Avis 28/2018

concernant le projet de décision d'exécution de la Commission européenne

constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon

Adopté le 5 décembre 2018

Table des matières

Le comité européen de la protection des données

vu l'article 70, paragraphe 1, point s), du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord EEE et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du Comité mixte de l'EEE nº 154/2018 du 6 juillet 2018,

vu les articles 12 et 22 de son règlement intérieur du 25 mai 2018,

A ADOPTÉ L'AVIS SUIVANT:

1 RÉSUMÉ

1. La Commission européenne a approuvé son projet de décision d'exécution constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon en vertu du règlement général sur la protection des données[1] le 5 septembre 2018[2]. La Commission européenne a ensuite lancé la procédure en vue de son adoption formelle.

2. Le 25 septembre 2018, la Commission européenne a demandé l'avis du comité européen de la protection des données (ci-après le «CEPD CEPDLa Commission a été invitée à fournir au CEPD tous les documents nécessaires concernant ce pays, y compris toute correspondance pertinente avec le gouvernement du Japon.

3. À la lumière des discussions qui ont eu lieu avec le CEPD, la Commission européenne a modifié à deux reprises son projet de décision d'adéquation, et lui en a transmis la dernière version le 13 novembre 2018[3]. Le CEPD a fondé le présent avis sur cette dernière version du projet de décision d'exécution (ci-après le «projet de décision d'adéquation»).

4. L'évaluation par le CEPD du niveau de protection assuré par la décision d'adéquation de la Commission a été effectuée sur la base de l'examen de la décision elle-même ainsi que d'une analyse de la documentation mise à disposition[4] par la Commission[5].

5. Le CEPD s'est concentré à la fois sur l'évaluation des aspects commerciaux du projet de décision d'adéquation et sur l'accès du gouvernement à des fins répressives et de sécurité nationale, aux

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.
[2] Voir le communiqué de presse http://europa.eu/rapid/press-release_IP-18-5433_fr.htm.
[3] Voir l'annexe I de l'avis de l'EDPB pour la version mise à jour du projet de décision d'exécution de la Commission européenne.
[4] L'EDPB a fondé son analyse sur des traductions fournies par les autorités japonaises, vérifiées par la Commission européenne.
[5] Voir l'annexe II de l'avis de l'EDPB pour la liste des documents non fournis par la Commission européenne à l'EDPB.

données à caractère personnel transférées depuis l'Union, y compris des voies de droit ouvertes aux citoyens de l'Union. Le CEPD a également examiné si les garanties prévues par le cadre juridique japonais étaient en place et effectives.

6. Le CEPD a principalement utilisé dans ce cadre son référentiel sur l'adéquation[6] adopté en février 2018.

1.1 Domaines de convergence

7. L'objectif principal du CEPD a été de donner un avis à la Commission européenne sur le niveau de protection garanti aux particuliers par le cadre japonais. Il importe de reconnaître que le CEPD ne s'attend pas à ce que le cadre juridique japonais reproduise la législation européenne en matière de protection des données à caractère personnel.

8. Toutefois, le CEPD rappelle que, pour que le niveau de protection soit considéré comme adéquat, la jurisprudence de la Cour de justice de l'Union européenne (ci-après la «CJUE») ainsi que l'article 45 du RGPD exigent que la législation du pays tiers soit alignée sur l'essence des principes fondamentaux inscrits dans le RGPD. Concernant la protection des données, le CEPD observe en outre qu'il existe des domaines clés de convergence entre le cadre du RGPD et le cadre japonais sur certaines dispositions essentielles telles que l'exactitude et la minimisation des données, la limitation de la durée de conservation , la sécurité des données, la limitation des finalités et l'existence d'une autorité de contrôle indépendante, à savoir la commission de protection des données à caractère personnel (la « PPC »).

9. Outre ce qui précède, le CEPD salue les efforts déployés par la Commission européenne et les autorités japonaises pour garantir que le Japon assure un niveau de protection adéquat aux exigences du RGPD, notamment en comblant les lacunes existant entre le RGPD et le cadre japonais en matière de protection des données par l'adoption par la PPC de règles supplémentaires uniquement applicables aux données à caractère personnel transférées depuis l'Union vers le Japon, à savoir les règles supplémentaires. Par exemple, le CEPD fait observer que la PPC a accepté d'inclure d'autres catégories de données dans les données sensibles (dans le cadre de la législation japonaise, les données sensibles ne comprennent pas l'orientation sexuelle ou l'appartenance à un syndicat). En outre, les règles supplémentaires garantissent que les droits des personnes concernées s'appliqueront à toutes les données à caractère personnel transférées depuis l'Union, indépendamment de leur durée de conservation (alors que le système juridique japonais prévoit que les droits des personnes concernées ne s'appliquent pas aux données à caractère personnel devant être effacées dans un délai de six mois).

10. Le CEPD prend également acte des efforts déployés par la Commission européenne afin de renforcer la décision d'adéquation en réponse aux préoccupations soulevées par le CEPD.

1.2 Défis généraux

11. Néanmoins, des difficultés subsistent et le CEPD considère que les principaux domaines devant être renforcés et suivis de près dans le système japonais sont ceux exposés ci-après.

12. La première difficulté concerne le suivi de cette nouvelle architecture d'adéquation, qui associe un cadre juridique existant et des règles supplémentaires spécifiques, afin de garantir qu'elle constituera un système durable et fiable, exempt de **problèmes pratiques sur le plan de sa conformité concrète et efficace** par les entités japonaises et de sa mise en œuvre par la PPC.

13. Ensuite, le CEPD prend acte des engagements et des assurances réitérés de la Commission européenne et des autorités japonaises concernant le caractère contraignant et exécutoire des règles

[6] WP 254, Critères de référence pour l'adéquation, 6 février 2018.

supplémentaires , tout en invitant la Commission européenne à **surveiller en permanence leur caractère contraignant et leur application effective au Japon**, étant donné que leur valeur juridique constitue un élément absolument essentiel de l'adéquation entre l'Union et le Japon. Pour ce qui est des lignes directrices de la PPC , le CEPD souhaiterait obtenir des éclaircissements en ce qui concerne **leur caractère contraignant et demande à la Commission européenne de suivre attentivement cet aspect**[7].

1.3 Aspects commerciaux spécifiques

14. Concernant les aspects commerciaux du projet de décision d'adéquation UE-Japon, le CEPD émet quelques réserves spécifiques et souhaiterait demander des éclaircissements sur certaines questions importantes.

1.3.1 Préoccupations du CEPD concernant les principes essentiels de la protection des données

15. Le CEPD se félicite que les règles supplémentaires excluent la possibilité que des données à caractère personnel transférées depuis l'Union soient ultérieurement transférées du Japon vers un pays tiers sur la base des règles transfrontalières de protection de la vie privée de la Coopération économique Asie-Pacifique. En outre, le CEPD reconnaît que dans la nouvelle version de son projet de décision d'adéquation, la Commission européenne s'est engagée à suspendre la décision d'adéquation lorsque les transferts ultérieurs ne garantissent plus la continuité de la protection.

16. En vertu de la législation japonaise, l'un des fondements juridiques sous-tendant les transferts ultérieurs réside dans la reconnaissance d'un pays tiers comme garantissant un niveau de protection adéquat à celui du Japon. Toutefois, l'évaluation par le Japon de l'adéquation d'un pays tiers semble ne pas tenir compte des «règles supplémentaires» spécifiques négociées entre la Commission européenne et la PPC, qui ne s'appliquent qu'aux données à caractère personnel transférées depuis l'Union afin d'assurer un niveau de protection substantiellement équivalent aux normes du RGPD. Il s'ensuit que les données à caractère personnel de l'Union qui sont transférées, sur la base d'une adéquation japonaise, du Japon vers un autre pays tiers non reconnu comme disposant d'un cadre substantiellement équivalent au RGPD en matière de protection des données ne bénéficieront plus nécessairement de la protection spécifique garantie pour les données à caractère personnel de l'Union.

17. **Il convient toutefois de garder à l'esprit que les transferts ultérieurs de données à caractère personnel peuvent avoir lieu vers des pays tiers qui pourraient faire l'objet d'une éventuelle future décision d'adéquation du Japon. Ces pays tiers peuvent ne pas avoir fait l'objet d'une évaluation antérieure ou d'un constat d'adéquation de l'Union. À ce stade, la Commission européenne doit assumer son rôle de contrôle et garantir le maintien du niveau de protection des données de l'Union ou envisager la suspension de la décision d'adéquation.**

18. En outre, le CEPD a des préoccupations concernant les **obligations de consentement et de transparence** des responsables du traitement (ci-après les «opérateurs commerciaux traitant des données à caractère personnel»). Le CEPD a examiné attentivement ces éléments au motif que, contrairement à la législation européenne en matière de protection des données, l'utilisation du consentement en tant que base des traitements et des transferts joue un rôle central dans le système juridique japonais. Par exemple, le CEPD est préoccupé par la notion de consentement, qui n'est pas définie de manière à inclure le droit de retrait, qui est un élément essentiel de la législation de l'Union en vue de garantir à la personne concernée le contrôle effectif sur ses données à caractère personnel.

[7] Pour de plus amples informations, voir la section 1.3.4 du présent avis.

En ce qui concerne les obligations de transparence auxquelles sont soumis les opérateurs commerciaux traitant des données à caractère personnel, des doutes existent quant à la question de savoir si des informations proactives sont fournies aux personnes concernées.

19. Le CEPD s'inquiète du fait que le **système de recours japonais** n'est peut-être pas facile d'accès pour les citoyens de l'Union qui ont besoin d'une aide ou souhaitent déposer une plainte étant donné que l'aide offerte par la PPC est uniquement accessible via le service d'assistance et en japonais. Il en va de même pour le service de médiation mis en place par la PPC puisque l'existence du système n'est pas portée à l'attention du public sur la version anglaise de son site web et que des documents d'information importants, tels que les questions fréquemment posées sur la loi sur la protection des informations personnelles, ne sont également disponibles qu'en japonais. À cet égard, le CEPD souhaiterait que la Commission puisse discuter avec la PPC de la possibilité de mettre en place un service en ligne, au moins en anglais, ayant pour mission de fournir une assistance aux citoyens de l'Union et de traiter leurs plaintes, à l'instar de celui envisagé à l'annexe II de la décision d'adéquation. La Commission européenne devra également surveiller attentivement l'efficacité des sanctions et des voies de recours pertinentes.

1.3.2 Besoin de précisions

20. Le CEPD souhaiterait des garanties sur certains aspects du projet de la décision d'adéquation, qui nécessitent des éclaircissements supplémentaires.

21. Ces précisions concernent, par exemple, certaines notions fondamentales de la législation japonaise. Plus précisément, un manque de clarté entoure le **statut du «mandataire»**, une figure qui évoque celle du responsable du traitement dans le RGPD, mais dont la capacité à déterminer et à modifier les finalités et les moyens du traitement des données à caractère personnel reste ambiguë.

22. Le CEPD souhaiterait également des garanties, en raison de l'absence de documents pertinents, permettant d'établir si les **limitations des droits des personnes** (en particulier, les droits d'accès, de rectification et d'objection) sont nécessaires et proportionnées dans une société démocratique et respectent l'essence des droits fondamentaux.

23. Le CEPD escompte également que la Commission européenne surveille de près la protection effective des **données à caractère personnel transférées depuis l'Union vers le Japon, sur la base du projet de décision d'adéquation, tout au long de leur «cycle de vie»**, même si la législation japonaise impose une obligation de conservation de l'origine des données d'une durée maximale de trois ans.

1.4 Concernant l'accès des autorités publiques aux données transférées au Japon

24. Le CEPD a également analysé le cadre juridique relatif à l'accès des entités gouvernementales japonaises à des fins répressives ou de sécurité nationale à des données à caractère personnel transférées depuis l'Union vers le Japon. Tout en prenant acte des assurances fournies par le gouvernement japonais, figurant à l'annexe II du projet de décision d'adéquation, le CEPD a identifié un certain nombre d'aspects requérant des clarifications et soulevant des inquiétudes, dont ceux énoncés ci-après, qui méritent d'être soulignés.

25. Dans le domaine répressif, le CEPD fait observer que les principes juridiques applicables à l'accès aux données semblent souvent similaires à ceux de l'Union, dans la limite où ils sont disponibles. L'absence de traductions de divers textes juridiques et de la jurisprudence pertinente permet toutefois difficilement de conclure que toutes les procédures d'accès aux données sont nécessaires et proportionnées et que l'application de ces principes est «substantiellement équivalente» au droit de l'Union.

26. Dans le domaine de la sécurité nationale, le CEPD reconnaît que le gouvernement japonais a réaffirmé que les informations ne peuvent être obtenues qu'à partir de sources librement accessibles ou par divulgation volontaire par les entreprises, et qu'il ne collecte pas d'informations sur le grand public. Le comité, qui est toutefois conscient des préoccupations exprimées par les experts et dans les médias, apprécierait de plus amples précisions concernant les mesures de surveillance prises par les entités gouvernementales japonaises.

27. En ce qui concerne les recours juridiques accessibles aux citoyens de l'Union dans le domaine répressif et de la sécurité nationale, le CEPD se félicite que la Commission européenne et le gouvernement japonais aient négocié un mécanisme complémentaire offrant aux citoyens de l'Union une voie de recours supplémentaire, étendant ainsi les pouvoirs de l'autorité japonaise chargée de la protection des données. Toutefois, il reste à craindre que ce nouveau mécanisme ne compense pas entièrement les lacunes en matière de contrôle et de recours de la législation japonaise. Le CEPD souhaiterait donc de plus amples éclaircissements afin de garantir que ce nouveau mécanisme compense pleinement ces lacunes.

1.5 Conclusion

28. Le CEPD estime que cette décision d'adéquation est d'une importance capitale. En tant que première décision d'adéquation depuis l'entrée en vigueur du RGPD, elle constituera **un précédent pour les futures demandes d'adéquation ainsi que pour la révision des décisions d'adéquation rendues en vertu de la directive 95/46/CE**[8]. Il importe également de souligner que les citoyens sont de plus en plus conscients de l'impact de la mondialisation sur leur vie privée et attendent de leurs autorités de contrôle qu'elles veillent à ce que des garanties adéquates soient en place lorsque leurs données à caractère personnel sont transférées à l'étranger. À la lumière de ces implications, le CEPD estime que la Commission européenne doit s'assurer que la protection offerte par l'adéquation UE-Japon ne présente aucune lacune et que ce type d'adéquation spécifique soit conforme aux exigences de l'article 45 du RGPD.

29. Le CEPD salue les efforts déployés par la Commission européenne et la PPC pour aligner autant que possible le cadre juridique japonais sur le cadre européen. Les **améliorations** apportées par les règles supplémentaires pour remédier à certaines différences entre les deux cadres sont très importantes et bien accueillies.

30. Toutefois, à la suite d'une analyse approfondie du projet de décision d'adéquation de la Commission et du cadre japonais en matière de protection des données, le CEPD observe qu'**un certain nombre de préoccupations subsistent, de même que la nécessité de clarifications supplémentaires**. En outre, ce type particulier d'adéquation combinant un cadre national existant et des règles spécifiques supplémentaires soulève également des questions quant à sa mise en œuvre opérationnelle. À la lumière de ce qui précède, le CEPD recommande à la Commission européenne de répondre aux préoccupations et aux demandes d'éclaircissements formulées par le CEPD et de fournir des éléments de preuve et des explications complémentaires sur les questions soulevées. Le CEPD invite également la Commission européenne à procéder à un réexamen de ce constat d'adéquation (au moins) tous les deux ans, et non tous les quatre ans, comme suggéré dans l'actuel projet de décision d'adéquation.

[8] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

2 INTRODUCTION

2.1 Cadre japonais de protection des données

31. Le cadre japonais de protection des données a été modernisé très récemment, en 2017. Il comprend plusieurs piliers, organisés autour d'une loi générale, à savoir la loi sur la protection des informations personnelles. Le décret ministériel portant exécution de la loi sur la protection des informations personnelles (ci-après le «décret ministériel»), qui en spécifie certains principes fondamentaux, constitue un autre texte législatif important.

32. Sur la base d'une décision du gouvernement, adoptée le 12 juin 2018[9], et de l'article 6 de la loi sur la protection des informations personnelles, la PPC a été investie du pouvoir de «*prendre les mesures nécessaires pour combler les différences entre les systèmes et opérations du Japon et du pays étranger concerné, afin que les informations personnelles reçus de ce pays soient traitées de manière appropriée*»[10]. Le décret laisse également entendre que les règles plus strictes adoptées par la PPC qui complètent et excèdent celles énoncées dans la loi sur la protection des informations personnelles seraient contraignantes pour les opérateurs économiques japonais et auraient force exécutoire[11].

33. En conséquence, la PPC a entamé des négociations avec la Commission européenne et a adopté, en juin 2018, des règles plus strictes que celles énoncées dans la loi sur la protection des informations personnelles et dans le décret ministériel concernant les données transférées depuis l'Union. Il s'agit des règles supplémentaires au titre de la loi sur la protection des informations personnelles applicables au traitement des données à caractère personnel transférées depuis l'Union sur la base d'une décision d'adéquation, ci-après les «règles supplémentaires »[12]. Ces règles supplémentaires sont également annexées au projet de décision d'exécution de la Commission publié en juillet 2018.

34. Il importe de souligner que les règles supplémentaires ne s'appliquent qu'aux données à caractère personnel transférées depuis l'Union européenne vers le Japon sur la base de la décision d'adéquation et visent à renforcer la protection garantie à ces données. En tant que telles, elles ne s'appliquent pas aux données à caractère personnel des personnes établies au Japon ou provenant de pays autres que ceux de l'EEE.

35. En outre, le CEPD souhaite attirer l'attention sur le fait que la loi modifiée sur la protection des informations personnelles est entrée en vigueur le 30 mai 2017, alors que la PPC telle qu'elle existe dans sa forme actuelle a été établie en 2016. Par ailleurs, les règles supplémentaires négociées par la PPC avec la Commission européenne doivent encore entrer en vigueur, étant donné que cette entrée en vigueur dépendra de la reconnaissance par la Commission européenne du Japon en tant que juridiction adéquate à celle de l'Union.

