Parlement européen
2014-2019

TEXTES ADOPTÉS

P8_TA(2018)0529

Adéquation de la protection des données à caractère personnel assurée par le Japon

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

Le Parlement européen,

– vu le traité sur l'Union européenne, le traité sur le fonctionnement de l'Union européenne et les articles 6, 7, 8, 11, 16, 47 et 52 de la charte des droits fondamentaux de l'Union européenne,

– vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)[1], et l'acquis de l'Union pertinent dans le domaine de la protection des données,

– vu l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015 dans l'affaire C-362/14, Maximillian Schrems/Data Protection Commissioner[2],

– vu l'arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016 dans les affaires jointes C-203/15, Tele2 Sverige AB/Post- och telestyrelsen, et C-698/15, Secretary of State for the Home Department/Tom Watson e.a.[3],

– vu sa résolution du 12 décembre 2017 intitulée «Vers une stratégie pour le commerce numérique»[4],

– vu le document adopté par le groupe de travail «Article 29» le 6 février 2018, intitulé «Critères de référence pour l'adéquation»[5], qui fournit à la Commission et au comité européen de la protection des données des orientations, conformément au règlement

---

1 JO L 119 du 4.5.2016, p. 1.
2 ECLI:EU:C:2015:650.
3 ECLI:EU:C:2016:970.
4 JO C 369 du 11.10.2018, p. 22.
5 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108; adopté par le comité européen de la protection des données lors de sa première séance plénière.

général sur la protection des données (RGPD), pour évaluer le degré de protection des données dans les pays tiers et les organisations internationales,

– vu l'avis du comité européen de la protection des données du 5 décembre 2018 sur le projet de décision d'adéquation UE-Japon,

– vu le projet de décision d'exécution de la Commission 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 (COM(2018)XXXX),

– vu les conclusions de la délégation ad hoc de la commission des libertés civiles, de la justice et des affaires intérieures qui s'est rendue au Japon en octobre 2017 dans le cadre des négociations d'adéquation pour y rencontrer les autorités et parties prenantes japonaises compétentes afin de débattre des éléments essentiels que la Commission examinera lorsqu'elle adoptera sa décision d'adéquation,

– vu l'article 123, paragraphe 2, de son règlement intérieur,

A. considérant que le RGPD est applicable depuis le 25 mai 2018; que l'article 45, paragraphe 2, du RGPD définit les éléments dont la Commission doit tenir compte lorsqu'elle évalue le caractère adéquat du niveau de protection assuré par un pays tiers ou une organisation internationale;

B. considérant le Commission doit, en particulier, prendre en considération l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que l'existence et le bon fonctionnement d'une ou de plusieurs autorités de contrôle indépendantes, ainsi que les engagements internationaux pris par le pays tiers ou l'organisation internationale;

C. considérant que dans son arrêt du 6 octobre 2015 dans l'affaire C-362/14, Maximillian Schrems/Data Protection Commissioner, la Cour de justice de l'Union européenne a précisé qu'un niveau de protection adéquat dans un pays tiers doit s'entendre comme «substantiellement équivalent» à la protection garantie dans l'Union en vertu de la directive 95/46/CE lue à la lumière de la charte;

D. considérant que le Japon est l'un des partenaires commerciaux les plus importants de l'Union européenne, et que les deux parties ont récemment conclu un accord de partenariat économique (APE) qui consacre leurs valeurs et principes communs tout en ménageant les sensibilités des deux parties; que la reconnaissance commune des droits fondamentaux, y compris le respect de la vie privée et la protection des données, est essentielle à la décision d'adéquation qui constituera la base juridique du transfert des données à caractère personnel de l'Union vers le Japon;

E. considérant que la délégation ad hoc de la commission des libertés civiles, de la justice et des affaires intérieures qui s'est rendue au Japon a été sensibilisée à l'intérêt que portent les autorités japonaises et les parties prenantes non seulement à l'application du nouveau RGPD, mais aussi à la mise au point d'un mécanisme de transfert des données à caractère personnel robuste et de haut niveau entre l'Union et le Japon qui remplirait les conditions prévues par le cadre juridique de l'Union pour en matière de protection,

entendue comme substantiellement équivalente à la protection garantie par la législation de l'Union en matière de protection de données;

