre dommage.

Article 2 de l'arrêté ministériel

Les autres descriptions, etc., fixées par arrêté ministériel en vertu de l'article 2, paragraphe 3, de la loi sont des descriptions, etc., contenant l'un des éléments énumérés ci-après (à l'exclusion de ceux relevant des antécédents médicaux ou du casier judiciaire de la personne concernée):

i) le fait de souffrir d'une incapacité physique, d'une déficience intellectuelle ou d'une déficience mentale (y compris de troubles du développement) ou d'autres incapacités fonctionnelles physiques ou mentales au sens des règles de la Commission de protection des données à caractère personnel;

ii) les résultats d'un contrôle médical ou autre (dénommé ci-après «contrôle médical») réalisé sur une personne concernée par un médecin ou une personne posant des actes médicaux en vue de prévenir ou de déceler à un stade précoce une maladie (dénommé ci-après le «médecin»);

iii) le fait qu'une personne concernée ait reçu des conseils en vue de l'amélioration de son état mental et physique, que des soins médicaux lui aient été prodigués ou qu'une prescription lui ait été délivrée par un médecin ou une personne posant des actes médicaux à la suite d'un contrôle médical, etc., ou en raison d'une maladie, d'une blessure ou d'autres altérations mentales ou physiques;

iv) le fait qu'une arrestation, une perquisition, une saisie, une détention, des poursuites ou d'autres procédures liées à une affaire pénale aient été menées à l'encontre d'une personne concernée en sa qualité de suspect ou de partie défenderesse;

([2]) Par «raison légitime», il convient d'entendre un événement de nature extraordinaire échappant au contrôle de l'opérateur économique traitant des informations à caractère personnel et ne pouvant raisonnablement pas être prévu (comme, par exemple, des catastrophes naturelles), ou les cas dans lesquels la nécessité de prendre des mesures concernant une recommandation émise par l'opérateur économique traitant des informations à caractère personnel en vertu de l'article 42, paragraphe 1, de la loi a disparu, ledit opérateur ayant pris une autre mesure qui remédie pleinement à la violation.

v) la réalisation d'une enquête, l'adoption d'une mesure d'observation et de protection, la tenue d'une audition et l'adoption d'une décision, l'adoption d'une mesure conservatoire ou la mise en œuvre d'autres procédures ayant trait à une affaire liée à la protection de la jeunesse à l'égard d'une personne concernée en tant que délinquant juvénile ou d'une personne soupçonnée d'avoir commis un tel acte au sens de l'article 3, paragraphe 1, de la loi sur les mineurs.

Article 5 des règles

Les incapacités fonctionnelles physiques et mentales énumérées dans les règles de la Commission de protection des données à caractère personnel conformément à l'article 2, point i), de l'arrêté sont les suivantes:

i) incapacités physiques mentionnées dans le tableau annexé à la loi pour le bien-être des personnes souffrant d'une incapacité physique (loi n° 283 de 1949);

ii) déficiences intellectuelles énumérées dans la loi pour le bien-être des personnes souffrant d'une déficience intellectuelle (loi n° 37 de 1960);

iii) déficiences mentales visées par la loi relative à la santé mentale et au bien-être des personnes souffrant de déficiences mentales (loi n° 123 de 1950) (y compris les troubles du développement visés à l'article 2, paragraphe 1, de la loi relative à l'aide aux personnes souffrant de troubles du développement, et à l'exclusion des déficiences intellectuelles visées par la loi relative au bien-être des personnes souffrant d'une déficience intellectuelle);

iv) maladies pour lesquelles il n'existe aucun traitement établi ou autres maladies spécifiques dont la gravité est déterminée par arrêté ministériel en vertu de l'article 4, paragraphe 1, de la loi concernant le dispositif global d'aide à la vie quotidienne et sociale en faveur des personnes souffrant d'un handicap (loi n° 123 de 2005), équivalentes à celles prescrites par le ministre de la santé, du travail et du bien-être audit paragraphe.

Si les données à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation contiennent des données concernant la vie ou l'orientation sexuelles ou l'appartenance syndicale d'une personne physique, données définies comme relevant de catégories particulières de données à caractère personnel en vertu du RGPD, les opérateurs économiques traitant des informations à caractère personnel sont tenus de leur réserver un traitement identique à celui des informations à caractère personnel nécessitant des précautions particulières au sens de l'article 2, paragraphe 3, de la loi.

(2) Données à caractère personnel conservées (article 2, paragraphe 7, de la loi)

Article 2 (paragraphe 7) de la loi

7. Au sens de la loi, on entend par «données à caractère personnel conservées» les données à caractère personnel qu'un opérateur économique traitant des informations à caractère personnel est habilité à divulguer et à corriger, auxquelles il peut ajouter ou desquelles il peut supprimer du contenu, qu'il peut cesser d'utiliser, supprimer ou cesser de fournir à des tiers et qui ne sont ni des données dont un arrêté ministériel détermine qu'elles sont susceptibles de porter atteinte aux intérêts publics ou autres si leur présence ou absence vient à être connue, ni des données dont l'effacement est prévu dans un délai n'excédant pas un an, défini par arrêté ministériel.

Article 4 de l'arrêté ministériel

Les données prévues par arrêté ministériel en vertu de l'article 2, paragraphe 7, sont les suivantes:

i) données à caractère personnel pour lesquelles le risque existe, si la présence ou l'absence desdites données à caractère personnel est connue, que cela porte atteinte à la vie, à l'intégrité physique ou aux biens d'une personne concernée ou d'un tiers;

ii) données à caractère personnel pour lesquelles le risque existe, si la présence ou l'absence desdites données à caractère personnel est connue, que cela encourage ou provoque un acte illégal ou abusif;

iii) données pour lesquelles le risque existe, si la présence ou l'absence desdites données à caractère personnel est connue, que cela porte atteinte à la sécurité nationale, détruise une relation de confiance avec un pays étranger ou une organisation internationale ou cause un préjudice dans les négociations avec un pays étranger ou une organisation internationale;

iv) les données à caractère personnel pour lesquelles le risque existe, si la présence ou l'absence desdites données à caractère personnel est connue, que cela fasse obstacle au maintien de l'ordre public et de la sécurité publique, par exemple pour ce qui est de la prévention des délits ainsi que de la lutte et des enquêtes en la matière.

Article 5 de l'arrêté ministériel

Toute période fixée par arrêté ministériel en vertu de l'article 2, paragraphe 7, de la loi a une durée de six mois.

Les données à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation doivent être traitées comme des données à caractère personnel conservées au sens de l'article 2, paragraphe 7, de la loi, quelle que soit la période au terme de laquelle elles doivent être supprimées.

Si les données à caractère personnel transférées depuis l'UE sur la base d'une décision d'adéquation relèvent de catégories de données à caractère personnel définies par arrêté ministériel comme étant «susceptibles de porter atteinte aux intérêts publics ou autres si leur présence ou absence vient à être connue», elles ne doivent pas être traitées comme des données à caractère personnel conservées (voir l'article 4 de l'arrêté ministériel et les lignes directrices (règles générales), «2-7. Données à caractère personnel conservées»).

(3) Définition de la finalité de l'utilisation, limitation due à la finalité de l'utilisation (article 15, paragraphe 1, article 16, paragraphe 1, et article 26, paragraphes 1 et 3, de la loi)

Article 15 (paragraphe 1) de la loi

(1) Un opérateur économique traitant des informations à caractère personnel doit, lorsqu'il traite des informations à caractère personnel, préciser la finalité de l'utilisation desdites informations (dénommée ci-après la «finalité de l'utilisation») de façon aussi explicite que possible.

Article 16 (paragraphe 1) de la loi

(1) Un opérateur économique traitant des informations à caractère personnel ne peut traiter des informations à caractère personnel, sans obtenir préalablement le consentement de la personne concernée, au-delà de la mesure nécessaire pour atteindre une finalité d'utilisation spécifiée conformément aux dispositions de l'article précédent.

Article 26 (paragraphes 1 et 3) de la loi

(1) Un opérateur économique traitant des informations à caractère personnel doit, lorsqu'il reçoit des données à caractère personnel d'un tiers, vérifier les éléments suivants établis conformément aux règles de la Commission de protection des données à caractère personnel: (omission)

i) (omission)

ii) les circonstances dans lesquelles ces données ont été acquises par ce tiers.

(3) Un opérateur économique traitant des informations à caractère personnel doit, après avoir procédé aux vérifications conformément aux dispositions du paragraphe 1, garder une trace, conformément aux règles fixées par la Commission de protection des données à caractère personnel, de la date de réception des données à caractère personnel, d'un élément concernant ladite confirmation et d'autres éléments prévus par les règles fixées par la Commission de protection des données à caractère personnel.

Si des opérateurs économiques traitant des informations à caractère personnel traitent des informations à caractère personnel dans une mesure allant au-delà de la mesure nécessaire pour atteindre la finalité de l'utilisation prévue à l'article 15, paragraphe 1, de la loi, ils doivent obtenir préalablement le consentement de la personne concernée (article 16, paragraphe 1, de la loi). Lorsqu'ils reçoivent des données à caractère personnel de la part d'un tiers, les opérateurs économiques traitant des informations à caractère personnel doivent, conformément aux règles, vérifier des éléments tels que les circonstances dans lesquelles ce tiers a acquis ces données et garder une trace de ces éléments (article 26, paragraphes 1 et 3, de la loi).

Lorsqu'un opérateur économique traitant des informations à caractère personnel reçoit des données à caractère personnel en provenance de l'UE sur la base d'une décision d'adéquation, les circonstances entourant l'acquisition de ces données, qui doivent être vérifiées et dont une trace doit être gardée conformément à l'article 26, paragraphes 1 et 3, sont, notamment, la finalité de l'utilisation pour laquelle elles ont été transférées depuis l'UE.

De même, lorsqu'un opérateur économique traitant des informations à caractère personnel reçoit d'un autre opérateur économique traitant des informations à caractère personnel des données à caractère personnel transférées précédemment depuis l'UE sur la base d'une décision d'adéquation, les circonstances entourant l'acquisition de ces données, qui doivent être vérifiées et dont une trace doit être gardée conformément à l'article 26, paragraphes 1 et 3, sont, notamment, la finalité de l'utilisation pour laquelle elles ont reçues.

Dans les cas susmentionnés, l'opérateur économique traitant des informations à caractère personnel est tenu de préciser la finalité de l'utilisation de ces données conformément à la finalité de l'utilisation pour laquelle ces données ont été reçues initialement ou ultérieurement, telles qu'elles ont été vérifiées et dont une trace a été gardée conformément à l'article 26, paragraphes 1 et 3, et d'utiliser ces données en respectant la portée indiquée (conformément à l'article 15, paragraphe 1, et à l'article 16, paragraphe 1, de la loi).

(4) Limitation concernant la fourniture à un tiers dans un pays étranger (article 24 de la loi et article 11, paragraphe 2, des règles)

Article 24 de la loi

Un opérateur économique traitant des informations à caractère personnel, à l'exception des cas définis dans chacun des éléments du paragraphe 1 de l'article précédent, doit, lorsqu'il fournit des données à caractère personnel à un tiers (sauf si celui-ci établit un système conforme aux normes prescrites par les règles de la Commission de protection des données à caractère personnel comme étant nécessaires pour l'adoption continue de mesures équivalentes à celle qu'un opérateur économique traitant des informations à caractère personnel doit prendre aux fins du traitement des données à caractère personnel conformément aux dispositions de la présente section; même dénomination ci-après dans le présent article) dans un pays étranger (à savoir, un pays ou une région située hors du territoire du Japon; même dénomination ci-après) (à l'exclusion de ceux définis dans les règles de la Commission de protection des données à caractère personnel comme étant des pays étrangers établissant un système de protection des informations à caractère personnel reconnu comme appliquant des normes équivalentes à celles du Japon en ce qui concerne la protection des droits et intérêts d'une personne; même dénomination ci-après dans le présent article), obtenir préalablement le consentement de la personne concernée signifiant qu'elle autorise la fourniture de ses données à un tiers dans un pays étranger. Dans ce cas, les dispositions de l'article précédent ne s'appliquent pas.