2.2 Portée de l'évaluation du CEPD

36. Le projet de décision d'adéquation de la Commission européenne est le fruit d'une évaluation des règles japonaises en matière de protection des données et des négociations qui ont suivi avec les autorités japonaises. L'issue de ces négociations se reflète dans les deux annexes jointes au projet de décision d'adéquation: la première prévoit des mesures de protection supplémentaires que les

[9] L'EDPB fait observer que, selon le projet de décision d'adéquation, le décret ministériel a été adopté le 12 juin 2018. Toutefois, l'EDPB n'a reçu que le projet de décret, daté d'avril 2018.
[10] Décision du Conseil des ministres du 25 avril 2018.
[11] Pour de plus amples informations, voir la section 1.3.4 ci-après.
[12] Règles complémentaires, annexe I de la décision d'exécution de la Commission du XXXX 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, transmises à l'EDPB en septembre 2018.

opérateurs commerciaux japonais devront appliquer au traitement des données à caractère personnel transférées depuis l'Union, tandis que la deuxième formule des garanties et des engagements du gouvernement japonais concernant l'accès des autorités publiques aux données.

37. Le CEPD a examiné le cadre japonais relatif à la protection des données, les règles supplémentaires négociées par la Commission européenne et les garanties et engagements du gouvernement japonais. Le CEPD doit rendre un avis indépendant sur les conclusions de la Commission européenne, recenser les insuffisances du cadre d'adéquation, le cas échéant, et s'efforcer de proposer des modifications ou des amendements pour y remédier.

38. Comme indiqué dans le référentiel d'adéquation du CEPD, «*les informations fournies par la Commission européenne devraient être exhaustives et permettre au comité de procéder à sa propre évaluation concernant le niveau de protection des données dans le pays tiers*»[13].

39. Toutefois, c'est dans des versions traduites en anglais que le CEPD a reçu la plupart des documents référencés dans le projet de décision d'adéquation qui constituent un élément essentiel du système juridique japonais. Par conséquent, le CEPD rend le présent avis sur la base de l'analyse des documents disponibles en anglais. Le CEPD a tenu compte du cadre applicable en matière de protection des données dans l'Union européenne, y compris l'article 8 de la convention européenne des droits de l'homme (ci-après la «CEDH») protégeant le droit au respect de la vie privée et familiale, ainsi que les articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne (ci-après la «charte») garantissant respectivement le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel et le droit à un recours effectif et à accéder à un tribunal impartial. Outre ce qui précède, le CEPD a examiné les exigences du RGPD et a analysé la jurisprudence pertinente.

40. L'objectif de cet exercice est de garantir que le cadre japonais en matière de protection des données est substantiellement équivalent à celui de l'Union européenne. Ce concept de «niveau de protection adéquat», qui existait déjà dans le cadre de la directive 95/46/CE, a été renforcé par la CJUE. Il importe de rappeler la norme définie par la CJUE dans l'arrêt Schrems, à savoir que si le «niveau de protection» dans le pays tiers doit être «substantiellement équivalent» à celui garanti dans l'Union, «les moyens auxquels ce pays tiers a recours, à cet égard, pour assurer un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union»[14]. Par conséquent, l'objectif n'est pas de refléter point par point la législation européenne, mais d'établir les exigences essentielles et fondamentales de cette législation. L'adéquation peut être obtenue en combinant les droits des personnes concernées et les obligations de ceux qui traitent les données ou qui exercent un contrôle sur ce traitement et la supervision par des organes indépendants. Toutefois, les règles sur la protection des données ne sont efficaces que si elles sont applicables et suivies en pratique. Il convient donc de tenir compte non seulement du contenu des règles applicables aux données personnelles transférées vers un pays tiers ou une organisation internationale, mais également du système mis en place afin de garantir l'effectivité de ces règles. Des mécanismes d'application efficaces sont essentiels pour assurer l'effectivité des règles sur la protection des données[15].

2.3 Commentaires généraux et inquiétudes

[13] WP 254, p. 5.
[14] Arrêt du 6 octobre 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650, points 73 et 74.
[15] WP 254, p. 4.

2.3.1 Spécificités de ce type de décision d'adéquation

41. L'adéquation UE-Japon est la première à être examinée au regard du nouveau contexte juridique du RGPD. Cet aspect rend les travaux du CEPD d'autant plus importants à la lumière des effets de ce projet de décision d'adéquation sur les futures demandes d'adéquation.

42. L'adéquation entre l'Union et le Japon serait également la première adéquation mutuelle. Le cas échéant, quand l'Union reconnaîtra le Japon comme offrant un niveau de protection substantiellement équivalent à celui garanti par le RGPD, le Japon rendra également sa propre décision d'adéquation en vertu de l'article 24 de la loi sur la protection des informations personnelles et reconnaîtra ainsi que l'Union offre un niveau de protection adéquat à celui assuré par le cadre japonais de protection des données. Dès lors, l'adéquation Japon-UE envisagée présente une nature particulière, dont le CEPD a tenu compte dans son évaluation. Comme indiqué ci-dessus, la PPC a négocié des règles spécifiques plus strictes avec la Commission européenne, uniquement applicables aux données à caractère personnel transférées depuis l'Union. Ces règles plus strictes sont contraignantes et ont force exécutoire conformément au décret ministériel et doivent être respectées par tous les opérateurs commerciaux japonais lorsqu'ils traitent des données à caractère personnel provenant de l'Union en vertu du présent projet de décision d'adéquation.

43. La Commission européenne a donc fondé son constat d'adéquation non seulement sur le cadre général existant en matière de protection des données au Japon, mais aussi sur ces règles spécifiques. Le fait que des règles supplémentaires aient été nécessaires pour compléter la loi sur la protection des informations personnelles témoigne du fait que la Commission européenne reconnaît que la législation japonaise en matière de protection des données n'est pas, en soi, substantiellement équivalente au RGPD.

44. **À la lumière de ce qui précède, le CEPD invite la Commission européenne à s'assurer que cette nouvelle architecture d'adéquation, la première à être adoptée au titre du RGPD, reposant sur des règles supplémentaires , constituera un système durable et fiable qui ne soulèvera pas de problèmes pratiques en ce qui concerne son respect concret et efficace par les entités japonaises et son application effective par la commission de protection des données à caractère personnel.**

2.3.2 Exactitude des traductions

45. À l'instar de la Commission européenne, le CEPD a travaillé sur la base de traductions anglaises fournies par les autorités japonaises[16]. Le CEPD invite la Commission européenne à préciser qu'elle a fondé son projet de décision d'adéquation sur les traductions anglaises reçues et a dûment vérifié la qualité et l'exactitude de ces traductions.

2.3.3 Adéquation sectorielle

46. Le constat d'adéquation de ce projet de décision d'adéquation est limité à la protection des informations personnelles par les opérateurs commerciaux traitant des données à caractère personnel au sens de la loi sur la protection des informations personnelles. Cela signifie que l'adéquation est sectorielle puisqu'elle ne s'applique qu'au secteur privé et exclut de son champ d'application les transferts de données à caractère personnel entre autorités et organismes publics. À l'heure actuelle, la Commission européenne mentionne brièvement cette spécificité du champ d'application de l'adéquation au considérant 10 du projet de décision d'adéquation.

[16] La Commission européenne a vérifié ces traductions.

47. **Le CEPD invite la Commission européenne à mentionner explicitement la nature sectorielle de ce constat d'adéquation dans l'intitulé de la décision d'exécution ainsi que dans son article premier, conformément à l'article 45, paragraphe 3, du RGPD.**

2.3.4 Caractère contraignant des règles supplémentaires et des lignes directrices de la PPC

48. L'article 6 de la loi sur la protection des informations personnelles énonce que «le gouvernement [...] prend les mesures législatives et autres dispositions nécessaires pour pouvoir adopter des mesures discrètes de protection des données à caractère personnel, exigeant spécifiquement l'application stricte d'un traitement adéquat, afin de renforcer la protection des droits et des intérêts des personnes, et prend les mesures nécessaires, en collaboration avec les gouvernements d'autres pays, en vue de développer un système conforme au niveau international en matière de protection des données à caractère personnel et encourage à cet effet la coopération avec les organisations internationales et d'autres cadres internationaux». Bien que le gouvernement soit clairement identifié dans cet article de la loi sur la protection des informations personnelles comme étant compétent pour prendre de telles mesures juridiques, la PPC n'est pas désignée directement comme étant l'organe compétent pour adopter des règles spécifiques[17]. En raison de contraintes de temps, le CEPD n'a pas été en mesure de rassembler, d'analyser et d'examiner les éléments de preuve existants sur ce point.

49. **Compte tenu de l'importance de cette question, le CEPD prend acte des engagements et des garanties réitérés de la Commission européenne et des autorités japonaises concernant le caractère contraignant et la force exécutoire des règles supplémentaires. Le CEPD invite la Commission européenne à surveiller en permanence leur caractère contraignant et leur application effective au Japon, étant donné que leur valeur juridique constitue un élément essentiel de l'adéquation entre l'Union et le Japon.**

50. En outre, la Commission européenne fait référence aux lignes directrices de la PPC (ci-après les «lignes directrices») dans plusieurs sections de son projet de décision d'adéquation.

51. Bien qu'au considérant 16 de son projet de décision d'adéquation, la Commission européenne précise que les lignes directrices donnent une interprétation faisant autorité de la loi sur la protection des informations personnelles, elle évoque leur caractère contraignant dans ce même considérant: «*[s]elon les informations fournies par la commission de protection des données à caractère personnel, ces lignes directrices sont considérées comme des règles contraignantes faisant partie intégrante du cadre juridique et devant être lues conjointement au texte de la loi sur la protection des informations personnelles, au décret ministériel, aux règles de la PPC et à une série de questions et réponses élaborées par la commission de protection des données à caractère personnel*»[18].

52. Toutefois, sur la base des mêmes informations fournies par la PPC, le CEPD considère que les lignes directrices ne sont pas juridiquement contraignantes. Elles donnent plutôt une «interprétation faisant autorité» de la loi. La PPC fait valoir que les lignes directrices sont suivies dans la pratique par les opérateurs commerciaux traitant des données à caractère personnel, sont utilisées par la PPC dans l'application de la loi à l'égard de ces opérateurs commerciaux et sont utilisées par les tribunaux

[17] Selon un article publié en juillet 2018, lorsque les règles supplémentairesn'en étaient encore qu'au stade du projet, leur nature juridique contraignante était susceptible de faire l'objet d'un débat interne dans le pays. Voir Fujiwara S., «Comparison between the EU and Japan's Data Protection Legal Frameworks», *Jurist*, vol. 1521, juillet 2018, p. 19.

[18] Décision d'exécution de la Commission européenne du XXXX, conformément au règlement nº 2016/679 du Parlement européen et du Conseil, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, envoyée au comité européen de la protection des données le 13 novembre 2018, considérant 16.

lorsqu'ils statuent. Toutefois, ces éléments ne constituent pas une preuve suffisante du caractère légalement contraignant des lignes directrices.

53. **Le CEPD souhaiterait obtenir des éclaircissements dans la décision d'adéquation concernant le caractère contraignant des lignes directrices de la PPC et demande à la Commission européenne de contrôler attentivement cet aspect.**

54. Selon la PPC, les lignes directrices sont respectées dans la pratique, selon la coutume locale. La PPC indique que les tribunaux japonais se réfèrent aux lignes directrices lorsqu'ils doivent statuer en application des règles de la loi sur la protection des informations personnelles. La Commission européenne se réfère à une décision de justice[19] datant de 2006 pour démontrer que les tribunaux japonais se fondent sur les lignes directrices dans leurs conclusions. Bien qu'il n'ait pas reçu cette décision, le CEPD apprécierait que la Commission européenne lui fasse parvenir, si possible, une décision de justice plus récente rendue dans le domaine de la protection des données ou dans un autre domaine et dans laquelle les juridictions japonaises ont utilisé les lignes directrices de la PPC ou d'autres lignes directrices similaires pour fonder leur décision.

2.3.5 Réexamen périodique du constat d'adéquation

55. L'article 45, paragraphe 3, du RGPD dispose qu'un réexamen périodique doit avoir lieu au moins tous les quatre ans. Conformément au référentiel d'adéquation du CEPD[20], il s'agit toutefois d'un calendrier général qui doit être adapté à chaque pays tiers ou organisation internationale pour lequel ou laquelle il existe une décision d'adéquation. En fonction des circonstances particulières, un cycle d'examen plus court pourrait être justifié. De même, des incidents ou d'autres informations sur le cadre juridique ou des modifications de ce dernier dans le pays tiers ou l'organisation internationale en question pourraient nécessiter de procéder à un examen plus tôt. Il semble également nécessaire de procéder assez rapidement à un premier examen d'une décision d'adéquation totalement nouvelle et d'adapter progressivement le cycle d'examen en fonction du résultat.

56. Compte tenu d'un certain nombre de facteurs, notamment le fait que la loi sur la protection des informations personnelles est entrée en vigueur en 2017, que la PPC a été établie en 2016 et qu'il n'existe pas encore d'informations ni d'éléments de preuve concernant l'application pratique des règles supplémentaires , **le CEPD invite la Commission européenne à procéder à un examen de ce constat d'adéquation (au moins) tous les deux ans et non tous les quatre ans, comme suggéré dans l'actuel projet de décision d'adéquation**.

2.3.6 Engagements internationaux contractés par le Japon

57. Conformément à l'article 45, paragraphe 2, point c), du RGPD et au référentiel d'adéquation du CEPD [21], lorsqu'elle évalue le caractère adéquat du niveau de protection dans un pays tiers, la Commission européenne doit tenir compte, entre autres, des engagements internationaux pris par le pays tiers, ou d'autres obligations découlant de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel, ainsi que de la mise en œuvre de ces obligations. En outre, il y a lieu de prendre en considération l'adhésion du pays tiers à la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du

[19] Décision d'exécution de la Commission européenne du XXXX, conformément au règlement nº 2016/679 du Parlement européen et du Conseil, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, envoyée au comité européen de la protection des données le 13 novembre 2018, page 5, note de bas de page 16, «Tribunal d'arrondissement d'Osaka, jugement du 19 mai 2006, Hanrei Jiho, Vol. 1948, p. 122».
[20] WP 254, p. 5.
[21] WP 254, p. 4.

traitement automatisé des données à caractère personnel (la «convention 108+»)[22] et à son protocole additionnel.

58. **À cet égard, le CEPD constate que le Japon a un statut d'observateur au sein du comité consultatif de la convention 108 +.**

2.3.7 Pouvoirs des autorités chargées de la protection des données[23] de former un recours en justice concernant la validité d'une décision d'adéquation

59. Le CEPD souligne que, bien que le considérant 179 du projet de décision d'adéquation ne mentionne que des cas dans lesquels une autorité chargée de la protection des données a reçu une plainte remettant en cause la compatibilité d'une décision d'adéquation avec les droits fondamentaux de la personne concernée au respect de la vie privée et à la protection des données, cette déclaration doit être perçue comme un exemple de situation dans laquelle une autorité chargée de la protection des données peut saisir une juridiction nationale, même en l'absence de plainte, plutôt que comme une restriction des pouvoirs conférés aux autorités chargées de la protection des données en vertu du RGPD et des législations nationales des États membres à cet égard. En effet, les dispositions du RGPD prévoient à la fois le pouvoir de suspendre les transferts de données même lorsqu'ils sont fondés sur une décision d'adéquation et de former un recours concernant la validité d'une décision d'adéquation et ne se limitent pas aux cas dans lesquels une plainte a été reçue, si le droit national accorde un pouvoir d'action plus vaste et indépendant d'une plainte, conformément aux dispositions pertinentes du RGPD.

60. **Le CEPD invite la Commission européenne à préciser dans son projet de décision d'adéquation que le pouvoir des autorités de contrôle de former un recours contre la validité d'une décision d'adéquation à la suite d'une plainte n'est qu'une illustration des pouvoirs plus vastes des autorités chargées de la protection des données découlant du RGPD, qui incluent le pouvoir de suspendre les transferts et de former un recours concernant la validité d'une décision d'adéquation en l'absence de plainte si le droit national le prévoit.**

3 ASPECTS COMMERCIAUX

3.1 Principes généraux fondamentaux

61. Le chapitre 3 du référentiel d'adéquation est consacré aux «principes généraux fondamentaux ». Le système d'un pays tiers ou d'une organisation internationale doit comporter ces principes pour que le niveau de protection assuré puisse être considéré comme substantiellement équivalent à celui garanti par la législation européenne. Le CEPD reconnaît que le système juridique japonais adopte une approche différente de celle du RGPD lorsqu'il s'agit de donner effet au droit au respect de la vie privée. Bien que le droit au respect de la vie privée ne soit pas consacré par la constitution japonaise en soi, il a été reconnu comme un droit constitutionnel dans la jurisprudence, comme indiqué dans la décision de la Commission européenne[24].

[22] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Convention 108+, 18 mai 2018.
[23] Arrêt du 6 octobre 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650.
[24] L'EDPB n'a pas reçu de traduction en anglais de ce jugement. Voir la décision d'exécution de la Commission européenne du XXXX, conformément au règlement nº 2016/679 du Parlement européen et du Conseil, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, envoyée au comité européen de la protection des données le 13 novembre 2018, note de bas de page 9.

62. En particulier, étant donné que l'approche japonaise diffère sensiblement de l'approche européenne, il convient d'établir attentivement si, au-delà de certains aspects, le système dans son ensemble fournit un niveau de protection «substantiellement équivalent». Dès lors, des «lacunes» potentielles concernant un principe touchant au contenu pourraient être compensées par d'autres éléments fournissant des contrepoids adéquats.

3.1.1 Notions

63. Sur la base des critères de référence pour l'adéquation, des notions et/ou principes fondamentaux en matière de protection des données doivent exister dans le cadre juridique du pays tiers. Ils ne doivent pas reprendre la terminologie du RGPD, mais doivent refléter les notions ancrées dans la législation européenne relative à la protection des données et être cohérents avec ces dernières. À titre d'exemple, le RGPD inclut les notions importantes suivantes: «données à caractère personnel», «traitement de données à caractère personnel», «responsable du traitement», «sous-traitant», «destinataire» et «données sensibles»[25].

64. La loi japonaise sur la protection des informations personnelles définit aussi un certain nombre de termes et, notamment, «informations à caractère personnel», «données à caractère personnel» et «opérateur commercial traitant des données à caractère personnel». **Il semble toutefois qu'elle ne définisse pas la notion de «gestion de données à caractère personnel», qui est similaire à celle de «traitement de données à caractère personnel».**

65. En ce qui concerne la définition de la notion de «gestion de données à caractère personnel», la PPC a répondu par écrit à la question du CEPD. La Commission européenne a cité cette réponse dans son projet de décision d'adéquation: «*[s]i la loi sur la protection des informations personnelles n'utilise pas le terme "traitement", celui-ci se fonde sur le concept équivalent de "gestion" qui, selon les informations reçues de la PPC, recouvre "toute opération concernant des données à caractère personnel", y compris l'acquisition, la saisie, la collecte, l'organisation, le stockage, la modification/le traitement, le renouvellement, la production, la sécurisation, l'extraction, l'utilisation ou la fourniture d'informations à caractère personnel*»[26].

