Recueil de la jurisprudence

ARRÊT DE LA COUR (grande chambre)

16 juillet 2020*

« Renvoi préjudiciel – Protection des personnes physiques à l'égard du traitement des données à caractère personnel – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 47 – Règlement (UE) 2016/679 – Article 2, paragraphe 2 – Champ d'application – Transferts de données à caractère personnel vers des pays tiers à des fins commerciales – Article 45 – Décision d'adéquation de la Commission – Article 46 – Transferts moyennant des garanties appropriées – Article 58 – Pouvoirs des autorités de contrôle – Traitement des données transférées par les autorités publiques d'un pays tiers à des fins de sécurité nationale – Appréciation du caractère adéquat du niveau de protection assuré dans le pays tiers – Décision 2010/87/UE – Clauses types de protection pour le transfert de données à caractère personnel vers des pays tiers – Garanties appropriées offertes par le responsable du traitement – Validité – Décision d'exécution (UE) 2016/1250 – Adéquation de la protection assurée par le bouclier de protection des données Union européenne-États-Unis – Validité – Plainte d'une personne physique dont les données ont été transférées depuis l'Union européenne vers les États-Unis »

Dans l'affaire C-311/18,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par la High Court (Haute Cour, Irlande), par décision du 4 mai 2018, parvenue à la Cour le 9 mai 2018, dans la procédure

Data Protection Commissioner

contre

Facebook Ireland Ltd,

Maximillian Schrems,

en présence de :

The United States of America,

Electronic Privacy Information Centre,

BSA Business Software Alliance Inc.,

Digitaleurope,

* Langue de procédure : l'anglais.

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M^me^ R. Silva de Lapuerta, vice-présidente, M. A. Arabadjiev, M^me^ A. Prechal, MM. M. Vilaras, M. Safjan, S. Rodin, P. G. Xuereb, M^me^ L. S. Rossi et M. I. Jarukaitis, présidents de chambre, MM. M. Ilešič, T. von Danwitz (rapporteur) et D. Šváby, juges,

avocat général : M. H. Saugmandsgaard Øe,

greffier : M^me^ C. Strömholm, administratrice,

vu la procédure écrite et à la suite de l'audience du 9 juillet 2019,

considérant les observations présentées :

– pour le Data Protection Commissioner, par M. D. Young, solicitor, MM. B. Murray et M. Collins, SC, ainsi que par M^me^ C. Donnelly, BL,

– pour Facebook Ireland Ltd, par M. P. Gallagher et M^me^ N. Hyland, SC, M^me^ A. Mulligan et M. F. Kieran, BL, ainsi que par MM. P. Nolan, C. Monaghan, C. O'Neill et R. Woulfe, solicitors,

– pour M. Schrems, par M^e^ H. Hofmann, Rechtsanwalt, MM. E. McCullough, J. Doherty et S. O'Sullivan, SC, ainsi que par M. G. Rudden, solicitor,

– pour The United States of America, par M^me^ E. Barrington, SC, M^me^ S. Kingston, BL, ainsi que par MM. S. Barton et B. Walsh, solicitors,

– pour l'Electronic Privacy Information Centre, par M^me^ S. Lucey, solicitor, M^me^ G. Gilmore et M. A. Butler, BL, ainsi que par M. C. O'Dwyer, SC,

– pour BSA Business Software Alliance Inc., par M^es^ B. Van Vooren et K. Van Quathem, advocaten,

– pour Digitaleurope, par M^me^ N. Cahill, barrister, M. J. Cahir, solicitor, et M. M. Cush, SC,

– pour l'Irlande, par M. A. Joyce et M^me^ M. Browne, en qualité d'agents, assistés de M. D. Fennelly, BL,

– pour le gouvernement belge, par MM. J.-C. Halleux et P. Cottin, en qualité d'agents,

– pour le gouvernement tchèque, par MM. M. Smolek, J. Vláčil et O. Serdula ainsi que par M^me^ A. Kasalická, en qualité d'agents,

– pour le gouvernement allemand, par MM. J. Möller, D. Klebs et T. Henze, en qualité d'agents,

– pour le gouvernement français, par M^me^ A.-L. Desjonquères, en qualité d'agent,

– pour le gouvernement néerlandais, par M^mes^ C. S. Schillemans, M. K. Bulterman et M. Noort, en qualité d'agents,

– pour le gouvernement autrichien, par M^me^ J. Schmoll et M. G. Kunnert, en qualité d'agents,

– pour le gouvernement polonais, par M. B. Majczyna, en qualité d'agent,

– pour le gouvernement portugais, par M. L. Inez Fernandes ainsi que par M^mes^ A. Pimenta et C. Vieira Guerra, en qualité d'agents,

– pour le gouvernement du Royaume-Uni, par M. S. Brandon, en qualité d'agent, assisté de M. J. Holmes, QC, et de M. C. Knight, barrister,

– pour le Parlement européen, par M^me^ M. J. Martínez Iglesias et M. A. Caiola, en qualité d'agents,

– pour la Commission européenne, par MM. D. Nardi, H. Krämer et H. Kranenborg, en qualité d'agents,

– pour le comité européen de la protection des données (EDPB), par M^me^ A. Jelinek et M. K. Behn, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 19 décembre 2019,

rend le présent

Arrêt

1 La demande de décision préjudicielle porte, en substance,

– sur l'interprétation de l'article 3, paragraphe 2, premier tiret, des articles 25 et 26 ainsi que de l'article 28, paragraphe 3, de la 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 (JO 1995, L 281, p. 31), lus à la lumière de l'article 4, paragraphe 2, TUE et des articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »),

– sur l'interprétation et la validité de la décision 2010/87/UE de la Commission, du 5 février 2010, relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46 (JO 2010, L 39, p. 5), telle que modifiée par la décision d'exécution (UE) 2016/2297 de la Commission, du 16 décembre 2016 (JO 2016, L 344, p. 100) (ci-après la « décision CPT »), ainsi que

– sur l'interprétation et la validité de la décision d'exécution (UE) 2016/1250 de la Commission, du 12 juillet 2016, conformément à la directive 95/46 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (JO 2016, L 207, p. 1, ci-après la « décision BPD »).

2 Cette demande a été présentée dans le cadre d'un litige opposant le Data Protection Commissioner (commissaire à la protection des données, Irlande) (ci-après le « commissaire ») à Facebook Ireland Ltd et à M. Maximillian Schrems au sujet d'une plainte introduite par celui-ci concernant le transfert de ses données à caractère personnel par Facebook Ireland à Facebook Inc. aux États-Unis.

Le cadre juridique

La directive 95/46

3 L'article 3 de la directive 95/46, intitulé « Champ d'application », énonçait, à son paragraphe 2 :

« La présente directive ne s'applique pas au traitement de données à caractère personnel :

– mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal,

[...] »

4 L'article 25 de cette directive disposait :

« 1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel [...] ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.

2. Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ; [...]

[...]

6. La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes.

Les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission. »

5 L'article 26, paragraphes 2 et 4, de ladite directive prévoyait :

« 2. Sans préjudice du paragraphe 1, un État membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat au sens de l'article 25 paragraphe 2, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ; ces garanties peuvent notamment résulter de clauses contractuelles appropriées.

[...]

4. Lorsque la Commission décide, conformément à la procédure prévue à l'article 31 paragraphe 2, que certaines clauses contractuelles types présentent les garanties suffisantes visées au paragraphe 2, les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission. »

6 Aux termes de l'article 28, paragraphe 3, de la même directive :

« Chaque autorité de contrôle dispose notamment :

– de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle,

– de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques,

– du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

[...] »

Le RGPD

7 La directive 95/46 a été abrogée et remplacée par 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 (règlement général sur la protection des données) (JO 2016, L 119, p. 1, ci-après le « RGPD »).

8 Les considérants 6, 10, 101, 103, 104, 107 à 109, 114, 116 et 141 du RGPD énoncent :

« (6) L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel.

[...]

(10) Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. En ce qui concerne le traitement de données à caractère personnel nécessaire au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application des règles du présent règlement. Parallèlement à la législation générale et horizontale relative à la protection des données mettant en œuvre la directive

95/46/CE, il existe, dans les États membres, plusieurs législations sectorielles spécifiques dans des domaines qui requièrent des dispositions plus précises. Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées "données sensibles"). À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite.

[...]

(101) Les flux de données à caractère personnel à destination et en provenance de pays en dehors de l'Union et d'organisations internationales sont nécessaires au développement du commerce international et de la coopération internationale. L'augmentation de ces flux a créé de nouveaux enjeux et de nouvelles préoccupations en ce qui concerne la protection des données à caractère personnel. Cependant, il importe que, lorsque des données à caractère personnel sont transférées de l'Union à des responsables du traitement, sous-traitants ou autres destinataires dans des pays tiers ou à des organisations internationales, le niveau de protection des personnes physiques garanti dans l'Union par le présent règlement ne soit pas compromis, y compris en cas de transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale à des responsables du traitement ou sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale. En tout état de cause, les transferts vers des pays tiers et à des organisations internationales ne peuvent avoir lieu que dans le plein respect du présent règlement. Un transfert ne pourrait avoir lieu que si, sous réserve des autres dispositions du présent règlement, les dispositions du présent règlement relatives au transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales sont respectées par le responsable du traitement ou le sous-traitant.

[...]

(103) La Commission peut décider, avec effet dans l'ensemble de l'Union, qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale offre un niveau adéquat de protection des données, assurant ainsi une sécurité juridique et une uniformité dans l'ensemble [de] l'Union en ce qui concerne le pays tiers ou l'organisation internationale qui est réputé offrir un tel niveau de protection. Dans ce cas, les transferts de données à caractère personnel vers ce pays tiers ou cette organisation internationale peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autre autorisation. La Commission peut également décider, après en avoir informé le pays tiers ou l'organisation internationale et lui avoir fourni une justification complète, de révoquer une telle décision.

(104) Eu égard aux valeurs fondamentales sur lesquelles est fondée l'Union, en particulier la protection des droits de l'homme, la Commission devrait, dans son évaluation d'un pays tiers, d'un territoire ou d'un secteur déterminé dans un pays tiers, prendre en considération la manière dont un pays tiers déterminé respecte l'[É]tat de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal. Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, il y a lieu de tenir compte de critères clairs et objectifs, tels que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union, en particulier quand les données à caractère personnel sont traitées dans un ou plusieurs secteurs spécifiques. Plus

particulièrement, le pays tiers devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités de protection des données des États membres, et les personnes concernées devraient se voir octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif et juridictionnel.

[...]

(107) La Commission peut constater qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale n'assure plus un niveau adéquat de protection des données. En conséquence, le transfert de données à caractère personnel vers ce pays tiers ou à cette organisation internationale devrait être interdit, à moins que les exigences du présent règlement relatives aux transferts faisant l'objet de garanties appropriées, y compris des règles d'entreprise contraignantes et des dérogations pour des situations particulières, soient respectées. Dans ce cas, il y aurait lieu de prévoir des consultations entre la Commission et le pays tiers ou l'organisation internationale en question. La Commission devrait informer en temps utile le pays tiers ou l'organisation internationale des motifs de sa conclusion et engager des consultations avec ceux-ci en vue de remédier à la situation.

(108) En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant devrait prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Ces garanties peuvent consister à recourir à des règles d'entreprise contraignantes, des clauses types de protection des données adoptées par la Commission, des clauses types de protection des données adoptées par une autorité de contrôle ou des clauses contractuelles autorisées par une autorité de contrôle. Ces garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée au traitement au sein de l'Union, y compris l'existence de droits opposables de la personne concernée et de voies de droit effectives, ce qui comprend le droit d'engager un recours administratif ou juridictionnel effectif et d'introduire une action en réparation, dans l'Union ou dans un pays tiers. Ces garanties devraient porter, en particulier, sur le respect des principes généraux concernant le traitement des données à caractère personnel et des principes de protection des données dès la conception et de protection des données par défaut. [...]

(109) La possibilité qu'ont les responsables du traitement et les sous-traitants de recourir à des clauses types de protection des données adoptées par la Commission ou par une autorité de contrôle ne devrait pas les empêcher d'inclure ces clauses dans un contrat plus large, tel qu'un contrat entre le sous-traitant et un autre sous-traitant, ni d'y ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses contractuelles types adoptées par la Commission ou par une autorité de contrôle et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées. Les responsables du traitement et les sous-traitants devraient être encouragés à fournir des garanties supplémentaires par l'intermédiaire d'engagements contractuels qui viendraient compléter les clauses types de protection.

[...]

(114) En tout état de cause, lorsque la Commission ne s'est pas prononcée sur le caractère adéquat du niveau de protection des données dans un pays tiers, le responsable du traitement ou le sous-traitant devrait adopter des solutions qui garantissent aux personnes concernées des droits opposables et effectifs en ce qui concerne le traitement de leurs données dans l'Union une fois que ces données ont été transférées, de façon à ce que lesdites personnes continuent de bénéficier des droits fondamentaux et des garanties.

[...]

(116) Lorsque des données à caractère personnel franchissent les frontières extérieures de l'Union, cela peut accroître le risque que les personnes physiques ne puissent exercer leurs droits liés à la protection des données, notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations. De même, les autorités de contrôle peuvent être confrontées à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées en dehors de leurs frontières. Leurs efforts pour collaborer dans le contexte transfrontalier peuvent également être freinés par les pouvoirs insuffisants dont elles disposent en matière de prévention ou de recours, par l'hétérogénéité des régimes juridiques et par des obstacles pratiques tels que le manque de ressources. [...]

[...]

(141) Toute personne concernée devrait avoir le droit d'introduire une réclamation auprès d'une seule autorité de contrôle, en particulier dans l'État membre où elle a sa résidence habituelle, et disposer du droit à un recours juridictionnel effectif conformément à l'article 47 de la Charte si elle estime que les droits que lui confère le présent règlement sont violés ou si l'autorité de contrôle ne donne pas suite à sa réclamation, la refuse ou la rejette, en tout ou en partie, ou si elle n'agit pas alors qu'une action est nécessaire pour protéger les droits de la personne concernée. [...] »

9 L'article 2, paragraphes 1 et 2, de ce règlement prévoit :

« 1. Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué :

a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ;

b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne ;

c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique ;

d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. »

10 L'article 4 dudit règlement dispose :

« Aux fins du présent règlement, on entend par :

[...]

2) "traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

[...]

7) “responsable du traitement”, la personne physique ou morale, l’autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l’Union ou le droit d’un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l’Union ou par le droit d’un État membre ;

8) “sous-traitant”, la personne physique ou morale, l’autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ;

9) “destinataire”, la personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu’il s’agisse ou non d’un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d’une mission d’enquête particulière conformément au droit de l’Union ou au droit d’un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ;

[...] »

11 L’article 23 du même règlement énonce :

« 1. Le droit de l’Union ou le droit de l’État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l’article 34, ainsi qu’à l’article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu’une telle limitation respecte l’essence des libertés et droits fondamentaux et qu’elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir :

a) la sécurité nationale ;

b) la défense nationale ;

c) la sécurité publique ;

d) la prévention et la détection d’infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l’exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;

[...]

2. En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant :

a) aux finalités du traitement ou des catégories de traitement ;

b) aux catégories de données à caractère personnel ;

c) à l’étendue des limitations introduites ;

d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;

e) à la détermination du responsable du traitement ou des catégories de responsables du traitement ;

f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ;

g) aux risques pour les droits et libertés des personnes concernées ; et

h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation. »

12 Le chapitre V du RGPD, intitulé « Transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales », comprend les articles 44 à 50 de ce règlement. Aux termes de l'article 44 de celui-ci, intitulé « Principe général applicable aux transferts » :

« Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis. »

13 L'article 45 de ce règlement, intitulé « Transferts fondés sur une décision d'adéquation », prévoit, à ses paragraphes 1 à 3 :

« 1. Un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

2. Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte, en particulier, des éléments suivants :

a) l'[É]tat 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 la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ;

b) l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des

pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres ; et

c) les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

3. La Commission, après avoir évalué le caractère adéquat du niveau de protection, peut décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, assure un niveau de protection adéquat au sens du paragraphe 2 du présent article. L'acte d'exécution prévoit un mécanisme d'examen périodique, au moins tous les quatre ans, qui prend en compte toutes les évolutions pertinentes dans le pays tiers ou au sein de l'organisation internationale. L'acte d'exécution précise son champ d'application territorial et sectoriel et, le cas échéant, nomme la ou des autorités de contrôle visées au paragraphe 2, point b), du présent article. L'acte d'exécution est adopté en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2. »

14 L'article 46 dudit règlement, intitulé « Transferts moyennant des garanties appropriées », dispose, à ses paragraphes 1 à 3 :

« 1. En l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

2. Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela nécessite une autorisation particulière d'une autorité de contrôle, par :

a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics ;

b) des règles d'entreprise contraignantes conformément à l'article 47 ;

c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2 ;

d) des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2 ;

e) un code de conduite approuvé conformément à l'article 40, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées ; ou

f) un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

3. Sous réserve de l'autorisation de l'autorité de contrôle compétente, les garanties appropriées visées au paragraphe 1 peuvent aussi être fournies, notamment, par :

a) des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale ; ou

b) des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées. »

15 L'article 49 du même règlement, intitulé « Dérogations pour des situations particulières », énonce :

« 1. En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes :

a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées ;

b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée ;

c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale ;

d) le transfert est nécessaire pour des motifs importants d'intérêt public ;

e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ;

f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;

g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce.

Lorsqu'un transfert ne peut pas être fondé sur une disposition de l'article 45 ou 46, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières visées au premier alinéa du présent paragraphe n'est applicable, un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère

personnel. Le responsable du traitement informe l'autorité de contrôle du transfert. Outre qu'il fournit les informations visées aux articles 13 et 14, le responsable du traitement informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

2. Un transfert effectué en vertu du paragraphe 1, premier alinéa, point g), ne porte pas sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre. Lorsque le registre est destiné à être consulté par des personnes justifiant d'un intérêt légitime, le transfert n'est effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires.

3. Les points a), b), et c) du premier alinéa du paragraphe 1 et le deuxième alinéa du paragraphe 1 ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.

4. L'intérêt public visé au paragraphe 1, premier alinéa, point d), est reconnu par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis.