Article 11, paragraphe 2, des règles

Les normes prescrites par les règles de la Commission de protection des données à caractère personnel en vertu de l'article 24 de la loi doivent satisfaire à chacun des éléments suivants:

i) l'opérateur économique traitant des informations à caractère personnel et une personne à laquelle sont fournies des données à caractère personnel ont garanti, en ce qui concerne le traitement des données à caractère personnel par la personne qui reçoit les données, la mise en œuvre de mesures conformes à la finalité des dispositions du chapitre IV, section 1, de la loi au moyen d'une méthode appropriée et raisonnable;

ii) la personne à laquelle sont fournies des données à caractère personnel a obtenu une reconnaissance sur la base d'un cadre international concernant le traitement des informations à caractère personnel.

Lorsqu'il fournit à un tiers, dans un pays étranger, des données à caractère personnel en provenance de l'UE sur la base d'une décision d'adéquation, un opérateur économique traitant des informations à caractère personnel doit obtenir préalablement le consentement de la personne concernée signifiant qu'elle autorise la fourniture de ses données à un tiers dans un pays étranger conformément à l'article 24 de la loi, consentement donné après avoir reçu des informations sur les circonstances entourant le transfert, nécessaires pour lui permettre de prendre une décision quant à son consentement, à l'exclusion des cas relevant de l'un des points i) à iii) ci-après:

i) lorsque le tiers se trouve dans un pays décrit dans les règles comme étant un pays étranger établissant un système de protection des informations à caractère personnel reconnu comme appliquant des normes équivalentes à celles du Japon en ce qui concerne la protection des droits et intérêts d'une personne;

ii) lorsqu'un opérateur économique traitant des informations à caractère personnel et le tiers qui reçoit les données à caractère personnel ont, en ce qui concerne le traitement des données à caractère personnel par le tiers, mis en œuvre conjointement des mesures offrant un niveau de protection équivalent à celui de la loi, lue en combinaison avec les présentes règles, au moyen d'une méthode appropriée et raisonnable (à savoir, une convention, d'autres types d'accords contraignants ou des accords contraignants au sein d'un groupe d'entreprises);

iii) dans les cas relevant de chacun des éléments énoncés à l'article 23, paragraphe 1, de la loi.

(5) Informations traitées de manière anonyme (article 2, paragraphe 9, et article 36, paragraphes 1 et 2, de la loi)

Article 2 (paragraphe 9) de la loi

(9) Au sens de la présente loi, on entend par «informations traitées de manière anonyme» les informations relatives à une personne qui peuvent être produites à l'issue du traitement d'informations à caractère personnel de façon telle qu'il n'est pas possible d'identifier une personne donnée en prenant les mesures prévues dans chacun des points suivants, conformément à la répartition des informations à caractère personnel établie dans chaque point en question ni de restaurer les informations à caractère personnel.

i) informations à caractère personnel relevant du paragraphe 1, point i);

supprimer une partie des descriptions, etc. contenues dans lesdites informations à caractère personnel (y compris remplacer ladite partie des descriptions, etc. par d'autres descriptions, etc. à l'aide d'une méthode sans régularité permettant de restaurer ladite partie des descriptions, etc.)

ii) informations à caractère personnel relevant du paragraphe 1, point ii);

supprimer tous les codes d'identification individuels contenus dans lesdites informations à caractère personnel (y compris remplacer lesdits codes d'identification individuels par d'autres descriptions, etc. à l'aide d'une méthode sans régularité permettant de restaurer lesdits codes d'identification individuels)

Article 36 (paragraphe 1) de la loi

(1) Un opérateur économique traitant des informations à caractère personnel doit, lorsqu'il produit des informations traitées de manière anonyme (limitées à celles qui constituent une base de données d'informations traitées de manière anonyme, etc.; ci-après dénommées de la même manière), traiter les informations à caractère personnel conformément aux normes prescrites par les règles de la Commission de protection des informations à caractère personnel comme celles nécessaires pour rendre impossible l'identification d'une personne donnée ou de restaurer les informations à caractère personnel utilisées pour la production.

Article 19 des règles

Les normes prescrites par les règles de la Commission de protection des informations à caractère personnel au titre de l'article 36, paragraphe 1, de la loi sont les suivantes.

i) supprimer la totalité ou une partie des descriptions, etc. qui permettent d'identifier une personne donnée contenues dans lesdites informations à caractère personnel (y compris remplacer ces descriptions, etc. par d'autres descriptions, etc. à l'aide d'une méthode sans régularité permettant de restaurer la totalité ou une partie des descriptions, etc.)

ii) supprimer tous les codes d'identification individuels contenus dans les informations à caractère personnel (y compris remplacer ces codes par d'autres descriptions, etc. à l'aide d'une méthode sans régularité permettant de restaurer les codes d'identification individuels)

iii) supprimer les codes (limités aux codes reliant des informations multiples effectivement traitées par un opérateur économique traitant des informations à caractère personnel) qui mettent en relation des informations à caractère personnel et des informations obtenues en prenant des mesures relatives aux informations à caractère personnel (y compris le remplacement desdits codes par d'autres codes qui ne peuvent relier lesdites informations à caractère personnel et les informations obtenues en ayant pris des mesures relatives auxdites informations à caractère personnel à l'aide d'une méthode sans régularité permettant de restaurer lesdits codes)

iv) supprimer les descriptions idiosyncratiques, etc. (y compris remplacer ces descriptions, etc. par d'autres descriptions, etc. à l'aide d'une méthode sans régularité permettant de restaurer les descriptions idiosyncratiques, etc.)

v) outre les mesures énoncées dans chacun des points précédents, prendre les mesures appropriées en fonction des résultats de l'examen de l'attribut, etc., de la base de données des informations à caractère personnel, etc., comme la différence entre les descriptions, etc., contenues dans les informations à caractère personnel et les descriptions, etc., contenues dans d'autres informations à caractère personnel constituant la base de données d'informations à caractère personnel, etc., contenant lesdites informations à caractère personnel

Article 36 (paragraphe 2) de la loi

(2) Un opérateur économique traitant des informations à caractère personnel, lorsqu'il a produit des informations traitées de manière anonyme, doit, conformément aux normes prescrites par les règles de la Commission de protection des informations à caractère personnel comme celles nécessaires pour empêcher la fuite d'informations relatives à ces descriptions, etc. et des codes d'identification individuels supprimés des informations à caractère personnel utilisées pour produire les informations traitées de manière anonyme, ainsi que des informations liées à l'application d'une méthode de traitement, conformément aux dispositions du paragraphe précédent, prendre des mesures en vue du contrôle de la sécurité de ces informations.

Article 20 des règles

Les normes prescrites par les règles de la Commission de protection des informations à caractère personnel au titre de l'article 36, paragraphe 2, de la loi sont les suivantes.

i) définir clairement l'autorité et la responsabilité d'une personne qui traite les informations relatives à ces descriptions, etc., et les codes d'identification individuels qui ont été supprimés des informations à caractère personnel utilisées pour produire des informations traitées de manière anonyme et des informations relatives à une méthode de traitement effectuée conformément aux dispositions de l'article 36, paragraphe 1, (limitées à celles qui peuvent restaurer les données à caractère personnel en utilisant ces informations connexes) (ci-après dénommées «informations liées à la méthode de traitement, etc.» au sens du présent article.)

ii) établir des règles et des procédures concernant le traitement des informations liées à la méthode de traitement, etc., le traitement approprié des informations liées à la méthode de traitement, etc., conformément aux règles et procédures, évaluer la situation en matière de traitement et, sur la base des résultats de cette évaluation, prendre les mesures nécessaires pour rechercher des améliorations

iii) prendre les mesures nécessaires et appropriées pour empêcher une personne n'ayant pas l'autorité légitime de traiter les informations liées à la méthode de traitement, etc, de traiter les informations liées à la méthode de traitement, etc.

Les informations à caractère personnel fournies par l'UE en application d'une décision d'adéquation ne sont considérées comme des informations traitées de manière anonyme au sens de l'article 2, paragraphe 9, de la loi que si l'opérateur économique traitant des informations à caractère personnel prend des mesures rendant l'anonymisation de la personne irréversible pour quiconque, notamment en supprimant les informations liées à la méthode de traitement, etc. (c'est-à-dire des informations relatives aux descriptions et aux codes d'identification individuels qui ont été supprimés des informations à caractère personnel utilisées pour produire des informations à caractère personnel traitées de manière anonyme, ainsi que des informations relatives à l'application d'une méthode de traitement effectuée conformément aux dispositions de l'article 36, paragraphe 1, de la loi (limitées à celles qui peuvent restaurer les informations à caractère personnel en utilisant ces informations connexes).

ANNEXE 2

S.E. Mme Věra Jourová, commissaire européenne chargée de la justice, des consommateurs et de l'égalité des genres

Excellence,

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

À la demande de la Commission européenne adressée au gouvernement du Japon, 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 japonais.

Ce document concerne de nombreux ministères et agences du gouvernement japonais, et s'agissant du contenu du document, les ministères et agences compétents (secrétariat du cabinet, police nationale, Commission de protection des informations à caractère personnel, ministère des affaires intérieures et des communications, ministère de la justice, agence de renseignement en matière de sécurité publique, ministère de la défense) sont responsables des passages qui relèvent 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.

(Formule de politesse)

Yoko Kamikawa

Ministre de la justice

Ce document a été élaboré par le ministère de la justice et les ministères et agences concernés suivants.

Koichi Hamano

Conseiller, secrétariat du cabinet

Schunichi Kuryu

Commissaire général de la police nationale

Mari Sonoda

Secrétaire général de la Commission de protection des informations à caractère personnel

Mitsuru Yasuda

Vice-ministre, ministère des affaires intérieures et des communications

Seimei Nakagawa

Agence de renseignement en matière de sécurité publique

Kenichi Takahashi

Vice-ministre administratif de la défense

14 septembre 2018

Collecte et utilisation d'informations à caractère personnel par les autorités publiques japonaises à des fins répressives et à des fins 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 (électroniques) par les autorités publiques japonaises à des fins répressives et à des fins 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, y compris la surveillance indépendante et les possibilités de recours individuels. Cet exposé est adressé à la Commission européenne en vue d'exprimer l'engagement et de garantir que l'accès des pouvoirs publics aux informations à caractère personnel transférées de l'UE vers le Japon se limite à ce qui est nécessaire et proportionné, sous réserve d'un contrôle indépendant et que les personnes concernées pourront obtenir réparation en cas de violation éventuelle de leur droit fondamental à la vie privée et à la protection des données. Cet exposé prévoit également la création d'un nouveau mécanisme de recours, administré par la Commission de protection des informations à caractère personnel (PPC), pour traiter les plaintes déposées par des citoyens de l'UE concernant l'accès des pouvoirs publics à leurs données à caractère personnel transférées de l'UE au Japon.