66. Toutefois, étant donné que le texte de référence de cette définition n'a pas été fourni, le CEPD invite **la Commission européenne à contrôler attentivement si la définition de la notion susmentionnée, telle que fournie par la PPC, est effectivement respectée dans la pratique**.

3.1.1.1 Notion de sous-traitant et obligations d'un «mandataire»

67. Comme susmentionné, le référentiel d'adéquation exige que des notions et/ou principes fondamentaux en matière de protection des données existent dans le cadre juridique du pays tiers.

68. La loi japonaise sur la protection des informations personnelles comporte une définition du terme «opérateur commercial traitant des données à caractère personnel» qui, d'après la Commission européenne, recouvre à la fois les notions de «responsable du traitement» et de «sous-traitant» telles que définies par le RGPD et ne fait pas de distinction entre les deux[27]. Toutefois, la loi japonaise sur la

[25] WP 254, p. 6.
[26] Décision d'exécution de la Commission européenne du XXXX, conformément au règlement nº 2016/679 du Parlement européen et du Conseil, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, envoyée au comité européen de la protection des données le 13 novembre 2018, considérant 17.
[27] Décision d'exécution de la Commission européenne du XXXX, conformément au règlement nº 2016/679 du Parlement européen et du Conseil, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, envoyée au comité européen de la protection des données le 13 novembre 2018, considérant 35.

protection des informations personnelles fait également mention du «mandataire» dans son article 22, qui peut être assimilé à certains égards au terme «sous-traitant» utilisé dans le RGPD.

69. Comme expliqué par la PPC dans ses réponses fournies au CEPD et également incluses dans le projet de décision d'adéquation de la Commission européenne, un mandataire est considéré comme l'équivalent d'un sous-traitant au titre du RGPD: il est chargé du traitement de données à caractère personnel par un opérateur commercial traitant des données à caractère personnel. Ce mandataire a les mêmes obligations et droits que tout opérateur commercial traitant des données à caractère personnel, y compris ceux prévus par les règles supplémentaires à l'égard des données à caractère personnel transférées depuis l'Union. L'opérateur commercial traitant des données à caractère personnel qui confie le traitement de données à caractère personnel à un mandataire est tenu «d'exercer une supervision nécessaire et appropriée»[28] sur le mandataire.

70. **Le CEPD invite la Commission européenne à expliquer le statut et les obligations du mandataire lorsque celui-ci modifie les finalités et les moyens du traitement et à préciser si le consentement de la personne concernée demeure une condition nécessaire à ce changement de finalité ou des moyens[29].**

3.1.1.2 Notion de données à caractère personnel conservées

71. La loi japonaise sur la protection des informations personnelles comporte également la notion de «données à caractère personnel conservées», qui sont considérées comme une sous-catégorie de données à caractère personnel. Selon cette loi, les dispositions relatives aux droits de la personne concernée[30] ne s'appliquent qu'aux données à caractère personnel conservées. La définition des données à caractère personnel conservées figure à l'article 2, paragraphe 7, de la loi sur la protection des informations personnelles.

72. Les données à caractère personnel conservées sont les données à caractère personnel autres que celles qui i) doivent être effacées dans un délai n'excédant pas six mois[31], ou qui ii) relèvent des exceptions prévues à l'article 4 du décret ministériel et sont susceptibles de porter préjudice aux intérêts publics ou autres si leur présence ou leur absence est révélée.

73. La deuxième règle complémentaire dispose que «*les données à caractère personnel transférées depuis l'Union sur la base d'une décision d'adéquation doivent être traitées comme des données à caractère personnel conservées, quel que soit le délai prévu pour leur effacement*».

74. Toutefois, les données à caractère personnel relevant des exceptions prévues à l'article 4 du décret ministériel ne devront pas être traitées comme des données à caractère personnel conservées et les droits des personnes concernées ne s'appliqueront pas.

75. L'article 23 du RGPD dispose qu'à l'instar de l'article 4 du décret ministériel, le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent limiter la portée des obligations qui lui sont applicables et des droits dont jouit la personne concernée. Cette restriction peut intervenir par voie de mesures législatives. Une telle limitation doit respecter

[28] Article 22 de la loi modifiée sur la protection des informations personnelles, entrée en vigueur le 30 mai 2017.
[29] Article 23, paragraphe 5, point i), de la loi sur la protection des informations personnelles. Voir également la section sur le principe de transparence ci-dessous.
[30] Articles 27 à 30 de la loi sur la protection des informations personnelles.
[31] Modification du décret ministériel portant exécution de la loi sur la protection des informations personnelles (décret ministériel), entrée en vigueur le 30 mai 2017, article 5.

l'essence des libertés et droits fondamentaux et constituer une mesure nécessaire et proportionnée dans une société démocratique.

76. En ce qui concerne le fond des exceptions prévues à l'article 4 du décret ministériel, le CEPD n'a pas reçu de documentation suffisante sur ces restrictions ou d'autres éléments permettant de clarifier le champ d'application de ces dispositions[32]. Le CEPD n'est pas en mesure d'évaluer si ces restrictions des droits des personnes concernées sont limitées à ce qui est considéré comme strictement nécessaire et proportionné au regard du droit de l'Union, de sorte à être substantiellement équivalents aux droits conférés aux personnes concernées de l'Union.

77. **En raison de l'absence de certains documents pertinents, le CEPD souhaiterait également des garanties de la Commission européenne permettant d'établir si les restrictions des droits des personnes (en particulier, les droits d'accès, de rectification et d'objection) sont nécessaires et proportionnées dans une société démocratique et respectent l'essence des droits fondamentaux.**

78. L'une des exigences essentielles du RGPD est que les données à caractère personnel soient protégées tout au long de leur «cycle de vie».

79. Compte tenu du fait que les règles supplémentaires s'appliquent uniquement aux données à caractère personnel transférées à partir de l'Union, le CEPD apprécierait de recevoir de plus amples informations sur la mise en œuvre pratique de ces règles par les opérateurs commerciaux traitant des données à caractère personnel, en particulier lorsque ces données sont communiquées à un autre opérateur après leur première transmission au Japon.

80. La Commission européenne a précisé au considérant 15 de son projet de décision d'adéquation que les opérateurs commerciaux traitant des données à caractère personnel qui reçoivent et/ou traitent des données à caractère personnel en provenance de l'Union seront légalement tenus de se conformer aux règles supplémentaires et, pour ce faire, ils devront veiller à pouvoir identifier ces données à caractère personnel tout au long de leur «cycle de vie».

81. Dans ses réponses, la PPC[33] a expliqué que cette identification se fera par des moyens techniques (ajout de balises) ou organisationnels (stockage des données provenant de l'Union dans une base de données spécifique).

82. Dans la note de bas de page 14 de son projet de décision d'adéquation, la Commission européenne explique que les opérateurs commerciaux traitant des données à caractère personnel doivent enregistrer les informations relatives à l'origine des données provenant de l'Union aussi longtemps que nécessaire afin de pouvoir se conformer aux règles complémentaires. Cette obligation est également énoncée à l'article 26, paragraphes 1, 3 et 4 de la loi sur la protection des informations personnelles, qui dispose qu'un opérateur commercial traitant des données à caractère personnel est tenu de confirmer et d'enregistrer la source de ces données, ainsi que toutes les circonstances entourant leur acquisition.

83. Toutefois, le CEPD fait observer que l'article 18 des règles portant exécution de la loi sur la protection des informations personnelles[34] spécifie que les obligations de conservation de registres incombant aux opérateurs commerciaux traitant des données à caractère personnel sont limitées à un maximum

[32] L'EDPB n'a pas reçu les décisions de la Cour suprême visées au considérant 53 du projet de décision d'adéquation.

[33] Annexe III du présent avis.

[34] Règles portant exécution de la loi sur la protection des informations personnelles, entrées en vigueur le 30 mai 2017, article 16.

de trois ans pour les cas qui ne relèvent pas des méthodes spécifiques de conservation décrites à l'article 16 de ces mêmes règles (au moyen d'un document écrit, d'un enregistrement électromagnétique ou d'un microfilm). La Commission européenne l'a également précisé au considérant 71 de son projet de décision d'adéquation: «*[c]omme indiqué à l'article 18 des règles portant exécution de la loi sur la protection des informations personnelles, les registres doivent être conservés pendant une période allant d'un à trois ans, en fonction des circonstances*».

84. Même si, comme la Commission européenne l'indique à la note de bas de page 14 de son projet de décision d'adéquation, les opérateurs commerciaux traitant des données à caractère personnel ne sont pas soumis à l'interdiction de conserver des registres concernant l'origine des données pendant plus de trois ans, afin de pouvoir remplir leurs obligations au titre de la deuxième règle supplémentaire , cet aspect n'est reflété clairement ni dans la législation japonaise ni dans les règles supplémentaires . Le CEPD estime qu'il existe un risque que les opérateurs commerciaux traitant des données à caractère personnel se conforment dans la pratique à l'article 18 des règles portant exécution de la loi sur la protection des informations personnelles même lorsqu'ils traitent des données provenant de l'Union. En effet, à la connaissance du CEPD et sur la base des documents disponibles, il n'existe actuellement aucune disposition obligeant les opérateurs commerciaux traitant des données à caractère personnel à se conformer plutôt aux règles complémentaires. Dès lors, les données transférées depuis l'Union ne seraient plus protégées par les garanties additionnelles prévues par les règles complémentaires.

85. **Le CEPD invite la Commission européenne à surveiller de près la protection effective des données à caractère personnel transférées depuis l'Union vers le Japon sur la base du projet de décision d'adéquation, tout au long de leur cycle de vie, même si la législation japonaise impose une obligation de conservation de l'origine des données d'une durée maximale de trois ans.**

3.1.2 Fondements du traitement loyal et licite pour des finalités légitimes

86. Selon le référentiel d'adéquation, et conformément au RGPD, les données doivent être traitées de manière loyale, licite et légitime[35]. Les fondements légitimes au titre desquels des données à caractère personnel peuvent être traitées loyalement, licitement et légitimement, doivent être définis de façon suffisamment claire. Le cadre européen reconnaît plusieurs de ces fondements légitimes, notamment des dispositions de la législation nationale, le consentement de la personne concernée, l'exécution d'un contrat ou l'intérêt légitime du responsable du traitement ou d'une tierce partie qui ne l'emporte pas sur les intérêts de la personne concernée.

87. En vertu de la loi sur la protection des informations personnelles, le consentement joue un rôle central dans le système juridique japonais de protection des données. Le consentement est le fondement juridique central du traitement des données à caractère personnel au Japon, ainsi que l'un des principaux fondements juridiques du transfert de données à caractère personnel depuis le Japon vers un pays tiers. En outre, le consentement est requis en vue d'une modification de la finalité du traitement.

88. Conformément à la troisième règle supplémentaire, le traitement des données à caractère personnel transférées depuis l'Union vers le Japon reposera sur le même fondement juridique que le transfert vers le Japon. Si l'opérateur commercial traitant des données à caractère personnel souhaite traiter ultérieurement ces données pour une autre finalité, il doit obtenir au préalable le consentement de la personne concernée.

[35] WP 254, p. 6.

89. Le CEPD estime que la qualité du consentement, notamment en raison de son rôle central dans le cadre juridique japonais, doit être conforme aux exigences fondamentales de la notion de consentement, à savoir, selon le droit de l'Union, une «*manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte* [...]». La personne concernée peut retirer ce consentement à tout moment, en tant que garantie essentielle de sa libre volonté[36]. Le droit de retrait, qui constitue un élément obligatoire du consentement, semble être absent dans le cadre juridique japonais. En effet, selon les lignes directrices de la PPC[37], le retrait est simplement «souhaitable» et subordonné aux «caractéristiques, à la taille et au statut des activités commerciales».

3.1.3 Le principe de transparence

90. Sur la base de l'article 5 du RGPD, la transparence est un principe fondamental du système de protection des données de l'Union[38]. Le référentiel d'adéquation considère la «transparence» comme l'un des principes touchant au contenu dont il convient de tenir compte lors de l'évaluation du niveau de protection substantiellement équivalent assuré par un pays tiers. Le principe de transparence et d'équité vise à garantir que la personne concernée a le contrôle de ses données et, à cette fin, des informations doivent lui être fournies, en règle générale de manière proactive. Dans le cas du bouclier de protection des données, dans son avis 1/2016, le groupe de travail «article 29»[39] fait référence à l'annexe II, II.1.b de l'accord relatif au bouclier (avis à la personne concernée) et a déclaré que si les données ne sont pas collectées directement, une organisation devrait en informer la personne concernée «au moment où les données sont enregistrées par l'organisation participant au bouclier» (section 2.2.1.a). La mise à la disposition du public de la politique de protection de la vie privée constitue un critère supplémentaire (voir la section 2.2.1.b). Dès lors, en vertu de la directive 95/46/CE, il a été jugé nécessaire d'informer directement la personne concernée.

91. Une première préoccupation concerne la modalité d'information de la personne concernée prévue par la loi sur la protection des informations personnelles. En vertu de l'article 27, paragraphe 1, de la loi sur la protection des informations personnelles, un opérateur commercial traitant des données à caractère personnel est tenu de fournir les informations mentionnées dans cet article en «faisant en sorte que la personne concernée puisse en prendre connaissance». Toutefois, cette formulation n'indique pas clairement dans quelle mesure l'opérateur commercial traitant des données à caractère personnel doit prendre des mesures positives pour informer effectivement la personne concernée.

92. **Le CEPD invite la Commission à préciser la signification de l'expression «puisse en prendre connaissance» et à spécifier si la loi sur la protection des informations personnelles prévoit légalement l'obligation d'informer effectivement les personnes concernées.**

---

[36] Article 4, paragraphe 11, du RGPD. Pour de plus amples informations, voir également les lignes directrices pertinentes de l'EDPB concernant le consentement, WP 259, 10 avril 2018.

[37] Data Protection Legal and Technical Research and Analysis Consortium (DPC), «An assessment of the level of protection of personal data provided under Japanese law», p. 46: «[e]n outre, du point de vue de la protection des droits et des intérêts d'un mandant, tel qu'un consommateur, en cas de réception d'une demande du mandant concernant des données à caractère personnel conservées, il est souhaitable de répondre à la demande du mandant par la cessation de tout autre envoi de démarchage ou par la cessation volontaire de toute utilisation, par exemple, en tenant compte des caractéristiques, de la taille et du statut des activités commerciales».

[38] WP 254, chapitre 3, point 7, p. 7; voir également le considérant 39 du RGPD.

[39] Ce groupe de travail a été institué par l'article 29 de la directive 95/46/CE. Il s'agissait d'un organe consultatif européen indépendant sur la protection des données et le respect de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE. Le groupe de travail «article 29» est désormais devenu le comité européen de la protection des données.

93. En outre, en vertu du référentiel d'adéquation, des restrictions peuvent s'appliquer concernant les informations à fournir aux personnes concernées, à l'instar de l'article 23 du RGPD. Dans le même ordre d'idées, l'article 14, paragraphe 5, du RGPD prévoit une exception au droit d'être informé lorsque la fourniture des informations est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement. Toutefois, en pareil cas, le responsable du traitement fournit quand même certaines informations, par exemple en rendant des informations «généralisées» publiquement disponibles. En outre, lorsque le risque cesse d'exister, la personne concernée doit en être informée[40]. Ces aspects sont importants pour garantir le principe fondamental de loyauté.

94. En vertu de l'article 23 de la loi sur la protection des informations personnelles, un opérateur commercial traitant des données à caractère personnel est tenu, en règle générale, d'informer au préalable la personne concernée du transfert de ses données à un tiers, soit implicitement lorsqu'il obtient son consentement, soit explicitement par une notification par laquelle la personne concernée peut signifier son refus. Le CEPD comprend qu'il n'y a pas de notification à la personne concernée, l'informant du fait que ses données ne constituent pas des données à caractère personnel conservées dans le cadre de la loi sur la protection des informations personnelles étant donné qu'elles relèvent des exceptions prévues à l'article 4 du décret ministériel. En conséquence, la personne ne peut jouir pleinement de ses droits. Les personnes concernées ne sont pas non plus informées dans les cas énoncés à l'article 18, paragraphe 4, de la loi sur la protection des informations personnelles.

95. **Le CEPD reconnaît que les droits peuvent être limités pour des objectifs légitimes poursuivis par l'opérateur commercial traitant des données à caractère personnel et par les autorités nationales. Dans un même temps, le CEPD estime que les personnes concernées doivent au moins être informées au préalable de manière générale de la possibilité de restriction de leurs droits aux fins visées par la loi et qu'elles doivent être informées lorsque les risques au regard desquels l'information est restreinte cessent d'exister.**

96. Enfin, d'autres aspects de la transparence sont développés plus en détail ci-après. Il s'agit des risques que comporte le transfert vers un pays tiers[41] et des informations sur la logique du traitement dans le contexte du processus de prise de décision automatisé, y compris le profilage[42].

3.1.4 Restrictions applicables aux transferts ultérieurs

97. Le CEPD salue les efforts déployés par les autorités japonaises et par la Commission européenne pour renforcer le niveau de protection des transferts ultérieurs dans la quatrième règle supplémentaire, qui exclut le transfert ultérieur de données à caractère personnel de l'Union vers un pays tiers sur la base des règles transfrontalières de protection de la vie privée de la Coopération économique Asie-Pacifique. En outre, le CEPD reconnaît qu'aux considérants 177 et 184 de la nouvelle version de son projet de décision d'adéquation, la Commission européenne s'est engagée à suspendre la décision d'adéquation lorsque les transferts ultérieurs ne garantissent plus la continuité de la protection. Toutefois, le CEPD souhaite soulever deux points concernant ces transferts de données à caractère personnel de l'Union du Japon vers des pays tiers.

98. **L'utilisation du consentement comme fondement pour les transferts de données du Japon vers un pays tiers dans le système juridique japonais suscite des inquiétudes, étant donné que le CEPD**

[40] Arrêts du 21 décembre 2016, Tele2, affaires jointes C-203/15 et C-698/15, EU:C:2016:970, point 121; et du 8 avril 2014, Digital Rights Ireland, affaires jointes C-293/12 et C-594/12, EU:C:2014:238, points 54 à 62.
[41] Voir la section 2.1.4.
[42] Voir la section 2.1.6.

estime que les informations fournies à la personne concernée de l'Union avant qu'elle ne donne son consentement ne semblent pas exhaustives.