5. En l'absence de décision d'adéquation, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou à une organisation internationale. Les États membres notifient de telles dispositions à la Commission.

6. Le responsable du traitement ou le sous-traitant documente, dans les registres visés à l'article 30, l'évaluation ainsi que les garanties appropriées visées au paragraphe 1, deuxième alinéa, du présent article. »

16 Aux termes de l'article 51, paragraphe 1, du RGPD :

« Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union (ci-après dénommée "autorité de contrôle"). »

17 Conformément à l'article 55, paragraphe 1, de ce règlement, « [c]haque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement sur le territoire de l'État membre dont elle relève ».

18 L'article 57, paragraphe 1, dudit règlement prévoit :

« Sans préjudice des autres missions prévues au titre du présent règlement, chaque autorité de contrôle, sur son territoire :

a) contrôle l'application du présent règlement et veille au respect de celui-ci ;

[...]

f) traite les réclamations introduites par une personne concernée [...], examine l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire ;

[...] »

19 Aux termes de l'article 58, paragraphes 2 et 4, du même règlement :

« 2. Chaque autorité de contrôle dispose du pouvoir d'adopter toutes les mesures correctrices suivantes :

[...]

f) imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;

[...]

j) ordonner la suspension des flux de données adressés à un destinataire situé dans un pays tiers ou à une organisation internationale.

[...]

4. L'exercice des pouvoirs conférés à l'autorité de contrôle en application du présent article est subordonné à des garanties appropriées, y compris le droit à un recours juridictionnel effectif et à une procédure régulière, prévues par le droit de l'Union et le droit des États membres conformément à la Charte. »

20 L'article 64, paragraphe 2, du RGPD énonce :

« Toute autorité de contrôle, le président du [comité européen de la protection des données (EDPB)] ou la Commission peuvent demander que toute question d'application générale ou produisant des effets dans plusieurs États membres soit examinée par le comité en vue d'obtenir un avis, en particulier lorsqu'une autorité de contrôle compétente ne respecte pas les obligations relatives à l'assistance mutuelle conformément à l'article 61 ou les obligations relatives aux opérations conjointes conformément à l'article 62. »

21 Aux termes de l'article 65, paragraphe 1, de ce règlement :

« En vue d'assurer l'application correcte et cohérente du présent règlement dans les cas d'espèce, le comité adopte une décision contraignante dans les cas suivants :

[...]

c) lorsqu'une autorité de contrôle compétente ne demande pas l'avis du comité dans les cas visés à l'article 64, paragraphe 1, ou qu'elle ne suit pas l'avis du comité émis en vertu de l'article 64. Dans ce cas, toute autorité de contrôle concernée ou la Commission peut saisir le comité de la question. »

22 L'article 77 dudit règlement, intitulé « Droit d'introduire une réclamation auprès d'une autorité de contrôle », énonce :

« 1. Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement.

2. L'autorité de contrôle auprès de laquelle la réclamation a été introduite informe l'auteur de la réclamation de l'état d'avancement et de l'issue de la réclamation, y compris de la possibilité d'un recours juridictionnel en vertu de l'article 78. »

23 L'article 78 du même règlement, intitulé « Droit à un recours juridictionnel effectif contre une autorité de contrôle », prévoit, à ses paragraphes 1 et 2 :

« 1. Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne physique ou morale a le droit de former un recours juridictionnel effectif contre une décision juridiquement contraignante d'une autorité de contrôle qui la concerne.

2. Sans préjudice de tout autre recours administratif ou extrajudiciaire, toute personne concernée a le droit de former un recours juridictionnel effectif lorsque l'autorité de contrôle qui est compétente en vertu des articles 55 et 56 ne traite pas une réclamation ou n'informe pas la personne concernée, dans un délai de trois mois, de l'état d'avancement ou de l'issue de la réclamation qu'elle a introduite au titre de l'article 77. »

24 L'article 94 du RGPD dispose :

« 1. La directive [95/46] est abrogée avec effet au 25 mai 2018.

2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive [95/46] s'entendent comme faites au comité européen de la protection des données institué par le présent règlement. »

25 Selon l'article 99 de ce règlement :

« 1. Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

2. Il est applicable à partir du 25 mai 2018. »

La décision CPT

26 Le considérant 11 de la décision CPT est libellé comme suit :

« Les autorités de contrôle des États membres jouent un rôle clé dans ce mécanisme contractuel en garantissant la protection adéquate des données à caractère personnel après le transfert. Dans les cas exceptionnels où les exportateurs de données refusent ou ne sont pas en mesure d'instruire convenablement l'importateur de données et où il existe un risque imminent de dommage grave pour les personnes concernées, les clauses contractuelles types doivent permettre aux autorités de contrôle de soumettre les importateurs de données et les sous-traitants ultérieurs à des vérifications et, lorsque cela se révèle approprié, de prendre des décisions auxquelles ces derniers devront se plier. Les autorités de contrôle doivent avoir la faculté d'interdire ou de suspendre un transfert de données ou un ensemble de transferts fondé sur les clauses contractuelles types dans les cas exceptionnels où il est établi qu'un transfert fondé sur des termes contractuels risque d'avoir des conséquences négatives importantes pour les garanties et les obligations offrant un niveau de protection adéquat à la personne concernée. »

27 L'article 1er de cette décision dispose :

« Les clauses contractuelles types figurant en annexe sont considérées comme offrant des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants comme l'exige l'article 26, paragraphe 2, de la directive [95/46]. »

28 Conformément à l'article 2, second alinéa, de ladite décision, celle-ci « s'applique au transfert de données à caractère personnel par des responsables du traitement établis dans l'Union européenne à des destinataires établis en dehors du territoire de l'Union européenne qui agissent exclusivement en tant que sous-traitants ».

29 L'article 3 de la même décision dispose :

« Aux fins de la présente décision, on entend par :

[...]

c) "exportateur de données" : le responsable du traitement qui transfère les données à caractère personnel ;

d) "importateur de données" : le sous-traitant établi dans un pays tiers qui accepte de recevoir de l'exportateur de données des données à caractère personnel destinées à être traitées pour le compte de ce dernier après le transfert conformément à ses instructions et aux conditions de la présente décision et qui n'est pas soumis au mécanisme d'un pays tiers assurant une protection adéquate au sens de l'article 25, paragraphe 1, de la directive [95/46] ;

[...]

f) "droit applicable à la protection des données" : la législation protégeant les libertés et les droits fondamentaux des personnes, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans l'État membre où l'exportateur de données est établi ;

[...] »

30 Dans sa version initiale, antérieure à l'entrée en vigueur de la décision d'exécution 2016/2297, l'article 4 de la décision 2010/87 prévoyait :

« 1. Sans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées conformément aux chapitres II, III, V et VI de la directive [95/46], les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour interdire ou suspendre les flux de données vers des pays tiers afin de protéger les individus à l'égard du traitement de leurs données à caractère personnel, et ce dans les cas où :

a) il est établi que le droit auquel l'importateur de données ou un sous-traitant ultérieur est soumis oblige ce dernier à déroger au droit applicable à la protection des données au-delà des limitations nécessaires dans une société démocratique pour l'une des raisons énoncées à l'article 13 de la directive [95/46] lorsque cette obligation risque d'avoir des conséquences négatives importantes pour les garanties offertes par le droit applicable à la protection des données et les clauses contractuelles types ;

b) une autorité compétente a établi que l'importateur de données ou un sous-traitant ultérieur n'a pas respecté les clauses contractuelles types figurant en annexe ; ou

c) il est fort probable que les clauses contractuelles types figurant en annexe ne sont pas ou ne seront pas respectées et que la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves.

2. L'interdiction ou la suspension visée au paragraphe 1 est levée dès que les raisons qui la motivaient disparaissent.

3. Lorsque les États membres adoptent des mesures conformément aux paragraphes 1 et 2, ils en informent sans délai la Commission, qui transmet l'information aux autres États membres. »

31 Le considérant 5 de la décision d'exécution 2016/2297, adoptée à la suite du prononcé de l'arrêt du 6 octobre 2015, Schrems (C-362/14, EU:C:2015:650), est libellé comme suit :

« Mutatis mutandis, une décision de la Commission adoptée conformément à l'article 26, paragraphe 4, de la directive [95/46] est contraignante pour tous les organes des États membres qui en sont destinataires, y compris leurs autorités de contrôle indépendantes, dans la mesure où elle a pour effet de reconnaître que des transferts effectués sur la base de clauses contractuelles types qu'elle contient présentent des garanties suffisantes, comme l'exige l'article 26, paragraphe 2, de ladite directive. Cela n'empêche nullement une autorité nationale de contrôle d'exercer ses pouvoirs de contrôle des flux de données, notamment le pouvoir de suspendre ou d'interdire un transfert de données à caractère personnel, lorsqu'elle constate que ce transfert est effectué en violation de la législation de l'Union européenne ou de l'État membre en matière de protection des données, comme, par exemple, lorsque l'importateur de données ne respecte pas les clauses contractuelles types. »

32 Dans sa version actuelle, issue de la décision d'exécution 2016/2297, l'article 4 de la décision CPT énonce :

« Lorsque les autorités compétentes d'un État membre exercent leurs pouvoirs conformément à l'article 28, paragraphe 3, de la directive [95/46] pour suspendre ou interdire définitivement les flux de données vers des pays tiers afin de protéger les individus à l'égard du traitement de leurs données à caractère personnel, l'État membre concerné en informe sans délai la Commission, qui transmet l'information aux autres États membres. »

33 L'annexe de la décision CPT, intitulée « Clauses contractuelles types (sous-traitants) », comprend douze clauses types. La clause 3 de celle-ci, elle-même intitulée « Clause du tiers bénéficiaire », prévoit :

« 1. La personne concernée peut faire appliquer contre l'exportateur de données la présente clause, ainsi que la clause 4, points b) à i), la clause 5, points a) à e) et points g) à j), la clause 6, paragraphes 1 et 2, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 en tant que tiers bénéficiaire.

2. La personne concernée peut faire appliquer contre l'importateur de données la présente clause, ainsi que la clause 5, points a) à e) et g), la clause 6, la clause 7, la clause 8, paragraphe 2, et les clauses 9 à 12 dans les cas où l'exportateur de données a matériellement disparu ou a cessé d'exister en droit, à moins que l'ensemble de ses obligations juridiques n'ait été transféré, par contrat ou par effet de la loi, à l'entité qui lui succède, à laquelle reviennent par conséquent les droits et les obligations de l'exportateur de données, et contre laquelle la personne concernée peut donc faire appliquer lesdites clauses.

[...] »

34 Aux termes de la clause 4 de cette annexe, intitulée « Obligations de l'exportateur de données » :

« L'exportateur de données accepte et garantit ce qui suit :

a) le traitement, y compris le transfert proprement dit des données à caractère personnel, a été et continuera d'être effectué conformément aux dispositions pertinentes du droit applicable à la protection des données (et, le cas échéant, a été notifié aux autorités compétentes de l'État membre dans lequel l'exportateur de données est établi) et n'enfreint pas les dispositions pertinentes dudit État ;

b) il a chargé, et chargera pendant toute la durée des services de traitement de données à caractère personnel, l'importateur de données de traiter les données à caractère personnel transférées pour le compte exclusif de l'exportateur de données et conformément au droit applicable à la protection des données et aux présentes clauses ;

[...]

f) si le transfert porte sur des catégories particulières de données, la personne concernée a été informée ou sera informée avant le transfert ou dès que possible après le transfert que ses données pourraient être transmises à un pays tiers n'offrant pas un niveau de protection adéquat au sens de la directive [95/46] ;

g) il transmettra toute notification reçue de l'importateur de données ou de tout sous-traitant ultérieur conformément à la clause 5, point b), et à la clause 8, paragraphe 3), à l'autorité de contrôle de la protection des données s'il décide de poursuivre le transfert ou de lever sa suspension ;

[...] »

35 La clause 5 de ladite annexe, intitulée « Obligations de l'importateur de données [...] », stipule :

« L'importateur de données accepte et garantit ce qui suit :

a) il traitera les données à caractère personnel pour le compte exclusif de l'exportateur de données et conformément aux instructions de ce dernier et aux présentes clauses ; s'il est dans l'incapacité de s'y conformer pour quelque raison que ce soit, il accepte d'informer dans les meilleurs délais l'exportateur de données de son incapacité, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat ;

b) il n'a aucune raison de croire que la législation le concernant l'empêche de remplir les instructions données par l'exportateur de données et les obligations qui lui incombent conformément au contrat, et si ladite législation fait l'objet d'une modification susceptible d'avoir des conséquences négatives importantes pour les garanties et les obligations offertes par les clauses, il communiquera la modification à l'exportateur de données sans retard après en avoir eu connaissance, auquel cas ce dernier a le droit de suspendre le transfert de données et/ou de résilier le contrat ;

[...]

d) il communiquera sans retard à l'exportateur de données :
   i) toute demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre, sauf disposition contraire, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière ;
   ii) tout accès fortuit ou non autorisé ; et
   iii) toute demande reçue directement des personnes concernées sans répondre à cette demande, à moins qu'il n'ait été autorisé à le faire ;

[...] »

36 La note en bas de page à laquelle renvoie le titre de cette clause 5 énonce :

« Les exigences impératives de la législation nationale le concernant et qui ne vont pas au-delà de celles qui sont nécessaires dans une société démocratique pour l'un des intérêts énoncés à l'article 13, paragraphe 1, de la directive [95/46], c'est-à-dire si elles constituent une mesure nécessaire pour

sauvegarder la sûreté de l'État ; la défense ; la sécurité publique ; la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas de professions réglementées ; un intérêt économique ou financier important d'un État ou la protection de la personne concernée ou des droits et libertés d'autrui, ne vont pas à l'encontre des clauses contractuelles types. [...] »

37 La clause 6 de l'annexe de la décision CPT, intitulée « Responsabilité », prévoit :

« 1. Les parties conviennent que toute personne concernée ayant subi un dommage du fait d'un manquement aux obligations visées à la clause 3 ou à la clause 11 par une des parties ou par un sous-traitant ultérieur a le droit d'obtenir de l'exportateur de données réparation du préjudice subi.

2. Si une personne concernée est empêchée d'intenter l'action en réparation visée au paragraphe 1 contre l'exportateur de données pour manquement par l'importateur de données ou par son sous-traitant ultérieur à l'une ou l'autre de ses obligations visées à la clause 3 ou à la clause 11, parce que l'exportateur de données a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable, l'importateur de données accepte que la personne concernée puisse déposer une plainte à son encontre comme s'il était l'exportateur de données [...]

[...] »

38 La clause 8 de cette annexe, intitulée « Coopération avec les autorités de contrôle », stipule, à son paragraphe 2 :

« Les parties conviennent que l'autorité de contrôle a le droit d'effectuer des vérifications chez l'importateur de données et chez tout sous-traitant ultérieur dans la même mesure et dans les mêmes conditions qu'en cas de vérifications opérées chez l'exportateur de données conformément au droit applicable à la protection des données. »

39 La clause 9 de ladite annexe, intitulée « Droit applicable », précise que les clauses sont régies par le droit de l'État membre où l'exportateur de données est établi.

40 Aux termes de la clause 11 de la même annexe, intitulée « Sous-traitance ultérieure » :

« 1. L'importateur de données ne sous-traite aucune de ses activités de traitement effectuées pour le compte de l'exportateur de données conformément aux présentes clauses sans l'accord écrit préalable de l'exportateur de données. L'importateur de données ne sous-traite les obligations qui lui incombent conformément aux présentes clauses, avec l'accord de l'exportateur de données, qu'au moyen d'un accord écrit conclu avec le sous-traitant ultérieur, imposant à ce dernier les mêmes obligations que celles qui incombent à l'importateur de données conformément aux présentes clauses [...]

2. Le contrat écrit préalable entre l'importateur de données et le sous-traitant ultérieur prévoit également une clause du tiers bénéficiaire telle qu'énoncée à la clause 3 pour les cas où la personne concernée est empêchée d'intenter l'action en réparation visée à la clause 6, paragraphe 1, contre l'exportateur de données ou l'importateur de données parce que ceux-ci ont matériellement disparu, ont cessé d'exister en droit ou sont devenus insolvables, et que l'ensemble des obligations juridiques de l'exportateur de données ou de l'importateur de données n'a pas été transféré, par contrat ou par effet de la loi, à une autre entité leur ayant succédé. Cette responsabilité civile du sous-traitant ultérieur doit être limitée à ses propres activités de traitement conformément aux présentes clauses.

[...] »

41 La clause 12 de l'annexe de la décision CPT, intitulée « Obligation après la résiliation des services de traitement des données à caractère personnel », énonce, à son paragraphe 1 :

« Les parties conviennent qu'au terme des services de traitement des données, l'importateur de données et le sous-traitant ultérieur restitueront à l'exportateur de données, et à la convenance de celui-ci, l'ensemble des données à caractère personnel transférées ainsi que les copies, ou détruiront l'ensemble de ces données et en apporteront la preuve à l'exportateur de données, à moins que la législation imposée à l'importateur de données ne l'empêche de restituer ou de détruire la totalité ou une partie des données à caractère personnel transférées. [...] »

La décision BPD

42 Par arrêt du 6 octobre 2015, Schrems (C-362/14, EU:C:2015:650), la Cour a invalidé la décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46, relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (JO 2000, L 215, p. 7), dans laquelle la Commission avait constaté que ce pays tiers assurait un niveau adéquat de protection.