I. **Les principes juridiques généraux applicables à l'accès des pouvoirs publics**

En tant qu'exercice de l'autorité publique, l'accès des pouvoirs publics aux données doit intervenir dans le respect total de la loi (principe de légalité). Au Japon, les informations à caractère personnel sont protégées, tant dans le secteur privé que dans le secteur public, par un mécanisme à plusieurs niveaux.

A. Cadre constitutionnel et principe de la réserve de la loi

L'article 13 de la Constitution et la jurisprudence reconnaissent le droit au respect de la vie privée en tant que droit constitutionnel. À cet égard, la Cour suprême a statué qu'il est naturel que les particuliers ne veuillent pas que d'autres connaissent leurs informations à caractère personnel sans raison valable, et que cette attente devrait être protégée [1]. D'autres protections sont consacrées par l'article 21, paragraphe 2, de la Constitution, qui garantit le respect du secret des communications, et l'article 35 de la Constitution, qui garantit le droit de ne pas faire l'objet de perquisitions et de saisies sans mandat, ce qui signifie que la collecte d'informations à caractère personnel, y compris l'accès, par des moyens obligatoires, doit toujours être fondée sur un mandat judiciaire. Un tel mandat ne peut être délivré qu'aux fins d'une enquête sur une infraction déjà commise. Par conséquent, dans le cadre juridique du Japon, la collecte d'informations par des moyens obligatoires aux fins de la sécurité nationale (et non d'une enquête pénale) n'est pas autorisée.

En outre, conformément au principe de la réserve de la loi, la collecte obligatoire d'informations doit être expressément autorisée par la loi. En cas de collecte non obligatoire/volontaire, les informations sont obtenues auprès d'une source librement accessible ou pouvant être reçue sur la base d'une demande de divulgation volontaire, c'est-à-dire d'une demande qui ne peut être opposée à la personne physique ou morale détenant ces informations. Toutefois, cela n'est autorisé que dans la mesure où l'autorité publique est compétente pour mener l'enquête, étant donné que chaque autorité publique ne peut agir que dans le cadre de sa compétence administrative prévue par la loi (que ses activités portent ou non atteinte aux droits et libertés des personnes). Ce principe s'applique à la capacité de l'autorité à recueillir des informations à caractère personnel.

B. Règles spécifiques relatives à la protection des informations à caractère personnel

La loi sur la protection des informations à caractère personnel (APPI) et la loi sur la protection des informations à caractère personnel détenues par des instances administratives (APPIHAO), qui se fondent sur les dispositions constitutionnelles et les précisent, garantissent le droit à des informations à caractère personnel tant dans le secteur privé que public.

L'article 7 de l'APPI dispose que la PPC définit la «politique de base relative à la protection des informations à caractère personnel» (ci-après la «politique de base»). La politique de base, qui est adoptée par décision du cabinet du Japon en tant qu'organe central du gouvernement japonais (Premier ministre et ministres d'État), fixe les orientations en matière de protection des informations à caractère personnel au Japon. De cette manière, la PPC, en tant qu'autorité de surveillance indépendante, fait office de «centre de commandement» du système japonais de protection des informations à caractère personnel.

Chaque fois que les organes administratifs recueillent des informations à caractère personnel, qu'ils le fassent par des moyens obligatoires ou non, ils doivent en principe [2] se conformer aux exigences de l'APPIHAO. L'APPIHAO est une loi générale applicable au traitement des «informations à caractère personnel conservées» [3] par les «organes administratifs» (tels que définis à l'article 2, paragraphe 1, de l'APPIHAO). Elle couvre donc également le traitement des données dans le

[1] Cour suprême, arrêt du 12 septembre 2003 [2002 (Ju) n° 1656].

[2] Pour les exceptions concernant le chapitre 4 de l'APPIHAO, voir ci-après, p. 16.

[3] On entend par «informations à caractère personnel conservées» figurant à l'article 2, paragraphe 5, de l'APPIHAO, des informations à caractère personnel préparées ou obtenues par un agent d'une instance administrative dans l'exercice de ses fonctions et détenues par ladite instance administrative à des fins organisationnelles par ses agents.

domaine de l'application du droit pénal et de la sécurité nationale. Parmi les autorités publiques habilitées à mettre en œuvre l'accès des pouvoirs publics, toutes les autorités, à l'exception de la police préfectorale, sont des autorités gouvernementales nationales qui relèvent de la définition des «organes administratifs». Le traitement des informations à caractère personnel par la police préfectorale est régi par des arrêtés préfectoraux ([4]) qui prévoient des principes de protection des informations à caractère personnel, des droits et des obligations, équivalents à ceux de l'APPIHAO.

II. **Accès des autorités publiques à des fins répressives**

A) Bases juridiques et limitations

1) Collecte d'informations personnelles par des moyens de contrainte

a) Bases juridiques

En vertu de l'article 35 de la Constitution, le droit de chacun à l'intégrité du foyer, de la correspondance et des effets à l'abri des perquisitions, recherches et saisies ne peut être enfreint en l'absence d'un mandat «valablement motivé» décrivant, en particulier, le lieu soumis à perquisition et les choses sujettes à saisie. Par conséquent, la collecte par voie de contrainte d'informations électroniques par les autorités publiques dans le cadre d'une enquête pénale ne peut avoir lieu que sur la base d'un mandat. Cela vaut à la fois pour la collecte d'enregistrements électroniques contenant des informations (personnelles) et pour l'interception en temps réel de communications («écoutes»). La seule exception à cette règle (qui n'est toutefois pas pertinente dans le contexte d'un transfert électronique d'informations personnelles à partir de l'étranger) est l'article 220, paragraphe 1, du code de procédure pénale ([5]), aux termes duquel un procureur, un assistant du procureur ou un fonctionnaire de police judiciaire peut, au moment de l'arrestation d'un suspect ou d'un contrevenant en «flagrant délit», effectuer, si nécessaire, une perquisition et une saisie «sur place au moment de l'arrestation».

Aux termes de l'article 197, paragraphe 1, du code de procédure pénale, les mesures d'enquête par voie de contrainte «ne s'appliquent pas à moins que des dispositions spéciales aient été prévues dans le présent code». En ce qui concerne la collecte d'informations électroniques par voie de contrainte, les bases juridiques applicables à cet égard sont l'article 218, paragraphe 1, du code de procédure pénale (selon lequel un procureur, un assistant du procureur ou un fonctionnaire de police judiciaire peut, si l'instruction d'une infraction l'exige, effectuer une perquisition, une saisie ou une inspection sur la base d'un mandat émis par un juge) et l'article 222, paragraphe 2, dudit code (qui prévoit que les mesures de contrainte pour l'interception de communications électroniques sans le consentement de l'une ou l'autre des parties sont exécutées sur la base d'autres lois). Cette dernière disposition renvoie à la loi sur les écoutes téléphoniques pour les enquêtes pénales («loi sur les écoutes»), qui, en son article 3, paragraphe 1, dispose que les conditions dans lesquelles les communications liées à certaines infractions graves peuvent être écoutées sur la base d'un mandat d'écoute téléphonique émis par un juge ([6]).

En ce qui concerne la police, le pouvoir d'enquête appartient dans tous les cas à la police préfectorale, tandis que l'Agence nationale de police (NPA) ne mène pas d'enquête pénale sur la base du code de procédure pénale.

b) Limitations

La collecte par voie de contrainte d'informations électroniques est limitée par la Constitution et par les lois organiques, telles qu'interprétées dans la jurisprudence, qui prévoient en particulier les critères devant être appliqués par les juridictions lors de l'émission d'un mandat. En outre, l'APPIHAO impose un certain nombre de limitations applicables tant à la collecte des informations qu'à leur traitement (alors que les arrêtés municipaux reproduisent pour l'essentiel les mêmes critères pour la police préfectorale).

(1) Limitations découlant de la Constitution et de la législation organique

Aux termes de l'article 197, paragraphe 1, du code de procédure pénale, les mesures de contrainte ne doivent pas s'appliquer à moins que des dispositions spéciales aient été prévues dans ledit code. L'article 218, paragraphe 1, du code de procédure pénale dispose ensuite que la saisie, etc., peut être effectuée sur la base d'un mandat émis par un juge

([4]) Chaque préfecture dispose de son propre «arrêté préfectoral» applicable à la protection des informations à caractère personnel par la police préfectorale. Il n'existe pas de traduction en anglais de ces arrêtés préfectoraux.

([5]) L'article 220, paragraphe 1, du code de procédure pénale dispose que lorsqu'un procureur, un assistant du procureur ou un fonctionnaire de police judiciaire procède à l'arrestation d'un suspect, il peut, si nécessaire, prendre les mesures suivantes: a) pénétrer dans le domicile d'une autre personne, etc., pour rechercher le suspect; b) effectuer une perquisition, une saisie ou une inspection sur place au moment de l'arrestation.

([6]) Plus précisément, cette disposition prévoit que «le procureur ou la police judiciaire peut, dans les cas relevant de l'un des éléments suivants, lorsque les circonstances sont suffisantes pour présumer que des communications auront lieu concernant la commission et la préparation d'actes ultérieurs ou une collusion en la matière, comme la destruction de preuves, etc., des instructions et autres échanges de communications sur l'infraction, comme indiqué dans chacun desdits éléments (ci-après dénommés "une série d'infractions" dans les deuxième et troisième points), ainsi que des communications contenant les aspects liés à cette infraction (ci-après dénommées "communications relatives à l'infraction" dans le présent paragraphe) et dans les cas où il est extrêmement difficile d'identifier l'auteur de l'infraction ou de clarifier les circonstances/détails de la commission d'une quelconque autre manière, la communication "écoutée" relative à l'infraction, fondée sur le mandat correspondant émis par un juge, concernant un moyen de communication, qui est caractérisé par un numéro de téléphone et d'autres numéros/codes pour identifier la source ou la destination de l'appel et qui est utilisé par le suspect sur la base du contrat avec des entreprises de télécommunications, etc. (à l'exception de ceux qui peuvent être considérées comme n'étant pas suspects de servir à des "communications relatives à l'infraction"), ou ceux pour lesquels il y a lieu de suspecter qu'ils servent à des "communications liées à l'infraction", l'écoute des communications relatives à l'infraction par ce moyen de communication peut être effectuée.»

uniquement «si l'instruction d'une infraction l'exige». Bien que les critères pour juger de cette nécessité ne soient pas davantage précisés dans le droit organique, la Cour suprême ([7]) a statué que, lorsqu'il évalue la nécessité de telles dispositions, le juge doit procéder à une appréciation globale prenant en considération en particulier les éléments suivants:

a) la gravité de l'infraction et la manière dont elle a été commise;

b) la valeur et l'importance des éléments saisis en tant que preuves;

c) la probabilité de la dissimulation ou de la destruction d'éléments saisis;

d) l'ampleur des inconvénients dus à une saisie;

e) d'autres conditions connexes.

Des limitations découlent également de l'obligation, énoncée à l'article 35 de la Constitution, d'invoquer un «motif valable». En vertu de ce critère de «motif valable», des mandats peuvent être émis si: [1] une enquête pénale est requise [voir l'arrêt de la Cour suprême du 18 mars 1969 (1968 (Shi) nº 100) susmentionné], [2] il existe une situation dans laquelle le suspect (l'accusé) est considéré comme ayant commis une infraction (article 156, paragraphe 1, du règlement de procédure pénale) ([8]), [3] le mandat d'enquête s'appliquant au corps, aux effets, au domicile ou à tout autre lieu d'une personne autre que l'accusé ne doit être émis que si on peut raisonnablement supposer que les effets devant être saisis existent (article 102, paragraphe 2, du code de procédure pénale). Lorsqu'il estime que les preuves documentaires produites par les autorités enquêtrices ne constituent pas des motifs suffisants pour suspecter une infraction, le juge rejette la demande de mandat. À cet égard, il convient de noter qu'en vertu de la loi sur la répression de la criminalité organisée et le contrôle des produits du crime, les «actes préparatoires à la commission» d'un crime prémédité (par exemple, la réunion de fonds pour commettre un crime terroriste) constituent eux-mêmes un acte criminel et peuvent donc faire l'objet d'une enquête coercitive reposant sur un mandat.