99. L'article 24 de la loi sur la protection des informations personnelles interdit le transfert de données à caractère personnel vers un tiers situé hors du territoire du Japon sans le consentement préalable de la personne concernée. La quatrième règle supplémentaire dispose que les personnes concernées de l'Union doivent recevoir des informations sur les circonstances entourant le transfert qui sont nécessaires pour qu'elles puissent prendre une décision quant à l'opportunité de donner leur consentement.

100. Dans son projet de décision d'adéquation, la Commission européenne conclut que la quatrième règle supplémentaire garantit un consentement particulièrement éclairé de la personne concernée de l'Union[43], étant donné qu'elle sera informée du fait que ses données seront transférées à l'étranger, ainsi que du pays de destination spécifique. Une telle information permettrait à la personne concernée d'évaluer le risque lié au respect de sa vie privée associé au transfert.

101. En vertu du principe de transparence du référentiel d'adéquation, un certain degré de loyauté doit être garanti lorsque les personnes concernées sont informées. Dans le contexte des transferts ultérieurs fondés sur le consentement, le CEPD est d'avis que, pour garantir un tel degré approprié de loyauté, les personnes concernées devraient être explicitement informées des risques éventuels impliqués par de tels transferts découlant de l'absence de protection adéquate dans le pays tiers et de l'absence de garanties appropriées avant le consentement. Cet avertissement devrait par exemple indiquer que le pays tiers est susceptible de ne pas disposer d'une autorité de contrôle et/ou de principes de traitement des données, et/ou de droits des personnes concernées[44]. Pour le CEPD, il est essentiel de fournir ces informations à la personne concernée afin de lui permettre de donner son consentement en pleine connaissance de ces faits particuliers concernant le transfert[45].

102. Le consentement éclairé est également important en ce qui concerne les exclusions sectorielles. La décision d'adéquation ne couvre pas certains types de traitement par certains organismes comme les universités qui traitent des données à caractère personnel à des fins académiques. Les préoccupations exprimées par le CEPD concernent le cas spécifique dans lequel des données transférées depuis l'Union dans le cadre de la décision d'adéquation, par exemple les données personnelles d'étudiants Erasmus au Japon, sont ensuite utilisées à des fins différentes échappant au champ d'application de la décision d'adéquation (par exemple, à des fins de recherche), avec le consentement de la personne concernée, et ne sont donc plus couvertes par la protection supplémentaire garantie par les règles complémentaires.

103. La Commission européenne déclare au considérant 38 de son projet de décision d'adéquation qu'un tel scénario relèvera du cadre des transferts ultérieurs et qu'en pareil cas, l'opérateur commercial traitant des données à caractère personnel doit fournir à la personne concernée toutes les informations nécessaires avant d'obtenir son consentement, y compris l'informer du fait que les

[43] Décision d'exécution de la Commission européenne du XXXX, conformément au règlement nº 2016/679 du Parlement européen et du Conseil, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, envoyée au comité européen de la protection des données le 13 novembre 2018, considérant 76.

[44] Lignes directrices 2/2018 du comité européen de la protection des données relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, 25 mai 2018, p. 9.

[45] Lignes directrices 2/2018 du comité européen de la protection des données relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, 25 mai 2018, p. 9.

informations à caractère personnel ne relèveraient pas de la protection assurée par les règles de la loi sur la protection des informations personnelles.

104. La quatrième règle supplémentaire exige uniquement que l'opérateur commercial traitant des données à caractère personnel obtienne le consentement de la personne concernée après lui avoir fourni des informations sur les circonstances entourant le transfert qui sont nécessaires pour qu'elle puisse prendre une décision quant à l'opportunité de donner son consentement.

105. **Le CEPD invite la Commission européenne à veiller à ce que les informations devant être fournies à la personne concernée «sur les circonstances entourant le transfert» comprennent les informations relatives aux risques éventuels impliqués par de tels transferts découlant de l'absence de protection adéquate dans le pays tiers et de l'absence de garanties appropriées ou, dans le cas des exclusions sectorielles, de l'absence de la protection assurée par les règles supplémentaires et par la loi sur la protection des informations personnelles.**

106. **Des transferts ultérieurs de données à caractère personnel peuvent avoir lieu vers des pays tiers, qui feront l'objet d'une éventuelle décision d'adéquation ultérieure du Japon.**

107. Sans préjudice des dérogations prévues à l'article 23, paragraphe 1, de la loi sur la protection des informations personnelles, les données initialement transférées depuis l'Union vers le Japon peuvent être transférées du Japon vers un pays tiers sans consentement dans deux cas:

- si l'opérateur commercial traitant des données à caractère personnel et le bénéficiaire tiers ont conjointement mis en place des mesures garantissant un niveau de protection équivalent à celui garanti par la loi sur la protection des informations personnelles lue en conjonction avec les règles supplémentaires , au moyen d'un contrat, d'autres formes d'accords contraignants ou d'accords contraignants au sein d'un groupe d'entreprises[46];
- si le pays tiers a été reconnu par la PPC en vertu de l'article 24 de la loi sur la protection des informations personnelles et de l'article 11 des règles de la PPC[47] comme offrant un niveau de protection équivalent à celui garanti au Japon.

108. Le CEPD considère l'article 24 de la loi sur la protection des informations personnelles comme une règle plus spécifique, énonçant une dérogation à la règle générale figurant à l'article 23. Par conséquent, le CEPD ne partage pas l'appréciation formulée par la Commission européenne dans la nouvelle dernière phrase du considérant 78 du projet de décision d'adéquation indiquant que, même dans ces cas, le transfert à destination du tiers reste soumis à l'obligation d'obtenir un consentement au titre de l'article 23, paragraphe 1, de la loi sur la protection des informations personnelles.

109. Conformément à l'article 11, paragraphe 1, des règles de la PPC, une décision d'adéquation de la PPC requiert des normes matérielles équivalentes à celles de la loi sur la protection des informations personnelles, dont la mise en œuvre est assurée dans le pays tiers et qui sont effectivement contrôlées par une autorité indépendante chargée de faire appliquer la législation. En outre, la PPC peut imposer les conditions nécessaires pour protéger les droits et les intérêts des personnes au Japon, conformément à l'article 11, paragraphe 2, des règles qu'elle a édictées.

[46] Quatrième règle complémentaire, point ii).

[47] Règles du 30 mai 2017 portant exécution de la loi sur la protection des informations personnelles. Une traduction en anglais du nouvel article 11 a été communiquée à l'EDPB par la Commission européenne, mais cet article n'a pas encore été publié.

110. La quatrième règle supplémentaire dispose que les données à caractère personnel de l'Union peuvent être transférées vers un pays tiers faisant l'objet d'une décision d'adéquation du Japon sans autres restrictions. Toutefois, l'article 44 du RGPD prévoit que tout transfert de données à caractère personnel vers un pays tiers doit remplir les conditions énoncées au chapitre V du RGPD, y compris pour les transferts ultérieurs du pays tiers vers un autre pays tiers. Le niveau de protection des personnes physiques dont les données sont transférées ne doit pas être compromis par le transfert ultérieur[48]. Bien que cette interprétation soit en principe également partagée par la Commission européenne dans son projet de décision d'adéquation[49], elle ne semble pas être complètement suivie. La Commission européenne a négocié l'interdiction du transfert des données provenant de l'Union vers un pays tiers sur la base des règles transfrontalières de protection de la vie privée (ci-après les «RTPVP») de la Coopération économique Asie-Pacifique (APEC). À la lumière de l'outil mis au point en 2014 dans le cadre de la directive européenne comparant les règles d'entreprise contraignantes et les règles transfrontalières de protection de la vie privée, qui met en évidence les exigences, convergences et différences des deux systèmes (avis 02/2014 du G29), le CEPD est préoccupé par l'utilisation des RTPVP comme outil de transfert ultérieur de données à caractère personnel transférées depuis l'Union vers des pays autres que le Japon.

111. En revanche, les transferts ultérieurs de données à caractère personnel transférées de l'Union vers le Japon sur la base d'une décision d'adéquation japonaise semblent être acceptés par la Commission européenne, sans que la PPC puisse imposer les règles supplémentaires comme conditions en vue de protéger les droits et les intérêts des citoyens de l'Union, si nécessaire. Le CEPD déduit de l'article 44 du RGPD que la protection renforcée des données transférées de l'Union vers le Japon prévue dans les règles supplémentaires doit toujours être étendue lorsque des données à caractère personnel transférées depuis l'Union vers le Japon sont ultérieurement transférées vers un pays tiers, si le cadre de protection des données de ce pays n'est pas reconnu comme étant substantiellement équivalent au RGPD.

112. **Par conséquent, le CEPD invite la Commission européenne à assumer son rôle de contrôle et à garantir le maintien du niveau de protection des données de l'Union ou à envisager la suspension de cette décision d'adéquation si des données à caractère personnel transférées de l'Union vers le Japon sont ultérieurement transférées vers des pays tiers sous réserve d'une éventuelle future décision d'adéquation du Japon, lorsque ces pays tiers n'ont pas fait l'objet d'une évaluation préalable ou d'un constat d'adéquation de l'Union.**

3.1.5 Démarchage

113. Conformément à la troisième règle supplémentaire, un opérateur commercial traitant des données à caractère personnel n'est pas autorisé à traiter à des fins de démarchage des données transférées depuis l'Union européenne à une autre fin, si la personne concernée de l'Union n'a pas donné son consentement à la modification de la finalité de l'utilisation.

114. Selon le référentiel d'adéquation, si les données sont traitées à des fins de démarchage, la personne concernée devrait avoir le droit de s'opposer à tout moment, sans frais, au traitement des données la concernant à ces fins. En vertu de l'article 16 de la loi sur la protection des informations personnelles, un opérateur commercial traitant des données à caractère personnel n'est autorisé à traiter des

[48] WP 254, p. 7.

[49] Décision d'exécution de la Commission européenne du XXXX, conformément au règlement nº 2016/679 du Parlement européen et du Conseil, constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, envoyée au comité européen de la protection des données le 13 novembre 2018, considérant 75.

informations à caractère personnel que si la personne concernée donne son consentement. Le retrait du consentement pourrait avoir le même effet que le droit privilégié à s'opposer au démarchage.

115. Le cadre japonais en matière de protection des données ne prévoit pas de droit privilégié d'opposition et, comme expliqué ci-dessus dans la section relative au consentement, le retrait du consentement dans le cadre des lignes directrices de la PPC est simplement souhaitable et conditionnel et ne peut donc être considéré comme équivalent à un droit d'opposition permanent, comme l'exigent le référentiel d'adéquation. **Le CEPD invite la Commission européenne à fournir des garanties quant au droit de retrait du consentement et à examiner des cas de démarchage.**

3.1.6 Prise de décision automatisée et profilage

116. Selon le référentiel d'adéquation, les décisions prises sur le seul fondement d'un traitement automatisé (prise de décision individuelle automatisée), y compris le profilage, qui produisent des effets juridiques ou affectent la personne concernée de manière significative ne sont possibles que dans certaines conditions définies dans le cadre juridique du pays tiers. Par conséquent, tous les cas de prise de décision automatisée et de profilage dans les circonstances susmentionnées doivent reposer sur un fondement juridique.

117. Dans le cadre européen, ces conditions correspondent notamment à la nécessité d'obtenir le consentement explicite[50] de la personne concernée ou à la nécessité de cette décision pour la conclusion d'un contrat. Si la décision ne respecte pas les conditions telles qu'elles sont définies dans le cadre juridique du pays tiers, la personne concernée devrait avoir le droit de ne pas être soumise à la décision. La législation du pays tiers devrait, dans tous les cas, prévoir les garanties nécessaires, notamment le droit d'être informé des raisons particulières sous-tendant la décision et la logique concernée, de corriger des informations inexactes ou incomplètes et de contester la décision si elle est adoptée sur une base factuelle incorrecte.

118. La décision de la Commission fait uniquement référence au secteur bancaire, dans lequel des règles sectorielles[51] relatives aux décisions automatisées seraient applicables. Les lignes directrices détaillées pour la surveillance des grandes banques mentionnées au considérant 93 du projet de décision d'adéquation indiquent que la personne concernée doit recevoir des explications spécifiques sur les motifs du refus d'une demande de conclusion d'un contrat de prêt.

119. Les arguments de la Commission européenne présentés dans le projet de décision d'adéquation (considérant 94), selon lesquels l'absence de règles spécifiques concernant la prise de décision automatisée dans la loi sur la protection des informations personnelles n'est pas susceptible d'affecter le niveau de protection semblent (entre autres) ne pas tenir compte du cas dans lequel des données à caractère personnel transférées depuis l'Union sont ultérieurement traitées par un autre responsable du traitement japonais (différent de l'importateur de données initial japonais).

120. Il semble donc qu'il n'existe au Japon aucune règle générale applicable à l'ensemble des secteurs régissant la prise de décision automatisée et le profilage.

121. **Le CEPD invite la Commission européenne à examiner des cas de prise de décision automatisée et de profilage.**

3.2 Mécanismes en matière de procédure et d'application

[50] Pour les remarques critiques concernant la notion de consentement dans le cadre juridique japonais en matière de protection des données, voir 2.1. Généralités et 2.2.8. Démarchage.

[51] Ces règles sectorielles n'ont pas été fournies à l'EDPB.

122. Sur la base des principes établis dans le référentiel d'adéquation , le CEPD a analysé les aspects suivants de la protection des données et du cadre juridique japonais, tels que couverts par le projet de décision d'adéquation: l'existence d'une autorité de contrôle indépendante fonctionnant de manière efficace, l'existence d'un système garantissant un niveau de conformité satisfaisant et l'existence d'un système d'accès aux mécanismes de recours appropriés permettant aux citoyens de l'Union d'exercer leurs droits et de disposer de voies de recours administratives et judiciaires sans être confrontés à des obstacles majeurs.

123. Sur la base des paramètres établis par la CJUE dans l'affaire Schrems[52] et ceux décrits au considérant 104 et à l'article 45 du RGPD, le CEPD estime que, bien que le système japonais soit cohérent avec le système européen, il peut être difficilement accessible dans la pratique aux citoyens de l'Union dont les données seront transférées dans le cadre de la présente décision d'adéquation, compte tenu de l'existence d'obstacles linguistiques et institutionnels.

124. Les sections ci-dessous examinent les aspects susmentionnés du cadre japonais avant de formuler des recommandations à l'intention de la Commission.

3.2.1 Autorité de contrôle indépendante compétente

125. La PPC a été établie le 1er janvier 2016 à la suite des modifications apportées à la loi sur la protection des informations personnelles en 2015, en remplacement de la commission spécifique de protection des informations personnelles (créée en 2013 en vertu de la loi japonaise «Mon numéro»). Bien qu'elle n'ait été établie que récemment, la PPC a, depuis sa création, déployé des efforts considérables pour mettre en place l'infrastructure nécessaire à la mise en œuvre de la loi sur la protection des informations personnelles modifiée. Il convient de citer à cet égard l'élaboration de règles et de lignes directrices visant à fournir des orientations aux opérateurs commerciaux traitant des données à caractère personnel sur l'interprétation à donner à la loi sur la protection des informations personnelles, la publication d'un document de questions et réponses[53] et la mise en service d'une ligne d'assistance chargée de conseiller les opérateurs économiques et les citoyens sur les dispositions relatives à la protection des données, ainsi que d'un service de médiation compétent pour traiter les plaintes.

126. L'établissement et le fonctionnement de la PPC sont régis au chapitre V de la loi sur la protection des informations personnelles. Bien que la PPC relève de la compétence du Premier ministre, l'article 62 dispose qu'elle exerce sa fonction de manière indépendante. Le CEPD salue la clarification apportée par la Commission européenne dans le projet modifié de décision d'adéquation communiqué le 13 novembre 2018, destinée à décrire plus en détail le degré de liberté de la PPC à l'égard des influences internes et externes.

3.2.2 Le système de protection des données doit assurer un niveau de conformité satisfaisant

127. Le projet de décision d'adéquation procède à un examen complet des pouvoirs conférés à la PPC en vertu des articles 40, 41 et 42 de la loi sur la protection des informations personnelles afin d'assurer le suivi et l'application de la législation. L'article 40 habilite la PPC à demander aux opérateurs commerciaux traitant des données à caractère personnel de lui soumettre des rapports et des documents relatifs aux opérations de traitement et à procéder à des inspections sur place. En vertu de l'article 42, la PPC a le pouvoir d'émettre des recommandations lorsqu'elle reconnaît qu'il est

[52] Arrêt du 6 octobre 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14, EU:C:2015:650, points 73 et 74.
[53] Ce document n'a pas été fourni par la Commission européenne à l'EDPB en anglais.

nécessaire de protéger les droits individuels ou lorsqu'elle constate une violation des dispositions de la loi et, si cela ne suffit pas, elle peut ordonner à des opérateurs commerciaux traitant des données à caractère personnel de mettre un terme à la violation ou de prendre les mesures nécessaires pour remédier à cette violation.

128. En octobre 2018, la PPC a pris l'une de ses premières mesures au titre de l'article 41 de la loi modifiée sur la protection des informations personnelles et a émis des «directives» à l'intention d'un opérateur commercial traitant des données à caractère personnel, dans lesquelles elle recommande à la société de renforcer ses mesures de sécurité et de superviser efficacement les fournisseurs d'applications. Elle donne également des explications claires et faciles à comprendre sur la manière d'utiliser les informations à caractère personnel, d'obtenir préalablement le consentement lorsque les informations sont partagées avec un tiers et de répondre de manière adéquate à la demande des utilisateurs qui souhaitent obtenir l'effacement de leurs données. Dans les réponses fournies au CEPD[54], des responsables de la PPC ont indiqué que la société avait manifesté sa volonté de coopérer et qu'à défaut, elle lui enverrait des «recommandations» comme prévu par l'article 42, paragraphe 1, de la loi sur la protection des informations personnelles.

129. L'enquête menée par la PPC concernant l'opérateur commercial traitant des données à caractère personnel susmentionné est un indicateur très positif des efforts déployés par l'autorité de contrôle japonaise pour garantir un niveau de conformité satisfaisant dans le pays.