43 À la suite du prononcé de cet arrêt, la Commission a adopté la décision BPD, après avoir, aux fins de l'adoption de celle-ci, procédé à une évaluation de la réglementation des États-Unis, comme le précise le considérant 65 de ladite décision :

« La Commission a évalué les limitations et garanties prévues dans la législation des États-Unis en ce qui concerne l'accès aux données à caractère personnel transférées dans le cadre du bouclier de protection des données [Union européenne]-États-Unis et l'utilisation de ces données par les autorités publiques américaines à des fins de sécurité nationale, de respect de la loi ou d'intérêt public. En outre, le gouvernement américain, par l'intermédiaire de son bureau du directeur du renseignement national (Office of the Director of National Intelligence, ODNI) [...], a transmis à la Commission des observations et des engagements détaillés qui figurent à l'annexe VI de la présente décision. Par lettre signée par le secrétaire d'État américain, qui figure à l'annexe III de la présente décision, le gouvernement des États-Unis s'est également engagé à créer un nouveau mécanisme de surveillance pour les ingérences de la sécurité nationale, à savoir le médiateur du bouclier de protection des données, qui est indépendant de la communauté du renseignement. Enfin, une série d'observations du ministère de la justice américain, figurant à l'annexe VII de la présente décision, décrivent les limitations et garanties applicables à l'accès aux données et à l'utilisation de ces données par les autorités publiques aux fins de garantir le respect de la loi et à d'autres fins d'intérêt général. Afin d'accroître la transparence et de manifester la nature juridique de ces engagements, chacun des documents mentionnés et annexés à la présente décision sera publié au Journal officiel des États-Unis *(U.S. Federal Register)*. »

44 L'analyse effectuée par la Commission portant sur ces limitations et ces garanties est résumée aux considérants 67 à 135 de la décision BPD, tandis que les conclusions de cette institution portant sur le niveau adéquat de protection dans le cadre du bouclier de protection des données Union européenne-États-Unis figurent aux considérants 136 à 141 de celle-ci.

45 En particulier, les considérants 68, 69, 76, 77, 109, 112 à 116, 120, 136 et 140 de cette décision énoncent :

« (68) En vertu de la Constitution des États-Unis, il appartient au président, en tant que commandant en chef des forces armées et chef de l'exécutif, de garantir la sécurité nationale, et, en ce qui concerne le renseignement extérieur, de conduire les affaires étrangères des États-Unis [...]. Même si le Congrès a le pouvoir d'imposer certaines limitations et a déjà fait usage de ce

pouvoir à divers égards, le président peut, à l'intérieur de ces limites, diriger les activités de la communauté américaine du renseignement, notamment par des décrets présidentiels ou des directives présidentielles. [...] Actuellement les deux instruments juridiques essentiels à cet égard sont le décret présidentiel nº 12333 (*Executive Order 12333*, ci-après l'"E.O. 12333") [...] et la directive stratégique présidentielle nº 28 (*Presidential Policy directive 28*, ci-après la "PPD-28").

(69) La PPD-28, qui a été publiée le 17 janvier 2014, impose un certain nombre de limitations pour les opérations de "renseignement d'origine électromagnétique" [...]. Cette directive présidentielle a force obligatoire pour les autorités américaines de renseignement [...] et continue de produire ses effets après un changement de gouvernement américain [...]. La PPD-28 revêt une importance particulière pour les personnes qui ne sont pas américaines, y compris les personnes concernées de l'Union. [...]

[...]

(76) Même si les principes considérés [de la PPD-28] ne sont pas formulés dans un langage juridique, ils rendent l'essence des principes de nécessité et de proportionnalité. [...]

(77) Les exigences considérées, se présentant sous la forme d'une directive adoptée par le président en sa qualité de premier magistrat, sont contraignantes pour l'ensemble des services de renseignement et ont été mises en œuvre plus avant au moyen de règles et de procédures des agences qui transposent les principes généraux en orientations spécifiques pour les opérations quotidiennes. [...]

[...]

(109) Inversement, selon l'article 702 du [Foreign Intelligence Surveillance Act (FISA)], [l'United States Foreign Intelligence Surveillance Court (FISC) (tribunal de surveillance du renseignement extérieur des États-Unis)] n'autorise pas de mesures de surveillance individuelle, mais plutôt des programmes de surveillance (comme PRISM ou UPSTREAM) sur la base de certifications annuelles préparées par le [United States Attorney General (procureur général)] et le [Director of National Intelligence (DNI) (directeur du renseignement national)]. [...] Comme indiqué, les certifications qui doivent être approuvées par le FISC ne contiennent pas d'informations sur les personnes à cibler individuellement mais déterminent plutôt des catégories d'informations en matière de renseignement extérieur [...]. Même si le FISC n'évalue pas, à l'aune d'une cause ou de tout autre critère, si les personnes sont correctement ciblées pour se procurer des informations en matière de renseignement extérieur [...], son contrôle s'étend à la condition qu'"un objectif important de l'acquisition soit d'obtenir des informations en matière de renseignement extérieur" [...]

[...]

(112) Premièrement, le FISA prévoit un certain nombre de recours, également accessibles aux personnes non américaines, pour contester la surveillance électronique illégale [...]. Les personnes concernées peuvent notamment : intenter un recours civil pour demander des dommages et intérêts aux États-Unis lorsque des informations à leur sujet ont été utilisées ou divulguées illégalement et volontairement [...] ; poursuivre des fonctionnaires de l'État américain à titre personnel ("sous l'apparence du droit") pour obtenir des dommages et intérêts [...] ; et contester la légalité de la surveillance (et tenter de supprimer les informations) dans le cas où l'État américain envisagerait d'utiliser ou de divulguer toute information obtenue ou découlant de la surveillance électronique, à l'encontre de la personne visée par une procédure judiciaire ou administrative aux États-Unis [...]

(113) Deuxièmement, le gouvernement américain a communiqué à la Commission un certain nombre de voies de recours que les personnes de l'Union européenne concernées par les données à caractère personnel pourraient utiliser pour former un recours en justice contre des fonctionnaires de l'État en raison d'un accès ou d'un usage illégal de données à caractère personnel, y compris à des fins prétendues de sécurité nationale [...]

(114) Enfin, le gouvernement américain a décrit le [Freedom of information Act (FOIA) (loi sur la liberté de l'information)] comme un moyen pour les personnes non américaines de demander l'accès aux archives des organismes fédéraux, notamment lorsqu'elles contiennent les données à caractère personnel de la personne concernée [...]. Eu égard à son orientation, le FOIA ne prévoit pas de voie de recours pour des actions individuelles contre les ingérences proprement dites en matière de données à caractère personnel, même s'il pourrait en principe permettre aux personnes d'avoir accès aux informations pertinentes détenues par les agences nationales du renseignement. [...]

(115) Alors que les personnes physiques, notamment les personnes concernées de l'Union européenne, disposent donc d'un certain nombre de voies de recours lorsqu'elles ont fait l'objet d'une surveillance (électronique) illégale à des fins de sécurité nationale, il est également clair qu'au moins quelques bases juridiques pouvant être utilisées par les services de renseignement américains (comme l'E.O. 12333) ne sont pas couvertes. De plus, même lorsque des possibilités de recours juridictionnel existent en principe pour des personnes non américaines, comme par exemple pour la surveillance FISA, les moyens d'action sont limités [...] et les réclamations introduites par des personnes physiques (même américaines) seront déclarées irrecevables lorsqu'elles ne peuvent démontrer leur qualité pour agir [...], ce qui restreint l'accès aux juridictions ordinaires [...]

(116) Afin de fournir des voies de recours supplémentaires à toutes les personnes de l'Union européenne concernées, le gouvernement a décidé de créer un nouveau mécanisme de médiation tel que décrit dans la lettre adressée à la Commission par le secrétaire d'État américain, qui figure à l'annexe III de la présente décision. Ce mécanisme repose sur la désignation, au titre de la PPD-28, d'un coordinateur chevronné (niveau de sous-secrétaire) au département d'État en tant que point de contact permettant aux gouvernements étrangers d'exprimer leurs préoccupations à propos des activités américaines de renseignement d'origine électromagnétique, mais la portée de ce mécanisme est beaucoup plus vaste que le concept initial.

[...]

(120) [L]e gouvernement américain s'engage à faire en sorte que, dans l'exercice de ses fonctions, le médiateur du bouclier de protection des données soit en mesure de s'appuyer sur la coopération avec d'autres mécanismes de surveillance et de contrôle de respect du droit existant dans la législation américaine. [...] Lorsqu'un non-respect des normes est détecté par l'un de ces organismes de surveillance, la composante concernée des services de renseignement sera tenue de corriger ce manquement, car seule cette démarche permettra au médiateur de fournir une réponse "positive" (indiquant que tout manquement est donc corrigé) à la personne concernée, le gouvernement américain s'étant engagé à procéder de la sorte. [...]

[...]

(136) À la lumière de ces constatations, la Commission considère que les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées de l'Union européenne vers des organisations autocertifiées aux États-Unis dans le cadre du bouclier de protection des données [Union européenne]-États-Unis.

[...]

(140) Enfin, sur la base des informations disponibles concernant l'ordre juridique des États-Unis, y compris les observations et les engagements du gouvernement américain, la Commission considère que toute ingérence des autorités publiques américaines dans l'exercice des droits fondamentaux des personnes dont les données sont transférées de l'Union européenne vers les États-Unis dans le cadre du bouclier de protection des données pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois et, partant, les restrictions imposées aux organisations autocertifiées en ce qui concerne leur respect des principes seront limitées à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridictionnelle effective contre des ingérences de cette nature. »

46 Aux termes de l'article 1er de la décision BPD :

« 1. Aux fins de l'article 25, paragraphe 2, de la directive [95/46], les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis dans le cadre du bouclier de protection des données [Union européenne]-États-Unis.

2. Le bouclier de protection des données [Union européenne]-États-Unis se compose des principes publiés par le ministère américain du commerce le 7 juillet 2016, qui figurent à l'annexe II, et des observations et engagements officiels contenus dans les documents énumérés à l'annexe I et aux annexes III à VII.

3. Aux fins du paragraphe 1, les données à caractère personnel sont transférées dans le cadre du bouclier de protection des données [Union européenne]-États-Unis dès lors qu'elles sont transférées depuis l'Union vers des organisations établies aux États-Unis qui figurent sur la liste des organisations adhérant au bouclier de protection des données, tenue à jour et publiée par le ministère américain du commerce, conformément aux sections I et III des principes énoncés à l'annexe II. »

47 L'annexe II de la décision BPD, intitulée « Principes du cadre "bouclier de protection des données [Union européenne]-États-Unis" publiés par le ministère américain du commerce », prévoit, à son point I.5, que l'adhésion aux principes peut être limitée, notamment, par « les exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect de la législation ».

48 L'annexe III de cette décision contient une lettre de M. John Kerry, alors Secretary of State (secrétaire d'État, États-Unis), à la commissaire pour la justice, les consommateurs et l'égalité des genres, du 7 juillet 2016, à laquelle est joint, en annexe A, un mémorandum intitulé « Mécanisme de médiation du bouclier de protection des données [Union européenne]-États-Unis concernant le renseignement d'origine électromagnétique », qui contient le passage suivant :

« Eu égard à l'importance que revêt le cadre que constitue le bouclier de protection des données [Union européenne]-États-Unis, le présent mémorandum décrit la procédure de mise en œuvre d'un nouveau mécanisme, en conformité avec la PPD-28, concernant le renseignement d'origine électromagnétique.

[...] Le président Obama a annoncé l'adoption d'une nouvelle directive présidentielle, la PPD-28, en vue de "fixer clairement ce que nous faisons, et ce que nous ne faisons pas, en matière de surveillance à l'étranger".

La section 4(d) de la PPD-28 charge le secrétaire d'État de désigner un "coordinateur principal de la diplomatie internationale en matière de technologie de l'information" (le coordinateur principal) pour "servir de point de contact en ce qui concerne les activités de renseignement d'origine électromagnétique menées par les États-Unis".

[...]

1) [Le coordinateur principal] assumera les fonctions de médiateur du bouclier de protection des données et [...] travaillera en étroite collaboration avec les fonctionnaires d'autres ministères et agences chargés de traiter les demandes dans le respect de la législation et de la politique américaines en vigueur. Le médiateur est indépendant des services de renseignement. Il rend compte directement au secrétaire d'État, qui veillera à ce que le médiateur remplisse sa mission en toute objectivité et à l'abri de toute influence inappropriée susceptible d'affecter la réponse qu'il devra donner.

[...] »

49 L'annexe VI de la décision BPD contient une lettre du bureau du directeur du renseignement national (Office of the Director of National Intelligence) au ministère américain du Commerce ainsi qu'à l'administration du commerce international, du 21 juin 2016, dans laquelle il est précisé que la PPD-28 permet de procéder à une « collecte "en vrac" [...] d'un volume relativement important d'informations ou de données issues du renseignement d'origine électromagnétique dans des conditions où les services de renseignement ne peuvent pas utiliser d'identifiant associé à une cible spécifique [...] pour orienter la collecte ».

Le litige au principal et les questions préjudicielles

50 M. Schrems, ressortissant autrichien résidant en Autriche, est un utilisateur du réseau social Facebook (ci-après « Facebook ») depuis l'année 2008.

51 Toute personne résidant sur le territoire de l'Union et désirant utiliser Facebook est tenue de conclure, lors de son inscription, un contrat avec Facebook Ireland, filiale de Facebook Inc., elle-même établie aux États-Unis. Les données à caractère personnel des utilisateurs de Facebook résidant sur le territoire de l'Union sont, en tout ou en partie, transférées vers des serveurs appartenant à Facebook Inc., situés sur le territoire des États-Unis, où elles font l'objet d'un traitement.

52 Le 25 juin 2013, M. Schrems a saisi le commissaire d'une plainte par laquelle il demandait, en substance, à celui-ci d'interdire à Facebook Ireland de transférer ses données à caractère personnel vers les États-Unis, en faisant valoir que le droit et les pratiques en vigueur dans ce pays ne garantissaient pas une protection suffisante des données à caractère personnel conservées sur le territoire de celui-ci contre les activités de surveillance qui y étaient pratiquées par les autorités publiques. Cette plainte a été rejetée, au motif, notamment, que la Commission avait constaté, dans sa décision 2000/520, que les États-Unis assuraient un niveau adéquat de protection.

53 La High Court (Haute Cour, Irlande), devant laquelle M. Schrems avait introduit un recours contre le rejet de sa plainte, a saisi la Cour d'une demande de décision préjudicielle portant sur l'interprétation et la validité de la décision 2000/520. Par arrêt du 6 octobre 2015, Schrems (C-362/14, EU:C:2015:650), la Cour a déclaré invalide cette décision.

54 À la suite de cet arrêt, la juridiction de renvoi a annulé le rejet de la plainte de M. Schrems et a renvoyé celle-ci au commissaire. Dans le cadre de l'enquête ouverte par ce dernier, Facebook Ireland a expliqué qu'une grande partie des données à caractère personnel était transférée à Facebook Inc. sur le fondement des clauses types de protection des données figurant à l'annexe de la décision CPT. Compte tenu de ces éléments, le commissaire a invité M. Schrems à reformuler sa plainte.

55 Dans sa plainte ainsi reformulée, présentée le 1er décembre 2015, M. Schrems a fait valoir, notamment, que le droit américain impose à Facebook Inc. de mettre les données à caractère personnel qui lui sont transférées à la disposition des autorités américaines, telles que la National Security Agency (NSA) et le

Federal Bureau of Investigation (FBI). Il a soutenu que, ces données étant utilisées dans le cadre de différents programmes de surveillance d'une manière incompatible avec les articles 7, 8 et 47 de la Charte, la décision CPT ne peut justifier le transfert desdites données vers les États-Unis. Dans ces conditions, M. Schrems a demandé au commissaire d'interdire ou de suspendre le transfert de ses données à caractère personnel vers Facebook Inc.

56 Le 24 mai 2016, le commissaire a publié un « projet de décision » résumant les conclusions provisoires de son enquête. Dans ce projet, il a considéré provisoirement que les données à caractère personnel des citoyens de l'Union transférées vers les États-Unis risquent d'être consultées et traitées par les autorités américaines d'une manière incompatible avec les articles 7 et 8 de la Charte et que le droit des États-Unis n'offre pas à ces citoyens des voies de recours compatibles avec l'article 47 de la Charte. Le commissaire a estimé que les clauses types de protection des données figurant à l'annexe de la décision CPT ne sont pas de nature à remédier à ce défaut, dans la mesure où elles confèrent aux personnes concernées uniquement des droits contractuels contre l'exportateur et l'importateur des données, sans toutefois lier les autorités américaines.

57 Étant d'avis que, dans ces conditions, la plainte reformulée de M. Schrems soulevait la question de la validité de la décision CPT, le commissaire a, le 31 mai 2016, saisi la High Court (Haute Cour), en s'appuyant sur la jurisprudence issue de l'arrêt du 6 octobre 2015, Schrems (C-362/14, EU:C:2015:650, point 65), aux fins que cette dernière interroge la Cour sur cette question. Par décision du 4 mai 2018, la High Court (Haute Cour) a saisi la Cour du présent renvoi préjudiciel.

58 La High Court (Haute Cour) a annexé à ce renvoi préjudiciel un arrêt prononcé le 3 octobre 2017, dans lequel elle avait consigné le résultat de l'examen des preuves produites devant elle dans le cadre de la procédure nationale, procédure à laquelle avait participé le gouvernement américain.

59 Dans cet arrêt, auquel la demande de décision préjudicielle se réfère à plusieurs reprises, la juridiction de renvoi a relevé que, par principe, elle a non seulement le droit mais également l'obligation d'examiner l'ensemble des faits et des arguments invoqués devant elle afin de décider, sur la base de ceux-ci, si un renvoi préjudiciel est requis ou non. En tout état de cause, elle serait tenue de prendre en compte les éventuelles modifications du droit intervenant entre l'introduction du recours et l'audience organisée devant elle. Cette juridiction a précisé que, dans le cadre de la procédure au principal, sa propre appréciation n'est pas limitée aux moyens d'invalidité avancés par le commissaire, si bien qu'elle peut également relever d'office d'autres moyens d'invalidité et, sur la base de ceux-ci, procéder à un renvoi préjudiciel.

60 Selon les constatations figurant dans ledit arrêt, les activités de renseignement des autorités américaines en ce qui concerne les données à caractère personnel transférées vers les États-Unis se fondent, notamment, sur l'article 702 du FISA et sur l'E.O. 12333.

61 S'agissant de l'article 702 du FISA, la juridiction de renvoi précise, dans le même arrêt, que cet article permet au procureur général et au directeur du renseignement national d'autoriser conjointement, après approbation du FISC, aux fins de se procurer des « informations en matière de renseignement extérieur », la surveillance de ressortissants non américains se trouvant en dehors du territoire des États-Unis et sert, notamment, de fondement aux programmes de surveillance PRISM et UPSTREAM. Dans le cadre du programme PRISM, les fournisseurs de services Internet sont tenus, selon les constatations de cette juridiction, de fournir à la NSA toutes les communications envoyées et reçues par un « sélecteur », une partie d'entre elles étant également transmise au FBI et à la Central Intelligence Agency (CIA) (agence centrale de renseignement).