F. considérant que les transferts de données à caractère personnel entre l'Union et le Japon à des fins commerciales constituent un élément important des relations bilatérales, au vu de la numérisation toujours plus poussée de l'économie mondiale; que ces transferts devraient s'effectuer dans le strict respect du droit à la protection des données à caractère personnel et du droit au respect de la vie privée; que l'un des objectifs fondamentaux de l'Union est la protection des droits fondamentaux consacrés dans la charte des droits fondamentaux de l'Union européenne;

G. considérant que l'Union et le Japon ont entamé, en janvier 2017, des discussions en vue de faciliter le transfert de données à caractère personnel à des fins commerciales au moyen du tout premier «constat mutuel d'adéquation»; considérant que, dans sa résolution du 12 décembre 2017 intitulée «Vers une stratégie pour le commerce numérique», le Parlement a explicitement reconnu que «les décisions relatives à l'adéquation [...] représentent un mécanisme indispensable pour sécuriser les transferts de données depuis l'Union vers un pays tiers»;

H. considérant que la décision constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon, si elle était adoptée, constituerait la première décision de cet ordre adoptée conformément aux nouvelles règles, plus strictes, du RGPD;

I. considérant que le Japon a récemment modernisé et consolidé sa législation sur la protection des données pour l'aligner sur les normes internationales et notamment sur les garanties et les droits individuels offerts par le nouveau cadre législatif européen de protection des données; que le cadre juridique japonais en matière de protection des données comporte plusieurs volets, la loi sur la protection des informations personnelles étant l'acte législatif autour duquel s'organise le système;

J. considérant que le gouvernement japonais a adopté, le 12 juin 2018, un décret qui délègue à la commission nationale de protection des informations personnelles, en sa qualité d'autorité compétente pour la gestion et la mise en application de la loi sur la protection des informations personnelles, le pouvoir de prendre les mesures nécessaires pour combler les différences entre les systèmes et opérations du Japon et du pays étranger concerné, en vertu de l'article 6 de cette loi, afin que les renseignements personnels reçus de ce pays soient traités de manière appropriée; que cette décision recouvre également le pouvoir d'établir des protections renforcées en adoptant des règles plus strictes qui complètent et excèdent celles énoncées dans la loi et le décret du gouvernement; qu'en vertu de cette décision, ces règles plus strictes seraient contraignantes pour les opérateurs économiques japonais et auraient force exécutoire;

K. considérant que le projet de décision exécutive de la Commission constatant le niveau de protection adéquat des données à caractère personnel assuré par le Japon s'accompagne, à l'annexe I, des règles complémentaires adoptées par la commission de protection des informations personnelles le 15 juin 2018 au titre de l'article 6 de la loi sur la protection des informations personnelles, qui confère explicitement à la commission le pouvoir d'adopter des règles plus strictes, notamment dans le but de faciliter les transferts de données internationaux; que ces règles complémentaires n'ont pas encore été rendues publiques;

L. considérant que l'objectif des règles complémentaires est a priori de combler les écarts entre le droit japonais et le droit de l'Union en matière de protection des données qui empêchent de garantir un traitement adéquat des données à caractère personnel transférées par l'Union vers le Japon en vertu d'une décision d'adéquation, en particulier en ce qui concerne les données sensibles (pour lesquelles des précautions sont nécessaires), les données à caractère personnel conservées, le fait de spécifier une finalité de traitement, les restrictions résultant d'une finalité de traitement, les limitations au transfert des données à un tiers dans un pays étranger et les données traitées de manière anonyme;

M. considérant que les règles complémentaires seraient juridiquement contraignantes pour tout opérateur économique traitant des données à caractère personnel à qui de telles données sont transférées depuis l'Union en vertu d'une décision d'adéquation, et que cet opérateur économique devrait alors s'y plier ainsi qu'à tous les droits et devoirs y afférents, la commission de protection des informations personnelles et les juridictions japonaises étant compétentes pour contrôler l'application de ces règles;

N. considérant qu'afin de garantir un niveau de protection des données à caractère personnel transférées depuis l'Union vers le Japon qui soit substantiellement équivalent, les règles complémentaires instaurent des garanties complémentaires applicables sur la base de conditions ou restrictions plus strictes au traitement des données à caractère personnel en provenance de l'Union, notamment en ce qui concerne les données à caractère personnel sensibles, les transferts ultérieurs, les données anonymes et la limitation des finalités;

O. considérant que le cadre juridique japonais en matière de protection des données établit une distinction entre «informations personnelles» et «données à caractère personnel» et fait mention, dans certains cas, d'une catégorie spécifique de données à caractère personnel, les «données à caractère personnel conservées»;