130. Bien que les améliorations par rapport au cadre en place avant les modifications de 2015 soient manifestes, le CEPD note que la PPC dispose de moins de pouvoirs que les autorités de protection des données européennes en vertu du RGPD, en particulier en matière **répressive**. Les amendes administratives[55], par exemple, sont relativement modérées. La décision de la Commission européenne souligne au considérant 108 le fait qu'en cas de non-respect ou en présence de certaines violations de la loi sur la protection des informations personnelles, des sanctions pénales sont prévues et que le président de la PPC peut transmettre les dossiers au ministère public. Toutefois, la décision de la Commission européenne ne tient pas compte du fait que les poursuites publiques au Japon sont discrétionnaires et peuvent parfois faire l'objet de longues procédures d'enquête[56]. En outre, la peine d'emprisonnement (assortie ou non de travaux) associée à des violations de la loi sur la protection des informations personnelles en vertu des dispositions du chapitre VII peut être difficile à exécuter parce qu'elle s'adresse aux personnes physiques et, en tout état de cause, ne sanctionne pas l'opérateur commercial traitant des données à caractère personnel en tant qu'entité juridique n'exerçant pas ses obligations de responsabilité.

131. **À la lumière de ce qui précède, le CEPD invite la Commission européenne à surveiller de près l'efficacité des sanctions et des recours dans le système japonais de protection des données.**

[54] Annexe III.

[55] Elles figurent au chapitre VII de la loi sur la protection des informations personnelles. La peine maximale est fixée à l'article 83 (la fourniture ou l'utilisation non autorisée d'une base de données contenant des informations personnelles pour en tirer un profit illicite ou pour qu'un tiers en tire un profit illicite) et équivaut à une peine d'emprisonnement d'un an avec travaux ou à une amende d'un maximum de 500 000 yens (environ 3 900 euros). Selon les explications fournies par la Commission, les amendes sont cumulées par infraction. Même en cas d'amendes cumulatives, l'EDPB observe cependant que le montant total demeure généralement fort bas par rapport aux normes européennes.

[65] Oda H., Japanese Law, Oxford University Press (3e édition), 2009, p. 439 et 440.

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

132. La PPC fournit des informations et des lignes directrices détaillées sur son site web, qui visent à sensibiliser les opérateurs commerciaux traitant des données à caractère personnel à leurs obligations et responsabilités dans le cadre de la protection des données. Elle a également mis en place un service d'assistance chargé de fournir des informations et un soutien aux citoyens japonais en ce qui concerne les droits individuels dont ils disposent en vertu de la loi sur la protection des informations personnelles. Le site web comporte par ailleurs une section intitulée «chambre des enfants», explicitement destinée à un public d'enfants et de jeunes. Le CEPD fait observer que ces informations, ainsi que l'assistance, les lignes directrices et les questions & réponses, sont disponibles en japonais[57]. Par conséquent, le CEPD est fermement convaincu qu'il serait utile que la PPC intègre dans la version anglaise de son site web une page fournissant des informations sur les droits individuels au titre du cadre japonais de protection des données et des règles supplémentaires à l'intention des citoyens de l'Union dont les données seront transférées au Japon en vertu de la décision d'adéquation de la Commission européenne.

133. Le CEPD salue la clarification apportée par la Commission européenne au considérant 104 du projet modifié de décision d'adéquation communiqué le 13 novembre 2018 concernant le service de médiation géré par la PPC conformément à l'article 61, point ii), de la loi sur la protection des informations personnelles. Le CEPD souhaite toutefois soulever trois points à cet égard. Premièrement, le service de médiation ne fait pas l'objet d'une publicité sur la version anglaise du site web de la commission de protection des données à caractère personnel. Deuxièmement, le service n'est accessible que par téléphone et en japonais. Enfin, la médiation n'est qu'un processus de facilitation qui ne débouche pas sur un accord contraignant entre les parties, ce qui a des conséquences sur l'efficacité des voies de recours accessibles aux personnes concernées[58].

134. Enfin, le CEPD constate que le projet de décision d'adéquation met l'accent sur les voies de recours disponibles dans le cadre des procédures civiles et pénales, mais ne reconnaît pas l'existence d'**obstacles institutionnels aux procédures contentieuses** au Japon, tels que les frais de justice (les frais de justice sont répartis de manière égale entre le demandeur et le défendeur, quelle que soit la partie qui gagne le procès[59]), la pénurie d'avocats dans le pays[60], le fait que les avocats étrangers ne sont pas autorisés à pratiquer le droit national ainsi que la charge de la preuve exigée par le droit de la responsabilité délictuelle. Le CEPD craint que ces facteurs puissent dans la pratique entraver l'accès des particuliers à la justice et compromettre la possibilité de faire valoir leurs droits rapidement et sans coût prohibitif.

135. À la lumière de ce qui précède, **le CEPD craint qu'il existe un risque que les citoyens de l'Union éprouvent des difficultés à accéder aux voies de recours administratives et judiciaires** et, par conséquent, il apprécierait que la Commission européenne discute avec la PPC de la possibilité de mettre en place un service en ligne, au moins en anglais, **dans le but d'apporter un soutien aux**

[57] https://www.ppc.go.jp/en/contactus/piinquiry/.

[58] Kojima T., *Civil Procedure and ADR in Japan*, Chuo University Press, 2004; et Menkel-Meadow C., *Dispute Processing and Conflict Resolution: Theory, Practice and Policy*, Ashgate (2003).

[59] Wagatsuma (2012), «Recent Issues of Cost and Fee Allocation in Japanese Civil Procedure» dans Reimann (ed.), Cost and Fee Allocation in Civil Procedure – Ius Gentium; comparative Perspectives on Law and Justice Vol. 11, p. 195 à 200.

[60] Selon les derniers chiffres, le Japon compte 38 980 avocats, soit environ 290 par million d'habitants (Fédération japonaise des barreaux, Livre blanc sur les avocats, 2017 p. 8 et 9).

citoyens de l'Union et de traiter leurs plaintes[61]. En outre, le CEPD serait favorable à la possibilité d'autoriser les autorités de protection des données de l'Union européenne à agir en tant qu'intermédiaires pour les plaintes soumises par des personnes concernées de l'Union auprès d'organisations actives au Japon et auprès de la PPC.

4 CONCERNANT L'ACCÈS DES AUTORITÉS PUBLIQUES AUX DONNÉES TRANSFÉRÉES AU JAPON

136. L'intention de la Commission est de reconnaître, par le biais de la décision d'adéquation, que « le Japon assure un niveau de protection adéquat des données à caractère personnel transférées de l'Union européenne vers les opérateurs commerciaux traitant des données à caractère personnel au Japon », comme indiqué à l'article 1er du projet de décision d'adéquation. Conformément à l'article 45, paragraphe 2, du RGPD, la Commission a également analysé les restrictions et les garanties en ce qui concerne l'accès des autorités publiques aux données à caractère personnel. Le présent chapitre se concentre sur l'évaluation de l'accès aux données à caractère personnel par les autorités répressives et par d'autres entités publiques à des fins de sécurité nationale. L'analyse de le CEPD se fonde sur le projet de décision d'adéquation, sur son annexe II, dans laquelle le gouvernement japonais brosse un tableau du cadre juridique pertinent, et sur les textes juridiques japonais fournis par la Commission. Par conséquent, dans le contexte spécifique de cette évaluation, le CEPD a pris en considération certains éléments relatifs à la législation japonaise qui ne figurent pas dans les conclusions de la Commission européenne, mais sont pertinents pour apprécier les conditions et les garanties au titre desquelles les autorités publiques japonaises sont autorisées à avoir accès à des données à caractère personnel transférées depuis l'Union européenne.

4.1 Accès des services répressifs aux données

4.1.1 Procédures d'accès aux données dans le domaine du droit pénal

137. Le projet de décision d'adéquation présente trois voies, prévues par la législation japonaise, par lesquelles les autorités répressives peuvent accéder aux données au Japon.

4.1.1.1 Demandes d'accès sur la base d'un mandat délivré par un tribunal

138. Le projet de décision d'adéquation indique que les accès par le gouvernement japonais, et en particulier par les autorités chargées de faire appliquer le droit pénal, celles-ci doivent toujours disposer d'un mandat pour demander l'accès à des éléments de preuve électroniques dans le cadre d'enquêtes pénales, à moins d'avoir recours à la procédure de divulgation volontaire exposée ci-dessous.

4.1.1.1.1 Exigence d'une «cause adéquate», nécessité et proportionnalité des mandats

139. Le CEPD reconnaît qu'en vertu de la constitution japonaise, toute collecte contraignante de données à caractère personnel doit être fondée sur un mandat délivré par un juge. Plus précisément, le projet de décision d'adéquation indique que, dans tous les cas de « perquisitions et saisies », les mandats de justice doivent être délivrés pour une « cause adéquate », qui n'existe selon la Cour suprême que lorsque la personne concernée (suspect ou accusé) est considérée comme ayant commis une infraction et que la perquisition et la saisie sont nécessaires aux fins de l'enquête pénale. La Commission renvoie ici à l'arrêt de la Cour suprême japonaise du 18 mars 1969 rendu dans l'affaire nº 100 [1968 (Shi.)]. Le

[61] Semblable à celui envisagé à l'annexe II de la décision d'adéquation pour les plaintes des résidents de l'Union concernant l'accès à leurs données par les autorités publiques japonaises.

CEPD rappelle qu'en vertu de la jurisprudence de la CJUE[62], seule une juridiction, et non un procureur par exemple, peut autoriser la collecte de données relatives au trafic et des données de localisation en particulier.

140. À la lumière également de la jurisprudence de la CJUE selon laquelle l'accès aux données peut être soumis à la délivrance d'un mandat, comme dans l'affaire Tele2, le CEPD regrette qu'aucune information additionnelle n'ait été fournie afin de déterminer de quelle manière les critères d'évaluation de la nécessité de délivrance d'un mandat - à savoir la gravité des faits et la manière dont ils ont été commis, la valeur et l'importance des biens saisis en tant qu'éléments de preuve, la probabilité d'une dissimulation ou de la destruction des biens saisis, l'étendue du préjudice causé par la saisie et les autres conditions y relatives - ainsi que la notion de « cause adéquate » tirée de la constitution sont appliqués dans la pratique. Par conséquent, le CEPD invite la Commission à contrôler si la délivrance de mandats répond dans la pratique aux critères énoncés par la CJUE.

4.1.1.1.2 Types de crimes et délits pour lesquels des mandats peuvent être délivrés

141. La procédure d'émission d'un mandat n'est applicable que dans le cadre des « enquêtes obligatoires ». En principe, un mandat ne peut être délivré qu'en cas de violation de la loi. À cet égard, le CEPD prend acte de l'adoption récente, le 15 juin 2017, de la « loi sur la répression du crime organisé et sur le contrôle des revenus délictueux » à la suite de l'adhésion du Japon à la convention des Nations unies contre la criminalité transnationale organisée (UNTOC)[63]. En l'absence d'une version anglaise de cette loi, compte tenu de l'exigence énoncée dans la législation de l'Union de ne collecter certaines données que dans le cadre de la recherche, de la détection et de la poursuite de la criminalité grave[64], et eu égard aux préoccupations exprimées par plusieurs commentateurs, y compris le rapporteur spécial des Nations unies, Joseph Cannataci[65], concernant l'ampleur de la portée de la loi, qui s'appuie sur une définition du « groupe criminel organisé » qui serait vague et trop large, le CEPD n'est pas en mesure de conclure que l'accès aux preuves électroniques en vertu de la législation japonaise pertinente est limité comme prévu par le droit de l'Union européenne.

142. Il convient également de noter que la police préfectorale est compétente pour certains types d'infractions et qu'elle dispose de ses ordonnances de police spécifiques. Le CEPD n'a pas eu accès aux règles internes applicables à la police préfectorale.

143. Selon le projet de décision d'adéquation, la collecte d'informations électroniques dans le domaine de l'application du droit pénal relève de la compétence de la police préfectorale.

4.1.1.2 Mandats de mise sur écoute

144. L'annexe II du projet de décision d'adéquation indique que la loi sur les écoutes téléphoniques dans le cadre d'enquêtes pénales prévoit des spécificités concernant l'interception des communications. Cette législation a été communiquée très tardivement, de sorte qu'une analyse approfondie n'a pu être effectuée. Par conséquent, bien que de nombreuses garanties semblent être prévues dans ce cadre juridique, le CEPD n'est pas en mesure d'apprécier si les conditions fixées dans cet acte législatif sont entourées de garanties substantiellement équivalentes à celles exigées dans l'Union par la charte, telle

[62] Voir les arrêts du 21 décembre 2016, Tele2, C-203/15, EU:C:2016:970; et du 8 avril 2014, Digital Rights Ireland Ltd, affaires jointes C-293/12 et C-594/12, EU:C:2014:238.
[63] Voir: https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html.
[64] Voir les arrêts du 8 avril 2014, Digital Rights Ireland Ltd, affaires jointes C-293/12 et C-594/12, EU:C:2014:238; et du 21 décembre 2016, Tele2, C-203/15, EU:C:2016:970.
[65] Rapporteur spécial des Nations unies sur le droit à la vie privée, et Graham Greenleaf, chercheur en droit à l'Université de Nouvelle-Galles du Sud.

qu'interprétée par la Cour de justice de l'Union européenne et par la convention européenne des droits de l'homme, telle qu'interprétée par la Cour de Strasbourg.

4.1.1.3 Procédure de « divulgation volontaire » sur la base d'un formulaire de demande de renseignements

145. Ce type de coopération non obligatoire permet aux autorités publiques de demander aux responsables du traitement (à l'exception des entreprises de télécommunications) de leur fournir les données dont ils disposent. L'exécution ne peut être imposée. L'incertitude subsiste quant aux autorités qui peuvent utiliser ce type de procédure, mais il semble réservé à celles qui enquêtent sur des crimes et délits.

4.1.1.3.1 Conditions d'émission des « formulaires de demande de renseignements »

146. Le CEPD reconnaît que, par référence à la constitution, la Cour suprême japonaise a établi des restrictions à l'utilisation de la « divulgation volontaire »[66]. Il ressort du projet de décision d'adéquation que, concrètement, une « divulgation volontaire » ne peut être demandée par les autorités compétentes que sur la base de l'émission d'un « formulaire de demande de renseignements ». L'envoi d'un tel « formulaire de demande de renseignements » n'est admis que dans le cadre d'une enquête pénale, et implique donc toujours une suspicion concrète relative à un crime ou délit déjà commis. Ces enquêtes sont généralement menées par la police préfectorale, en application des restrictions prévues à l'article 2, paragraphe 2, de la loi sur la police, ce qui signifie qu'elles doivent être pertinentes pour les activités de la police. Toutefois, le CEPD souhaite de plus amples précisions concernant les contours concrets des critères permettant de délivrer un formulaire de demande de renseignements (telles que la jurisprudence illustrant l'application de ces critères) et la relation entre la procédure de divulgation volontaire et la saisie de données sur la base d'un mandat. En effet, il apparaît que même lorsque des données n'ont pas pu être obtenues par le biais de la procédure volontaire, elles peuvent encore être obtenues au moyen d'un mandat si elles sont indispensables aux autorités chargées de l'enquête[67].

4.1.1.3.2 Jurisprudence disponible concernant les limitations à l'utilisation de la divulgation volontaire

147. Les cas cités dans le projet de décision d'adéquation[68] pour illustrer les limitations à l'utilisation des procédures de divulgation volontaire concernent des affaires dans lesquelles la personne accusée a été directement photographiée ou filmée dans l'espace public par la police, et, partant, elles ne donnent que des indications limitées sur les situations dans lesquelles les autorités compétentes peuvent demander à un responsable du traitement de divulguer des données, notamment eu égard aux critères énumérés à l'annexe II concernant la « pertinence des méthodes », qui semblent avoir pour but d'apprécier si une enquête volontaire est « appropriée » ou raisonnable pour atteindre l'objectif de l'enquête. Il en va de même pour le critère général destiné à évaluer la légalité des enquêtes volontaires suivant que « cela puisse être considéré comme raisonnable eu égard aux conventions sociales acceptées ». En outre, l'agence nationale de la police, qui est l'autorité fédérale chargée de toutes les questions relatives à la police judiciaire, a émis des instructions à l'intention de la police préfectorale concernant l'« utilisation adéquate d'une demande de renseignements écrite dans le cadre d'une enquête ». Entre autres, l'enquêteur en chef doit obtenir l'approbation interne d'un fonctionnaire haut gradé. Le CEPD ne dispose d'aucune information quant au caractère contraignant de ces instructions. Le CEPD souligne néanmoins que le recours à cette procédure doit être proportionné ou nécessaire.

---

[66] Voir l'annexe II, page 8.

[67] Voir l'annexe II, page 7.

[68] Voir l'annexe II, page 8, reprenant deux décisions de la Cour suprême du 24 décembre 1969 [1965 (A) nº 1187] et du 15 avril 2008 [2007 (A) nº 839].

4.1.1.3.3 Droits et obligations des responsables du traitement dans le contexte de la divulgation volontaire

148. En outre, il appartient aux responsables du traitement d'accepter de fournir des données (mais ils ne semblent nullement soumis à l'obligation de demander le consentement des personnes concernées ou de les informer), lorsque les demandes ne vont pas à l'encontre d'autres obligations légales (comme les obligations de confidentialité). Le rapport fourni par la Commission semble indiquer qu'après s'être largement conformés aux demandes, les responsables du traitement ont commencé à prendre en considération la protection des données de leurs clients et ont donc commencé à y répondre moins fréquemment.

149. Il reste également à clarifier si les responsables du traitement sont incités à se conformer aux demandes (par exemple, s'ils en retirent un avantage ou s'ils sont exemptés de poursuites, etc.). En particulier, aucune mention n'est faite d'un quelconque principe tel que le « droit de ne pas s'auto-incriminer ».

150. Le CEPD souhaiterait obtenir des informations supplémentaires, si elles sont disponibles, les éventuels données concernant le nombre et le type de demandes, ainsi que les réponses fournies par les responsables du traitement sollicités. À défaut de jurisprudence et de chiffres, le CEPD invite la Commission à contrôler l'efficacité et l'application concrète de cette procédure dans la pratique.

151. Toutefois, le CEPD ne dispose pas de la jurisprudence et des données relatives à cette procédure permettant d'établir ces éléments. Par conséquent, le CEPD n'est pas en mesure d'apprécier l'efficacité et l'application concrète de cette procédure, en l'absence d'éléments supplémentaires concernant la pratique.

4.1.1.4 Conclusion concernant les procédures d'accès aux données à des fins répressives

152. En conclusion, le CEPD reconnaît que le principe selon lequel les autorités compétentes n'ont directement accès aux données à caractère personnel que dans les cas nécessaires et proportionnés à la finalité, et sur la base d'un mandat, correspond aux principales garanties essentielles prévues par la législation de l'Union et la CEDH. À la lumière des constatations ci-dessus, le CEPD demande à la Commission d'examiner le champ d'application de ces mesures, la portée de la procédure de divulgation volontaire et l'application de ces principes par la police préfectorale et par les tribunaux dans la jurisprudence pertinente, et de contrôler également si le cadre juridique japonais fournit les garanties essentielles énoncées par la CJUE sur la base de la Charte et par la Cour EDH sur la base de la convention.