62 S'agissant du programme UPSTREAM, ladite juridiction a constaté que, dans le cadre de ce programme, les entreprises de télécommunications exploitant la « dorsale » de l'internet – c'est-à-dire le réseau de câbles, commutateurs et routeurs – sont contraintes de permettre à la NSA de copier et de filtrer les flux de trafic Internet afin de recueillir des communications envoyées par ou reçues par ou

concernant le ressortissant non américain visé par un « sélecteur ». Dans le cadre dudit programme, la NSA a, selon les constatations de cette même juridiction, accès tant aux métadonnées qu'au contenu des communications concernées.

63 En ce qui concerne l'E.O. 12333, la juridiction de renvoi constate que celui-ci permet à la NSA d'accéder à des données « en transit » vers les États-Unis, en accédant aux câbles sous-marins posés sur le plancher de l'Atlantique, ainsi que de recueillir et de conserver ces données avant qu'elles arrivent aux États-Unis et y soient soumises aux dispositions du FISA. Elle précise que les activités fondées sur l'E.O. 12333 ne sont pas régies par la loi.

64 S'agissant des limites apportées aux activités de renseignement, la juridiction de renvoi met l'accent sur le fait que les personnes non américaines relèvent uniquement de la PPD-28 et que celle-ci se borne à indiquer que les activités de renseignement devraient être « aussi ciblées que possible » *(as tailored as feasible)*. Sur la base de ses constatations, ladite juridiction considère que les États-Unis procèdent à un traitement de données en masse, sans assurer une protection substantiellement équivalente à celle garantie par les articles 7 et 8 de la Charte.

65 Quant à la protection juridictionnelle, cette même juridiction expose que les citoyens de l'Union n'ont pas accès aux mêmes recours que ceux dont disposent les ressortissants américains contre les traitements de données à caractère personnel par les autorités américaines, dès lors que le quatrième amendement de la Constitution of the United States (Constitution des États-Unis), qui constitue, en droit américain, la protection la plus importante contre la surveillance illégale, est inapplicable aux citoyens de l'Union. À cet égard, la juridiction de renvoi précise que les recours restant à la disposition de ces derniers se heurtent à des obstacles importants, en particulier à l'obligation – selon elle excessivement difficile à satisfaire – de justifier de leur qualité pour agir. Par ailleurs, selon les constatations de cette juridiction, les activités de la NSA fondées sur l'E.O. 12333 ne font pas l'objet d'une surveillance judiciaire et ne sont pas susceptibles de recours juridictionnels. Enfin, ladite juridiction estime que, dans la mesure où, selon elle, le médiateur du bouclier de protection de données ne constitue pas un tribunal, au sens de l'article 47 de la Charte, le droit américain n'assure pas aux citoyens de l'Union un niveau de protection substantiellement équivalent à celui garanti par le droit fondamental consacré à cet article.

66 Dans sa demande de décision préjudicielle, la juridiction de renvoi précise encore que les parties à la procédure au principal s'opposent, notamment, sur la question de l'applicabilité du droit de l'Union à des transferts, vers un pays tiers, de données à caractère personnel qui sont susceptibles d'être traitées par les autorités de ce pays notamment à des fins de sécurité nationale ainsi que sur les éléments à prendre en considération aux fins de l'appréciation du niveau de protection adéquat assuré par ledit pays. En particulier, cette juridiction relève que, selon Facebook Ireland, les constatations de la Commission portant sur le caractère adéquat du niveau de protection assuré par un pays tiers, telles que celles figurant dans la décision BPD, lient les autorités de contrôle également dans le contexte d'un transfert de données à caractère personnel fondé sur les clauses types de protection des données figurant à l'annexe de la décision CPT.

67 En ce qui concerne ces clauses types de protection des données, ladite juridiction se demande si la décision CPT peut être considérée comme valide, alors même que, selon cette même juridiction, lesdites clauses sont dépourvues de caractère contraignant à l'égard des autorités étatiques du pays tiers concerné et, partant, ne sont pas de nature à remédier à une éventuelle absence de niveau de protection adéquat dans ce pays. À cet égard, elle estime que la possibilité, reconnue aux autorités compétentes des États membres, par l'article 4, paragraphe 1, sous a), de la décision 2010/87, dans sa version antérieure à l'entrée en vigueur de la décision d'exécution 2016/2297, d'interdire les transferts de données à caractère personnel vers un pays tiers imposant à l'importateur des obligations incompatibles avec les garanties contenues dans ces mêmes clauses, démontre que l'état du droit du pays tiers peut justifier l'interdiction d'un transfert de données, même effectué sur le fondement des clauses types de protection des données figurant à l'annexe de la décision CPT, et, partant, met en

évidence que celles-ci peuvent être insuffisantes pour assurer une protection adéquate. Cela étant, la juridiction de renvoi s'interroge sur l'étendue du pouvoir du commissaire d'interdire un transfert de données fondé sur ces clauses, tout en estimant qu'un pouvoir discrétionnaire ne saurait suffire pour assurer une protection adéquate.

68 C'est dans ces conditions que la High Court (Haute Cour) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) Lorsque des données à caractère personnel sont transférées, à des fins commerciales, par une société privée d'un État membre de l'[Union] à une société privée dans un pays tiers conformément à la décision [CPT] et sont susceptibles d'être ensuite traitées par les autorités du pays tiers à des fins de sécurité nationale mais également de maintien de l'ordre public et de conduite des affaires étrangères du pays tiers, le droit de l'Union, y compris la Charte, est-il applicable au transfert des données, nonobstant les dispositions de l'article 4, paragraphe 2, TUE relatives à la sécurité nationale et les dispositions du premier tiret de l'article 3, paragraphe 2, de la directive [95/46] relatives à la sécurité publique, la défense et la sûreté de l'État ?

2) a) Pour déterminer si le transfert de données, conformément à la décision [CPT], de l'[Union] vers un pays tiers où ces données sont susceptibles d'être ensuite traitées à des fins de sécurité nationale viole les droits d'un particulier, l'instrument de comparaison pertinent aux fins de la directive [95/46] est-il :
   i) la Charte, le traité UE, le traité FUE, la directive [95/46], la [convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950,] (ou toute autre disposition du droit de l'[Union]) ; ou
   ii) la législation interne d'un ou de plusieurs États membres ?
   b) Si l'instrument de comparaison pertinent est ii), les pratiques en matière de sécurité nationale dans un ou plusieurs États membres doivent-elles également être incluses dans l'instrument de comparaison ?

3) Pour évaluer si un pays tiers garantit aux données à caractère personnel qui y sont transférées le niveau de protection requis par le droit de l'Union aux fins de l'article 26 de la directive [95/46] convient-il de se référer :
   a) aux règles applicables dans le pays tiers résultant de son droit interne ou de ses engagements internationaux, et à la pratique visant à assurer le respect de ces règles, y compris les règles professionnelles et les mesures de sécurité qui sont observées dans le pays tiers ;

   ou

   b) aux règles mentionnées sous a), auxquelles s'ajoutent les pratiques administratives, réglementaires et de conformité ainsi que les garanties, procédures, protocoles, mécanismes de surveillance et recours extrajudiciaires tels qu'ils existent dans le pays tiers ?

4) Compte tenu des faits établis par la High Court [(Haute Cour)] concernant le droit des États-Unis, le transfert des données à caractère personnel de l'[Union] vers les États-Unis conformément à la décision [CPT] viole-t-il les droits des particuliers protégés par les articles 7 ou 8 de la Charte ?

5) Compte tenu des faits établis par la High Court [(Haute Cour)] concernant le droit des États-Unis, si des données à caractère personnel sont transférées de l'[Union] vers les États-Unis conformément à la décision [CPT] :
   a) Le niveau de protection accordé par les États-Unis respecte-t-il le contenu essentiel du droit d'un particulier à un recours juridictionnel pour violation de ses droits à la confidentialité des données garanti par l'article 47 de la Charte ?

En cas de réponse affirmative à la cinquième question, sous a) :

b) Les limitations imposées par le droit des États-Unis au droit d'un particulier à un recours juridictionnel sont-elles, dans le contexte de la sécurité nationale des États-Unis, proportionnées au sens de l'article 52 de la Charte et n'excèdent-elles pas ce qui est nécessaire à des fins de sécurité nationale dans une société démocratique ?

6) a) À la lumière des dispositions de la directive [95/46] et en particulier des articles 25 et 26 lus à la lumière de la Charte, quel est le niveau de protection requis à accorder aux données à caractère personnel transférées dans un pays tiers en vertu de clauses contractuelles types adoptées conformément à une décision de la Commission au titre de l'article 26, paragraphe 4, [de la directive 95/46] ?

b) Quels sont les aspects à prendre en compte pour évaluer si le niveau de protection accordé aux données transférées dans un pays tiers conformément à la décision [CPT] satisfait aux exigences de la directive [95/46] et de la Charte ?

7) Le fait que les clauses types de protection s'appliquent entre l'exportateur et l'importateur de données et ne lient pas les autorités nationales d'un pays tiers qui peuvent exiger de l'importateur qu'il mette à la disposition de ses services de sécurité, pour traitement ultérieur, les données à caractère personnel transférées conformément aux clauses prévues dans la décision [CPT], exclut-il que ces clauses offrent des garanties suffisantes telles qu'envisagées à l'article 26, paragraphe 2, de la directive [95/46] ?

8) Si un importateur de données d'un pays tiers est soumis à des règles de surveillance qui, du point de vue d'une autorité en charge de la protection des données, enfreignent les clauses types de protection ou les articles 25 et 26 de la directive [95/46] ou la Charte, une autorité en charge de la protection des données est-elle tenue de faire usage de ses pouvoirs d'exécution au titre de l'article 28, paragraphe 3, de la directive [95/46] afin de suspendre les flux de données, ou l'exercice de ces pouvoirs est-il limité aux seuls cas exceptionnels, à la lumière du considérant 11 de la décision [CPT], ou bien une autorité en charge de la protection des données peut-elle exercer son pouvoir discrétionnaire pour ne pas suspendre les flux de données ?

9) a) Aux fins de l'article 25, paragraphe 6, de la directive [95/46], la décision [BPD] constitue-t-elle une constatation d'application générale liant les autorités en charge de la protection des données et les juridictions des États membres, selon laquelle les États-Unis assurent un niveau de protection adéquat au sens de l'article 25, paragraphe 2, de la directive [95/46] en raison de leur droit interne ou de leurs engagements internationaux ?

b) Si tel n'est pas le cas, quelle est la pertinence, le cas échéant, de la décision [BPD] pour l'appréciation du caractère suffisant des garanties offertes aux données transférées aux États-Unis conformément à la décision [CPT] ?

10) Compte tenu des conclusions de la High Court [(Haute Cour)] en ce qui concerne le droit des États-Unis, la mise en place du médiateur "bouclier de protection des données" conformément à l'annexe A de l'annexe III de la décision [BPD], en combinaison avec le régime existant aux États-Unis, garantit-elle que les États-Unis offrent un recours compatible avec l'article 47 de la Charte aux personnes dont les données à caractère personnel sont transférées aux États-Unis conformément à la décision [CPT] ?

11) La décision [CPT] viole-t-elle les articles 7, 8 ou 47 de la Charte ? »

Sur la recevabilité de la demande de décision préjudicielle

69 Facebook Ireland ainsi que les gouvernements allemand et du Royaume-Uni font valoir que la demande de décision préjudicielle est irrecevable.

70 S'agissant de l'exception soulevée par Facebook Ireland, cette société fait observer que les dispositions de la directive 95/46 sur lesquelles sont fondées les questions préjudicielles ont été abrogées par le RGPD.

71 À cet égard, s'il est vrai que la directive 95/46 a été, en vertu de l'article 94, paragraphe 1, du RGPD, abrogée avec effet au 25 mai 2018, cette directive était encore en vigueur lors de la formulation, le 4 mai 2018, de la présente demande de décision préjudicielle parvenue à la Cour le 9 mai 2018. En outre, l'article 3, paragraphe 2, premier tiret, les articles 25 et 26 ainsi que l'article 28, paragraphe 3, de la directive 95/46, auxquels se réfèrent les questions préjudicielles, ont été en substance repris, respectivement, à l'article 2, paragraphe 2, ainsi qu'aux articles 45, 46 et 58 du RGPD. Par ailleurs, il y a lieu de rappeler que la Cour a pour mission d'interpréter toutes les dispositions du droit de l'Union dont les juridictions nationales ont besoin afin de statuer sur les litiges qui leur sont soumis, même si ces dispositions ne sont pas indiquées expressément dans les questions qui lui sont adressées par ces juridictions (arrêt du 2 avril 2020, Ruska Federacija, C-897/19 PPU, EU:C:2020:262, point 43 et jurisprudence citée). Pour ces différents motifs, la circonstance que la juridiction de renvoi a formulé les questions préjudicielles en se référant uniquement aux dispositions de la directive 95/46 ne saurait entraîner l'irrecevabilité de la présente demande de décision préjudicielle.

72 De son côté, le gouvernement allemand fonde son exception d'irrecevabilité sur la circonstance, d'une part, que le commissaire n'a exposé que des doutes, et non une opinion définitive, quant à la question de la validité de la décision CPT et, d'autre part, que la juridiction de renvoi s'est abstenue de vérifier si M. Schrems avait indubitablement donné son consentement aux transferts de données en cause au principal, ce qui, si tel avait été le cas, aurait pour effet de rendre inutile une réponse à cette question. Enfin, selon le gouvernement du Royaume-Uni, les questions préjudicielles ont un caractère hypothétique dès lors que cette juridiction n'a pas constaté que ces données avaient effectivement été transférées sur le fondement de ladite décision.

73 Il résulte de la jurisprudence constante de la Cour qu'il appartient au seul juge national, qui est saisi du litige et qui doit assumer la responsabilité de la décision juridictionnelle à intervenir, d'apprécier, au regard des particularités de l'affaire, tant la nécessité d'une décision préjudicielle pour être en mesure de rendre son jugement que la pertinence des questions qu'il pose à la Cour. En conséquence, dès lors que les questions posées portent sur l'interprétation ou la validité d'une règle du droit de l'Union, la Cour est, en principe, tenue de statuer. Il s'ensuit que les questions posées par les juridictions nationales bénéficient d'une présomption de pertinence. Le refus de la Cour de statuer sur une question préjudicielle posée par une juridiction nationale n'est possible que s'il apparaît que l'interprétation sollicitée n'a aucun rapport avec la réalité ou l'objet du litige au principal, si le problème est de nature hypothétique ou encore si la Cour ne dispose pas des éléments de fait et de droit nécessaires pour répondre de façon utile auxdites questions (arrêts du 16 juin 2015, Gauweiler e.a., C-62/14, EU:C:2015:400, points 24 et 25 ; du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 45, ainsi que du 19 décembre 2019, Dobersberger, C-16/18, EU:C:2019:1110, points 18 et 19).

74 En l'occurrence, la demande de décision préjudicielle contient des éléments de fait et de droit suffisants pour comprendre la portée des questions préjudicielles. En outre et surtout, aucun élément du dossier dont dispose la Cour ne permet de considérer que l'interprétation sollicitée du droit de l'Union n'aurait pas de rapport avec la réalité ou l'objet du litige au principal ou serait de nature hypothétique, notamment en raison du fait que le transfert des données à caractère personnel en cause au principal serait fondé sur le consentement explicite de la personne concernée à ce transfert, et non sur la décision CPT. En effet, selon les indications figurant dans cette demande, Facebook Ireland a reconnu qu'elle transfère à Facebook Inc. les données à caractère personnel de ses abonnés résidant dans l'Union et qu'une grande partie de ces transferts, dont M. Schrems conteste la licéité, est effectuée sur le fondement des clauses types de protection des données figurant à l'annexe de la décision CPT.

75 Par ailleurs, il est sans incidence sur la recevabilité de la présente demande de décision préjudicielle que le commissaire n'ait pas exprimé d'opinion définitive concernant la validité de cette décision, dès lors que la juridiction de renvoi considère que la réponse aux questions préjudicielles portant sur l'interprétation et la validité de règles du droit de l'Union est nécessaire à la solution du litige au principal.

76 Il s'ensuit que la demande de décision préjudicielle est recevable.

Sur les questions préjudicielles

77 À titre liminaire, il y a lieu de rappeler que la présente demande de décision préjudicielle trouve son origine dans une plainte de M. Schrems visant à ce que le commissaire ordonne la suspension ou l'interdiction, pour l'avenir, du transfert par Facebook Ireland de ses données à caractère personnel vers Facebook Inc. Or, alors que les questions préjudicielles se réfèrent aux dispositions de la directive 95/46, il est constant que le commissaire n'avait pas encore adopté de décision finale sur cette plainte lorsque cette directive a été abrogée et remplacée par le RGPD, avec effet au 25 mai 2018.

78 Cette absence de décision nationale distingue la situation en cause au principal de celles ayant conduit aux arrêts du 24 septembre 2019, Google (Portée territoriale du déréférencement) (C-507/17, EU:C:2019:772), et du 1er octobre 2019, Planet49 (C-673/17, EU:C:2019:801), dans lesquelles étaient en cause des décisions adoptées antérieurement à l'abrogation de ladite directive.

79 Dès lors, il y a lieu de répondre aux questions préjudicielles au regard des dispositions du RGPD, et non de celles de la directive 95/46.

Sur la première question

80 Par sa première question, la juridiction de renvoi cherche, en substance, à savoir si l'article 2, paragraphe 1, et l'article 2, paragraphe 2, sous a), b) et d), du RGPD, lus en combinaison avec l'article 4, paragraphe 2, TUE, doivent être interprétés en ce sens que relève du champ d'application de ce règlement un transfert de données à caractère personnel effectué par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, lorsque, au cours ou à la suite de ce transfert, ces données sont susceptibles d'être traitées par les autorités de ce pays tiers à des fins de sécurité publique, de défense et de sûreté de l'État.