P. considérant qu'au sens de l'article 2, paragraphe 1, de la loi sur la protection des informations personnelles, le concept d'«informations personnelles» recouvre toute information sur une personne vivante qui permet de l'identifier; que la définition distingue deux catégories d'informations personnelles, le numéro personnel d'identification, d'une part, et les autres informations personnelles qui permettent d'identifier une personne précise, d'autre part; que la seconde catégorie comprend des informations qui, en elles-mêmes, ne permettent pas d'identifier la personne, mais qui sont susceptibles, lorsqu'elles sont promptement collationnées à d'autres informations, de permettre l'identification d'une personne précise;

Q. considérant qu'au sens de l'article 2, paragraphe 4, de la loi sur la protection des informations personnelles, il est entendu par «données à caractère personnel» des informations personnelles constituant une base de données d'informations personnelles, etc.; qu'au sens de l'article 2, paragraphe 1, de ladite loi précise que les informations contenues dans ces bases de données font l'objet d'un agencement systématique comparable à la notion de «fichier» visée à l'article 2, paragraphe 1, du RGPD; qu'au sens de l'article 4, paragraphe 1, du RGPD, on entend par «données à caractère personnel» toute information concernant une personne physique identifiée ou identifiable; qu'est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de

localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale; que, pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage;

R. considérant qu'au sens de l'article 2, paragraphe 7, de la loi sur la protection des informations personnelles, il est entendu par «données à caractère personnel conservées» des données à caractère personnel qu'un opérateur économique chargé du traitement de ce type de données est autorisé à divulguer, corriger, compléter ou supprimer, cesser d'utiliser, effacer ou cesser de fournir en tant que tiers, et qui ne sont ni des données dont une décision du gouvernement détermine qu'elles sont susceptibles de nuire à l'intérêt public ou à un autre intérêt si leur présence ou absence vient à être connue, ni des données dont l'effacement est prévu après un délai inférieur à un an par décret ministériel; que les règles complémentaires alignent la notion de «données à caractère personnel conservées» sur celle de «données à caractère personnel» pour garantir que les limites aux droits individuels associés à la première ne s'appliquent pas aux données transférées depuis l'Union;

S. considérant que la loi japonaise sur la protection des données qui fait l'objet du projet de décision d'exécution de la Commission exclut de son champ d'application divers secteurs lorsqu'ils traitent des données à caractère personnel à des fins particulières; que le projet de décision d'exécution ne s'appliquerait pas au transfert de données à caractère personnel depuis l'Union vers un destinataire relevant d'une des exceptions susmentionnées prévues par ladite loi japonaise;

T. considérant qu'au sujet des transferts ultérieurs, du Japon vers un pays tiers, de données à caractère personnel provenant de l'Union, le projet de décision d'exécution exclut l'utilisation d'instruments de transfert qui ne crée pas de relation contraignante entre l'exportateur japonais de données et l'importateur de données dans le pays tiers et ne garantissent pas le niveau de protection requis; qu'un des instruments ainsi exclus serait par exemple le système des règles en matière de respect de la vie privée dans un contexte transfrontalier de la Coopération économique Asie-Pacifique (système APEC CBPR), auquel le Japon est partie, étant donné qu'en vertu de ce système, les garanties offertes ne sont pas le produit d'un accord créant une relation contraignante entre l'exportateur et l'importateur dans leur relation bilatérale et qu'en outre, la protection des données est nettement moins élevée que celle garantie par l'ensemble que constituent la loi japonaise sur la protection des informations personnelles et les règles complémentaires;

U. considérant que, dans son avis du 5 décembre 2018, le comité européen de la protection des données évalue, sur la base des documents que la Commission a mis à sa disposition, si le cadre juridique japonais en matière de protection des données offre des garanties suffisantes assurant un niveau approprié de protection des données des personnes physiques; que le comité européen de la protection des données se félicite des efforts déployés par la Commission et la commission japonaise de protection des informations personnelles en vue d'un rapprochement des cadres juridiques du Japon et de l'Union pour faciliter le transfert de données à caractère personnel; que ledit comité reconnaît que les améliorations apportées par les règles complémentaires pour combler certaines différences entre les deux cadres sont très importantes et bien accueillies; que

ledit comité constate qu'il subsiste un certain nombre de questions, telles que la protection des données à caractère personnel transférées depuis l'Union vers le Japon tout au long de leur cycle de vie, et qu'il recommande à la Commission de fournir des éléments de preuve et des explications supplémentaires en ce qui concerne les questions soulevées, et qu'il suit de près l'application effective des règles;