Enfin, lorsque l'enquête s'applique au corps, aux effets, au domicile ou à tout autre lieu d'une personne autre que le suspect ou l'accusé, le mandat correspondant n'est émis que si on peut raisonnablement supposer que les effets qui doivent être saisis existent (article 102, paragraphe 2, et article 222, paragraphe 1, du code de procédure pénale).

En ce qui concerne spécifiquement l'interception de communications aux fins d'enquêtes pénales sur la base de la loi sur les écoutes téléphoniques, celle-ci ne peut être effectuée que lorsque les exigences strictes prévues à l'article 3, paragraphe 1, sont remplies. Aux termes de cette disposition, l'interception nécessite toujours un mandat préalablement établi par une juridiction, qui ne peut être émis que dans des cas limités ([9]).

2) Limitations découlant de l'APPIHAO

En ce qui concerne la collecte ([10]) et le traitement ultérieur (notamment la conservation, la gestion et l'utilisation) d'informations personnelles par des instances administratives, l'APPIHAO prévoit en particulier les limitations suivantes:

a) Aux termes de l'article 3, paragraphe 1, de l'APPIHAO, les instances administratives ne peuvent conserver des informations personnelles que lorsque la conservation est nécessaire à l'exercice des fonctions relevant de leur juridiction conformément aux dispositions législatives et réglementaires. Lors de la conservation, elles sont également tenues d'indiquer (dans la mesure du possible) la finalité de l'utilisation des informations personnelles. En vertu de l'article 3, paragraphes 2 et 3, de l'APPIHAO, les instances administratives ne conservent pas les informations personnelles au-delà de ce qui est nécessaire à la réalisation de la finalité d'utilisation ainsi spécifiée et ne changent pas la finalité d'utilisation au-delà de ce qui peut raisonnablement être considéré comme étant, de manière appropriée, pertinent pour la finalité initiale.

b) L'article 5 de l'APPIHAO prévoit que le responsable d'une instance administrative doit veiller à ce que les informations personnelles conservées restent exactes et à jour, dans la mesure nécessaire à la réalisation de la finalité d'utilisation.

c) L'article 6, paragraphe 1, de l'APPIHAO dispose que le responsable d'une instance administrative doit prendre les mesures nécessaires pour prévenir toute fuite, toute perte ou tout dommage ainsi que pour assurer la bonne gestion des informations personnelles conservées.

d) En vertu de l'article 7 de l'APPIHAO, aucun employé (ni ancien employé) ne doit divulguer les informations personnelles acquises à un tiers sans motif justifiable, ou utiliser ces informations à des fins injustifiées.

([7]) Arrêt du 18 mars 1969 [1968 (Shi) nº 100].
([8]) L'article 156, paragraphe 1, du code de procédure pénale dispose: «En déposant la demande visée au paragraphe 1 de l'article qui précède, le demandeur fournit les éléments sur la base desquels le suspect ou l'accusé doit être considéré comme ayant commis une infraction.»
([9]) Voir la note de bas de page 6.
([10]) L'article 3, paragraphes 1 et 2, de l'APPIHAO limite l'étendue de la conservation et, partant, également la collecte d'informations personnelles.

e) En outre, l'article 8, paragraphe 1, de l'APPIHAO prévoit que le responsable d'une instance administrative ne peut, sauf lorsque des actes législatifs et réglementaires en disposent autrement, ni utiliser ni transmettre à un tiers des informations personnelles conservées pour des fins autres que la finalité pour laquelle ces informations sont utilisées. Bien que l'article 8, paragraphe 2, contienne des exceptions à cette règle dans des situations spécifiques, ces exceptions ne s'appliquent que si une divulgation exceptionnelle ne risque pas de causer un préjudice «injustifié» aux droits et intérêts de la personne concernée ou d'un tiers.

f) Conformément à l'article 9 de l'APPIHAO, lorsque des informations personnelles conservées sont transmises à un tiers, le responsable de l'instance administrative impose, le cas échéant, des restrictions à la finalité ou à la méthode d'utilisation, ou toute autre restriction nécessaire; il peut aussi demander au destinataire de ces informations de prendre les mesures nécessaires pour prévenir toute fuite et pour assurer la bonne gestion des informations.

g) L'article 48 de l'APPIHAO prévoit que le responsable d'une instance administrative doit veiller à traiter, de manière appropriée et sans délai, toute plainte portant sur le traitement des informations personnelles.

2) Collecte d'informations personnelles par la voie de demandes de coopération volontaire (enquête reposant sur une action volontaire)

a) Base juridique

Mis à part les moyens de contrainte, les informations personnelles sont obtenues soit d'une source librement accessible, soit sur la base d'une divulgation volontaire, notamment de la part des opérateurs économiques détenant ces informations.

En ce qui concerne ce dernier point, l'article 197, paragraphe 2, du code de procédure pénale habilite le ministère public et la police judiciaire à soumettre des «demandes écrites de renseignements sur des matières relevant de l'enquête» (appelées «fiches de renseignements»). En vertu du code de procédure pénale, les personnes sollicitées sont invitées à communiquer les informations aux autorités enquêtrices. Toutefois, il n'y a aucun moyen de contrainte si les administrations, ou les organisations publiques et/ou privées, destinataires de la demande de renseignements refusent d'y donner suite. Si elles ne répondent pas à une telle demande, aucune sanction pénale ou autre ne peut être infligée. Si elles estiment que les renseignements demandés sont indispensables, les autorités enquêtrices devront les obtenir par voie de perquisition et de saisie sur la base d'un mandat émis par une juridiction.

Compte tenu de la prise de conscience croissante par les individus de leur droit à la vie privée, ainsi que de la charge de travail causée par ces demandes, les opérateurs économiques sont de plus en plus prudents dans leurs réponses à ces demandes ([11]). Lorsqu'ils décident de coopérer, les opérateurs économiques tiennent compte, en particulier, de la nature des renseignements demandés, de leur relation avec la personne dont les informations sont en jeu, des risques pour leur réputation, des risques de contentieux, etc.

b) Limitations

Comme la collecte par voie de contrainte d'informations électroniques, l'enquête fondée sur une action volontaire est elle aussi limitée par la Constitution, telle qu'interprétée dans la jurisprudence, et par la législation organique. En outre, les opérateurs économiques ne sont pas autorisés, légalement, à divulguer des informations dans certaines situations. Enfin, l'APPIHAO prévoit un certain nombre de limitations applicables tant à la collecte des informations qu'à leur traitement (tandis que les arrêtés municipaux reproduisent pour l'essentiel les mêmes critères pour la police préfectorale).

1) Limitations découlant de la Constitution et de la législation organique

Prenant en considération la finalité de l'article 13 de la Constitution, la Cour suprême a imposé, dans deux décisions du 24 décembre 1969 [1965 (A) n° 1187] et du 15 avril 2008 [2007 (A) n° 839], des limites aux enquêtes reposant sur une action volontaire menées par les autorités enquêtrices. Alors que ces décisions concernaient des cas dans lesquels des informations personnelles (sous forme d'images) étaient recueillies au moyen de photographies/prises de vues, les conclusions sont pertinentes pour les enquêtes fondées sur une action volontaire (non contraignantes) qui interfèrent avec la vie privée d'une personne en général. Par conséquent, elles s'appliquent, et doivent être respectées, en ce qui concerne la collecte d'informations personnelles par la voie d'une enquête sur la base d'une action volontaire, compte tenu des circonstances propres à chaque cas.

Selon ces décisions, la légalité de l'enquête fondée sur une action volontaire dépend du respect de trois critères, à savoir:

— «suspicion d'une infraction» (c'est-à-dire qu'il faut évaluer si une infraction a été commise),

— «nécessité d'une enquête» (c'est-à-dire qu'il faut évaluer si la demande reste dans le cadre de ce qui est nécessaire aux fins de l'enquête), et

([11]) Voir aussi la notification de l'Agence nationale de police du 7 décembre 1999 (voir ci-après, p. 9), qui cite ce même point.

— «caractère approprié des méthodes» (c'est-à-dire qu'il faut évaluer si l'enquête fondée sur une action volontaire est «appropriée» ou raisonnable pour la réalisation de l'objectif de l'enquête) ([12]).

En général, compte tenu des trois critères susmentionnés, la légalité de l'enquête fondée sur une action volontaire est jugée du point de vue de la question de savoir si ladite enquête peut être considérée comme raisonnable au regard des conventions socialement acceptées.

En outre, l'exigence du caractère «nécessaire» de l'enquête découle directement de l'article 197 du code de procédure pénale, et a été confirmée dans les instructions adressées par l'Agence nationale de police (NPA) à la police préfectorale en ce qui concerne l'utilisation des «fiches de renseignements». La notification de la NPA du 7 décembre 1999 prévoit un certain nombre de limitations procédurales, notamment l'obligation de n'utiliser les «fiches de renseignements» que si cela est nécessaire aux fins de l'enquête. Par ailleurs, l'article 197, paragraphe 1, du code de procédure pénale se limite aux enquêtes pénales et ne peut donc être appliqué qu'en cas de suspicion concrète d'une infraction déjà commise. À l'inverse, cette base juridique n'est pas applicable pour la collecte et l'utilisation d'informations personnelles lorsqu'aucune violation de la loi n'a encore eu lieu.

2) Limitations concernant certains opérateurs économiques

Des limitations supplémentaires s'appliquent dans certains domaines sur la base des protections prévues par d'autres lois.

Tout d'abord, les autorités enquêtrices ainsi que les entreprises de télécommunications détenant des informations personnelles ont le devoir de respecter le secret des communications tel qu'il est garanti par l'article 21, deuxième alinéa, de la Constitution ([13]). En outre, les entreprises de télécommunications sont soumises au même devoir en vertu de l'article 4 de la loi sur les activités de télécommunications ([14]). Aux termes des «lignes directrices sur la protection des informations personnelles dans le secteur des télécommunications», émises par le ministère de l'intérieur et des communications (MIC) sur la base de la Constitution et de la loi sur les activités de télécommunications, lorsque le secret des communications est en jeu, les entreprises de télécommunications ne doivent pas divulguer à des tiers d'informations personnelles concernant le secret des communications, sauf si elles ont obtenu le consentement de l'intéressé ou si elles peuvent invoquer l'un des «motifs justifiables» pour ne pas se conformer aux dispositions du code pénal. En ce qui concerne ces motifs, il s'agit des «actes justifiables» (article 35 du code pénal), de l'«autodéfense» (article 36 du code pénal) et de la «prévention d'un danger immédiat» (article 37 du code pénal). Les «actes justifiables» au regard du code pénal désignent uniquement les actes d'une entreprise de télécommunications par lesquels cette dernière se conforme aux mesures de contrainte de l'État, ce qui exclut les enquêtes fondées sur une action volontaire. Par conséquent, si les autorités enquêtrices demandent des informations personnelles sur la base d'une «fiche de renseignements» (article 197, paragraphe 2, du code de procédure pénale), il est interdit à une entreprise de télécommunications de divulguer les données.