81 À cet égard, il convient de relever d'emblée que la disposition contenue à l'article 4, paragraphe 2, TUE, selon laquelle, au sein de l'Union, la sécurité nationale reste de la seule responsabilité de chaque État membre, concerne exclusivement les États membres de l'Union. Par conséquent, cette disposition n'est pas pertinente, en l'occurrence, pour interpréter l'article 2, paragraphe 1, et l'article 2, paragraphe 2, sous a), b) et d), du RGPD.

82 Aux termes de son article 2, paragraphe 1, le RGPD s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. L'article 4, point 2, de ce règlement définit la notion de « traitement » comme visant « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel » et cite, à titre d'exemples, « la communication par transmission, la diffusion ou toute autre forme de mise à disposition », sans distinguer selon que ces opérations sont réalisées à l'intérieur de l'Union ou présentent un lien avec un pays tiers. En outre, ledit règlement soumet les transferts de données à caractère personnel vers des pays tiers à des règles particulières figurant dans son chapitre V, intitulé « Transferts de données à caractère personnel vers

des pays tiers ou à des organisations internationales », et confère, par ailleurs, aux autorités de contrôle des pouvoirs spécifiques à cet effet, figurant à l'article 58, paragraphe 2, sous j), du même règlement.

83 Il s'ensuit que l'opération consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers constitue, en tant que telle, un traitement de données à caractère personnel, au sens de l'article 4, point 2, du RGPD, effectué sur le territoire d'un État membre, traitement auquel ce règlement s'applique en vertu de son article 2, paragraphe 1 [voir par analogie, en ce qui concerne l'article 2, sous b), et l'article 3, paragraphe 1, de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 45 et jurisprudence citée].

84 En ce qui concerne la question de savoir si une telle opération peut être considérée comme étant exclue du champ d'application du RGPD en vertu de l'article 2, paragraphe 2, de celui-ci, il convient de rappeler que cette disposition prévoit des exceptions au champ d'application de ce règlement, tel que défini à son article 2, paragraphe 1, et que ces exceptions doivent recevoir une interprétation stricte (voir par analogie, en ce qui concerne l'article 3, paragraphe 2, de la directive 95/46, arrêt du 10 juillet 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, point 37 et jurisprudence citée).

85 En l'occurrence, le transfert de données à caractère personnel en cause au principal étant effectué par Facebook Ireland vers Facebook Inc., à savoir entre deux personnes morales, ce transfert ne relève pas de l'article 2, paragraphe 2, sous c), du RGPD, qui vise le traitement de données effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique. Ledit transfert ne relève pas non plus des exceptions figurant à l'article 2, paragraphe 2, sous a), b) et d), de ce règlement, dès lors que les activités qui y sont mentionnées à titre d'exemples sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers (voir par analogie, en ce qui concerne l'article 3, paragraphe 2, de la directive 95/46, arrêt du 10 juillet 2018, Jehovan todistajat, C-25/17, EU:C:2018:551, point 38 et jurisprudence citée).

86 Or, la possibilité que les données à caractère personnel transférées entre deux opérateurs économiques à des fins commerciales subissent, au cours ou à la suite du transfert, un traitement à des fins de sécurité publique, de défense et de sûreté de l'État par les autorités du pays tiers concerné ne saurait exclure ledit transfert du champ d'application du RGPD.

87 D'ailleurs, en faisant explicitement obligation à la Commission, lorsqu'elle évalue le caractère adéquat du niveau de protection offert par un pays tiers, de tenir compte, notamment, de « 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 la mise en œuvre de ladite législation », le libellé même de l'article 45, paragraphe 2, sous a), de ce règlement met en évidence le fait que le traitement éventuel, par un pays tiers, des données concernées à des fins de sécurité publique, de défense et de sûreté de l'État ne remet pas en cause l'applicabilité dudit règlement au transfert en cause.

88 Il s'ensuit qu'un tel transfert ne saurait échapper au champ d'application du RGPD au motif que les données en cause sont susceptibles d'être traitées, au cours ou à la suite de ce transfert, par les autorités du pays tiers concerné, à des fins de sécurité publique, de défense et de sûreté de l'État.

89 Partant, il y a lieu de répondre à la première question que l'article 2, paragraphes 1 et 2, du RGPD doit être interprété en ce sens que relève du champ d'application de ce règlement un transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, nonobstant le fait que, au cours ou à la suite de ce transfert, ces données sont susceptibles d'être traitées par les autorités du pays tiers concerné à des fins de sécurité publique, de défense et de sûreté de l'État.

Sur les deuxième, troisième et sixième questions

90 Par ses deuxième, troisième et sixième questions, la juridiction de renvoi interroge la Cour, en substance, sur le niveau de protection requis à l'article 46, paragraphe 1, et à l'article 46, paragraphe 2, sous c), du RGPD dans le cadre d'un transfert de données à caractère personnel vers un pays tiers fondé sur des clauses types de protection des données. En particulier, cette juridiction demande à la Cour de préciser les éléments à prendre en considération aux fins de déterminer si ce niveau de protection est assuré dans le contexte d'un tel transfert.

91 En ce qui concerne le niveau de protection requis, il résulte d'une lecture combinée de ces dispositions que, en l'absence de décision d'adéquation adoptée au titre de l'article 45, paragraphe 3, de ce règlement, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers que s'il a prévu des « garanties appropriées » et à la condition que les personnes concernées disposent « de droits opposables et de voies de droit effectives », ces garanties appropriées pouvant être fournies, notamment, par des clauses types de protection des données adoptées par la Commission.

92 Si l'article 46 du RGPD ne précise pas la nature des exigences qui découlent de cette référence aux « garanties appropriées », aux « droits opposables » et aux « voies de droit effectives », il y a lieu de relever que cet article figure dans le chapitre V de ce règlement et, partant, doit être lu à la lumière de l'article 44 dudit règlement, intitulé « Principe général applicable aux transferts », qui dispose que « [t]outes les dispositions [de ce chapitre] sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par [le même] règlement ne soit pas compromis ». Ce niveau de protection doit, par conséquent, être garanti quelle que soit la disposition dudit chapitre sur le fondement de laquelle est effectué un transfert de données à caractère personnel vers un pays tiers.

93 En effet, comme l'a relevé M. l'avocat général au point 117 de ses conclusions, les dispositions du chapitre V du RGPD visent à assurer la continuité du niveau élevé de cette protection en cas de transfert de données à caractère personnel vers un pays tiers, conformément à l'objectif précisé au considérant 6 de ce règlement.

94 L'article 45, paragraphe 1, première phrase, du RGPD prévoit qu'un transfert de données à caractère personnel vers un pays tiers peut être autorisé au moyen d'une décision prise par la Commission selon laquelle ce pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans celui-ci, assure un niveau de protection adéquat. À cet égard, sans exiger que le pays tiers concerné garantisse un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union, l'expression « niveau de protection adéquat » doit être comprise, ainsi que le confirme le considérant 104 de ce règlement, comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu dudit règlement, lu à la lumière de la Charte. En effet, à défaut d'une telle exigence, l'objectif mentionné au point précédent serait méconnu (voir par analogie, en ce qui concerne l'article 25, paragraphe 6, de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 73).

95 Dans ce contexte, le considérant 107 du RGPD énonce que, lorsqu'« un pays tiers, un territoire ou un secteur déterminé dans un pays tiers [...], n'assure plus un niveau adéquat de protection des données [...], le transfert de données à caractère personnel vers ce pays tiers [...] devrait être interdit, à moins que les exigences [de ce règlement] relatives aux transferts faisant l'objet de garanties appropriées [...] soient respectées ». À cet effet, le considérant 108 dudit règlement précise que, en l'absence de décision d'adéquation, les garanties appropriées qu'il appartient au responsable du traitement ou au sous-traitant de prendre conformément à l'article 46, paragraphe 1, du même règlement doivent « compenser l'insuffisance de la protection des données dans le pays tiers » pour « assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée au traitement au sein de l'Union ».

96 Il en résulte, comme M. l'avocat général l'a relevé au point 115 de ses conclusions, que ces garanties appropriées doivent être de nature à assurer que les personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient, comme dans le cadre d'un transfert fondé sur une décision d'adéquation, d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union.

97 La juridiction de renvoi s'interroge également sur le point de savoir si ce niveau de protection substantiellement équivalent à celui garanti au sein de l'Union doit être déterminé au regard du droit de l'Union, notamment des droits garantis par la Charte, et/ou au regard des droits fondamentaux consacrés par la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la « CEDH ») ou encore au regard du droit national des États membres.

98 À cet égard, il convient de rappeler que si, comme le confirme l'article 6, paragraphe 3, TUE, les droits fondamentaux consacrés par la CEDH font partie du droit de l'Union en tant que principes généraux et si l'article 52, paragraphe 3, de la Charte dispose que les droits contenus dans celle-ci correspondant à des droits garantis par la CEDH ont le même sens et la même portée que ceux que leur confère ladite convention, cette dernière ne constitue pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement intégré à l'ordre juridique de l'Union (arrêts du 26 février 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, point 44 et jurisprudence citée, ainsi que du 20 mars 2018, Menci, C-524/15, EU:C:2018:197, point 22).

99 Dans ces conditions, la Cour a jugé que l'interprétation du droit de l'Union ainsi que l'examen de la validité des actes de l'Union doivent être opérés au regard des droits fondamentaux garantis par la Charte (voir, par analogie, arrêt du 20 mars 2018, Menci, C-524/15, EU:C:2018:197, point 24).

100 Par ailleurs, il est de jurisprudence constante que la validité des dispositions du droit de l'Union et, en l'absence d'un renvoi exprès au droit national des États membres, leur interprétation ne sauraient être appréciées au regard de ce droit national, même de rang constitutionnel, en particulier, des droits fondamentaux tels que formulés dans leur constitution nationale (voir, en ce sens, arrêts du 17 décembre 1970, Internationale Handelsgesellschaft, 11/70, EU:C:1970:114, point 3 ; du 13 décembre 1979, Hauer, 44/79, EU:C:1979:290, point 14, ainsi que du 18 octobre 2016, Nikiforidis, C-135/15, EU:C:2016:774, point 28 et jurisprudence citée).

101 Il s'ensuit que, dès lors que, d'une part, un transfert de données à caractère personnel, tel que celui en cause au principal, effectué à des fins commerciales par un opérateur économique établi dans un État membre, à destination d'un autre opérateur économique établi dans un pays tiers, relève, ainsi qu'il ressort de la réponse à la première question, du champ d'application du RGPD et que, d'autre part, ce règlement vise notamment, ainsi qu'il ressort de son considérant 10, à assurer un niveau cohérent et élevé de protection des personnes physiques au sein de l'Union et, à cette fin, à assurer une application cohérente et homogène des règles de protection des libertés et des droits fondamentaux de ces personnes à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union, le niveau de protection des droits fondamentaux requis à l'article 46, paragraphe 1, dudit règlement doit être déterminé sur le fondement des dispositions du même règlement, lues à la lumière des droits fondamentaux garantis par la Charte.

102 La juridiction de renvoi cherche encore à savoir quels éléments il convient de prendre en considération aux fins de déterminer le caractère adéquat du niveau de protection dans le contexte d'un transfert de données à caractère personnel vers un pays tiers sur le fondement de clauses types de protection des données adoptées au titre de l'article 46, paragraphe 2, sous c), du RGPD.

103 À cet égard, si cette disposition n'énumère pas les différents éléments dont il y a lieu de tenir compte aux fins d'évaluer le caractère adéquat du niveau de protection à respecter dans le cadre d'un tel transfert, l'article 46, paragraphe 1, de ce règlement précise que les personnes concernées doivent bénéficier de garanties appropriées et disposer de droits opposables et de voies de droit effectives.

104 L'évaluation requise, à cet effet, dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel transférées, les éléments pertinents du système juridique de celui-ci. À ce dernier égard, les éléments qu'il convient de prendre en considération dans le contexte de l'article 46 dudit règlement correspondent à ceux énoncés, de manière non exhaustive, à l'article 45, paragraphe 2, de celui-ci.

105 Partant, il y a lieu de répondre aux deuxième, troisième et sixième questions que l'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du RGPD doivent être interprétés en ce sens que les garanties appropriées, les droits opposables et les voies de droit effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union par ce règlement, lu à la lumière de la Charte. À cet effet, l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci, notamment ceux énoncés à l'article 45, paragraphe 2, dudit règlement.

Sur la huitième question

106 Par sa huitième question, la juridiction de renvoi cherche, en substance, à savoir si l'article 58, paragraphe 2, sous f) et j), du RGPD doit être interprété en ce sens que l'autorité de contrôle compétente est tenue de suspendre ou d'interdire un transfert de données à caractère personnel vers un pays tiers fondé sur des clauses types de protection des données adoptées par la Commission, lorsque cette autorité de contrôle estime que ces clauses ne sont pas ou ne peuvent pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union, en particulier par les articles 45 et 46 du RGPD ainsi que par la Charte, ne peut pas être assurée, ou en ce sens que l'exercice de ces pouvoirs est limité à des hypothèses exceptionnelles.

107 Conformément à l'article 8, paragraphe 3, de la Charte ainsi qu'à l'article 51, paragraphe 1, et à l'article 57, paragraphe 1, sous a), du RGPD, les autorités nationales de contrôle sont chargées de contrôler le respect des règles de l'Union relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Dès lors, chacune d'entre elles est investie de la compétence de vérifier si un transfert de données à caractère personnel depuis l'État membre dont elle relève vers un pays tiers respecte les exigences posées par ce règlement (voir par analogie, en ce qui concerne l'article 28 de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 47).

108 Il découle de ces dispositions que les autorités de contrôle ont pour mission première de contrôler l'application du RGPD et de veiller au respect de celui-ci. L'exercice de cette mission revêt une importance particulière dans le contexte d'un transfert de données à caractère personnel vers un pays tiers, dès lors que, ainsi qu'il ressort des termes mêmes du considérant 116 de ce règlement, « [l]orsque des données à caractère personnel franchissent les frontières extérieures de l'Union, cela peut accroître le risque que les personnes physiques ne puissent exercer leurs droits liés à la protection des données, notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations ». Dans cette hypothèse, ainsi qu'il est précisé à ce même considérant, « les autorités de contrôle peuvent être confrontées à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées en dehors de leurs frontières ».

109 En outre, en vertu de l'article 57, paragraphe 1, sous f), du RGPD, chaque autorité de contrôle est tenue, sur son territoire, de traiter les réclamations que toute personne, conformément à l'article 77, paragraphe 1, de ce règlement, est en droit d'introduire lorsqu'elle considère qu'un traitement de données à caractère personnel la concernant constitue une violation dudit règlement, et d'en examiner l'objet dans la mesure du nécessaire. L'autorité de contrôle doit procéder au traitement d'une telle réclamation avec toute la diligence requise (voir par analogie, en ce qui concerne l'article 25, paragraphe 6, de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 63).

110 L'article 78, paragraphes 1 et 2, du RGPD reconnaît à toute personne le droit de former un recours juridictionnel effectif, notamment, lorsque l'autorité de contrôle omet de traiter sa réclamation. Le considérant 141 de ce règlement fait également référence à ce « droit à un recours juridictionnel effectif conformément à l'article 47 de la Charte » dans le cas où cette autorité de contrôle « n'agit pas alors qu'une action est nécessaire pour protéger les droits de la personne concernée ».

111 Aux fins de traiter les réclamations introduites, l'article 58, paragraphe 1, du RGPD investit chaque autorité de contrôle d'importants pouvoirs d'enquête. Lorsqu'une telle autorité estime, à l'issue de son enquête, que la personne concernée dont les données à caractère personnel ont été transférées vers un pays tiers ne bénéficie pas dans celui-ci d'un niveau de protection adéquat, elle est tenue, en application du droit de l'Union, de réagir de manière appropriée afin de remédier à l'insuffisance constatée, et ce indépendamment de l'origine ou de la nature de cette insuffisance. À cet effet, l'article 58, paragraphe 2, de ce règlement énumère les différentes mesures correctrices que l'autorité de contrôle peut adopter.

112 Bien que le choix du moyen approprié et nécessaire relève de l'autorité de contrôle et que celle-ci doive opérer ce choix en prenant en considération toutes les circonstances du transfert de données à caractère personnel en cause, cette autorité n'en est pas moins tenue de s'acquitter avec toute la diligence requise de sa mission consistant à veiller au plein respect du RGPD.

113 À cet égard et ainsi que M. l'avocat général l'a également relevé au point 148 de ses conclusions, ladite autorité est tenue, en vertu de l'article 58, paragraphe 2, sous f) et j), de ce règlement, de suspendre ou d'interdire un transfert de données à caractère personnel vers un pays tiers lorsqu'elle considère, à la lumière de l'ensemble des circonstances propres à ce transfert, que les clauses types de protection des données ne sont pas ou ne peuvent pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union ne peut pas être assurée par d'autres moyens, à défaut pour le responsable du traitement ou son sous-traitant établis dans l'Union d'avoir lui-même suspendu le transfert ou d'avoir mis fin à celui-ci.

114 L'interprétation figurant au point précédent n'est pas infirmée par l'argumentation du commissaire selon laquelle l'article 4 de la décision 2010/87, dans sa version antérieure à l'entrée en vigueur de la décision d'exécution 2016/2297, lu à la lumière du considérant 11 de cette décision, limitait à certaines hypothèses exceptionnelles le pouvoir des autorités de contrôle de suspendre ou d'interdire un transfert de données à caractère personnel vers un pays tiers. En effet, dans sa version issue de la décision d'exécution 2016/2297, l'article 4 de la décision CPT évoque le pouvoir dont disposent ces autorités, désormais en vertu de l'article 58, paragraphe 2, sous f) et sous j), du RGPD, de suspendre ou d'interdire un tel transfert, sans aucunement limiter l'exercice de ce pouvoir à des circonstances exceptionnelles.

115 En tout état de cause, le pouvoir d'exécution que l'article 46, paragraphe 2, sous c), du RGPD reconnaît à la Commission aux fins d'adopter des clauses types de protection des données ne lui confère pas la compétence de restreindre les pouvoirs dont disposent les autorités de contrôle au titre de l'article 58, paragraphe 2, de ce règlement (voir par analogie, s'agissant de l'article 25, paragraphe 6, et de l'article 28 de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, points 102 et 103). Au demeurant, le considérant 5 de la décision d'exécution 2016/2297 confirme

que la décision CPT « n'empêche nullement une [autorité de contrôle] d'exercer ses pouvoirs de contrôle des flux de données, notamment le pouvoir de suspendre ou d'interdire un transfert de données à caractère personnel, lorsqu'elle constate que ce transfert est effectué en violation de la législation de l'Union européenne ou de l'État membre en matière de protection des données ».