V. considérant que le projet de décision d'exécution s'accompagne également, à l'annexe II, d'une lettre du ministère de la justice du 14 septembre 2018 qui fait référence à un document, qui a été élaboré par ce ministère et plusieurs autres ministères et organismes, sur la collecte et le traitement des informations personnelles par les pouvoirs publics japonais à des d'application du droit pénal et de sécurité nationale, qui passe en revue le cadre juridique applicable et fournit à la Commission des déclarations officielles, assurances et engagements signés au plus haut niveau dans les ministères et les organismes;

1. prend acte de l'analyse détaillée fournie par la Commission dans son projet de décision en ce qui concerne les garanties, y compris les mécanismes de contrôle et de recours, applicables au traitement des données par des opérateurs économiques ainsi qu'à l'accès aux données par les pouvoirs publics japonais, en particulier dans le domaine des services répressifs et de la sécurité nationale;

2. prend acte de la préparation en parallèle, par le Japon, de la reconnaissance du niveau de protection des données à caractère personnel transférées depuis le Japon vers l'Union au titre de l'article 23 de la loi sur la protection des informations personnelles, ce qui aboutirait, à l'échelle mondiale, au tout premier constat mutuel d'adéquation et à la création de la plus grande zone de libre circulation de flux de données sécurisés;

3. salue cette évolution, qui témoigne de la diffusion mondiale de normes rigoureuses en matière de protection des données; souligne néanmoins que cela ne doit en aucun cas conduire à l'adoption d'une démarche de marchandage dans les décisions d'adéquation de l'Union; rappelle que pour prendre une décision d'adéquation conformément au RGPD, la Commission doit évaluer objectivement la situation juridique et pratique dans le pays tiers, le territoire, le secteur ou l'organisation internationale en question;

4. souligne que la Cour de justice de l'Union européenne a statué que l'expression «niveau de protection adéquat» n'implique pas un niveau de protection identique à celui garanti dans l'Union européenne, mais doit être comprise comme exigeant que le pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la charte;

5. relève que le droit au respect de la vie privée et à la protection des données à caractère personnel est garanti au niveau constitutionnel tant au Japon que dans l'Union, mais qu'une harmonisation complète des règles des deux parties ne sera pas possible compte tenu des différences de structure constitutionnelle et de culture;

6. prend acte des modifications apportées à la loi sur la protection des informations personnelles, entrées en vigueur le 30 mai 2017; salue les grands progrès qu'elles représentent;

7. relève que les catégories d'opérateurs économiques et d'activités de traitement qui sont exclues du champ d'application matériel de la loi japonaise sur la protection des informations personnelles ont été expressément exclues du champ d'application du constat d'adéquation;

8. estime qu'à la suite de l'adoption des modifications apportées à la loi sur la protection des informations personnelles et de l'adoption du RGPD en 2016, les systèmes japonais et européens de protection des données convergent fortement au regard des principes, des garanties et des droits individuels, ainsi que des mécanismes de surveillance et de contrôle de l'application; attire notamment l'attention sur la création d'une autorité de surveillance indépendante, la commission de protection des informations personnelles, à la suite de l'adoption des modifications apportées à la loi sur la protection des informations personnelles;

9. relève néanmoins que la commission elle-même constate que, «malgré une forte convergence entre les deux systèmes, il subsiste entre eux des différences non négligeables»; relève également qu'afin de garantir une protection plus élevée des données à caractère personnel transférées depuis l'Union, la commission a adopté des règles complémentaires le 15 juin 2018;

10. salue les précisions importantes apportées par les règles complémentaires, notamment l'harmonisation de la définition du terme «informations personnelles anonymes» utilisé dans la loi japonaise avec la définition du terme «informations anonymes» employé dans le RGPD;

11. estime que les protections supplémentaires offertes par les règles complémentaires ne recouvrent que les transferts effectués en vertu de décisions d'adéquation; rappelle qu'eu égard au champ d'application de la décision d'adéquation, certains transferts de données seront réalisés au titre de ces autres mécanismes disponibles;

12. constate que les protections supplémentaires prévues par les règles complémentaires se limitent aux données à caractère personnel transférées depuis l'Europe, et que les opérateurs économiques qui devront traiter simultanément les données à caractère personnel japonaises et européennes devront par conséquent se conformer aux règles complémentaires par des moyens techniques (ajout de balises) ou organisationnels (stockage dans une base de données spéciale) afin de pouvoir identifier ces données à caractère personnel tout au long de leur cycle de vie; invite la Commission à suivre la situation afin d'éviter de possibles failles que les opérateurs économiques pourraient exploiter pour contourner les obligations prévues par les règles complémentaires en transférant des données par l'intermédiaire de pays tiers;