Ensuite, les opérateurs économiques sont tenus de refuser les demandes de coopération volontaire lorsque la loi leur interdit de divulguer des informations personnelles. À titre d'exemple, cela inclut les cas dans lesquels l'opérateur a le devoir de respecter la confidentialité des informations, par exemple en vertu de l'article 134 du code pénal ([15]).

3) Limitations fondées sur l'APPIHAO

En ce qui concerne la collecte et le traitement ultérieur d'informations personnelles par des instances administratives, l'APPIHAO prévoit des limitations comme expliqué ci-dessus au point II.A.1) b) 2). Des limitations équivalentes découlent des arrêtés préfectoraux applicables à la police préfectorale.

B) Contrôle

1) Contrôle judiciaire

La collecte d'informations à caractère personnel par des moyens de contrainte doit se faire sur la base d'un mandat ([16]) et donner lieu dès lors à un contrôle préalable par un juge. Si l'enquête était illicite, un juge peut exclure de telles preuves lorsque l'affaire est jugée au pénal. Une personne peut demander une telle exclusion dans son procès pénal en faisant valoir que l'enquête pénale était illicite.

([12]) La gravité de l'infraction et l'urgence sont des facteurs pertinents pour évaluer le «caractère approprié des méthodes».

([13]) L'article 21, deuxième alinéa, de la Constitution dispose ce qui suit: «Il n'existe ni censure, ni violation du secret des moyens de communication.»

([14]) L'article 4 de la loi sur les activités de télécommunications prévoit ce qui suit: «1) Le secret des communications traitées par une entreprise de télécommunications ne peut être violé. 2) Toute personne qui exerce une activité dans les télécommunications s'abstient de divulguer les secrets portés à sa connaissance pendant la durée de ses fonctions en ce qui concerne les communications traitées par l'entreprise de télécommunications. Il en est de même après la cessation de ses fonctions.»

([15]) L'article 134 du code pénal dispose: «1) Lorsqu'un médecin, un pharmacien, un distributeur de produits pharmaceutiques, une sage-femme, un avocat, un conseil, un notaire ou toute autre personne ayant exercé une telle profession divulgue, sans motif justifiable, les informations confidentielles d'une autre personne qui ont été portées à sa connaissance dans le cadre de cette profession, une peine d'emprisonnement accompagnée de travaux d'une durée maximale de 6 mois ou une amende n'excédant pas 100 000 yens est infligée. 2) Il en va de même lorsqu'une personne qui exerce ou a exercé une activité religieuse divulgue, sans motif justifiable, des informations confidentielles d'une autre personne qui ont été portées à sa connaissance dans le cadre de ces activités religieuses.»

([16]) En ce qui concerne l'exception à cette règle, voir la note de bas de page n° 5.

2) Contrôle basé sur l'APPIHAO

Au Japon, le ministre ou chef de chaque ministère ou agence dispose de la compétence de contrôle et d'application basée sur l'APPIHAO, tandis que le ministre des affaires intérieures et des communications peut vérifier la bonne application de l'APPIHAO par l'ensemble des autres ministères.

Si le ministre des affaires intérieures et des communications – sur la base, par exemple, de l'enquête sur l'état d'avancement de l'application de l'APPIHAO ([17]), le traitement de plaintes ou de demandes adressées à l'un de ses centres d'information globale – le juge nécessaire, aux fins de réaliser l'objectif de l'APPIHAO, il peut demander au chef d'une instance administrative de soumettre des documents et des explications concernant le traitement d'informations personnelles par l'instance administrative en question, sur la base de l'article 50 de l'APPIHAO. Le ministre peut adresser des avis au chef de l'instance administrative concernant le traitement des informations personnelles dans ladite instance, s'il le juge nécessaire pour atteindre l'objectif du présent acte. En outre, le ministre peut, par exemple, demander une révision des mesures au moyen des mesures qu'il peut prendre en vertu des articles 50 et 51 de l'acte, dès lors que l'on soupçonne qu'une violation de l'acte ou une application inappropriée de ce dernier a eu lieu. Cela contribue à garantir l'application uniforme de l'APPIHAO et son respect.

3) Contrôle exercé par les commissions de sûreté publique en ce qui concerne la police

Pour ce qui est de l'administration de la police, l'Agence nationale de police (NPA) est soumise au contrôle de la commission nationale de sûreté publique, tandis que la police préfectorale est soumise au contrôle de l'une des commissions préfectorales de sûreté publique établies au sein de chaque préfecture. Chacune de ces instances de contrôle veille à la gestion démocratique et à la neutralité politique de l'administration de la police.

La commission nationale de sûreté publique est responsable des affaires qui relèvent de sa compétence en vertu de la loi sur la police et d'autres législations. En font notamment partie la nomination du commissaire général de la police nationale et des hauts responsables locaux de la police, ainsi que l'élaboration de politiques globales qui définissent des orientations ou mesures de base relatives à l'administration de la police nationale.

Les commissions préfectorales de sûreté publique sont composées de membres représentant la population dans chaque préfecture sur la base de la loi sur la police; elles gèrent la police préfectorale en tant que système de conseil indépendant. Leurs membres sont nommés par le gouverneur préfectoral avec le consentement de l'assemblée préfectorale, sur la base de l'article 39 de la loi sur la police. Disposant d'un mandat de trois ans, ils ne peuvent être démis de leurs fonctions contre leur gré que pour l'une des raisons particulières énumérées dans la loi (telles que l'incapacité d'exercer leurs fonctions, le non-respect de leurs obligations, un comportement répréhensible, etc.), ce qui assure leur indépendance (voir articles 40 et 41 de la loi sur la police). De plus, afin de garantir leur neutralité politique, l'article 42 de la loi sur la police interdit à un membre de la commission, concurremment à l'exercice de sa fonction, d'être membre d'une instance législative, de devenir membre exécutif d'un parti politique ou de tout autre organe politique, ou encore de participer activement à des mouvements politiques. Si chaque commission relève de la compétence de son gouverneur préfectoral, cela n'empêche en rien une autorité quelconque du gouverneur de donner des instructions relatives à l'exercice de ses fonctions.

Conformément à l'article 38, paragraphe 3, en liaison avec l'article 2 et l'article 36, paragraphe 2, de la loi sur la police, les commissions préfectorales de sûreté publique sont chargées de «la protection des droits et de la liberté d'un individu». À cet effet, elles reçoivent des rapports des chefs de la police préfectorale concernant les activités relevant de leur juridiction, y compris à l'occasion de réunions périodiques tenues trois à quatre fois par mois. Les commissions fournissent des orientations concernant ces questions en élaborant des stratégies globales.

De plus, dans le cadre de l'exercice de leur fonction de contrôle, les commissions préfectorales de sûreté publique peuvent donner à la police préfectorale des orientations dans des affaires individuelles concrètes, lorsqu'elles le jugent nécessaire dans le contexte d'une inspection des activités de la police préfectorale ou en cas de comportement répréhensible de son personnel. Les commissions peuvent, en outre, lorsqu'elles le jugent nécessaire, charger un commissaire spécialement désigné de faire le point sur l'avancement de la mise en œuvre de l'orientation donnée (article 43, paragraphe 2, de la loi sur la police).

([17]) Afin de garantir la transparence et de faciliter le contrôle par le ministère des affaires intérieures et des communications, il est demandé au chef d'une instance administrative, conformément à l'article 11 de l'APPIHAO, d'enregistrer chaque article prescrit à l'article 10, paragraphe 1, de l'APPIHAO, comme le nom de l'instance administrative qui conserve le dossier, la finalité de ce dossier, la méthode de collecte des informations à caractère personnel, etc. (le «registre des fichiers d'informations à caractère personnel»). Toutefois, les fichiers d'informations qui relèvent de l'article 10, paragraphe 2, de l'APPIHAO, dont ceux préparés ou obtenus dans le cadre d'une enquête pénale ou concernant des questions relatives à la sécurité nationale, sont exemptés de l'obligation d'en informer le ministère des affaires intérieures et des communications et de les inclure dans le registre public. Toutefois, conformément à l'article 7 du Public Records and Archives Management Act, le chef d'une instance administrative est toujours tenu d'enregistrer le numéro de classement, le titre, la durée de conservation et le lieu de stockage, etc. des documents administratifs («registre de gestion des fichiers de documents administratifs»). L'index des informations des deux registres est publié sur internet et permet aux personnes de vérifier le type d'informations à caractère personnel contenues dans le fichier et de savoir quelle instance administrative conserve les informations.

4) Contrôle par la Diète

La Diète peut mener des enquêtes en rapport avec les activités des autorités publiques et demander à cette fin la production de documents et le témoignage de témoins (article 62 de la Constitution). Dans ce contexte, la commission compétente de la Diète peut examiner le caractère approprié des activités de collecte d'informations menées par la police.

Ces pouvoirs sont précisés plus en détail dans le règlement de la Diète. Conformément à l'article 104, la Diète peut demander au gouvernement et aux agences publiques de produire les rapports et les enregistrements nécessaires à des fins d'enquête. En outre, les membres de la Diète peuvent soumettre des «questions écrites» en vertu de l'article 74 du règlement de la Diète. De telles questions doivent être approuvées par le président de la Chambre des représentants et, en principe, recevoir une réponse écrite de la part du gouvernement dans les sept jours (en cas d'impossibilité de répondre dans ce délai, une justification doit être apportée et un nouveau délai fixé, article 75 du règlement de la Diète). Par le passé, des questions écrites rédigées par la Diète ont également porté sur le traitement, par l'administration, d'informations à caractère personnel ([18]).

C) Recours individuel

En vertu de l'article 32 de la Constitution japonaise, nul ne peut se voir refuser le droit de recours devant les tribunaux. En outre, l'article 17 de la Constitution garantit que toute personne qui a subi un dommage du fait d'un acte illégal d'un fonctionnaire a la faculté d'en demander réparation auprès de l'État ou d'une personne morale publique, dans les conditions prévues par la loi.

1) Recours en justice contre la collecte obligatoire d'informations sur la base d'un mandat (article 430 du code de procédure pénale)

Conformément à l'article 430, paragraphe 2, du code de procédure pénale, une personne mécontente des mesures prises par un fonctionnaire de police concernant la saisie d'articles (y compris lorsque ceux-ci contiennent des informations à caractère personnel) sur la base d'un mandat peut présenter une demande (ou «quasi-plainte») auprès de la juridiction compétente en vue de «l'annulation ou de la modification» de ces mesures.

Un tel recours peut être déposé sans que la personne n'ait à attendre la conclusion de l'affaire. Si la juridiction estime que la saisie n'était pas nécessaire, ou qu'il existe d'autres raisons pour considérer cette saisie illégitime, elle peut ordonner que de telles mesures soient annulées ou modifiées.

2) Recours en justice en vertu du code de procédure pénale et de la loi sur les recours auprès de l'État

Si des personnes considèrent que leur droit au respect de la vie privée au sens de l'article 13 de la Constitution a été violé, elles peuvent porter plainte au civil en demandant la suppression d'informations à caractère personnel collectées dans le cadre d'une enquête pénale.

Une personne peut également intenter une action en réparation en vertu de la loi sur les recours auprès de l'État, en liaison avec les articles correspondants du code civil si elle considère que son droit au respect de la vie privée a été enfreint et qu'elle a subi un préjudice en raison de la collecte d'informations à caractère personnel la concernant ou d'une surveillance dont elle a fait l'objet ([19]). Étant donné que le «préjudice» qui fait l'objet d'une demande en réparation ne se limite pas au seul préjudice matériel (article 710 du code civil), il peut aussi englober la «souffrance morale». Le montant de l'indemnisation correspondant à une telle souffrance morale sera estimé par le juge sur la base d'une «libre appréciation tenant compte de divers facteurs dans chaque affaire» ([20]).