116 Il importe toutefois de préciser que les pouvoirs de l'autorité de contrôle compétente sont soumis au plein respect de la décision par laquelle la Commission constate, le cas échéant, en application de l'article 45, paragraphe 1, première phrase, du RGPD, qu'un pays tiers déterminé assure un niveau de protection adéquat. En effet, dans une telle hypothèse, il ressort de l'article 45, paragraphe 1, seconde phrase, de ce règlement, lu en combinaison avec le considérant 103 de celui-ci, que les transferts de données à caractère personnel vers le pays tiers concerné peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autorisation spécifique.

117 En vertu de l'article 288, quatrième alinéa, TFUE, une décision d'adéquation de la Commission a, dans tous ses éléments, un caractère contraignant pour tous les États membres destinataires et s'impose donc à tous leurs organes, en ce qu'elle constate que le pays tiers concerné garantit un niveau de protection adéquat et qu'elle a pour effet d'autoriser ces transferts de données (voir par analogie, en ce qui concerne l'article 25, paragraphe 6, de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 51 et jurisprudence citée).

118 Ainsi, aussi longtemps que la décision d'adéquation n'a pas été déclarée invalide par la Cour, les États membres et leurs organes, au nombre desquels figurent leurs autorités de contrôle indépendantes, ne sauraient adopter des mesures contraires à cette décision, telles que des actes visant à constater avec effet contraignant que le pays tiers visé par ladite décision n'assure pas un niveau de protection adéquat (arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 52 et jurisprudence citée) et, en conséquence, à suspendre ou interdire des transferts de données à caractère personnel vers ce pays tiers.

119 Toutefois, une décision d'adéquation de la Commission adoptée au titre de l'article 45, paragraphe 3, du RGPD ne saurait empêcher les personnes dont les données à caractère personnel ont été ou pourraient être transférées vers un pays tiers de saisir, en application de l'article 77, paragraphe 1, du RGPD, l'autorité nationale de contrôle compétente d'une réclamation relative à la protection de leurs droits et de leurs libertés à l'égard du traitement de ces données. De même, une décision de cette nature ne saurait ni annihiler ni réduire les pouvoirs expressément reconnus aux autorités nationales de contrôle par l'article 8, paragraphe 3, de la Charte ainsi que par l'article 51, paragraphe 1, et par l'article 57, paragraphe 1, sous a), dudit règlement (voir par analogie, en ce qui concerne l'article 25, paragraphe 6, et l'article 28 de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 53).

120 Ainsi, même en présence d'une décision d'adéquation de la Commission, l'autorité nationale de contrôle compétente, saisie par une personne d'une réclamation relative à la protection de ses droits et de ses libertés à l'égard d'un traitement de données à caractère personnel la concernant, doit pouvoir examiner, en toute indépendance, si le transfert de ces données respecte les exigences posées par le RGPD et, le cas échéant, introduire un recours devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision d'adéquation, à un renvoi préjudiciel aux fins de l'examen de cette validité (voir par analogie, en ce qui concerne l'article 25, paragraphe 6, et l'article 28 de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, points 57 et 65).

121 Eu égard aux considérations qui précèdent, il y a lieu de répondre à la huitième question que l'article 58, paragraphe 2, sous f) et j), du RGPD doit être interprété en ce sens que, à moins qu'il existe une décision d'adéquation valablement adoptée par la Commission, l'autorité de contrôle compétente est tenue de suspendre ou d'interdire un transfert de données vers un pays tiers fondé sur des clauses types de protection des données adoptées par la Commission, lorsque cette autorité de

contrôle considère, à la lumière de l'ensemble des circonstances propres à ce transfert, que ces clauses ne sont pas ou ne peuvent pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union, en particulier par les articles 45 et 46 du RGPD et par la Charte, ne peut pas être assurée par d'autres moyens, à défaut pour le responsable du traitement ou son sous-traitant établis dans l'Union d'avoir lui-même suspendu le transfert ou d'avoir mis fin à celui-ci.

Sur les septième et onzième questions

122 Par ses septième et onzième questions, qu'il convient d'examiner ensemble, la juridiction de renvoi interroge la Cour, en substance, sur la validité de la décision CPT au regard des articles 7, 8 et 47 de la Charte.

123 En particulier, ainsi qu'il ressort des termes mêmes de la septième question et des explications y afférentes figurant dans la demande de décision préjudicielle, la juridiction de renvoi se demande si la décision CPT est à même d'assurer un niveau de protection adéquat des données à caractère personnel transférées vers des pays tiers, dans la mesure où les clauses types de protection des données qu'elle prévoit ne lient pas les autorités de ces pays tiers.

124 L'article 1er de la décision CPT dispose que les clauses types de protection des données figurant à l'annexe de celle-ci sont considérées comme offrant des garanties appropriées au regard de la protection de la vie privée ainsi que des libertés et des droits fondamentaux des personnes, conformément aux exigences de l'article 26, paragraphe 2, de la directive 95/46. Cette dernière disposition a été reprise, en substance, à l'article 46, paragraphe 1, et à l'article 46, paragraphe 2, sous c), du RGPD.

125 Toutefois, alors que ces clauses sont contraignantes pour le responsable du traitement établi dans l'Union et le destinataire du transfert de données à caractère personnel établi dans un pays tiers, dans le cas où ils ont conclu un contrat par référence à ces clauses, il est constant que lesdites clauses ne sont pas susceptibles de lier les autorités de ce pays tiers, puisque ces dernières ne sont pas parties au contrat.

126 S'il existe, dès lors, des situations dans lesquelles, en fonction de l'état du droit et des pratiques en vigueur dans le pays tiers concerné, le destinataire d'un tel transfert est en mesure de garantir la protection des données nécessaire sur la base des seules clauses types de protection des données, il en existe d'autres dans lesquelles les stipulations contenues dans ces clauses pourraient ne pas constituer un moyen suffisant permettant d'assurer, en pratique, la protection effective des données à caractère personnel transférées dans le pays tiers concerné. Tel est le cas, notamment, lorsque le droit de ce pays tiers permet aux autorités publiques de celui-ci des ingérences dans les droits des personnes concernées relatifs à ces données.

127 Ainsi, se pose la question de savoir si une décision de la Commission portant sur des clauses types de protection des données, adoptée sur le fondement de l'article 46, paragraphe 2, sous c), du RGPD, est invalide, en l'absence, dans cette décision, de garanties opposables aux autorités publiques des pays tiers vers lesquels des données à caractère personnel sont ou pourraient être transférées sur le fondement de ces clauses.

128 L'article 46, paragraphe 1, du RGPD prévoit que, en l'absence d'une décision d'adéquation, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives. Selon l'article 46, paragraphe 2, sous c), de ce règlement, ces garanties peuvent être fournies par des clauses types de

protection des données adoptées par la Commission. Or, ces dispositions n'énoncent pas que l'ensemble desdites garanties doit nécessairement être prévu par une décision de la Commission telle que la décision CPT.

129 Il importe, à cet égard, de relever qu'une pareille décision se distingue d'une décision d'adéquation adoptée au titre de l'article 45, paragraphe 3, du RGPD, laquelle vise, à la suite d'un examen de la réglementation du pays tiers concerné tenant compte, notamment, de la législation pertinente en matière de sécurité nationale et d'accès des autorités publiques aux données à caractère personnel, à constater avec effet contraignant qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans celui-ci, assure un niveau de protection adéquat et que, dès lors, l'accès des autorités publiques dudit pays tiers à de telles données ne fait pas obstacle aux transferts de celles-ci vers le même pays tiers. Une telle décision d'adéquation ne peut donc être adoptée par la Commission qu'à la condition que celle-ci ait constaté que la législation pertinente du pays tiers en la matière comporte effectivement l'ensemble des garanties requises permettant de considérer qu'elle assure un niveau de protection adéquat.

130 En revanche, s'agissant d'une décision de la Commission adoptant des clauses types de protection des données, telle que la décision CPT, dans la mesure où une telle décision ne vise pas un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans celui-ci, il ne saurait être inféré de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, sous c), du RGPD que la Commission serait tenue de procéder, avant l'adoption d'une telle décision, à une évaluation du caractère adéquat du niveau de protection assuré par les pays tiers vers lesquels des données à caractère personnel pourraient être transférées sur le fondement de telles clauses.

131 À cet égard, il y a lieu de rappeler que, aux termes de l'article 46, paragraphe 1, de ce règlement, en l'absence de décision d'adéquation de la Commission, il incombe au responsable du traitement ou au sous-traitant établis dans l'Union de prévoir, notamment, des garanties appropriées. Les considérants 108 et 114 dudit règlement confirment que, lorsque la Commission ne s'est pas prononcée sur le caractère adéquat du niveau de protection des données dans un pays tiers, le responsable du traitement ou, le cas échéant, son sous-traitant « devrait prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée » et que « [c]es garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée au traitement au sein de l'Union, y compris l'existence de droits opposables de la personne concernée et de voies de droit effectives [...] dans l'Union ou dans un pays tiers ».

132 Dès lors que, comme il ressort du point 125 du présent arrêt, il est inhérent au caractère contractuel des clauses types de protection des données que celles-ci ne sauraient lier les autorités publiques des pays tiers, mais que l'article 44, l'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du RGPD, interprétés à la lumière des articles 7, 8 et 47 de la Charte, exigent que le niveau de protection des personnes physiques garanti par ce règlement ne soit pas compromis, il peut s'avérer nécessaire de compléter les garanties que contiennent ces clauses types de protection des données. À cet égard, le considérant 109 dudit règlement énonce que « [l]a possibilité qu'ont les responsables du traitement [...] de recourir à des clauses types de protection des données adoptées par la Commission [...] ne devrait pas les empêcher [...] d'y ajouter d'autres clauses ou des garanties supplémentaires » et précise, en particulier, que ceux-ci « devraient être encouragés à fournir des garanties supplémentaires [...] qui viendraient compléter les clauses types de protection [des données] ».

133 Il apparaît ainsi que les clauses types de protection des données adoptées par la Commission au titre de l'article 46, paragraphe 2, sous c), du même règlement visent uniquement à fournir aux responsables du traitement ou à leurs sous-traitants établis dans l'Union des garanties contractuelles s'appliquant de manière uniforme dans tous les pays tiers et, dès lors, indépendamment du niveau de protection garanti dans chacun d'entre eux. Dans la mesure où ces clauses types de protection des données ne peuvent, eu égard à leur nature, fournir des garanties allant au-delà d'une obligation

contractuelle de veiller à ce que le niveau de protection requis par le droit de l'Union soit respecté, elles peuvent nécessiter, en fonction de la situation prévalant dans tel ou tel pays tiers, l'adoption de mesures supplémentaires par le responsable du traitement afin d'assurer le respect de ce niveau de protection.

134 À cet égard, ainsi que M. l'avocat général l'a relevé au point 126 de ses conclusions, le mécanisme contractuel prévu à l'article 46, paragraphe 2, sous c), du RGPD repose sur la responsabilisation du responsable du traitement ou de son sous-traitant établis dans l'Union ainsi que, à titre subsidiaire, de l'autorité de contrôle compétente. Il appartient, dès lors, avant tout, à ce responsable du traitement ou à son sous-traitant de vérifier, au cas par cas et, le cas échéant, en collaboration avec le destinataire du transfert, si le droit du pays tiers de destination assure une protection appropriée, au regard du droit de l'Union, des données à caractère personnel transférées sur le fondement de clauses types de protection des données, en fournissant, au besoin, des garanties supplémentaires à celles offertes par ces clauses.

135 À défaut, pour le responsable du traitement ou son sous-traitant établis dans l'Union, de pouvoir prendre des mesures supplémentaires suffisantes pour garantir une telle protection, ceux-ci ou, à titre subsidiaire, l'autorité de contrôle compétente sont tenus de suspendre ou de mettre fin au transfert de données à caractère personnel vers le pays tiers concerné. Tel est notamment le cas lorsque le droit de ce pays tiers impose au destinataire d'un transfert de données à caractère personnel en provenance de l'Union des obligations qui sont contraires auxdites clauses et, partant, de nature à remettre en cause la garantie contractuelle d'un niveau de protection adéquat contre l'accès des autorités publiques dudit pays tiers à ces données.

136 Partant, le seul fait que des clauses types de protection des données figurant dans une décision de la Commission adoptée en application de l'article 46, paragraphe 2, sous c), du RGPD, telles que celles figurant à l'annexe de la décision CPT, ne lient pas les autorités des pays tiers vers lesquels des données à caractère personnel sont susceptibles d'être transférées ne saurait affecter la validité de cette décision.

137 Cette validité dépend, en revanche, du point de savoir si, conformément à l'exigence résultant de l'article 46, paragraphe 1, et de l'article 46, paragraphe 2, sous c), du RGPD, interprétés à la lumière des articles 7, 8 et 47 de la Charte, une telle décision comporte des mécanismes effectifs permettant, en pratique, d'assurer que le niveau de protection requis par le droit de l'Union soit respecté et que les transferts de données à caractère personnel, fondés sur de telles clauses, soient suspendus ou interdits en cas de violation de ces clauses ou d'impossibilité de les honorer.

138 En ce qui concerne les garanties contenues dans les clauses types de protection des données figurant à l'annexe de la décision CPT, il ressort de la clause 4, sous a) et b), de la clause 5, sous a), de la clause 9 ainsi que de la clause 11, paragraphe 1, de celle-ci que le responsable du traitement établi dans l'Union, le destinataire du transfert de données à caractère personnel ainsi que l'éventuel sous-traitant de ce dernier s'engagent mutuellement à ce que le traitement de ces données, y compris leur transfert, a été et continuera d'être effectué conformément au « droit applicable à la protection des données », à savoir, selon la définition figurant à l'article 3, sous f), de ladite décision, « la législation protégeant les libertés et les droits fondamentaux des personnes, notamment le droit à la vie privée à l'égard du traitement des données à caractère personnel, et s'appliquant à un responsable du traitement dans l'État membre où l'exportateur de données est établi ». Or, les dispositions du RGPD, lues à la lumière de la Charte, font partie de cette législation.

139 En outre, le destinataire du transfert de données à caractère personnel établi dans un pays tiers s'engage, en vertu de cette clause 5, sous a), à informer, dans les meilleurs délais, le responsable du traitement établi dans l'Union de son éventuelle incapacité de se conformer aux obligations lui incombant au titre du contrat conclu. En particulier, selon ladite clause 5, sous b), ce destinataire certifie qu'il n'a aucune raison de croire que la législation le concernant l'empêche de remplir les obligations lui incombant conformément au contrat conclu et il s'engage à communiquer au

responsable du traitement, sans retard après en avoir pris connaissance, toute modification de la législation nationale le concernant qui est susceptible d'avoir des conséquences négatives importantes pour les garanties et les obligations offertes par les clauses types de protection des données figurant à l'annexe de la décision CPT. Par ailleurs, si la même clause 5, sous d), i), permet au destinataire du transfert de données à caractère personnel, en cas de législation lui en faisant défense, telle qu'une interdiction de caractère pénal visant à préserver le secret d'une enquête policière, de ne pas communiquer au responsable du traitement établi dans l'Union une demande contraignante de divulgation des données à caractère personnel émanant d'une autorité de maintien de l'ordre, il est néanmoins tenu, conformément à la clause 5, sous a), de l'annexe de la décision CPT d'informer le responsable du traitement de son incapacité de se conformer aux clauses types de protection des données.

140 Dans les deux hypothèses qu'elle envisage, cette clause 5, sous a) et b), confère au responsable du traitement établi dans l'Union le droit de suspendre le transfert de données et/ou de résilier le contrat. Eu égard aux exigences résultant de l'article 46, paragraphe 1, et paragraphe 2, sous c), du RGPD, lu à la lumière des articles 7 et 8 de la Charte, la suspension du transfert de données et/ou la résiliation du contrat revêtent un caractère obligatoire pour le responsable du traitement lorsque le destinataire du transfert n'est pas, ou n'est plus, en mesure de respecter les clauses types de protection des données. À défaut, le responsable du traitement méconnaîtrait les exigences lui incombant au titre de la clause 4, sous a), de l'annexe de la décision CPT interprétée à la lumière des dispositions du RGPD et de la Charte.

141 Il apparaît ainsi que la clause 4, sous a), et la clause 5, sous a) et b), de cette annexe font obligation au responsable du traitement établi dans l'Union et au destinataire du transfert de données à caractère personnel de s'assurer que la législation du pays tiers de destination permet audit destinataire de se conformer aux clauses types de protection des données figurant à l'annexe de la décision CPT, avant de procéder à un transfert de données à caractère personnel vers ce pays tiers. S'agissant de cette vérification, la note en bas de page relative à ladite clause 5 précise que des exigences impératives de cette législation n'allant pas au-delà de celles qui sont nécessaires dans une société démocratique pour sauvegarder, notamment, la sûreté de l'État, la défense et la sécurité publique ne vont pas à l'encontre de ces clauses types de protection des données. À l'inverse, ainsi que l'a souligné M. l'avocat général au point 131 de ses conclusions, le fait de se conformer à une obligation dictée par le droit du pays tiers de destination qui va au-delà de ce qui est nécessaire à de telles fins doit être considéré comme une violation desdites clauses. L'appréciation, de la part de ces opérateurs, du caractère nécessaire d'une telle obligation doit, le cas échéant, tenir compte de la constatation du caractère adéquat du niveau de protection assuré par le pays tiers concerné figurant dans une décision d'adéquation de la Commission, adoptée au titre de l'article 45, paragraphe 3, du RGPD.

142 Il en résulte que le responsable du traitement établi dans l'Union et le destinataire du transfert de données à caractère personnel sont tenus de vérifier, au préalable, le respect, dans le pays tiers concerné, du niveau de protection requis par le droit de l'Union. Le destinataire de ce transfert est, le cas échéant, dans l'obligation, en vertu de la même clause 5, sous b), d'informer le responsable du traitement de son éventuelle incapacité de se conformer à ces clauses, à charge alors pour ce dernier de suspendre le transfert de données et/ou de résilier le contrat.