13. relève que la définition du terme «données à caractère personnel» dans la loi japonaise ne recouvre pas les données «dont une décision du gouvernement a déterminé, au vu de leur méthode de traitement, qu'elles comportaient peu de risques de porter atteinte aux droits et intérêts d'une personne physique»; invite instamment la Commission à déterminer si ce principe fondé sur les risques est compatible avec celui de l'Union, en vertu duquel tout traitement de données à caractère personnel relève du droit sur la protection des données; note cependant que cet principe s'appliquerait dans des situations très limitées;

14. relève, en outre, que la définition du terme «informations personnelles» qui figure dans

la loi japonaise ne recouvre que les informations «qui permettent d'identifier une personne précise»; observe également que cette définition ne recouvre pas la précision apportée par le RGPD, selon laquelle les informations personnelles doivent également être considérées comme des données à caractère personnel lorsqu'elles suffisent à «distinguer» une personne physique, comme l'a clairement constaté la Cour de justice;

15. craint que la définition plus étroite du terme «données à caractère personnel» (fondée sur la définition du terme «informations personnelles») dans la loi japonaise ne puisse être considérée comme «substantiellement équivalente» aux dispositions du RGPD et à la jurisprudence de la Cour de justice; remet dès lors en question l'affirmation qui figure dans le projet de décision d'exécution de la Commission, selon laquelle «les données en provenance de l'Union relèveront toujours de la catégorie des «données à caractère personnel» au sens de la loi japonaise»; invite la Commission à suivre de près les enjeux concrets de ces différentes notions lors de l'application de la décision d'adéquation et de son examen périodique;

16. invite la Commission à fournir des précisions supplémentaires et, si nécessaire, à demander aux autorités japonaises d'adopter davantage de règles complémentaires contraignantes, afin de garantir que toutes les données à caractère personnel au sens du RGPD sont protégées en cas de transfert vers le Japon;

17. relève avec préoccupation qu'en ce qui concerne la prise de décision et le profilage automatisés, contrairement à ce qui est prévu dans le droit de l'Union, ni la loi japonaise ni les lignes directrices ne prévoient de dispositions juridiques, et que seules certaines règles sectorielles régissent cette question, sans fournir de cadre juridique global et complet doté de garanties fondamentales solides qui protègent de la prise de décision et du profilage automatisés; demande à la Commission d'expliquer quelles sont exactement, à cet égard, les dispositions du cadre juridique japonais en matière de protection des données qui permettent de garantir une protection équivalente; estime que cette question est particulièrement pertinente à la lumière des cas récents de profilage dans l'affaire Facebook-Cambridge Analytica;

18. estime qu'à la lumière du référentiel d'adéquation du comité européen de la protection des données, des précisions complémentaires sur le démarchage commercial sont nécessaires, compte tenu de l'absence de dispositions spécifiques dans la loi japonaise, pour démontrer le niveau équivalent de protection des données personnelles au Japon;

19. prend acte de l'avis du comité européen de la protection des données qui recense plusieurs sujets de préoccupation, tels que la protection des données à caractère personnel transférées depuis l'Union vers le Japon tout au long de leur cycle de vie; engage la Commission à y répondre et à fournir, dans la décision d'exécution, des preuves et des explications supplémentaires démontrant l'existence de garanties appropriées;

20. invite la Commission à déterminer si, en ce qui concerne les transferts ultérieurs, la solution prévue dans les règles complémentaires, qui impose le consentement préalable des personnes européennes dont les données font l'objet d'un traitement à un transfert ultérieur à un tiers dans un autre pays, omet certains éléments fondamentaux qui permettraient aux personnes dont les données font l'objet d'un traitement de donner leur consentement, étant donné qu'elle ne définit pas explicitement le champ d'application du concept d'«informations sur les circonstances du transfert nécessaires pour que [la

personne dont les données font l'objet d'un traitement] donne son consentement éclairé», conformément à l'article 13 du RGPD, comme par exemple des informations sur le pays tiers de destination du transfert ultérieur; invite la Commission à apporter des précisions quant aux conséquences, pour la personne dont les données font l'objet d'un traitement, d'un refus de consentement à un transfert ultérieur de ses données à caractère personnel;