L'article 1er, paragraphe 1, de la loi sur les recours auprès de l'État accorde un droit à réparation lorsque i) le fonctionnaire qui exerce l'autorité publique de l'État ou d'une entité publique a, ii) dans l'exercice de ses fonctions, iii) intentionnellement ou par négligence, iv) en agissant illicitement, v) porté préjudice à une autre personne.

La personne peut intenter une action conformément au code de procédure civil. Conformément aux règles applicables, elle peut l'intenter auprès de la juridiction compétente du lieu où le tort a été commis.

([18]) Voir, par exemple, la question écrite de la Chambre des conseillers nº 92 du 27 mars 2009 concernant le traitement des informations collectées dans le contexte des enquêtes pénales, y compris les violations des obligations de confidentialité par la police et les autorités chargées des poursuites.

([19]) On trouve un exemple d'une telle action dans «l'affaire de la liste de l'Agence de la défense» [tribunal du district de Niigata, décision du 11 mai 2006 (2002(Wa) nº 514)]. Dans cette affaire, un fonctionnaire de l'Agence de la défense avait préparé, conservé et distribué une liste des personnes qui avaient introduit des demandes de divulgation de documents administratifs auprès de ladite agence. Cette liste comportait des descriptions d'informations à caractère personnel concernant le plaignant. Insistant sur le fait que son droit au respect de la vie privée, son droit de connaître, etc. avaient été violés, ce dernier a mis en demeure la défenderesse de lui verser une indemnité en réparation des préjudices subis en vertu de l'article 1er, paragraphe 1, de la loi sur les recours auprès de l'État. La Cour a fait droit en partie à ladite demande en accordant au plaignant une indemnisation partielle.

([20]) Cour suprême, décision du 5 avril 1910 [1910(O) nº 71].

3) Recours à titre individuel contre les enquêtes illicites/abusives menées par la police: plainte auprès de la commission préfectorale de sûreté publique (article 79 de la loi sur la police)

Conformément à l'article 79 de la loi sur la police ([21]), comme précisé de manière encore plus détaillée dans une instruction du chef de la police nationale à la police préfectorale et aux commissions préfectorales de sûreté publique ([22]), des personnes peuvent déposer une plainte par écrit ([23]) auprès de la commission préfectorale de sûreté publique compétente contre tout comportement illégal ou inadéquat d'un fonctionnaire de police dans l'exercice de ses fonctions, ce qui englobe notamment ses obligations en matière de collecte et d'utilisation d'informations à caractère personnel. La Commission traitera ces plaintes loyalement, dans le respect des lois et des arrêtés municipaux, et informera le plaignant par écrit du résultat de l'enquête.

Sur la base de l'autorité qui lui incombe en matière de contrôle, conformément à l'article 38, paragraphe 3, de la loi sur la police, la commission préfectorale de sûreté publique donne pour instruction à la police préfectorale d'instruire les faits et d'appliquer les mesures nécessaires en fonction du résultat de l'examen, puis de rendre compte des résultats à ladite commission. Lorsqu'elle l'estime nécessaire, la commission peut aussi donner une instruction concernant le traitement de la plainte, par exemple si elle estime insuffisante l'enquête menée par la police. Cette mise en œuvre est décrite dans la note adressée par l'Agence nationale de police aux chefs de la police préfectorale.

La notification au plaignant du résultat de l'enquête tient également compte des rapports de la police concernant l'enquête et des mesures prises à la demande de la commission.

4) Recours à titre individuel prévu par l'APPIHAO et le code de procédure pénale

a) APPIHAO

En vertu de l'article 48 de l'APPIHAO, les instances administratives sont tenues de s'efforcer de traiter de manière appropriée et sans délai les plaintes portant sur le traitement des informations à caractère personnel. Afin de fournir des informations consolidées aux personnes (par ex. sur le droit à la divulgation, le droit de rectification ou le droit à la suspension de l'utilisation en vertu de l'APPIHAO), le ministère des affaires intérieures et de la communication a mis en place des centres d'information globale sur la divulgation des informations et la protection des informations à caractère personnel dans chaque préfecture, en vertu de l'article 47, paragraphe 2, de l'APPIHAO. Des demandes de renseignements peuvent également être adressées par des non-résidents. À titre d'exemple, au cours de l'exercice 2017 (d'avril 2017 à mars 2018), on a recensé 5186 cas au total dans lesquels les centres d'information globale ont répondu à de telles demandes, etc.

Les articles 12 et 27 de l'APPIHAO accordent aux personnes qui le souhaitent le droit de demander la divulgation et la correction d'informations à caractère personnel conservées. De plus, conformément à l'article 36 de l'APPIHAO, des personnes peuvent demander la suspension de l'utilisation ou la suppression de leurs informations à caractère personnel conservées lorsque l'instance administrative n'a pas obtenu légalement lesdites données ou les utilise en violation de la loi.

Toutefois, pour ce qui est des informations à caractère personnel collectées (soit sur la base d'un mandat, soit au moyen d'une «demande de renseignements») et conservées dans le cadre d'enquêtes pénales ([24]), ces informations rentrent généralement dans la catégorie des «informations à caractère personnel figurant dans des documents relatifs à des procès et à des biens saisis». Ces informations à caractère personnel sont donc exclues du champ d'application des droits individuels du chapitre IV de l'APPIHAO, conformément à l'article 53, paragraphe 2, du code de procédure pénale ([25]). Le traitement de telles informations à caractère personnel et les droits d'accès et de correction des personnes sont par contre soumis à des règles spéciales en vertu du code de procédure pénale et de la loi sur les dossiers des

([21]) Article 79 de la loi sur la police (extrait):
1. Quiconque souhaite déposer une plainte contre le personnel de la police préfectorale pour l'exercice, par celui-ci, de ses fonctions peut déposer une plainte par écrit auprès de la commission préfectorale de sûreté publique au moyen de la procédure prescrite dans l'arrêté de la commission nationale de sûreté publique.
2. La commission préfectorale de sûreté publique qui a reçu une plainte telle que prévue au précédent paragraphe la traitera loyalement, dans le respect des lois et des arrêtés municipaux, et informera le plaignant par écrit de son résultat, sauf dans les cas suivants:
   1) La plainte peut être considérée comme avoir été portée dans le but de faire obstruction à l'exercice légitime des fonctions de la police préfectorale;
   2) La résidence actuelle du plaignant est inconnue;
   3) La plainte peut être considérée comme avoir été portée conjointement avec d'autres plaignants ayant déjà été informés du résultat de leur plainte conjointe.

([22]) Agence nationale de police, note sur la marche à suivre pour le traitement des plaintes relatives à l'exercice de leurs fonctions par les agents de police, 13 avril 2001, assortie de l'annexe 1 «Normes pour l'interprétation et la mise en œuvre de l'article 79 de la loi sur la police».

([23]) Selon la note de l'Agence nationale de police (voir note de bas de page précédente), les personnes ayant des difficultés à formuler une plainte par écrit doivent bénéficier d'une assistance. Cela inclut expressément les ressortissants étrangers.

([24]) Par contre, certains documents ne figurent pas dans la catégorie des «documents relatifs à des procès», n'étant pas eux-mêmes des informations obtenues par un mandat ni par des demandes de renseignements écrites en matière d'enquête, mais ayant été créés sur la base de tels documents. Tel serait le cas d'informations privées ne relevant pas de l'article 45, paragraphe 1, de l'APPIHAO, ces informations n'étant dès lors pas exclues de l'application du chapitre IV de l'APPIHAO.

([25]) L'article 53, paragraphe 2, 2e alinéa, du code de procédure pénale prévoit que les dispositions du chapitre IV of the APPIHAO ne s'appliquent pas aux informations à caractère personnel figurant dans des documents relatifs à des procès et à des biens saisis.

affaires pénales closes (voir ci-dessous) ([26]). Cette exclusion est justifiée par divers facteurs, tels que la protection de la vie privée des personnes concernées, le secret de l'enquête et le bon déroulement du procès pénal. Cela dit, les dispositions du chapitre II de l'APPIHAO qui régissent les principes inhérents au traitement de telles informations demeurent applicables.

b) Code de procédure pénale

En vertu du code de procédure pénale, les possibilités d'accès aux informations à caractère personnel collectées aux fins d'une enquête pénale dépendent à la fois du stade de la procédure et du rôle des personnes dans l'enquête (suspect, accusé, victime, etc.).

Par exception à la règle énoncée à l'article 47 du code de procédure pénale, qui dispose que les documents ayant trait à un procès ne doivent pas être rendus publics avant le commencement dudit procès (car cela pourrait constituer une atteinte à l'honneur et/ou à la vie privée des personnes concernées et entraver l'enquête/le procès), la consultation de ces informations par la victime d'un délit est en principe autorisée, dans la mesure où cette consultation est jugée raisonnable, compte tenu de l'objet de la disposition figurant à l'article 47 du code ([27]).

En ce qui concerne les suspects, ils apprennent généralement qu'ils sont mis en cause dans le cadre d'une enquête pénale en étant interrogés, soit par la police judiciaire, soit par un procureur. Si le procureur décide par la suite de ne pas ouvrir de poursuites, il en informe rapidement le suspect à sa demande (article 259 du code de procédure pénale).

En outre, après l'ouverture de poursuites, le procureur donne à l'accusé ou à son conseil l'occasion de consulter les preuves à l'avance avant de demander leur examen par la Cour (article 299 du code de procédure pénale). Cela permet à l'accusé de vérifier ses informations à caractère personnel collectées dans le cadre d'une enquête pénale.

Enfin, la protection des informations à caractère personnel collectées dans le cadre d'une enquête pénale, qu'elles concernent un suspect, l'accusé ou toute autre personne (comme la victime d'un délit, par exemple), est garantie par l'obligation de confidentialité (article 100 de la loi sur le service public national) et par la menace d'une sanction en cas de fuite d'informations à caractère personnel traitées dans l'exercice de missions publiques [article 109 (xii) de la loi sur le service public national].

5) Recours individuel contre les enquêtes illicites/injustifiées d'autorités publiques: plainte auprès de la PPC

Conformément à l'article 6 de l'APPI, le gouvernement prend, en concertation avec les gouvernements de pays tiers, les mesures nécessaires pour bâtir un système concernant les informations à caractère personnel qui soit compatible avec les normes internationales, en promouvant la coopération avec les organisations internationales et d'autres cadres internationaux. Sur le fondement de cette disposition, la politique de base relative à la protection des informations à caractère personnel (adoptée par décision du cabinet) délègue à la PPC, en sa qualité d'autorité chargée de l'application générale de l'APPI, le pouvoir de prendre les mesures nécessaires pour combler les divergences entre les systèmes et opérations du Japon et ceux du pays étranger concerné, de manière à garantir le traitement approprié des informations à caractère personnel reçues de ce pays.

En outre, comme le prévoit l'article 61, points i) et ii), de l'APPI, la PPC est chargée de formuler et de promouvoir une politique de base, ainsi que d'assurer la médiation concernant les plaintes déposées contre des opérateurs économiques. Enfin, les organes administratifs communiquent et coopèrent étroitement (article 80 de l'APPI).

Sur la base de ces dispositions, la PPC traitera les plaintes déposées par les particuliers comme suit:

a) Quiconque soupçonne que ses données transférées depuis l'UE ont été collectées ou utilisées par les autorités publiques japonaises, y compris les autorités responsables des activités visées aux chapitres II et III de la présente déclaration, en violation des règles applicables, et notamment celles soumises à ladite déclaration, peut déposer plainte auprès de la PPC (personnellement ou par l'intermédiaire de son APD);

b) La PPC traite la plainte, en faisant notamment usage des pouvoirs qui lui sont conférés en vertu de l'article 6, de l'article 61, point ii), et de l'article 80 de l'APPI, et en informe les autorités publiques compétentes, y compris les organismes de surveillance compétents.