4.1.2 Contrôle dans le domaine du droit pénal

153. Le projet de décision d'adéquation et l'annexe II présentent quatre types de contrôles exercés sur la police, les ministères et les organismes publics.

4.1.2.1 Contrôle judiciaire

4.1.2.1.1 Cas dans lesquels des informations électroniques sont collectées par des moyens contraignants (perquisition et saisie)

154. Selon le projet de décision d'adéquation, dans tous les cas dans lesquels des informations électroniques sont collectées par des moyens obligatoires (perquisition et saisie), la police doit obtenir un mandat au préalable. Il existe toutefois une exception à cette règle[69]. En effet, l'article 220, paragraphe 1, du code de procédure pénale permet à un procureur, à son substitut, ou à un fonctionnaire de la police judiciaire, de rechercher ou de saisir des informations électroniques sur le

[69] Voir l'annexe II.

lieu de l'arrestation, lorsqu'ils arrêtent un suspect. Dans une telle situation, il reste la possibilité que ces informations soient exclues des éléments de preuve par un juge.

155. Le CEPD a conscience du fait que des exceptions similaires existent également dans le droit de l'Union. Il note qu'il n'y a pas toujours de contrôle judiciaire lorsque les informations électroniques sont collectées par des moyens contraignants, comme indiqué dans le projet de décision d'adéquation. Dans ce contexte, le CEPD rappelle la jurisprudence de la Cour EDH relative aux contrôles judiciaires a posteriori[70].

4.1.2.1.2 Cas des demandes de divulgation volontaire

156. Selon le projet de décision d'adéquation, dans les cas de demandes de divulgation volontaire, il n'y a pas de contrôle préalable par un juge. Dans un tel cas, la police préfectorale opère sous le contrôle du ministère public. Le projet de décision d'adéquation mentionne l'article 192, paragraphe 1, et l'article 246 sur la coopération mutuelle et la coordination entre les procureurs, la commission préfectorale de sécurité publique et les fonctionnaires de la police judiciaire ainsi que sur l'échange d'informations entre eux. Il fait également référence à l'article 193, paragraphe 1, selon lequel le ministère public peut donner les instructions nécessaires à la police judiciaire et fixer des normes en vue d'une enquête équitable. Enfin, il fait mention de l'article 194 portant sur les sanctions disciplinaires à l'encontre de la police judiciaire pour non-respect du ministère public, pouvant être prises par la commission de sécurité publique nationale ou préfectorale.

157. Le CEPD prend note de l'adoption des mesures précédentes et le contrôle exercé par la commission de sécurité publique nationale et préfectorale sur la police judiciaire (voir ci-dessous).

4.1.2.2 Contrôle exercé par les commissions de sécurité publique de la police

158. Conformément à l'annexe II du projet de décision d'adéquation, deux types de commissions exercent un contrôle sur la police. L'une et l'autre visent à garantir la gestion démocratique et la neutralité politique de l'administration de la police.

4.1.2.2.1 Contrôle exercé par la commission nationale de sécurité publique

159. L'annexe II du projet de décision d'adéquation fait état du contrôle exercé par la commission nationale de sécurité publique sur l'agence nationale de la police. La loi sur la police fixe la liste des missions de la commission, dont émanent ses pouvoirs de contrôle (voir l'article 5).

160. Conformément à l'article 4 de la loi japonaise sur la police, la commission nationale de sécurité publique relève de la compétence du Premier ministre et se compose d'un président et de cinq membres. L'article 7 fixe certaines restrictions à la nomination des membres de la commission. La durée du mandat des membres de la commission est de cinq ans et leur mandat ne peut être renouvelé qu'une seule fois, conformément à l'article 8. En outre, la Diète semble disposer d'une forte influence sur la nomination et la révocation des membres de la commission, assurant de la sorte l'indépendance de la commission nationale de sécurité publique.

161. De telles dispositions légales renforcent la neutralité politique de la commission nationale de sécurité publique.

4.1.2.2.2 Contrôle exercé par les commissions préfectorales de sécurité publique

162. La police préfectorale est soumise au contrôle des commissions préfectorales de sécurité publique établies dans chaque préfecture. Conformément à l'article 2 et à l'article 36, paragraphe 2, de la loi sur la police, les commissions préfectorales de sécurité publique sont chargées de « la protection des droits et des libertés des individus ». Les articles 38 et 42 de la loi sur la police énumèrent les

[70] Cour EDH, Modestou c. Grèce, 16 mars 2017, nº 51693/13.

obligations des commissions préfectorales de sécurité publique. Ces commissions ont également pour objectif de garantir la gestion démocratique et la neutralité politique de l'administration de la police, comme énoncé à l'article 43, paragraphe 2, en soumettant à la police préfectorale certains dossiers lorsqu'ils l'estiment nécessaire à la suite d'une inspection des activités de la police préfectorale ou en raison d'une faute professionnelle commise par un membre du personnel.

163. Toutefois, il n'apparaît pas clairement si ces commissions ont d'autres pouvoirs que le contrôle du comportement de la police. Le CEPD s'interroge sur la question de savoir si le terme « faute professionnelle » inclut l'accès illégal aux données et, en pareil cas, si ces commissions ont le pouvoir d'ordonner la suppression de données.

164. En ce qui concerne la neutralité et l'indépendance de ces commissions, comme indiqué dans le projet de décision d'adéquation[71], les commissions préfectorales de sécurité publique relèvent de la compétence du gouverneur de préfecture, qui nomme leurs membres sur approbation de l'assemblée préfectorale. Les membres de la commission préfectorale de sécurité publique ont un mandat de trois ans, renouvelable deux fois. L'article 39 de la loi sur la police a fixé des restrictions à la nomination des membres. Le projet de décision d'adéquation mentionne également le contrôle exercé sur la police préfectorale par l'assemblée locale et cite à cet égard l'article 100 de la loi japonaise relative à l'autonomie locale. Toutefois, le texte de cette loi n'a pas été transmis à le CEPD[72].

165. En outre, conformément à l'article 42, paragraphes 2 et 3, de la loi sur la police, « les membres de la commission ne peuvent pas simultanément exercer une fonction au sein de l'assemblée ou faire partie du personnel occupé à temps plein dans des entités publiques locales ou être engagés à temps partiel dans les conditions prévues à l'article 28, paragraphe 5, 1er alinéa, de la loi sur le service public local ».

166. Sur la base des éléments exposés ci-dessus et compte tenu de la collaboration entre les commissions préfectorales de sécurité publique et la commission nationale de sécurité publique, le CEPD marque son accord avec le projet de décision d'adéquation et se félicite de la neutralité et de l'indépendance des membres des commissions préfectorales de sécurité publique. Le CEPD comprend que les commissions préfectorales de sécurité publique n'ont qu'un pouvoir d'enquête concernant le comportement de la police et ne disposent d'aucun autre pouvoir de contrôle, y compris celui de supprimer les données recueillies par la police préfectorale. Par conséquent, il apparaît que des éclaircissements supplémentaires sont nécessaires afin de déterminer si la surveillance exercée par les commissions préfectorales de sécurité publique est suffisante eu égard aux normes établies par le droit de l'Union.

4.1.2.2.3 Contrôle exercé par la Diète

167. Le projet de décision d'adéquation[73] et l'annexe II[74] fournissent des informations sur le contrôle exercé par la Diète sur le gouvernement, y compris en ce qui concerne la légalité de la collecte de données par la police. En effet, tous deux font mention de l'article 62 de la constitution japonaise selon lequel la Diète peut demander la production de documents et des témoignages. Les deux documents mentionnent également les dispositions de la loi sur la Diète, en particulier son article 104 portant sur les pouvoirs de la Diète et son article 74 portant sur les demandes de renseignements écrites, auxquelles le gouvernement doit répondre par écrit dans un délai de sept jours, comme prévu par l'article 75. Le projet de décision d'adéquation ajoute également que « le rôle joué par la Diète dans le

[71] Voir le projet de décision d'adéquation, p. 31.
[72] Voir le projet de décision d'adéquation, p. 33.
[73] Voir le projet de décision d'adéquation, p. 30.
[74] Voir l'annexe II, p. 12.

contrôle de l'exécutif est conforté par des obligations de déclaration, par exemple en vertu de l'article 29 de la loi sur les écoutes téléphoniques ».

168. Le CEPD reconnaît l'implication de la Diète dans le contrôle du gouvernement et de la police quant à la légalité de la collecte des données.

4.1.2.2.4 Contrôle exercé par l'exécutif

169. Conformément à l'annexe II du projet de décision d'adéquation, d'une part, le ministre ou le responsable de chaque ministère ou agence dispose d'un pouvoir de contrôle et d'application du droit sur la base de la loi sur la protection des données à caractère personnel détenues par les organes administratifs[75]. D'autre part, le ministre de l'Intérieur et des Communications (ci-après le « MIC ») dispose d'un pouvoir d'enquête concernant l'application de cette dernière loi par tous les autres ministères, y compris le ministère de la justice pour ce qui concerne la police, comme indiqué dans le projet de décision d'adéquation[76].

170. Le ministre peut demander au responsable d'un organe administratif de fournir des documents et des explications concernant le traitement des données à caractère personnel par l'organe administratif concerné, sur la base de l'article 50 de la loi sur la protection des données à caractère personnel détenues par les organes administratifs. Il peut demander une révision des mesures en cas de suspicion de violation ou d'application inappropriée de la loi, et émettre des avis concernant le traitement des données à caractère personnel par l'organe administratif concerné conformément aux articles 50 et 51 de ladite loi.

171. Le projet de décision d'adéquation et l'annexe II mentionnent également la création de 51 centres d'information qui « garantissent la mise en œuvre harmonieuse de cette loi », conformément à l'article 47 de la loi sur la protection des données à caractère personnel détenues par les organes administratifs. Le CEPD fait observer que la loi sur la protection des données à caractère personnel détenues par les organes administratifs ne développe pas davantage le rôle et les pouvoirs de ces centres d'information, mais que le projet de décision d'adéquation fournit quelques précisions.

172. Par conséquent, le CEPD salue le contrôle exécutif exercé sur les ministères et les organes administratifs par le ministère de l'intérieur et des communications concernant le respect de la loi sur la protection des données à caractère personnel détenues par les organes administratifs.

173. En conclusion, comme indiqué dans la jurisprudence de leurs juridictions respectives, la législation de l'Union et la CEDH établissent des normes et des garanties selon lesquelles le contrôle doit être complet, neutre et indépendant. Le CEPD fait observer que la commission de protection des données à caractère personnel ne dispose d'aucun pouvoir de contrôle en matière répressive. En outre, si, eu égard au contrôle exercé par la Diète, les commissions nationale et préfectorales de sécurité publique semblent neutres et indépendantes, des éclaircissements supplémentaires sont nécessaires concernant les pouvoirs de surveillance des commissions préfectorales de sécurité publique.

4.1.3 Voies de recours dans le domaine du droit pénal

174. Le projet de décision d'adéquation, complété par l'annexe II, présente plusieurs moyens permettant aux individus de déposer leurs plaintes, à la fois devant des autorités indépendantes et devant les juridictions.

175. Ces moyens et les éléments essentiels de ces procédures découlant des documents disponibles sont présentés ci-dessous, après un bref aperçu des droits des personnes concernées, afin d'établir ce

[75] Voir l'annexe II, p. 10.
[76] Voir l'annexe II, p. 11.

qu'elles peuvent escompter des autorités publiques dans le cadre du traitement des données dans le domaine des procédures pénales.

4.1.3.1 Droits des personnes concernées dans le cadre des procédures pénales

176. Pour obtenir réparation, les personnes concernées doivent avoir des droits en vertu d'une loi pour pouvoir en faire valoir le non-respect. Par conséquent, le CEPD a également évalué les droits des personnes concernées dans le cadre des procédures pénales, telles que présentées dans le projet de décision d'adéquation.

4.1.3.1.1 Limitations générales aux droits des personnes concernées en vertu de la loi sur la protection des données à caractère personnel détenues par les organes administratifs

177. Dans son projet de décision d'adéquation, la Commission invoque et se fonde sur les principes généraux de la protection des données que les autorités publiques doivent respecter lorsqu'elles collectent des données à caractère personnel. Ces principes sont également décrits plus en détail à l'annexe II, de sorte que le CEPD a décidé de commenter aussi ces aspects.

178. En ce qui concerne les droits disponibles, le CEPD fait observer que, conformément à l'annexe II du projet de décision d'adéquation, certains droits généraux accordés aux personnes concernées dans le cadre des données traitées par les organes administratifs peuvent également être invoqués dans le contexte des enquêtes pénales. Toutefois, des limitations supplémentaires concernant la collecte et le traitement ultérieur des données à caractère personnel dans ce contexte découlent également directement de la loi sur la protection des données à caractère personnel détenues par les organes administratifs.

179. Ces restrictions, qui semblent s'appliquer pour les données collectées tant sur la base d'un mandat que sur la base d'un formulaire de demande de renseignements dans le contexte de la divulgation volontaire, soulèvent des questions concernant plusieurs aspects.

180. En ce qui concerne le principe de limitation des finalités, bien qu'en principe les organes administratifs soient tenus de préciser la finalité pour laquelle ils conservent des données à caractère personnel et qu'ils ne puissent les conserver au-delà de ce qui est nécessaire à la réalisation de l'objectif spécifié, ils sont autorisés à changer la finalité si cette modification est « ce qui peut être raisonnablement considéré comme approprié en fonction de la finalité initiale ».

181. La loi sur la protection des données à caractère personnel détenues par les organes administratifs prévoit également le principe de non-divulgation, en vertu duquel un salarié ne peut divulguer les informations à caractère personnel qu'il a acquises concernant une autre personne sans motif justifiable ni les utiliser à des fins injustes. Toutefois, aucune information supplémentaire n'est fournie concernant l'interprétation de ce qu'il convient d'entendre par « motif justifiable » ou « fin injuste », de sorte que des éclaircissements supplémentaires sont nécessaires pour l'évaluation.

182. L'article 8, paragraphe 1, de la loi sur la protection des données à caractère personnel détenues par les organes administratifs prévoit également l'interdiction d'utiliser ou de divulguer des données « sauf disposition contraire des lois et règlements ». Néanmoins, bien que cette disposition ne soit pas en principe contraire au niveau de protection garanti par le droit de l'Union, le CEPD ne dispose pas d'éléments supplémentaires concernant la mesure dans laquelle une surveillance ou des contrôles sont exercés lorsque la divulgation est prévue par des lois ou règlements. En outre, en vertu de l'article 8, paragraphe 2, des exceptions supplémentaires s'appliquent à cette règle lorsqu'« une telle divulgation exceptionnelle n'est pas susceptible de porter un préjudice injuste aux droits et intérêts de la personne concernée ou d'un tiers ». En l'absence d'autres éléments sur ce point, cette exception,

qui s'appuie sur la notion peu claire de préjudice « injuste », doit encore être clarifiée afin d'établir si elle est suffisamment limitée.

183. Enfin, l'article 9 de la loi sur la protection des données à caractère personnel détenues par les organes administratifs prévoit des restrictions supplémentaires concernant la finalité ou le mode d'utilisation ou toute autre restriction, pouvant être imposées par le responsable d'un organe administratif lors de la communication de données à caractère personnel conservées à une tierce personne. Étant donné que les notions de « toute autre restriction nécessaire » et de « communication à une tierce personne » sont très vastes, ces restrictions supplémentaires des droits des personnes concernées soulèvent des préoccupations en l'absence de plus amples précisions concernant leur portée.

184. Si le CEPD a pleinement conscience du fait que les droits d'accès et les autres principes en matière de protection des données sont également limités dans le cadre des procédures pénales en vertu du droit de l'Union, des garanties supplémentaires sont prévues lorsque de telles restrictions existent, y compris en matière de surveillance, contrôle et recours. En l'absence de suffisamment de jurisprudence relative à ces restrictions ou d'éléments supplémentaires permettant de clarifier la portée de ces dispositions, le CEPD n'est pas en mesure d'évaluer si ces restrictions des droits des personnes concernées sont limitées à ce qui peut être considéré comme strictement nécessaire et proportionné au regard du droit de l'Union, et seraient donc substantiellement équivalentes aux droits conférés aux personnes concernées de l'Union.

4.1.3.1.2 Limitations supplémentaires aux droits garantis par la loi sur la protection des données à caractère personnel détenues par les organes administratifs découlant du code de procédure pénale et des ordonnances de la police préfectorale

185. Le CEPD fait observer que, bien que la loi sur la protection des données à caractère personnel détenues par les organes administratifs semble applicable à tous les traitements effectués par les organes administratifs du Japon, certaines restrictions importantes des droits des personnes concernées découlent de législations spécifiques. En particulier, l'article 53, paragraphe 2, du code de procédure pénale[77] dispose que « les données à caractère personnel figurant dans les documents relatifs à des procès et à des biens saisis » sont exclues du champ d'application des droits des individus au titre du chapitre IV de la loi sur la protection des données à caractère personnel détenues par les organes administratifs. Concrètement, le CEPD comprend donc que, dans le cadre de procédures pénales, les personnes concernées ne bénéficient pas des droits à l'information, l'accès, la rectification ou l'effacement des données à caractère personnel enregistrées dans les documents relatifs à des procès et à des biens saisis.

186. En ce qui concerne ces restrictions, le CEPD comprend qu'elles s'appliquent aux données collectées sur la base de mandats, ainsi qu'aux données recueillies dans le cadre de la divulgation volontaire au moyen de formulaires de demande de renseignements (voir ci-dessous). En effet, le fondement juridique des deux procédures d'accès aux données (au moyen d'un mandat et d'un formulaire de demande de renseignements) est spécifié dans le code de procédure pénale et l'article 53-2 de ce code semble s'appliquer aux deux types de collecte. Toutefois, étant donné que l'article 53-2 fait référence aux biens « saisis », il serait nécessaire de clarifier si les restrictions des droits prévues par cette disposition s'appliquent également dans le contexte de la divulgation volontaire.

187. Le CEPD regrette de ne pas avoir reçu les ordonnances de la police préfectorale qui sont réputées protéger les données à caractère personnel, les droits et les obligations de la même manière que la loi

[77] Disponible à l'adresse suivante: http://www.japaneselawtranslation.go.jp/law/detail/?printID=&id=2283&re=02&vm=02 et cité à l'annexe II du projet de décision d'adéquation, note de bas de page nº 25.

sur la protection des données à caractère personnel détenues par les organes administratifs. Compte tenu du manque de clarté concernant l'interprétation à donner à la loi sur la protection des données à caractère personnel détenues par les organes administratifs et de l'indisponibilité des ordonnances de police préfectorales, le CEPD se demande si les droits accordés aux particuliers dans ce contexte et les mécanismes supplémentaires de contrôle et/ou de recours sont suffisants pour compenser l'absence de droits.