21. déplore qu'en ce qui concerne le contrôle effectif de l'application de la loi sur la protection des informations personnelles, le niveau des sanctions éventuelles au pénal soit insuffisant pour garantir un réel respect de la loi, puisque ce niveau ne semble être ni proportionné, ni efficace, ni dissuasif eu égard à la gravité des infractions prévues; relève toutefois que la loi sur la protection des informations personnelles prévoit également des sanctions pénales, y compris des peines d'emprisonnement; demande à la Commission de fournir des informations sur l'utilisation concrète des amendes administratives et des sanctions pénales par le passé;

22. observe que, si la commission de protection des informations personnelles n'exerce aucun contrôle sur les autorités répressives, d'autres mécanismes de suivi, comme par l'intermédiaire de la commission préfectorale de sécurité publique, une entité indépendante, sont possibles; relève que le Conseil national d'évaluation de la divulgation d'informations et de la protection des informations personnelles dispose de pouvoirs dans ce domaine, notamment l'examen des demandes d'accès et la publication des avis, mais que ses pouvoirs ne sont pas juridiquement contraignants; se félicite que l'Union et le Japon aient convenu de mettre en place un mécanisme de recours spécifique, géré et supervisé par la commission de protection des informations personnelles, qui s'appliquera au traitement des données à caractère personnel par les autorités répressives et de sécurité nationale;

23. relève qu'en vertu de la loi japonaise sur la protection des informations personnelles conservées par des organes administratifs, les opérateurs économiques peuvent également, à leur gré, transférer des données aux autorités répressives; souligne que cette possibilité n'est pas prévue dans le RGPD ni dans la directive sur la police; invite la Commission à déterminer si elle peut être considérée comme «substantiellement équivalente» aux dispositions du RGPD;

24. est au courant des informations parues dans les médias sur l'agence japonaise de renseignement d'origine électromagnétique, qui compterait près de 1 700 employés et disposerait d'au moins six installations de surveillance qui espionneraient en continu les appels téléphoniques, courriers électroniques et autres moyens de communication[1]; se dit préoccupé par l'absence de toute mention, dans le projet de décision d'exécution, de cette surveillance de masse indiscriminée; demande à la Commission de fournir davantage d'informations sur la surveillance de masse au Japon; se dit fortement préoccupé par le risque que cette surveillance de masse ne puisse satisfaire aux critères permettant d'établir une équivalence substantielle définis par la Cour de justice dans son arrêt dans l'affaire Schrems (C-362/14);

25. déplore que le document sur la collecte et le traitement des informations personnelles par les pouvoirs publics japonais à des fins d'application du droit pénal et de sécurité

---

[1] Ryan Gallagher, «The Untold Story of Japan's Secret Spy Agency», *The Intercept*, 19 mai 2018 (https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/)

nationale, repris à l'annexe II du projet de décision d'exécution, n'ait pas le même effet juridiquement contraignant que les règles complémentaires;

Conclusions

26. demande à la Commission de fournir davantage d'explications et d'éléments de preuve en ce qui concerne les points susmentionnés, y compris ceux recensés par le comité européen de la protection des données dans son avis du 5 décembre 2018, afin de prouver que le cadre juridique japonais en matière de protection des données garantit un niveau de protection suffisant qui soit substantiellement équivalent à celui garanti par le cadre juridique de l'Union en matière de protection des données;

27. estime que la décision d'adéquation, si elle est adoptée, peut en outre attirer l'attention du monde entier sur les avantages extrêmement concrets qu'offre la convergence vers les normes rigoureuses de l'Union en matière de protection des données; souligne, à cet égard, l'importance de cette décision d'adéquation, susceptible de faire jurisprudence pour de futurs partenariats avec d'autres pays qui ont adopté un cadre juridique moderne en matière de protection des données;

28. charge sa commission des libertés civiles, de la justice et des affaires intérieures de continuer à suivre l'évolution de la situation dans ce domaine, notamment les affaires examinées par la Cour de justice, et de veiller au suivi des recommandations formulées dans la présente résolution;

°

° °

29. charge son Président de transmettre la présente résolution au Conseil, à la Commission, aux gouvernements et aux parlements des États membres, au comité européen de la protection des données, au Contrôleur européen de la protection des données, au comité institué en vertu de l'article 93, paragraphe 1, du règlement général sur la protection des données, au Conseil de l'Europe et au gouvernement du Japon.