([26]) En vertu du code de procédure pénale et de la loi sur les dossiers des affaires pénales closes, l'accès aux biens saisis et aux documents et informations à caractère personnel concernant des procès pénaux et leur correction sont soumis à un système unique et distinct de dispositions qui vise à protéger la vie privée des personnes concernées, le secret de l'enquête et le bon déroulement du procès pénal, etc.

([27]) Plus précisément, la consultation d'informations relatives à des preuves objectives est en principe autorisée pour des victimes de délits en ce qui concerne les dossiers d'absence de poursuite pour les affaires donnant lieu à la participation des victimes, comme stipulé à l'article 316, paragraphe 33, du code de procédure pénale, afin de rendre plus satisfaisante la protection des victimes de délits.

Ces autorités sont tenues de coopérer avec la PPC en vertu de l'article 80 de l'APPI, notamment en fournissant les informations nécessaires et les éléments utiles pour permettre à la PPC de déterminer si la collecte ou l'utilisation ultérieure des informations à caractère personnel a eu lieu dans le respect des règles applicables. Dans le cadre de son évaluation, la PPC coopérera avec le MIC;

c) Si l'évaluation montre que les règles applicables n'ont pas été respectées, la coopération entre les autorités publiques concernées et la PPC suppose l'obligation de mettre fin à l'infraction.

Cela inclut la suppression des données à caractère personnel collectées de manière illicite au titre des règles applicables.

En cas d'infraction aux règles applicables, la PPC confirmera également, avant de conclure l'évaluation, que des mesures ont été prises pour remédier intégralement à l'infraction;

d) Après la conclusion de l'évaluation, la PPC informe la personne, dans un délai raisonnable, du résultat de l'évaluation, et notamment des éventuelles mesures correctives qui ont été prises. Dans le cadre de cette notification, la PPC informe également la personne de la possibilité de demander confirmation du résultat auprès de l'autorité publique compétente et lui indique l'autorité à laquelle adresser une telle demande.

L'accès aux détails du résultat de l'évaluation peut être limité s'il existe des motifs raisonnables de penser que la communication de ces informations est de nature à porter préjudice à l'enquête en cours.

Lorsque la plainte concerne la collecte ou l'utilisation de données à caractère personnel dans le domaine répressif, la PPC informe la personne, dans le cas où l'évaluation révèle que des informations à caractère personnel la concernant ont été utilisées dans le cadre d'une affaire et que celle-ci est close, que le dossier peut être consulté en vertu de l'article 53 du code de procédure pénale et de l'article 4 de la loi sur les dossiers des affaires pénales closes.

Lorsque l'évaluation révèle qu'une personne est suspectée dans une affaire pénale, la PPC l'en informera et l'informera de la possibilité de présenter une demande en vertu de l'article 259 du code de procédure pénale;

e) Si une personne demeure insatisfaite du résultat de cette procédure, elle peut s'adresser à la PPC, qui l'informera des différentes possibilités et procédures détaillées pour obtenir réparation en vertu des lois et réglementations japonaises. La PPC viendra en aide à la personne, notamment en lui prodiguant conseil et assistance, pour engager une éventuelle action supplémentaire auprès de l'instance administrative ou judiciaire compétente.

III. **Accès des pouvoirs publics à des fins de sécurité nationale**

A. Bases juridiques et limitations de la collecte d'informations à caractère personnel

1) Bases juridiques de la collecte d'informations par le ministère ou l'agence concernés

Comme indiqué ci-dessus, la collecte d'informations à caractère personnel à des fins de sécurité nationale par des organes administratifs doit relever de leur compétence administrative.

Au Japon, aucune loi ne permet la collecte d'informations par des moyens obligatoires aux seules fins de la sécurité nationale. Conformément à l'article 35 de la Constitution, il n'est possible de recueillir des informations à caractère personnel par la contrainte que sur la base d'un mandat délivré par un tribunal dans le cadre d'une enquête sur une infraction. Ce type de mandat ne peut donc être émis qu'aux fins d'une enquête pénale. En d'autres termes, la collecte d'informations ou l'accès à des informations par des moyens obligatoires pour des raisons de sécurité nationale ne sont pas autorisés dans l'ordre juridique japonais. Au contraire, dans le domaine de la sécurité nationale, les ministères ou agences concernés ne peuvent obtenir des informations que de sources librement accessibles, ou recevoir des informations d'opérateurs économiques ou de particuliers par divulgation volontaire. Les opérateurs économiques qui reçoivent une demande de coopération volontaire n'ont aucune obligation légale de fournir ces informations et ne subissent dès lors aucune conséquence négative s'ils refusent de coopérer.

Un certain nombre de départements et d'agences ministériels exercent des responsabilités dans le domaine de la sécurité nationale.

(1) Secrétariat du cabinet

Le secrétariat du cabinet procède à la collecte et à la recherche d'informations concernant les politiques importantes du cabinet ([28]), prescrites à l'article 12-2 de la loi du cabinet ([29]). Toutefois, le secrétariat du cabinet n'est pas habilité à recueillir des informations à caractère personnel directement auprès des opérateurs économiques. Il recueille, incorpore, analyse et évalue les informations provenant de sources ouvertes, d'autres autorités publiques, etc.

(2) NPA/police préfectorale

Dans chaque préfecture, la police préfectorale est habilitée, en vertu de l'article 2 de la loi sur la police, à recueillir des informations relevant de sa compétence. Il peut arriver que la NPA recueille directement les informations relevant de sa compétence en vertu de la loi sur la police. Cela concerne notamment les activités du bureau de sécurité de la NPA et du service des affaires étrangères et du renseignement. En vertu de l'article 24 de la loi sur la police, le bureau de sécurité est chargé des questions concernant la police de sécurité ([30]), et le service des affaires étrangères et du renseignement des affaires concernant les ressortissants étrangers ainsi que les ressortissants japonais dont les lieux d'activité se situent dans des pays étrangers.

(3) Agence de renseignement en matière de sécurité publique (PSIA)

L'application de la loi sur la prévention des activités subversives (SAPA) et de la loi sur le contrôle des organisations ayant commis des massacres collectifs aveugles (ACO) incombe principalement à l'Agence de renseignement en matière de sécurité publique (PSIA). Il s'agit d'une agence du ministère de la justice.

La SAPA et l'ACO prévoient que des dispositions administratives (c'est-à-dire des mesures ordonnant la limitation des activités de ces organisations, leur dissolution...) peuvent, dans des conditions strictes, être adoptées, en vertu de la Constitution, à l'égard d'organisations qui commettent certains actes graves («activité subversive terroriste» ou «acte de massacre collectif aveugle») portant atteinte à la «sécurité publique» ou au «système fondamental de la société». La SAPA porte sur les «activités subversives terroristes» (article 4, relatif aux activités telles que l'insurrection, l'agression étrangère, l'homicide à caractère politique...), tandis que l'ACO concerne les «actes de massacre collectif aveugle» (article 4). Seules les organisations précisément identifiées qui font peser des menaces internes ou externes spécifiques sur la sécurité publique peuvent faire l'objet de dispositions prises au titre de la SAPA ou de l'ACO.

À cette fin, la SAPA et l'ACO fournissent une base juridique en matière d'enquête. Les pouvoirs d'enquête fondamentaux des agents de la PSIA (PSIO) sont définis à l'article 27 de la SAPA et à l'article 29 de l'ACO. Les enquêtes décidées par la PSIA au titre de ces dispositions sont menées pour autant qu'elles soient nécessaires au regard des dispositions précitées en matière de contrôle d'organisations (des groupes radicaux d'extrême gauche, la secte Aum Shinrikyo et certains groupes nationaux étroitement liés à la Corée du Nord ont, par exemple, déjà fait l'objet d'enquêtes). Toutefois, le recours à des moyens obligatoires dans le cadre de ces enquêtes est interdit; une organisation détenant des informations à caractère personnel ne peut dès lors être contrainte de fournir ces informations.

La collecte et l'utilisation des informations divulguées à la PSIA sur une base volontaire sont soumises aux garanties et limitations prévues par la loi, notamment le secret des communications garanti par la Constitution et les règles relatives au traitement des informations à caractère personnel prévues par l'APPIHAO.

(4) Ministère de la défense (MOD)

En ce qui concerne la collecte d'informations, le MOD recueille des informations sur la base des articles 3 et 4 de la loi portant création du ministère de la défense dans la mesure nécessaire à l'exercice de sa compétence administrative, notamment en ce qui concerne la défense et la protection, les mesures à prendre par les forces d'autodéfense ainsi que le déploiement des forces terrestres, maritimes et aériennes d'autodéfense. Le MOD ne peut recueillir des informations à ces fins que de sources librement accessibles et dans le cadre d'une coopération volontaire. Il ne recueille pas d'informations sur le grand public.

2) Limitations et garanties

a) Limitations légales

(1) Limitations générales fondées sur l'APPIHAO

L'APPIHAO est une loi générale qui s'applique à la collecte et au traitement des informations à caractère personnel par les organes administratifs, dans tout domaine d'activité de ces organes. Par conséquent, les limitations et garanties décrites à la section II.A.1) b) (2) s'appliquent également à la conservation, au stockage et à l'utilisation d'informations à caractère personnel dans le domaine de la sécurité nationale.

([28]) Dirigé par le bureau d'analyse et de renseignement du gouvernement (Cabinet Intelligence and Research Office), sur la base de l'article 4 du décret portant organisation du secrétariat du cabinet.

([29]) Cela comprend «la collecte et la recherche de renseignements concernant des politiques importantes du cabinet».

([30]) La police de sécurité est responsable des activités de contrôle de la criminalité liées à la sécurité publique et à l'intérêt de la nation. Il s'agit notamment du contrôle de la criminalité et de la collecte d'informations sur les actes illégaux liés à des groupes d'extrême gauche ou d'extrême droite et à des activités préjudiciables au Japon.

(2) Limitations particulières applicables à la police (NPA et police préfectorale)

Ainsi que le précise plus haut la section consacrée à la collecte d'informations à des fins répressives, la police ne peut recueillir que des informations qui relèvent de sa compétence, en agissant, conformément à l'article 2, paragraphe 2, de la loi sur la police, dans une mesure «strictement limitée» aux activités nécessaires à l'accomplissement de sa mission et «avec impartialité, avec neutralité, sans préjugé et avec équité». En outre, elle «ne doit jamais abuser de ses pouvoirs d'une manière qui interfère avec les droits et libertés d'une personne garantis par la Constitution du Japon».

(3) Limitations spécifiques applicables à la PSIA

Les articles 3 de la SAPA et de l'ACO disposent tous deux que les enquêtes menées au titre de ces actes se limitent au strict nécessaire pour parvenir à l'objectif poursuivi et ne restreignent pas de manière injustifiée les droits fondamentaux de l'homme. En outre, conformément à l'article 45 de la SAPA et à l'article 42 de l'ACO, tout abus d'autorité d'un agent de la PSIA constitue un crime passible de sanctions pénales plus lourdes que dans le cas d'un abus «général» d'autorité commis dans d'autres domaines du secteur public.