4.1.3.2 Recours via des autorités indépendantes

4.1.3.2.1 Recours administratif

188. Le CEPD relève que les organes administratifs collectant des données, tels que la police préfectorale, sont compétents pour traiter les demandes émanant de particuliers concernant leurs droits (limités) vis-à-vis de leurs données collectées dans le cadre d'enquêtes pénales (voir ci-dessus pour les droits disponibles) et qui semblent couvrir à la fois la collecte de données sur la base d'un mandat et sur la base de formulaires de demande de renseignements. Concrètement, ces droits semblent limités à des principes généraux, tels que la nécessité de la conservation des données en relation avec la finalité (voir l'article 3, paragraphe 1, de la loi sur la protection des données à caractère personnel détenues par les organes administratifs), le principe de limitation de la finalité (article 4) ou l'exactitude des données (article 5), tandis que les droits individuels, tels que le droit à l'information, à l'accès, à la rectification ou à l'effacement, sont exclus pour les données à caractère personnel enregistrées dans les documents relatifs à des procès ou à des biens saisis[78]. Bien que ces organes ne puissent être considérés comme indépendants et, par conséquent, comme mettant à disposition des voies de recours ou de contrôle indépendantes, le CEPD accueille favorablement cette voie. Toutefois, il souligne le fait que les plaintes déposées par cette voie ne portent que sur un nombre très limité de droits des personnes concernées, compte tenu des restrictions prévues par la loi sur la protection des données à caractère personnel détenues par les organes administratifs.

189. En outre, étant donné que les « données à caractère personnel figurant dans les documents relatifs à des procès et à des biens saisis » sont exclues du champ d'application des droits individuels définis au chapitre IV de la loi sur la protection des données à caractère personnel détenues par les organes administratifs en vertu de l'article 53-2 du code de procédure pénale, la possibilité de demander à avoir accès à des données à caractère personnel est également limitée aux procédures prévues par d'autres dispositions du code de procédure pénale. Il semble que seuls les victimes, les suspects ou les accusés puissent agir dans ce cadre et seulement à certains stades de la procédure pénale. Par conséquent, le CEPD s'inquiète de ce qu'aucun droit général d'accès et/ou de rectification ou de suppression des données ne soit accessible aux personnes concernées en vertu de la législation japonaise dans le cadre d'une procédure pénale, et que toutes les voies de recours disponibles requièrent soit d'être une victime (dans ce cas, la personne concernée saura probablement que ses données sont collectées), un suspect ou un accusé, soit de prouver l'existence d'un préjudice, alors que les personnes concernées devraient également pouvoir avoir accès à leurs données et, éventuellement, les faire rectifier ou supprimer lorsqu'elles n'ont subi aucun préjudice (ou dans le cas contraire) et/ou lorsqu'elles ne sont ni une victime, un suspect ou un accusé, mais un témoin, par exemple.

[78] Voir ci-dessus en ce qui concerne les restrictions de la loi sur la protection des données à caractère personnel détenues par les organes administratifs et, en particulier, l'article 53-2 du code de procédure pénale (non fourni mais cité à l'annexe II du projet de décision d'adéquation, à la note de bas de page nº 25).

4.1.3.2.2 Recours administratif par l'intermédiaire des commissions préfectorales de sécurité publique

190. En outre, les commissions préfectorales de sécurité publique semblent compétentes pour traiter les plaintes. Sur le fondement de l'article 79 de la loi sur la police visé dans le projet de décision d'adéquation, les particuliers peuvent porter plainte contre tout comportement illégal ou abusif d'un agent dans l'exercice de ses fonctions.

191. Le CEPD souhaiterait savoir si un traitement « illégal » de données à caractère personnel peut être considéré comme un « comportement illégal ou abusif d'un agent » et obtenir de plus amples précisions quant à la preuve à apporter d'un préjudice qui semble exigée de la personne concernée. En effet, l'avis adressé par l'agence nationale de la police à la police et aux commissions préfectorales de sécurité publique concernant le traitement approprié des plaintes relatives à l'exercice des fonctions des agents de police limite les plaintes aux demandes concrètes portant sur la « réparation d'un préjudice spécifique causé par le comportement illégal ou inapproprié d'un agent de police dans l'exercice de ses fonctions ou par le fait qu'il ait omis de prendre des mesures nécessaires », ainsi qu'à la possibilité d'exprimer « des doléances/un mécontentement concernant la manière inappropriée dont un agent de police exerce ses fonctions ». Il est expressément précisé que « les plaintes relatives à l'inexécution d'un agent de police dans tout domaine qui n'est pas considéré comme relevant de ses fonctions, ainsi que celles qui expriment un avis général ou une proposition et qui n'affectent pas directement la partie plaignante elle-même, sont exclues ».

192. En ce qui concerne les exigences procédurales relatives au dépôt de plaintes, bien que celles-ci doivent être déposées par écrit, le CEPD constate l'existence d'une assistance à la rédaction en vertu de la législation japonaise, y compris pour les étrangers. En outre, le gouvernement japonais semble avoir également confié à la commission de protection des données à caractère personnel la mission d'aider les personnes concernées de l'Union dans le cadre du traitement et de la résolution des plaintes dans ce domaine, ce dont le CEPD se félicite. Dans ce contexte, le CEPD souligne que, d'après ce qu'il comprend, la commission de protection des données à caractère personnel ne fera office que de point de contact entre les personnes concernées de l'Union et les autorités japonaises compétentes.

193. Les conclusions de la commission préfectorale de sécurité publique concernant une plainte ne sont pas communiquées dans les cas énumérés à l'article 79-2 de la loi sur la police, qui incluent les cas dans lesquels « la résidence du plaignant est inconnue ». Le CEPD reconnaît que la référence à la résidence ne signifie pas qu'en tout état de cause, les personnes concernées de l'Union seraient exclues de la notification des conclusions relatives à leurs plaintes au motif qu'elles ne résident pas au Japon.

4.1.3.2.3 Mécanisme ad hoc impliquant la commission de protection des données à caractère personnel

194. À la lumière des conclusions exposées ci-dessus, le CEPD salue le fait que le gouvernement japonais et la Commission européenne se sont accordés sur un mécanisme de recours supplémentaire offrant aux citoyens de l'Union une voie de recours additionnelle au Japon, par laquelle les particuliers peuvent également tenter d'obtenir réparation à l'égard d'enquêtes illicites ou abusives effectuées par les autorités publiques. Le CEPD constate également et se félicite du fait que les demandes puissent être déposées auprès de la commission de protection des données à caractère personnel, plutôt qu'auprès d'un autre fonctionnaire gouvernemental, étendant ainsi la portée de la compétence de la commission de protection des données à caractère personnel aux domaines de l'application des lois et de la sécurité nationale.

195. Lors de l'analyse du nouveau mécanisme, l'objectif du CEPD a été de comprendre les compétences de la commission de protection des données à caractère personnel dans ce contexte.

196. En dépit de quelques difficultés linguistiques, le CEPD comprend que le mécanisme de recours supplémentaire n'exige pas de « qualité pour agir » au sens où le demandeur n'est pas tenu de démontrer que ses données à caractère personnel sont susceptibles d'avoir fait l'objet d'une surveillance de la part d'une autorité japonaise. Le CEPD souhaiterait demander confirmation sur ce point à la Commission.

197. Conformément à son évaluation du mécanisme du médiateur, créé dans le cadre du bouclier de protection des données, le CEPD souligne la nécessité de conférer des pouvoirs effectifs au destinataire de la demande, en l'occurrence la commission de protection des données à caractère personnel, afin que le mécanisme de recours puisse être considéré comme étant substantiellement équivalent à un recours effectif au sens de l'article 47 de la charte des droits fondamentaux.

198. Lorsqu'il explique le mécanisme de recours, le gouvernement japonais fait référence à l'article 6, paragraphe 61, point ii), et à l'article 80, de la loi sur la protection des informations personnelles, et cite ces pouvoirs à l'annexe II. Le CEPD croit comprendre que la procédure décrite à l'annexe II précise ou étend les pouvoirs de la commission de protection des données à caractère personnel, étant donné que les termes utilisés à l'article 6, paragraphe 61, point ii), et à l'article 80, de la loi sur la protection des informations personnelles sont plutôt vagues et généraux. Dans la mesure où l'annexe II précise ou étend les pouvoirs de la commission de protection des données à caractère personnel, le CEPD souhaite demander des précisions quant au fait que les autres agences du gouvernement japonais sont subordonnées à ces pouvoirs.

199. Sur la base de la procédure décrite à l'annexe II, le CEPD relève que les autorités publiques japonaises compétentes sont tenues de coopérer avec la commission de protection des données à caractère personnel « y compris en lui fournissant les informations nécessaires et le matériel adapté, afin qu'elle puisse évaluer si la collecte ou l'utilisation subséquente d'informations à caractère personnel respecte les règles applicables ». Pour pouvoir évaluer l'effectivité du système, il est donc important de se référer une nouvelle fois aux pouvoirs dont disposent les autorités compétentes avec lesquelles la commission de protection des données à caractère personnel coopère. Selon la compréhension du CEPD, ces pouvoirs ne seraient pas étendus par les garanties fournies à l'annexe II.

200. Le CEPD note également que lorsqu'une violation des règles a été constatée, « la coopération des autorités publiques concernées avec la commission de protection des données à caractère personnel comporte l'obligation de remédier à la violation », ce qui inclut expressément la suppression des données recueillies en violation des règles applicables. Le CEPD comprend que les obligations auxquelles l'autorité compétente est soumise découlent de la « coopération avec la commission de protection des données à caractère personnel », plutôt que d'une décision de celle-ci.

201. Enfin, la commission de protection des données à caractère personnel informera le demandeur du « résultat de l'évaluation, y compris toute mesure corrective prise le cas échéant ». En outre, la commission de protection des données à caractère personnel informera le demandeur de la « possibilité d'obtenir une confirmation des résultats auprès de l'autorité publique compétente et de l'autorité à laquelle une telle demande de confirmation doit être adressée ».

202. De plus, la commission de protection des données à caractère personnel s'est engagée à aider le demandeur à introduire un nouveau recours en vertu du droit japonais, s'il n'est pas satisfait de l'issue de la procédure.

203. Compte tenu de la nécessité de disposer d'un mécanisme de recours effectif, substantiellement équivalent aux standards de l'Union, le CEPD se demande néanmoins si la commission de protection des données à caractère personnel possède des pouvoirs spécifiques autres que celui d'évaluer la

conformité de la collecte ou de l'utilisation subséquente d'informations à caractère personnel aux règles applicables et celui d'inviter les autorités compétentes à faire usage de leurs pouvoirs respectifs et à traiter les plaintes qu'elle leur transmet. Si la commission de protection des données à caractère personnel ne devait agir que comme point de contact pour les citoyens de l'Union, le CEPD considèrerait que cela ne suffit pas pour garantir un mécanisme de recours efficace, substantiellement équivalent aux standards de l'Union. Le CEPD invite donc la Commission à fournir des éclaircissements sur les points mentionnés dans le présent sous-chapitre, en particulier sur la question de savoir si et comment le mécanisme étend les obligations des autorités compétentes, sur la manière dont celles-ci sont liées par le mécanisme, et sur la manière dont la commission de protection des données à caractère personnel peut effectivement garantir le respect des dispositions, et non servir uniquement de point de contact pour les citoyens de l'Union.

4.1.3.3 Recours judiciaires

4.1.3.3.1 Mécanisme de quasi-plainte

204. La procédure dite de « quasi-plainte » permet d'agir contre la collecte obligatoire de données sur la base d'un mandat en vue de faire annuler ou modifier une saisie illégale.

205. Cette voie de recours implique que l'individu a connaissance de la saisie des données. Toutefois, le CEPD croit comprendre que la procédure de collecte de données sur la base d'un mandat ne fait pas l'objet d'une notification à la personne concernée. De même, il comprend que la divulgation volontaire n'implique pas que les entreprises requises ont l'obligation d'informer les personnes concernées des demandes reçues et exécutées. Par conséquent, bien qu'il soit souligné à l'annexe II qu'« un tel recours peut être formé sans que la personne concernée doive attendre la conclusion de la procédure », dans la pratique, hormis pour les mandats autorisant des écoutes téléphoniques pour lesquels la loi prévoit une obligation de notification[79], cette voie de recours semble n'être effectivement disponible qu'à partir du moment où la personne concernée est informée de la collecte dans le cadre d'une procédure à son égard.

4.1.3.3.2 Mesures injonctives

206. En outre, pour obtenir la suppression de données recueillies dans le cadre d'une procédure pénale (à savoir, les « mesures injonctives »), ou pour obtenir réparation de dommages, les particuliers peuvent également engager des procédures civiles devant un tribunal.

207. En ce qui concerne la réparation, le CEPD observe que la procédure semble être circonscrite à des situations dans lesquelles un fonctionnaire public dans l'exercice de ses fonctions a infligé des dommages à la personne concernée de manière illégale et fautive (que la faute soit délibérée ou due à la négligence). Le CEPD croit comprendre que les dommages incluent les dommages moraux. Aucun détail n'est toutefois fourni quant à ce que la personne qui a subi le dommage doit prouver. Le CEPD n'a pas été en mesure d'évaluer la jurisprudence relative à l'octroi d'une réparation et ne peut donc estimer si cette voie constitue un recours efficace en cas de préjudice.

208. En ce qui concerne les « mesures injonctives », le CEPD fait également observer que pour pouvoir introduire une demande, la personne concernée doit au préalable savoir que ses données ont été collectées et qu'elles sont toujours conservées. Par conséquent, compte tenu des droits limités d'information et d'accès des particuliers dans le cadre des enquêtes et procédures pénales, l'efficacité de la procédure semble plutôt limitée.

[79] L'article 23 de la loi japonaise sur les écoutes téléphoniques est mentionné à la page 33 du projet de décision d'adéquation, mais l'EDPB n'a pas reçu le texte et n'est donc pas en mesure d'apprécier dans quelle mesure cette obligation de notification s'applique et dans quels cas elle peut être limitée.

4.1.3.4 Évaluation globale des voies de recours

209. À la suite de l'évaluation de toutes les voies de recours ouvertes aux particuliers en vertu du droit japonais ainsi qu'aux personnes concernées de l'Union auprès de la commission de protection des données à caractère personnel, le CEPD salue le mécanisme *ad hoc* de résolution des litiges via la commission de protection des données à caractère personnel. Il présente une valeur ajoutée pour les personnes concernées de l'Union, notamment parce qu'il leur permet de comprendre quelles possibilités s'offrent à elles pour obtenir réparation et/ou un dédommagement, ainsi que pour introduire leurs demandes conformément aux exigences procédurales applicables en vertu du droit japonais. Toutefois, des éclaircissements supplémentaires sont nécessaires, en particulier sur la question de savoir si et comment le mécanisme étend les obligations des autorités compétentes, sur la manière dont celles-ci sont liées par le mécanisme, et sur la manière dont la commission de protection des données à caractère personnel peut effectivement garantir le respect des dispositions, afin d'assurer que le mécanisme constitue un moyen de recours efficace.

210. Cette évaluation montre qu'aucun mécanisme de recours en droit japonais ne semble permettre l'accès, la rectification ou la suppression des données de personnes concernées qui ne sont pas des victimes, des suspects ou des accusés dans le cadre d'une procédure pénale, par exemple pour remédier à la collecte ou à la conservation illicite de leurs données. Elle montre également que tous les mécanismes et procédures de recours et de réparation prévus par la législation japonaise à l'intention des victimes, des suspects ou des accusés impliquent que les personnes concernées aient connaissance de la collecte des données, ce qui ne semble pas toujours être le cas dans la pratique puisque les droits d'accès et d'information sont limités. En outre, des éclaircissements supplémentaires semblent nécessaires en ce qui concerne l'apport de la preuve d'un comportement illicite des autorités, en particulier concernant la question de savoir si le traitement illicite de données à caractère personnel ou un préjudice subi par la personne concernée constituent de tels comportements illicites.

211. Par conséquent, en l'absence d'autres documents et éléments, le CEPD s'inquiète de ce que les voies de recours prévues par la législation japonaise et par le projet de décision d'adéquation ne semblent suffisamment efficaces par rapport aux standards du droit de l'Union.

4.2 Accès à des fins de sécurité nationale

4.2.1 Portée de la surveillance

212. Dans le projet de décision d'adéquation, le chapitre consacré à « l'accès et l'utilisation des données par les autorités publiques japonaises à des fins de sécurité nationale » est introduit par une déclaration générale, dans la lignée de la garantie donnée par le gouvernement japonais à l'annexe II, selon laquelle aucune loi japonaise ne prévoit et, partant, ne permet les « collectes obligatoires d'informations ou "interceptions administratives" en dehors des enquêtes pénales ». En conclusion, il y est dit que « des informations ne peuvent être obtenues à des fins de sécurité nationale qu'à partir d'une source d'information librement accessible à tous ou par divulgation volontaire, ce qui exclut toute activité de surveillance secrète dans ce domaine. Les opérateurs commerciaux qui reçoivent une demande de coopération volontaire (sous la forme d'une divulgation d'informations électroniques) ne sont pas légalement tenus de fournir ces informations »[80].

213. Dans le cadre de ces limites, quatre entités gouvernementales sont citées comme disposant du pouvoir de collecter des informations électroniques détenues par des opérateurs commerciaux japonais pour des raisons de sécurité nationale. Le ministère de la défense, qui compte parmi ces quatre entités,

[80] Décision d'adéquation, paragraphe 151.

semble « n'avoir le pouvoir de collecter des informations (électroniques) que sur la base de divulgations volontaires »[81].

214. Pour son évaluation de la structure générale de la collecte de données à des fins de sécurité nationale, le CEPD souhaite rappeler la première des quatre « garanties essentielles », selon laquelle « le traitement doit être fondé sur des règles claires, précises et accessibles » [82]. Plus précisément, la Cour EDH a indiqué très clairement que les programmes de surveillance ne sont « conformes à la loi » que si les mesures de surveillance « reposent sur une base juridique nationale ». La cour a précisé que la compatibilité avec l'état de droit exige que la loi autorisant la mesure soit accessible et prévisible en ce qui concerne ses effets. Eu égard au risque d'arbitraire, la cour a exigé des « règles claires et détaillées sur les mesures de surveillance secrète », « suffisamment claires pour donner aux citoyens une indication exacte concernant les circonstances dans lesquelles et les conditions auxquelles les autorités publiques sont autorisées à avoir recours à de telles mesures »[83].