143 Si le destinataire du transfert des données à caractère personnel vers un pays tiers fait savoir au responsable du traitement, au titre de la clause 5, sous b), de l'annexe de la décision CPT, que la législation du pays tiers concerné ne lui permet pas de se conformer aux clauses types de protection des données figurant à cette annexe, il découle de la clause 12 de ladite annexe que les données qui ont déjà été transférées vers ce pays tiers et les copies doivent, dans leur totalité, être restituées ou détruites. En tout état de cause, la clause 6 de la même annexe sanctionne la méconnaissance de ces clauses types en conférant à la personne concernée le droit d'obtenir réparation du préjudice subi.

144 Il convient d'ajouter que, selon la clause 4, sous f), de l'annexe de la décision CPT, le responsable du traitement établi dans l'Union s'engage, lorsque des catégories particulières de données pourraient être transférées vers un pays tiers n'offrant pas un niveau de protection adéquat, à en informer la personne concernée avant le transfert ou dès que possible après celui-ci. Cette information est susceptible de mettre cette personne en mesure d'exercer le droit de recours que lui reconnaît la clause 3, paragraphe 1, de cette annexe contre le responsable du traitement, afin que celui-ci suspende le transfert envisagé, résilie le contrat conclu avec le destinataire du transfert de données à caractère personnel ou, le cas échéant, demande à ce dernier la restitution ou la destruction des données transférées.

145 Enfin, en vertu de la clause 4, sous g), de ladite annexe, le responsable du traitement établi dans l'Union est tenu, lorsque le destinataire du transfert de données à caractère personnel lui notifie, en application de la clause 5, sous b), de celle-ci, que la législation le concernant fait l'objet d'une modification susceptible d'avoir des conséquences négatives importantes pour les garanties offertes et les obligations imposées par les clauses types de protection des données, de transmettre cette notification à l'autorité de contrôle compétente s'il décide, en dépit de ladite notification, de poursuivre le transfert ou de lever sa suspension. La transmission d'une telle notification à cette autorité de contrôle et le droit de celle-ci de procéder à des vérifications auprès du destinataire du transfert de données à caractère personnel en application de la clause 8, paragraphe 2, de la même annexe permettent à ladite autorité de contrôle de vérifier s'il y a lieu de procéder à la suspension ou à l'interdiction du transfert envisagé aux fins d'assurer un niveau de protection adéquat.

146 Dans ce contexte, l'article 4 de la décision CPT, lu à la lumière du considérant 5 de la décision d'exécution 2016/2297, confirme que la décision CPT n'empêche nullement l'autorité de contrôle compétente de suspendre ou d'interdire, le cas échéant, un transfert de données à caractère personnel vers un pays tiers fondé sur les clauses types de protection des données figurant à l'annexe de cette décision. À cet égard, ainsi qu'il découle de la réponse à la huitième question, à moins qu'il existe une décision d'adéquation valablement adoptée par la Commission, l'autorité de contrôle compétente est tenue, en vertu de l'article 58, paragraphe 2, sous f) et j), du RGPD, de suspendre ou d'interdire un tel transfert, lorsqu'elle considère, à la lumière de l'ensemble des circonstances propres à ce transfert, que ces clauses ne sont pas ou ne peuvent pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union ne peut pas être assurée par d'autres moyens, à défaut pour le responsable du traitement ou son sous-traitant établis dans l'Union d'avoir lui-même suspendu le transfert ou d'avoir mis fin à celui-ci.

147 En ce qui concerne la circonstance, mise en avant par le commissaire, selon laquelle des transferts de données à caractère personnel vers un tel pays tiers pourraient éventuellement faire l'objet de décisions divergentes des autorités de contrôle dans différents États membres, il convient d'ajouter que, ainsi qu'il ressort de l'article 55, paragraphe 1, et de l'article 57, paragraphe 1, sous a), du RGPD, la mission de veiller au respect de ce règlement est confiée, en principe, à chaque autorité de contrôle sur le territoire de l'État membre dont elle relève. En outre, aux fins d'éviter des décisions divergentes, l'article 64, paragraphe 2, de dudit règlement prévoit la possibilité pour une autorité de contrôle qui estimerait que les transferts de données vers un pays tiers doivent, d'une manière générale, être interdits de saisir pour avis le comité européen de la protection des données (EDPB), celui-ci pouvant, en application de l'article 65, paragraphe 1, sous c), du même règlement, adopter une décision contraignante, notamment lorsqu'une autorité de contrôle ne suit pas l'avis émis.

148 Il s'ensuit que la décision CPT prévoit des mécanismes effectifs permettant, en pratique, d'assurer que le transfert vers un pays tiers de données à caractère personnel sur le fondement des clauses types de protection des données figurant à l'annexe de cette décision soit suspendu ou interdit lorsque le destinataire du transfert ne respecte pas lesdites clauses ou se trouve dans l'incapacité de les respecter.

149 Au vu de l'ensemble des considérations qui précèdent, il y a lieu de répondre aux septième et onzième questions que l'examen de la décision CPT au regard des articles 7, 8 et 47 de la Charte n'a révélé aucun élément de nature à affecter la validité de cette décision.

Sur les quatrième, cinquième, neuvième et dixième questions

150 Par sa neuvième question, la juridiction de renvoi cherche, en substance, à savoir si et dans quelle mesure une autorité de contrôle d'un État membre est liée par les constatations figurant dans la décision BPD selon lesquelles les États-Unis assurent un niveau de protection adéquat. Par ses quatrième, cinquième et dixième questions, cette juridiction demande, en substance, si, compte tenu de ses propres constatations relatives au droit des États-Unis, le transfert vers ce pays tiers de données à caractère personnel sur le fondement des clauses types de protection des données figurant à l'annexe de la décision CPT viole les droits garantis aux articles 7, 8 et 47 de la Charte et interroge la Cour, en particulier, sur le point de savoir si la mise en place du médiateur mentionné dans l'annexe III de la décision BPD est compatible avec cet article 47.

151 À titre liminaire, il importe de relever que, si le recours au principal introduit par le commissaire met en doute la validité de la seule décision CPT, ce recours a été introduit auprès de la juridiction de renvoi antérieurement à l'adoption de la décision BPD. Dans la mesure où, par ses quatrième et cinquième questions, cette juridiction interroge la Cour, de manière générale, sur la protection devant être assurée, en vertu des articles 7, 8 et 47 de la Charte, dans le contexte d'un tel transfert, l'examen de la Cour doit prendre en considération les conséquences résultant de l'adoption de la décision BPD, intervenue entretemps. Il en va d'autant plus ainsi que ladite juridiction demande explicitement, par sa dixième question, si la protection requise par cet article 47 est assurée par l'intermédiaire du médiateur mentionné dans cette dernière décision.

152 En outre, il ressort des indications figurant dans la demande de décision préjudicielle que, dans le cadre de la procédure au principal, Facebook Ireland a fait valoir que la décision BPD produisait, pour le commissaire, des effets contraignants en ce qui concerne la constatation du caractère adéquat du niveau de protection assuré par les États-Unis et, par suite, quant au caractère licite d'un transfert vers ce pays tiers de données à caractère personnel fondé sur les clauses types de protection des données figurant à l'annexe de la décision CPT.

153 Or, ainsi qu'il ressort du point 59 du présent arrêt, dans son arrêt du 3 octobre 2017, annexé à la demande de décision préjudicielle, la juridiction de renvoi a souligné qu'elle était tenue de prendre en compte les modifications du droit intervenues entre l'introduction du recours et l'audience organisée devant elle. Ainsi, cette juridiction semble être dans l'obligation de prendre en considération, pour trancher le litige au principal, le changement de circonstances résultant de l'adoption de la décision BPD ainsi que les éventuels effets contraignants de celle-ci.

154 En particulier, l'existence des effets contraignants qui s'attachent à la constatation par la décision BPD d'un niveau de protection adéquat aux États-Unis est pertinente aux fins de l'appréciation tant des obligations, rappelées aux points 141 et 142 du présent arrêt, qui incombent au responsable du traitement et au destinataire d'un transfert de données à caractère personnel vers un pays tiers effectué sur le fondement des clauses types de protection des données figurant à l'annexe de la décision CPT que des obligations qui pèsent, le cas échéant, sur l'autorité de contrôle de suspendre ou d'interdire un tel transfert.

155 S'agissant, en effet, des effets contraignants de la décision BPD, l'article 1er, paragraphe 1, de cette décision dispose que, aux fins de l'article 45, paragraphe 1, du RGPD, « les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis dans le cadre du bouclier de protection des données [Union européenne]-États-Unis ». Conformément à l'article 1er, paragraphe 3, de ladite décision, les données à

caractère personnel sont considérées comme étant transférées dans le cadre de ce bouclier lorsqu'elles le sont depuis l'Union vers des organisations établies aux États-Unis qui figurent sur la liste des organisations adhérant audit bouclier, tenue à jour et publiée par le ministère américain du Commerce, conformément aux sections I et III des principes énoncés à l'annexe II de la même décision.

156 Ainsi qu'il résulte de la jurisprudence rappelée aux points 117 et 118 du présent arrêt, la décision BPD a un caractère contraignant pour les autorités de contrôle en ce qu'elle constate que les États-Unis garantissent un niveau de protection adéquat et, partant, a pour effet d'autoriser des transferts de données à caractère personnel effectués dans le cadre du bouclier de protection des données Union européenne-États-Unis. Dès lors, aussi longtemps que cette décision n'a pas été déclarée invalide par la Cour, l'autorité de contrôle compétente ne saurait suspendre ou interdire un transfert de données à caractère personnel vers une organisation adhérant à ce bouclier au motif qu'elle considère, contrairement à l'appréciation retenue par la Commission dans ladite décision, que la législation des États-Unis régissant l'accès aux données à caractère personnel transférées dans le cadre dudit bouclier et l'utilisation de ces données par les autorités publiques de ce pays tiers à des fins de sécurité nationale, de respect de la loi ou d'intérêt public n'assure pas un niveau de protection adéquat.

157 Il n'en demeure pas moins que, conformément à la jurisprudence rappelée aux points 119 et 120 du présent arrêt, lorsqu'elle est saisie par une personne d'une réclamation, l'autorité de contrôle compétente doit examiner, en toute indépendance, si le transfert de données à caractère personnel en cause respecte les exigences posées par le RGPD et, dans l'hypothèse où elle estime fondés les griefs avancés par cette personne aux fins de mettre en cause la validité d'une décision d'adéquation, introduire un recours devant les juridictions nationales afin que ces dernières saisissent la Cour d'un renvoi préjudiciel en appréciation de la validité de cette décision.

158 En effet, une réclamation introduite au titre de l'article 77, paragraphe 1, du RGPD, par laquelle une personne dont les données à caractère personnel ont été ou pourraient être transférées vers un pays tiers, fait valoir que le droit et les pratiques de ce pays n'assurent pas, nonobstant ce qu'a constaté la Commission dans une décision adoptée au titre de l'article 45, paragraphe 3, de ce règlement, un niveau de protection adéquat, doit être comprise comme portant, en substance, sur la compatibilité de cette décision avec la protection de la vie privée ainsi que des libertés et des droits fondamentaux des personnes (voir par analogie, en ce qui concerne l'article 25, paragraphe 6, et l'article 28, paragraphe 4, de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 59).

159 En l'occurrence, M. Schrems a demandé en substance au commissaire d'interdire ou de suspendre le transfert par Facebook Ireland de ses données à caractère personnel à Facebook Inc., établie aux États-Unis, au motif que ce pays tiers n'assurait pas un niveau de protection adéquat. Le commissaire ayant, à l'issue d'une enquête sur les allégations de M. Schrems, saisi la juridiction de renvoi, cette dernière semble, au regard des preuves produites et du débat contradictoire tenu devant elle, s'interroger sur le bien-fondé des doutes de M. Schrems quant au caractère adéquat du niveau de protection assuré dans ledit pays tiers, en dépit de ce que la Commission a entretemps constaté dans la décision BPD, ce qui a conduit cette juridiction à poser à la Cour les quatrième, cinquième et dixième questions préjudicielles.

160 Ainsi que M. l'avocat général l'a relevé au point 175 de ses conclusions, ces questions préjudicielles doivent ainsi être comprises comme mettant, en substance, en cause le constat de la Commission, figurant dans la décision BPD, selon lequel les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers ce pays tiers et, partant, la validité de cette décision.

161 Eu égard aux considérations énoncées aux points 121 et 157 à 160 du présent arrêt et afin de donner une réponse complète à la juridiction de renvoi, il convient donc d'examiner si la décision BPD est conforme aux exigences découlant du RGPD, lu à la lumière de la Charte (voir, par analogie, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 67).

162 L'adoption par la Commission d'une décision d'adéquation au titre de l'article 45, paragraphe 3, du RGPD exige la constatation dûment motivée, de la part de cette institution, que le pays tiers concerné assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti dans l'ordre juridique de l'Union (voir par analogie, en ce qui concerne l'article 25, paragraphe 6, de la directive 95/46, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 96).

Sur le contenu de la décision BPD

163 La Commission a constaté, à l'article 1er, paragraphe 1, de la décision BPD, que les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis dans le cadre du bouclier de protection des données Union européenne-États-Unis, celui-ci se composant, notamment, en vertu de l'article 1er, paragraphe 2, de cette décision, des principes publiés par le ministère américain du Commerce le 7 juillet 2016, figurant à l'annexe II de ladite décision, ainsi que des observations et des engagements officiels contenus dans les documents énumérés aux annexes I, III à VII de la même décision.

164 Toutefois, la décision BPD précise également, au point I.5 de son annexe II, intitulée « Principes du cadre "bouclier de protection des données [Union européenne]-États-Unis" », que l'adhésion à ces principes peut être limitée par, notamment, « les exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect de la législation ». Ainsi, cette décision consacre, à l'instar de la décision 2000/520, la primauté de ces exigences sur lesdits principes, primauté en vertu de laquelle les organisations américaines autocertifiées recevant des données à caractère personnel depuis l'Union sont tenues d'écarter, sans limitation, les mêmes principes lorsque ces derniers entrent en conflit avec lesdites exigences et s'avèrent donc incompatibles avec celles-ci (voir par analogie, en ce qui concerne la décision 2000/520, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 86).

165 Eu égard à son caractère général, la dérogation figurant au point I.5 de l'annexe II de la décision BPD rend ainsi possibles des ingérences fondées sur des exigences relatives à la sécurité nationale et à l'intérêt public ou sur la législation interne des États-Unis dans les droits fondamentaux des personnes dont les données à caractère personnel sont ou pourraient être transférées depuis l'Union vers les États-Unis (voir par analogie, en ce qui concerne la décision 2000/520, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 87). Plus particulièrement, et ainsi qu'il est constaté dans la décision BPD, de telles ingérences peuvent résulter de l'accès aux données à caractère personnel transférées depuis l'Union vers les États-Unis et de l'utilisation de ces données par les autorités publiques américaines, dans le cadre des programmes de surveillance PRISM et UPSTREAM fondés sur l'article 702 du FISA, ainsi que sur le fondement de l'E.O. 12333.

166 Dans ce contexte, la Commission a évalué, aux considérants 67 à 135 de la décision BPD, les limitations et les garanties prévues dans la réglementation des États-Unis, notamment à l'article 702 du FISA, dans l'E.O. 12333 et dans la PPD-28, en ce qui concerne l'accès aux données à caractère personnel transférées dans le cadre du bouclier de protection des données Union européenne-États-Unis et l'utilisation de ces données par les autorités publiques américaines à des fins de sécurité nationale, de respect de la loi ainsi qu'à d'autres fins d'intérêt général.

167 Au terme de cette évaluation, la Commission a constaté, au considérant 136 de cette décision, que « les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées de l'[Union] vers des organisations autocertifiées aux États-Unis », et estimé, au

considérant 140 de ladite décision, que « sur la base des informations disponibles concernant l'ordre juridique des États-Unis, [...] toute ingérence des autorités publiques américaines dans l'exercice des droits fondamentaux des personnes dont les données sont transférées de l'Union européenne vers les États-Unis dans le cadre du bouclier de protection des données pour les besoins de la sécurité nationale, de l'intérêt public ou du respect des lois et, partant, les restrictions imposées aux organisations autocertifiées en ce qui concerne leur respect des principes seront limitées à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridictionnelle effective contre des ingérences de cette nature ».

Sur le constat relatif au niveau de protection adéquat

168 Eu égard aux éléments mentionnés par la Commission dans la décision BPD ainsi qu'à ceux établis par la juridiction de renvoi dans le cadre de la procédure au principal, cette juridiction nourrit des doutes sur le point de savoir si le droit des États-Unis assure effectivement le niveau de protection adéquat requis à l'article 45 du RGPD, lu à la lumière des droits fondamentaux garantis aux articles 7, 8 et 47 de la Charte. En particulier, ladite juridiction considère que le droit de ce pays tiers ne prévoit pas les limitations et les garanties nécessaires à l'égard des ingérences autorisées par sa réglementation nationale et n'assure pas non plus une protection juridictionnelle effective contre de telles ingérences. À ce dernier égard, elle ajoute que l'instauration du médiateur du bouclier de protection ne peut, selon elle, remédier à ces lacunes dès lors que ce médiateur ne saurait être assimilé à un tribunal, au sens de l'article 47 de la Charte.

169 S'agissant, en premier lieu, des articles 7 et 8 de la Charte, qui participent du niveau de protection requis au sein de l'Union et dont le respect doit être constaté par la Commission avant que celle-ci adopte une décision d'adéquation au titre de l'article 45, paragraphe 1, du RGPD, il y a lieu de rappeler que l'article 7 de la Charte garantit à toute personne le droit au respect de sa vie privée et familiale, de son domicile et de ses communications. Quant à l'article 8, paragraphe 1, de la Charte, celui-ci reconnaît explicitement à toute personne le droit à la protection des données à caractère personnel la concernant.