(4) Limitations spécifiques applicables au MOD

En ce qui concerne la collecte d'informations et son organisation par le MOD, l'article 4 de la loi portant création du ministère de la défense prévoit que l'activité de collecte d'informations du ministère se limite à ce qui est «nécessaire» pour mener à bien ses missions concernant 1) la défense et la protection, 2) les mesures à prendre par les forces d'autodéfense et 3) les organisations, les effectifs, la structure, l'équipement et le déploiement des forces terrestres, maritimes et aériennes d'autodéfense.

b) Autres limitations

Comme expliqué dans la section II.A.2) b) (1) relative aux enquêtes pénales, il découle de la jurisprudence de la Cour suprême que, pour pouvoir être adressée à un opérateur économique, une demande de coopération volontaire doit être nécessaire à l'enquête sur un délit présumé et être raisonnable aux fins de l'enquête.

Bien que la base juridique et la finalité des enquêtes effectuées par les services d'enquête en matière de sécurité nationale et celles réalisées par les services d'enquête en ce qui concerne l'application des lois soient différentes, les principes fondamentaux afférents à la «nécessité de l'enquête» et au «caractère adapté de la méthode utilisée» s'appliquent de la même manière dans le domaine de la sécurité nationale et doivent être respectés en tenant dûment compte des circonstances spécifiques de chaque cas.

La combinaison de ces limitations garantit que la collecte et le traitement des informations se font uniquement dans la mesure nécessaire à l'exécution des tâches spécifiques de l'autorité publique compétente et en fonction des menaces spécifiques. Cela exclut la collecte massive et indifférenciée ou l'accès à des informations à caractère personnel pour des raisons de sécurité nationale.

B. Surveillance

1) Surveillance au titre de l'APPIHAO

Comme expliqué au point II.B.2) ci-dessus, dans le secteur public japonais, le ministre ou le chef de chaque ministère ou agence est investi du pouvoir de surveiller et d'assurer le respect de l'APPIHAO au sein de son ministère ou de son agence. En outre, le ministre des affaires intérieures et des communications peut examiner l'état d'avancement de l'application de cette loi, demander à chaque ministre de fournir des documents et des explications sur la base des articles 49 et 50 de ladite loi et adresser des avis à chaque ministre sur la base de l'article 51 de ladite loi. Par exemple, il peut demander qu'il soit procédé à un réexamen des mesures au moyen des actions prévues aux articles 50 et 51 de ladite loi.

2) Contrôle de la police par les commissions de sûreté publique

Comme expliqué ci-dessus à la section «II. Collecte d'informations à des fins répressives», les commissions préfectorales indépendantes de sûreté publique supervisent les activités de la police préfectorale.

En ce qui concerne l'Agence nationale de police (NPA), les fonctions de surveillance sont exercées par la commission nationale de sécurité publique. En vertu de l'article 5 de la loi sur la police, cette commission est notamment responsable de «la protection des droits et de la liberté d'un individu». À cette fin, elle établit notamment des stratégies globales qui définissent les règles de gestion des affaires prescrites à chaque point de l'article 5, paragraphe 4, de la loi sur la police et définissent d'autres orientations ou mesures de base sur lesquelles il convient de se fonder pour la réalisation desdites activités. La commission nationale de sécurité publique jouit du même degré d'indépendance que les commissions de sûreté publique préfectorales.

3) Surveillance du ministère de la défense par le bureau de l'inspecteur général chargé du respect de la législation

Le bureau de l'inspecteur général chargé du respect de la législation est un bureau indépendant au sein du ministère de la défense qui est placé sous le contrôle direct du ministre de la défense en vertu de l'article 29 de la loi portant création du ministère de la défense. Le bureau de l'inspecteur général chargé du respect de la législation peut effectuer des inspections afin de vérifier le respect de la législation et de la réglementation par les fonctionnaires du ministère de la défense. Ces inspections sont appelées «inspections dans le domaine de la défense».

Le bureau de l'inspecteur général chargé du respect de la législation procède à des inspections en toute indépendance afin de garantir que la législation est respectée dans l'ensemble du ministère, y compris au sein des forces d'autodéfense. Il s'acquitte de ses missions indépendamment des services opérationnels du ministère de la défense. À la suite d'une inspection, le bureau de l'inspecteur général chargé du respect de la législation présente sans délai ses conclusions, ainsi que les mesures d'amélioration nécessaires, directement au ministre de la défense. Sur la base du rapport du bureau, le ministre de la défense peut ordonner la mise en œuvre des mesures nécessaires pour remédier à la situation. Le vice-ministre adjoint est chargé de la mise en œuvre de ces mesures et doit rendre compte au ministre de la défense sur l'état d'avancement de cette mise en œuvre.

En tant que mesure volontaire de transparence, les conclusions des inspections dans le domaine de la défense sont désormais publiées sur le site internet du ministère de la défense (bien que la loi ne l'exige pas).

Il existe trois catégories d'inspections dans le domaine de la défense:

i) les inspections régulières, qui sont effectuées périodiquement ([31]);

ii) les inspections dans le domaine de la défense à titre de vérifications, qui sont menées en vue de vérifier si des mesures d'amélioration ont été effectivement prises; et

iii) les inspections spéciales dans le domaine de la défense, qui sont menées dans le cadre de questions spécifiques ordonnées par le ministre de la défense.

Dans le cadre de ces inspections, l'inspecteur général peut demander des rapports au bureau concerné, demander la communication de documents, s'introduire sur des sites pour effectuer des inspections, demander des explications au vice-ministre adjoint, etc. Compte tenu de la nature de ses tâches d'inspection, le bureau de l'inspecteur général chargé du respect de la législation est dirigé par des experts juridiques de très haut rang (ancien procureur).

4) Surveillance de la PSIA

La PSIA procède à des inspections régulières et spéciales sur les activités de ses services et bureaux individuels (agence de renseignement en matière de sécurité publique, bureaux et services de renseignement en matière de sécurité publique, etc.). Aux fins de l'inspection régulière, un directeur général adjoint et/ou un directeur est désigné comme inspecteur. Ces inspections portent également sur la gestion des informations à caractère personnel.

5) Surveillance par la Diète

En ce qui concerne la collecte d'informations à des fins répressives, la Diète peut, par l'intermédiaire de sa commission compétente, examiner la légalité des activités de collecte d'informations dans le domaine de la sécurité nationale. Les pouvoirs d'enquête de la Diète sont fondés sur l'article 62 de la Constitution ainsi que sur les articles 74 et 104 du règlement de la Diète.

C. Recours individuel

Les voies de recours individuels sont les mêmes que dans le domaine de l'application du droit pénal et comprennent également le nouveau mécanisme de règlement des litiges, géré et contrôlé par le CPP, pour la gestion et le traitement des plaintes déposées par des citoyens de l'Union. À cet égard, veuillez consulter les passages pertinents de la section II.C.

En outre, il existe des voies de recours individuelles spécifiques dans le domaine de la sécurité nationale.

Les informations à caractère personnel recueillies par une instance administrative à des fins de sécurité nationale sont régies par les dispositions du chapitre 4 de l'APPIHAO. Cela inclut le droit de demander la divulgation (article 12) et la rectification (y compris l'ajout ou la suppression) (article 27) d'informations à caractère personnel conservées ainsi que le

([31]) On peut citer à titre d'exemple d'inspection portant sur les questions couvertes par la présente déclaration, l'inspection régulière de 2016 dans le domaine de la défense au sujet de la «sensibilisation/préparation au respect de la législation», étant donné que la protection des informations à caractère personnel était l'une des principales questions examinées dans le cadre de cette inspection. Plus précisément, cette inspection portait sur la situation de la gestion et du stockage, notamment, des informations à caractère personnel. Dans son rapport, le bureau de l'inspecteur général chargé du respect de la législation a relevé plusieurs dysfonctionnements dans la gestion des informations à caractère personnel auxquels il convient de remédier, comme l'absence de protection des données par un mot de passe. Le rapport peut être consulté sur le site internet du ministère de la défense.

droit de demander la suspension de l'utilisation des informations à caractère personnel dans le cas où l'instance administrative a obtenu les informations concernées de manière illicite (article 36). Cela étant, dans le domaine de la sécurité nationale, l'exercice de ces droits est soumis à certaines restrictions: les demandes de divulgation, de rectificatif ou de suspension ne sont pas acceptées lorsqu'elles concernent des «informations pour lesquelles le chef d'une instance administrative a des motifs raisonnables de penser que leur divulgation est susceptible de porter atteinte à la sécurité nationale, de causer un préjudice à la relation de confiance mutuelle avec un autre pays ou avec une organisation internationale, ou de causer un désavantage dans les négociations avec un autre pays ou une organisation internationale» [article 14, point iv)]. Par conséquent, les collectes volontaires d'informations relatives à la sécurité nationale ne relèvent pas toutes de cette dérogation, cette dernière nécessitant toujours une évaluation concrète des risques associés à leur divulgation.

En outre, si la demande est rejetée au motif que les informations concernées sont considérées comme non susceptibles de divulgation au sens de l'article 14, point iv), la personne peut introduire un recours administratif en vue d'obtenir un réexamen de cette décision, en affirmant par exemple que les conditions énoncées à l'article 14, point iv), ne sont pas remplies dans son cas. Dans ce cas, avant de prendre une décision, le chef de l'instance administrative concernée consulte le comité d'examen de la protection des informations à caractère personnel et de la divulgation des informations. Ce comité examinera le recours en toute indépendance. Il s'agit d'un organe hautement spécialisé et indépendant, dont les membres sont nommés par le premier ministre, avec l'accord des deux chambres de la Diète, parmi des personnes dotées d'une expertise exceptionnelle ([32]). Le comité dispose d'importants pouvoirs d'enquête, y compris la possibilité de demander la production de documents et la divulgation des informations à caractère personnel en question, de tenir des délibérations à huis clos et d'appliquer la procédure de l'index Vaughn ([33]). Il établit ensuite un rapport écrit qui est communiqué à la personne concernée ([34]). Les conclusions du rapport sont rendues publiques. Bien qu'officiellement, ces rapports ne soient pas juridiquement contraignants, l'instance administrative concernée se conforme à la quasi-totalité d'entre eux ([35]).

Enfin, conformément à l'article 3, paragraphe 3, de la loi sur les contentieux administratifs, une personne peut former un recours en vue d'obtenir la révocation de la décision prise par l'instance administrative de ne pas divulguer les informations à caractère personnel.

IV. **Examen périodique**

Dans le cadre de l'examen périodique de la décision d'adéquation, la PPC et la Commission européenne échangeront des informations sur le traitement des données dans les conditions définies dans le constat d'adéquation, y compris celles énumérées dans la présente déclaration.

([32]) Voir l'article 4 de la loi instaurant le comité d'examen de la protection des informations à caractère personnel et de la divulgation des informations.

([33]) Voir l'article 9 de la loi instaurant le comité d'examen de la protection des informations à caractère personnel et de la divulgation des informations.

([34]) Voir l'article 16 de la loi instaurant le comité d'examen de la protection des informations à caractère personnel et de la divulgation des informations.

([35]) Au cours des trois dernières années, il n'y a pas eu de précédent dans lequel l'instance administrative concernée a pris une décision différente des conclusions du comité. Si l'on remonte plus loin dans le temps, il n'y a eu que très peu de cas où cela s'est produit: seulement deux cas sur un total de 2 000 affaires depuis 2005 (l'année d'entrée en vigueur de l'APPIHAO). Lorsque l'instance administrative prend une décision qui diffère des conclusions du comité, elle en indique clairement les raisons, conformément à l'article 50, paragraphe 1, point 4, de la loi sur le réexamen des recours administratifs tel qu'appliqué avec le remplacement de l'article 42, paragraphe 2, de l'APPIHAO.