215. En ce qui concerne l'application de ces garanties essentielles au système juridique japonais, le CEPD a conscience du fait qu'en matière de sécurité nationale, non seulement les États disposent d'une vaste marge d'appréciation, reconnue par la Cour européenne des droits de l'homme, mais aussi que les pouvoirs dans ce domaine reflètent l'expérience historique des nations. Le CEPD comprend donc que, comme l'a souligné le gouvernement japonais, après la Seconde Guerre mondiale, les agences de renseignement nationales japonaises ont été dotées de pouvoirs plus limités que dans d'autres États.

216. D'après la lecture qu'en fait le CEPD, et conformément à l'assurance donnée par le gouvernement japonais, le projet de décision d'adéquation suggère que les organes gouvernementaux japonais ne gèrent aucun programme exerçant un contrôle stratégique ou une surveillance à grande échelle des communications (via internet). Comme susmentionné, le gouvernement japonais a garanti dans une lettre signée par le ministre de la justice que « des informations ne peuvent être obtenues à des fins de sécurité nationale qu'à partir d'une source d'information librement accessible à tous ou par divulgation volontaire ».

217. En ce qui concerne la base légale en vertu de laquelle le ministère de la défense opère, le CEPD fait observer que le projet de décision d'adéquation donne des informations générales sur ses compétences et cite sa mission consistant à « agir pour assurer la paix et l'indépendance nationales, ainsi que la sécurité de la nation ». Toutefois, le CEPD n'a pas reçu de traduction en anglais de ce fondement juridique.

218. Dans le même temps, le CEPD a connaissance de rapports publiés dans différents médias, suggérant que la direction des renseignements d'origine électromagnétique relevant du ministère japonais de la défense gère des programmes de surveillance[84]. Le rapport affirme également que, bien qu'il ait refusé d'évoquer des points précis du rapport, le ministère japonais de la défense « a reconnu que le Japon dispose de "bureaux dans tout le pays" qui interceptent des communications » et que ceux-ci « se concentrent sur les activités militaires et les "cybermenaces" », mais qu'ils « ne collectent pas

[81] Décision d'adéquation, paragraphe 153.

[82] G29, WP 237: Document de travail 01/2016 sur la justification des ingérences dans les droits fondamentaux au respect de la vie privée et à la protection des données par des mesures de surveillance lors du transfert de données à caractère personnel (garanties essentielles européennes).

[83] Voir, par exemple, Cour EDH, Big Brother Watch et autres c. Royaume-Uni, 13 septembre 2018, requêtes n^{os} 58170/13, 62322/14 et 24960/15, point 305.

[84] En mai 2018, le bulletin d'information en ligne «The Intercept» a publié un rapport intitulé «The untold story of Japan's secret spy agency» (L'histoire jamais contée des services secrets japonais).

d'informations sur le grand public ». Cette dernière déclaration (selon laquelle le ministère de la défense ne collecte pas d'informations sur le grand public) a été reprise par le gouvernement japonais.

219. Il est vrai que le gouvernement japonais a réaffirmé, dans une lettre signée par le ministre de la Justice, que le ministère de la défense ne collecte pas d'informations sur le grand public.

220. Il ne relève pas de la mission du CEPD de procéder à une évaluation générale des capacités de surveillance du gouvernement japonais. Ces activités n'ont d'importance dans le cadre de l'évaluation du comité que si elles sont pertinentes sur le plan du transfert de données à caractère personnel entre l'Union et le Japon. Dans ce contexte, le CEPD tient à réaffirmer l'approche déjà adoptée par son prédécesseur lorsqu'il a été invité à se prononcer sur le bouclier de protection des données UE-États-Unis. Lors de l'élaboration de son avis sur le bouclier de protection des données, le groupe de travail « article 29 » a inclus dans son analyse les pouvoirs des États-Unis et les restrictions auxquels ils sont soumis en matière de surveillance des données « durant leur transfert » vers ce pays[85]. En appliquant le même standard à la décision d'adéquation relative au Japon, le CEPD est d'avis que les informations relatives à la possibilité pour les autorités japonaises de surveiller les données « lors de leur transfert » vers le Japon sont pertinentes. Si ces pouvoirs de surveillance existent, l'arrêt rendu dans l'affaire Big Brother Watch par la Cour EDH semble suggérer qu'ils doivent être réglementés conformément aux standards établis par la CEDH.

221. Par conséquent, si les interceptions étaient limitées au « soutien à l'action militaire », elles pourraient ne pas être pertinentes pour l'évaluation de la décision d'adéquation. Il est donc dans l'intérêt du CEPD d'obtenir des éclaircissements sur les mesures de surveillance prises par les entités gouvernementales japonaises. À cet égard, une telle clarification serait utile afin de déterminer si les autorités japonaises compétentes pourraient avoir accès aux données à des fins de sécurité nationale durant leur transfert dans le cadre de la présente décision d'adéquation.

4.2.2 Divulgation volontaire dans le cadre de la sécurité nationale

222. Le projet de décision d'adéquation indique que les quatre organes gouvernementaux ne sont habilités à collecter des informations (électroniques) que dans le cadre d'une divulgation volontaire. Selon le projet de décision et l'annexe II, des restrictions légales s'appliquent, ce qui signifie que la collecte de données est limitée à ce qui est nécessaire à l'exécution des missions des organes.

223. Dans le domaine du droit pénal, comme indiqué dans la section relative à l'application de la loi, la divulgation volontaire n'est autorisée que dans le cadre d'une enquête pénale et suppose donc une suspicion concrète d'un délit déjà commis. Les enquêtes dans le domaine de la sécurité nationale diffèrent des enquêtes menées dans le domaine répressif. Le CEPD reconnaît que, conformément à l'annexe II, les principes centraux de « nécessité aux fins de l'enquête » et de « pertinence de la méthode » 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 l'espèce[86]. Il regrette que ce

[85] Voir WP 255, EU-U.S. Privacy Shield – First annual joint review, adopté le 28 novembre 2017, p. 16: «Le groupe de travail "article 29" est d'avis que l'analyse des lois du pays tiers pour lequel l'adéquation est envisagée ne devrait pas se limiter à la législation et aux pratiques permettant la surveillance à l'intérieur des frontières physiques de ce pays, mais devrait également inclure une analyse des fondements juridiques du droit de ce pays tiers, qui lui permettent d'exercer une surveillance en dehors de son territoire en ce qui concerne les données de l'Union. Comme déjà mentionné dans son avis précédent, il doit être clair que les principes du bouclier de protection des données s'appliqueront à compter du moment où le transfert de données a lieu et couvriront donc également les données "durant leur transfert" vers ce pays».

[86] Voir l'annexe II, p. 23.

point ne soit pas davantage précisé, notamment par une plus ample référence à la jurisprudence. Le CEPD rappelle néanmoins que le recours à cette procédure doit être proportionné et nécessaire.

224. Selon le projet de décision, lorsque des informations à caractère personnel ont été collectées (« obtenues »), leur traitement est régi par la loi sur la protection des données à caractère personnel détenues par les organes administratifs, sauf pour ce qui concerne la police préfectorale[87]. L'annexe II indique que le traitement des données à caractère personnel par la police préfectorale est régi par des ordonnances préfectorales qui énoncent des principes de protection des informations personnelles, des droits et des obligations équivalents à ceux de la loi sur la protection des données à caractère personnel détenues par les organes administratifs[88]. Étant donné qu'il n'existe pas de traduction en anglais de ces ordonnances, le CEPD n'est pas en mesure d'évaluer si les principes sont équivalents à ceux de la loi sur la protection des données à caractère personnel détenues par les organes administratifs.

225. Pour les autres commentaires concernant la divulgation volontaire, il est fait référence à la section relative à l'application de la loi.

4.2.3 Contrôle

4.2.3.1 Généralités

226. Les quatre organes gouvernementaux habilités à collecter des informations électroniques détenues par des opérateurs commerciaux japonais pour des raisons de sécurité nationale sont les suivants: i) le bureau de recherche et de renseignement du gouvernement; ii) le ministère de la défense; iii) la police (comprenant à la fois l'agence nationale de la police[89] et la police préfectorale); et iv) l'agence de renseignement de la sécurité publique.

227. Selon le projet de décision d'adéquation, ces organes gouvernementaux sont soumis à plusieurs niveaux de contrôle exercé par trois branches du gouvernement[90]. Le CEPD constate qu'il existe des mécanismes de contrôle au sein du pouvoir législatif (Diète japonaise) et du pouvoir exécutif (bureau de l'inspecteur général de la conformité juridique, commissions préfectorales de sécurité publique et commission d'examen de la sécurité publique). Le CEPD souligne que la Commission devrait donner de plus amples précisions concernant le contrôle judiciaire (d'office/garantie C énoncée dans le WP 237; un chapitre distinct est consacré aux recours dans le projet de décision et une garantie supplémentaire est prévue dans le WP 237) des organes publics susmentionnés, étant donné qu'il est difficile de déterminer si un tel contrôle judiciaire existe dans le domaine de la collecte d'informations à caractère personnel à des fins de sécurité nationale sans moyens contraignants.

4.2.3.2 Contrôle par la Diète japonaise

228. Le CEPD fait observer que la Diète japonaise peut mener des enquêtes concernant les activités des autorités publiques, et donc aussi pour tous les organes publics susmentionnés. En outre, la Diète peut également exiger la production de documents et la déposition de témoignages (*article 62 de la constitution japonaise, article 104 de la loi japonaise sur la Diète*). L'CEPD constate également que, conformément aux *articles 74 et 75 de la loi sur la Diète*, les membres de la Diète peuvent adresser des questions écrites au cabinet, auxquelles celui-ci peut répondre (*article 75 de la loi sur la Diète*). Enfin, l'EDPD prend également note de l'existence d'obligations de déclaration spécifiques, qui

[87] Décision d'adéquation, paragraphes 118 et 157.
[88] Voir l'annexe II, p. 3.
[89] Toutefois, d'après les informations reçues, le rôle principal de l'agence nationale de la police consiste à coordonner les enquêtes menées par les différents départements de la police préfectorale et ses activités de collecte d'informations se limitent à des échanges avec les autorités étrangères.
[90] Voir l'annexe II, p. 39.

s'appliquent notamment à l'agence de renseignement de la sécurité publique (article 36 de loi de prévention des activités subversives/article 31 de la loi sur le contrôle des organisations) qui doit soumettre un rapport annuel à la Diète. Aucun rapport de ce type n'a toutefois été transmis au CEPD.

4.2.3.3 Contrôle par le bureau de l'inspecteur général de la conformité juridique

229. Le CEPD constate qu'un organe de contrôle supervise l'activité du ministère de la défense, à savoir le bureau de l'inspecteur général de la conformité juridique. Le CEPD n'a pas reçu la loi portant création du ministère de la défense, mais a pu uniquement se baser sur les déclarations figurant à l'annexe II du projet de décision. Selon l'annexe II, le bureau de l'inspecteur général de la conformité juridique est un bureau indépendant créé au sein du ministère de la défense et placé sous le contrôle direct du ministre de la Défense, conformément à l'article 29 de la loi portant création du ministère de la défense. Le bureau de l'inspecteur général de la conformité juridique est habilité à contrôler le respect des lois et règlements par les fonctionnaires du ministère de la défense (dénommées les « inspections de la défense »), dans l'ensemble du ministère, y compris au sein des forces d'autodéfense.

230. D'après l'annexe II, le bureau de l'inspecteur général de la conformité juridique s'acquitte de ses tâches en toute indépendance par rapport aux départements opérationnels du ministère de la défense. Le CEPD note que le bureau de l'inspecteur général de la conformité juridique est un organe de contrôle *interne*.

231. Les inspections débouchent sur des conclusions et, pour garantir la conformité, sur des mesures qui sont directement communiquées au ministre de la Défense. Sur la base du rapport du bureau de l'inspecteur général de la conformité juridique, le ministre de la Défense peut ordonner la mise en œuvre des mesures nécessaires pour remédier à la situation. Le vice-ministre de la Défense est responsable de la mise en œuvre de ces mesures et doit rendre compte au ministre de la Défense de l'état d'avancement.

232. Sur la base de l'analyse de l'annexe II et sans avoir pu prendre connaissance des dispositions juridiques (loi portant création du ministère de la défense), le CEPD salue la possibilité d'ordonner la mise en œuvre des mesures nécessaires pour remédier à une situation de non-conformité. Toutefois, le CEPD émet des doutes quant à l'indépendance de bureau de l'inspecteur général de la conformité juridique, étant donné qu'il s'agit d'un bureau interne au ministère de la défense, placé sous la supervision directe du ministre de la Défense selon l'annexe II (d'après le document de travail 237, « *l'indépendance fonctionnelle n'est pas en soi suffisante pour protéger cette autorité de surveillance de toute influence extérieure* »).

233. Conformément à la jurisprudence de la Cour EDH et au document WP 237 et selon les considérations formulées à l'annexe II, l'inspecteur général peut demander des rapports au bureau concerné (documents, visites sur place, explications). Le CEPD estime nécessaire d'obtenir des précisions afin de savoir si les bureaux concernés sont tenus de donner suite à ces demandes et si les documents demandés peuvent inclure des documents confidentiels, comme l'indique le document WP 237.

234. Bien que le CEPD se félicite du fait que des experts juridiques très expérimentés (notamment un ancien procureur général) dirigent le bureau de l'inspecteur général de la conformité juridique, des éclaircissements concernant le mode de désignation des membres de cet organe de surveillance semblent nécessaires.

4.2.3.4 Contrôle par la commission d'examen de la sécurité publique

235. Conformément à l'annexe II (page 25), l'agence de renseignement de la sécurité publique procède à des inspections régulières et spéciales des opérations de ses bureaux et services (bureau de renseignement de la sécurité publique, services de renseignements de la sécurité publique et bureaux

subalternes, etc.). Aux fins de l'inspection régulière, un directeur général adjoint et/ou un directeur sont désignés comme inspecteurs. De telles inspections devraient également porter sur la gestion des données à caractère personnel.

236. Conformément au considérant 163 du projet de décision d'adéquation, la commission d'examen de la sécurité publique agit en tant qu'organisme de surveillance indépendant ex ante pour le compte de l'agence de renseignement de la sécurité publique, en ce qui concerne les questions relatives à la loi sur le contrôle des organisations[91] et à la loi sur la prévention des activités subversives[92]. Le CEPD s'en félicite.

237. Bien que le site internet du ministère japonais de la justice fournisse quelques informations[93], le CEPD n'est pas en mesure d'évaluer exactement l'indépendance de la commission d'examen de la sécurité publique, étant donné qu'il n'a pas reçu le texte de la loi en portant création[94], ni les règles qui lui sont applicables[95].

4.2.3.5 Contrôle par la commission nationale de sécurité publique, les commissions préfectorales de sécurité publique et la loi sur la protection des données à caractère personnel détenues par les organes administratifs (exécutif)

238. Voir 3.1.2.2.1. (commission nationale de sécurité publique), 3.1.2.2.2. (commissions préfectorales de sécurité publique) et 3.1.2.2.4. (exécutif).

4.2.3.6 Contrôle exercé par la commission de protection des données à caractère personnel

239. Le CEPD invite la Commission soit à indiquer au considérant 164 que la commission de protection des données à caractère personnel n'est pas un organe de contrôle des entités publiques susmentionnées et qu'elle n'est compétente que pour les recours des personnes physiques, soit à déplacer le passage du considérant 164 dans la section consacrée aux « recours individuels ».

4.2.4 Mécanisme de recours

240. Pour l'analyse du mécanisme de recours qui vient d'être négocié, le CEPD renvoie à la section relative à l'application de la loi.

241. En outre, il convient de noter que la législation japonaise prévoit un mécanisme de recours individuel spécifique dans le domaine de la sécurité nationale. Le CEPD croit comprendre que tous les individus, y compris les citoyens de l'Union, peuvent généralement demander la divulgation, la correction (y compris la suppression) ou la suspension de l'utilisation de leurs données auprès des organes administratifs, même si ces données sont traitées à des fins de sécurité nationale. Lorsqu'une telle demande est « rejetée au motif que les données concernées sont considérées comme ne pouvant pas être divulguées », un recours peut être formé et le « comité d'examen de la divulgation des informations et de la protection des données à caractère personnel » doit être consulté. Le comité est

[91] Loi sur le contrôle des organisations ayant commis des meurtres de masse aveugles (loi nº 147 du 7 décembre 1999).

[92] Loi sur la prévention des activités subversives (loi nº 240 du 21 juillet 1952).

[93] Voir http://www.moj.go.jp/ENGLISH/MEOM/meom-01.html (septembre 2018): l'organe extra-ministériel «*est composé d'un président et de six membres. Ils sont choisis parmi les personnalités de bonne réputation, capables de rendre un jugement équitable sur le contrôle des organisations et ayant une connaissance et une expérience solides de la loi et de la société. Ils sont nommés par le Premier ministre et doivent être approuvés par les deux chambres de la Diète. En ce qui concerne l'application des lois susmentionnées (loi sur la prévention des activités subversives et loi sur le contrôle des organisations), les membres exercent leurs fonctions de manière relativement indépendante, indépendamment de toute instruction ou de tout contrôle du Premier ministre ou du ministre de la justice».*

[94] http://www.japaneselawtranslation.go.jp/law/detail_main?re=&vm=2&id=613 (septembre 2018).

[95] Article 28 de la loi sur le contrôle des organisations.

composé de membres nommés par le Premier ministre avec le consentement des deux chambres et est doté de pouvoirs d'enquête. Il remet ses conclusions sous la forme d'un rapport écrit adressé à la personne concernée. Ces conclusions ne sont pas juridiquement contraignantes, mais sont presque toujours suivies[96]. Selon l'annexe II, dans seulement deux cas sur 2000 dossiers[97] une autorité administrative a pris une décision différente de celle préconisée par le comité .

242. Il ressort des explications fournies qu'un réexamen n'est pas possible dans les cas dans lesquels les informations peuvent être « divulguées », mais la personne concernée n'est pas satisfaite de l'issue de l'examen. Le CEPD reconnaît l'importance de cette voie de recours, mais souhaiterait obtenir des précisions sur ce dernier aspect, qui limiterait considérablement son champ d'application.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

[96] Voir l'annexe II, pages 25 et 26. Loi portant création du comité d'examen de la divulgation des informations et de la protection des données à caractère personnel, articles 4, 9 et 11.
[97] Annexe II, note de bas de page 35.