170 Ainsi, l'accès à des données à caractère personnel d'une personne physique en vue de leur conservation ou de leur utilisation affecte le droit fondamental de cette personne au respect de la vie privée, garanti à l'article 7 de la Charte, ce droit se rapportant à toute information concernant une personne physique identifiée ou identifiable. Lesdits traitements de données relèvent également de l'article 8 de la Charte en raison du fait qu'ils constituent des traitements de données à caractère personnel au sens de cet article et doivent, par suite, nécessairement satisfaire aux exigences de protection des données prévues audit article [voir, en ce sens, arrêts du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, points 49 et 52 ; du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 29, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 122 et 123].

171 La Cour a déjà jugé que la communication de données à caractère personnel à un tiers, tel qu'une autorité publique, constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure des informations communiquées. Il en va de même de la conservation de données à caractère personnel ainsi que de l'accès auxdites données en vue de leur utilisation par les autorités publiques, indépendamment du point de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible, ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, arrêts du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, points 74 et 75 ; du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 33 à 36, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126].

172 Toutefois, les droits consacrés aux articles 7 et 8 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société [voir, en ce sens, arrêts du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 48 et jurisprudence citée ; du 17 octobre 2013, Schwarz, C-291/12, EU:C:2013:670, point 33 et jurisprudence citée, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 136].

173 À cet égard, il convient de relever également que, aux termes de l'article 8, paragraphe 2, de la Charte, les données à caractère personnel doivent, notamment, être traitées « à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi ».

174 En outre, conformément à l'article 52, paragraphe 1, première phrase, de la Charte, toute limitation de l'exercice des droits et des libertés reconnus par celle-ci doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Selon l'article 52, paragraphe 1, seconde phrase, de la Charte, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

175 Il convient d'ajouter, à ce dernier égard, que l'exigence selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet l'ingérence dans ces droits doit définir elle-même la portée de la limitation de l'exercice du droit concerné [avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 139 et jurisprudence citée].

176 Enfin, pour satisfaire à l'exigence de proportionnalité selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, la réglementation en cause comportant l'ingérence doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données ont été transférées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 140 et 141 ainsi que jurisprudence citée].

177 À cet effet, l'article 45, paragraphe 2, sous a), du RGPD précise que, dans le cadre de son évaluation du caractère adéquat du niveau de protection assuré par un pays tiers, la Commission tient compte, notamment, « [d]es droits effectifs et opposables dont bénéficient les personnes concernées » dont les données à caractère personnel sont transférées.

178 En l'occurrence, la constatation opérée par la Commission dans la décision BPD selon laquelle les États-Unis assurent un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union par le RGPD, lu à la lumière des articles 7 et 8 de la Charte, a été remise en cause au motif, notamment, que les ingérences résultant des programmes de surveillance fondés sur l'article 702 du FISA et sur l'E.O. 12333 ne seraient pas soumises à des exigences assurant, dans le respect du principe de proportionnalité, un niveau de protection substantiellement équivalent à celui garanti par l'article 52, paragraphe 1, seconde phrase, de la Charte. Il y a donc lieu d'examiner si ces programmes de surveillance sont mis en œuvre dans le respect de telles exigences, sans qu'il soit nécessaire de vérifier au préalable le respect par ce pays tiers de conditions substantiellement équivalentes à celles prévues à l'article 52, paragraphe 1, première phrase, de la Charte.

179 À cet égard, en ce qui concerne les programmes de surveillance fondés sur l'article 702 du FISA, la Commission a constaté, au considérant 109 de la décision BPD, que, selon ledit article, « le FISC n'autorise pas de mesures de surveillance individuelle, mais plutôt des programmes de surveillance (comme PRISM ou UPSTREAM) sur la base de certifications annuelles préparées par le procureur général et le directeur du renseignement national (DNI) ». Ainsi qu'il ressort de ce considérant, le contrôle exercé par le FISC vise à vérifier si ces programmes de surveillance correspondent à l'objectif d'obtenir des informations en matière de renseignement extérieur, mais ne porte pas sur le point de savoir « si les personnes sont correctement ciblées pour se procurer des informations en matière de renseignement extérieur ».

180 Il apparaît ainsi que l'article 702 du FISA ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'il comporte pour la mise en œuvre des programmes de surveillance aux fins du renseignement extérieur, pas plus que l'existence de garanties pour des personnes non-américaines potentiellement visées par ces programmes. Dans ces conditions, et ainsi que M. l'avocat général l'a relevé, en substance, aux points 291, 292 et 297 de ses conclusions, cet article n'est pas susceptible d'assurer un niveau de protection substantiellement équivalent à celui garanti par la Charte, telle qu'interprétée par la jurisprudence rappelée aux points 175 et 176 du présent arrêt, selon laquelle une base légale qui permet des ingérences dans les droits fondamentaux doit, pour satisfaire au principe de proportionnalité, définir elle-même la portée de la limitation de l'exercice du droit concerné et prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales.

181 Selon les constatations figurant dans la décision BPD, les programmes de surveillance fondés sur l'article 702 du FISA doivent, certes, être mis en œuvre dans le respect des exigences résultant de la PPD-28. Toutefois, si la Commission a souligné, aux considérants 69 et 77 de la décision BPD, que de telles exigences revêtent un caractère contraignant pour les services de renseignement américains, le gouvernement américain a admis, en réponse à une question de la Cour, que la PPD-28 ne confère pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux. Dès lors, elle n'est pas susceptible d'assurer un niveau de protection substantiellement équivalent à celui résultant de la Charte, contrairement à ce qu'exige l'article 45, paragraphe 2, sous a), du RGPD, selon lequel la constatation de ce niveau dépend, notamment, de l'existence des droits effectifs et opposables dont bénéficient les personnes dont les données ont été transférées vers le pays tiers en cause.

182 S'agissant des programmes de surveillance fondés sur l'E.O. 12333, il ressort du dossier dont dispose la Cour que ce décret ne confère pas non plus de droits opposables aux autorités américaines devant les tribunaux.

183 Il convient d'ajouter que la PPD-28, qui doit être respectée dans le cadre de l'application des programmes visés aux deux points précédents, permet de procéder à une « collecte "en vrac" [...] d'un volume relativement important d'informations ou de données issues du renseignement d'origine électromagnétique dans des conditions où les services de renseignement ne peuvent pas utiliser d'identifiant associé à une cible spécifique [...] pour orienter la collecte », ainsi qu'il est précisé dans une lettre du 21 juin 2016 du bureau du directeur du renseignement national (Office of the Director of National Intelligence) au ministère américain du Commerce ainsi qu'à l'administration du commerce international, figurant à l'annexe VI de la décision BPD. Or, cette possibilité, qui permet, dans le cadre des programmes de surveillance fondés sur l'E.O. 12333, d'accéder à des données en transit vers les États-Unis sans que cet accès fasse l'objet d'une quelconque surveillance judiciaire, n'encadre, en tout état de cause, pas de manière suffisamment claire et précise la portée d'une telle collecte en vrac de données à caractère personnel.

184 Il apparaît, dès lors, que ni l'article 702 du FISA ni l'E.O. 12333, lus en combinaison avec la PPD-28, ne correspondent aux exigences minimales attachées, en droit de l'Union, au principe de proportionnalité, si bien qu'il n'est pas permis de considérer que les programmes de surveillance fondés sur ces dispositions sont limités au strict nécessaire.

185 Dans ces conditions, les limitations de la protection des données à caractère personnel qui découlent de la réglementation interne des États-Unis portant sur l'accès et l'utilisation, par les autorités publiques américaines, de telles données transférées depuis l'Union vers les États-Unis, et que la Commission a évaluées dans la décision BPD, ne sont pas encadrées d'une manière à répondre à des exigences substantiellement équivalentes à celles requises, en droit de l'Union, à l'article 52, paragraphe 1, seconde phrase, de la Charte.

186 S'agissant, en second lieu, de l'article 47 de la Charte, qui participe également du niveau de protection requis au sein de l'Union et dont la Commission doit constater le respect avant que celle-ci adopte une décision d'adéquation au titre de l'article 45, paragraphe 1, du RGPD, il convient de rappeler que le premier alinéa de cet article 47 exige que toute personne dont les droits et les libertés garantis par le droit de l'Union ont été violés ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article. Aux termes du deuxième alinéa dudit article, toute personne a droit à ce que sa cause soit entendue par un tribunal indépendant et impartial.

187 Selon une jurisprudence constante, l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit. Ainsi, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte (arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 95 et jurisprudence citée).

188 À cet effet, l'article 45, paragraphe 2, sous a), du RGPD exige que, dans le cadre de son évaluation du caractère adéquat du niveau de protection assuré par un pays tiers, la Commission tienne compte, notamment, « [d]es recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées ». Le considérant 104 du RGPD souligne, à cet égard, que le pays tiers « devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités de protection des données des États membres » et précise que « les personnes concernées devraient se voir octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif et juridictionnel ».

189 L'existence de telles possibilités effectives de recours dans le pays tiers concerné revêt une importance particulière dans le contexte d'un transfert de données à caractère personnel vers ce pays tiers, dans la mesure où, ainsi qu'il ressort du considérant 116 du RGPD, les personnes concernées peuvent être confrontées à l'insuffisance des pouvoirs et des moyens des autorités administratives et judiciaires des États membres pour donner une suite utile à leurs réclamations fondées sur un traitement prétendument illégal, dans ce pays tiers, de leurs données ainsi transférées, ce qui est de nature à les contraindre à s'adresser aux autorités et aux juridictions nationales de ce même pays tiers.

190 En l'occurrence, la constatation opérée par la Commission dans la décision BPD, selon laquelle les États-Unis assurent un niveau de protection substantiellement équivalent à celui garanti à l'article 47 de la Charte, a été remise en cause au motif, notamment, que l'instauration du médiateur du bouclier de protection des données ne saurait pallier les lacunes constatées par la Commission elle-même en ce qui concerne la protection juridictionnelle des personnes dont les données à caractère personnel sont transférées vers ce pays tiers.

191 À cet égard, la Commission a relevé, au considérant 115 de la décision BPD, que, si « les personnes physiques, notamment les personnes concernées de l'[Union], disposent [...] d'un certain nombre de voies de recours lorsqu'elles ont fait l'objet d'une surveillance (électronique) illégale à des fins de sécurité nationale, il est également clair qu'au moins quelques bases juridiques pouvant être utilisées par les services de renseignement américains (comme l'E.O. 12333) ne sont pas couvertes ». Ainsi, s'agissant de l'E.O. 12333, elle a mis l'accent, audit considérant 115, sur l'absence de toute voie de recours. Or, selon la jurisprudence rappelée au point 187 du présent arrêt, une telle lacune dans la protection juridictionnelle à l'égard des ingérences liées aux programmes de renseignement fondés sur ce décret présidentiel fait obstacle à ce qu'il soit conclu, comme l'a fait la Commission dans la décision BPD, que le droit des États-Unis assure un niveau de protection substantiellement équivalent à celui garanti à l'article 47 de la Charte.

192 Par ailleurs, en ce qui concerne tant les programmes de surveillance fondés sur l'article 702 du FISA que ceux fondés sur l'E.O. 12333, il a été relevé aux points 181 et 182 du présent arrêt que ni la PPD-28 ni l'E.O. 12333 ne confèrent aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux, si bien que ces personnes ne disposent pas d'un droit de recours effectif.

193 La Commission a toutefois constaté, aux considérants 115 et 116 de la décision BPD, que, en raison de l'existence du mécanisme de médiation mis en place par les autorités américaines, tel que décrit dans la lettre adressée le 7 juillet 2016 par le secrétaire d'État américain à la commissaire européenne pour la justice, les consommateurs et l'égalité des genres, qui figure à l'annexe III de cette décision, et de la nature de la mission confiée au médiateur, en l'occurrence un « coordinateur principal de la diplomatie internationale en matière de technologie de l'information », les États-Unis pouvaient être regardés comme assurant un niveau de protection substantiellement équivalent à celui garanti à l'article 47 de la Charte.

194 L'examen de la question de savoir si le mécanisme de médiation visé par la décision BPD est effectivement de nature à pallier les limitations du droit à une protection juridictionnelle constatées par la Commission doit, conformément aux exigences qui découlent de l'article 47 de la Charte et de la jurisprudence rappelée au point 187 du présent arrêt, partir du principe que les justiciables doivent disposer de la possibilité d'exercer des voies de droit devant un tribunal indépendant et impartial afin d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données.

195 Or, dans la lettre évoquée au point 193 du présent arrêt, le médiateur du bouclier de protection des données, quoique décrit comme étant « indépendant des services de renseignement », a été présenté comme « [rendant] compte directement au secrétaire d'État qui veillera à ce que le médiateur remplisse sa mission en toute objectivité et à l'abri de toute influence inappropriée susceptible d'affecter la réponse qu'il devra donner ». Par ailleurs, outre le fait que, ainsi que la Commission l'a constaté au considérant 116 de cette décision, le médiateur est désigné par le secrétaire d'État et fait partie intégrante du département d'État des États-Unis, il n'existe, dans ladite décision, comme M. l'avocat général l'a relevé au point 337 de ses conclusions, aucune indication selon laquelle la révocation du médiateur ou l'annulation de sa nomination seraient assorties de garanties particulières, ce qui est de nature à mettre en cause l'indépendance du médiateur par rapport au pouvoir exécutif (voir, en ce sens, arrêt du 21 janvier 2020, Banco de Santander, C-274/14, EU:C:2020:17, points 60 et 63 ainsi que jurisprudence citée).

196 De même, ainsi que M. l'avocat général l'a souligné, au point 338 de ses conclusions, si le considérant 120 de la décision BPD fait état d'un engagement du gouvernement américain à ce que la composante concernée des services de renseignement soit tenue de corriger toute violation des normes applicables détectée par le médiateur du bouclier de protection des données, ladite décision ne comporte aucune

indication selon laquelle ce médiateur serait habilité à prendre des décisions contraignantes à l'égard de ces services et ne fait pas non plus état de garanties légales dont serait assorti cet engagement et dont pourraient se prévaloir les personnes concernées.

197 Dès lors, le mécanisme de médiation visé par la décision BPD ne fournit pas de voie de recours devant un organe qui offre aux personnes dont les données sont transférées vers les États-Unis des garanties substantiellement équivalentes à celles requises à l'article 47 de la Charte.

198 Partant, en constatant, à l'article 1er, paragraphe 1, de la décision BPD, que les États-Unis assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies dans ce pays tiers dans le cadre du bouclier de protection des données Union européenne-États-Unis, la Commission a méconnu les exigences résultant de l'article 45, paragraphe 1, du RGPD, lu à la lumière des articles 7, 8 et 47 de la Charte.

199 Il s'ensuit que l'article 1er de la décision BPD est incompatible avec l'article 45, paragraphe 1, du RGPD, lu à la lumière des articles 7, 8 et 47 de la Charte, et qu'il est de ce fait invalide.

200 L'article 1er de la décision BPD étant indissociable des articles 2 à 6 ainsi que des annexes de celle-ci, son invalidité a pour effet d'affecter la validité de cette décision dans son ensemble.

201 Eu égard à l'ensemble des considérations qui précèdent, il convient de conclure que la décision BPD est invalide.

202 S'agissant du point de savoir s'il convient de maintenir les effets de cette décision aux fins d'éviter la création d'un vide juridique (voir, en ce sens, arrêt du 28 avril 2016, Borealis Polyolefine e.a., C-191/14, C-192/14, C-295/14, C-389/14 et C-391/14 à C-393/14, EU:C:2016:311, point 106), il y a lieu de noter que, en tout état de cause, compte tenu de l'article 49 du RGPD, l'annulation d'une décision d'adéquation telle que la décision BPD n'est pas susceptible de créer un tel vide juridique. En effet, cet article établit, de manière précise, les conditions dans lesquelles des transferts de données à caractère personnel vers des pays tiers peuvent avoir lieu en l'absence d'une décision d'adéquation en vertu de l'article 45, paragraphe 3, dudit règlement ou de garanties appropriées au titre de l'article 46 du même règlement.

Sur les dépens

203 La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

1) L'article 2, paragraphes 1 et 2, 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 (règlement général sur la protection des données), doit être interprété en ce sens que relève du champ d'application de ce règlement un transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, nonobstant le fait que, au cours ou à la suite de ce transfert, ces données sont susceptibles d'être traitées par les autorités du pays tiers concerné à des fins de sécurité publique, de défense et de sûreté de l'État.

2) **L'article 46, paragraphe 1, et l'article 46, paragraphe 2, sous c), du règlement 2016/679 doivent être interprétés en ce sens que les garanties appropriées, les droits opposables et les voies de droit effectives requis par ces dispositions doivent assurer que les droits des personnes dont les données à caractère personnel sont transférées vers un pays tiers sur le fondement de clauses types de protection des données bénéficient d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union européenne par ce règlement, lu à la lumière de la charte des droits fondamentaux de l'Union européenne. À cet effet, l'évaluation du niveau de protection assuré dans le contexte d'un tel transfert doit, notamment, prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union européenne et le destinataire du transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel ainsi transférées, les éléments pertinents du système juridique de celui-ci, notamment ceux énoncés à l'article 45, paragraphe 2, dudit règlement.**

3) **L'article 58, paragraphe 2, sous f) et j), du règlement 2016/679 doit être interprété en ce sens que, à moins qu'il existe une décision d'adéquation valablement adoptée par la Commission européenne, l'autorité de contrôle compétente est tenue de suspendre ou d'interdire un transfert de données vers un pays tiers fondé sur des clauses types de protection des données adoptées par la Commission, lorsque cette autorité de contrôle considère, à la lumière de l'ensemble des circonstances propres à ce transfert, que ces clauses ne sont pas ou ne peuvent pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union, en particulier par les articles 45 et 46 de ce règlement et par la charte des droits fondamentaux, ne peut pas être assurée par d'autres moyens, à défaut pour le responsable du traitement ou son sous-traitant établis dans l'Union d'avoir lui-même suspendu le transfert ou d'avoir mis fin à celui-ci.**

4) **L'examen de la décision 2010/87/UE de la Commission, du 5 février 2010, relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, telle que modifiée par la décision d'exécution (UE) 2016/2297 de la Commission, du 16 décembre 2016, au regard des articles 7, 8 et 47 de la charte des droits fondamentaux n'a révélé aucun élément de nature à affecter la validité de cette décision.**

5) **La décision d'exécution (UE) 2016/1250 de la Commission, du 12 juillet 2016, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, est invalide.**

Signatures