ARRÊT DE LA COUR (grande chambre)

6 octobre 2015 (*)

«Renvoi préjudiciel – Données à caractère personnel – Protection des personnes physiques à l'égard du traitement de ces données – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 47 – Directive 95/46/CE – Articles 25 et 28 – Transfert de données à caractère personnel vers des pays tiers – Décision 2000/520/CE – Transfert de données à caractère personnel vers les États-Unis – Niveau de protection inadéquat – Validité – Plainte d'une personne physique dont les données ont été transférées depuis l'Union européenne vers les États-Unis – Pouvoirs des autorités nationales de contrôle»

Dans l'affaire C-362/14,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par la High Court (Haute Cour de justice, Irlande), par décision du 17 juillet 2014, parvenue à la Cour le 25 juillet 2014, dans la procédure

**Maximillian Schrems**

contre

**Data Protection Commissioner,**

en présence de:

**Digital Rights Ireland Ltd,**

LA COUR (grande chambre),

composée de M. V. Skouris, président, M. K. Lenaerts, vice-président, M. A. Tizzano, M^me^ R. Silva de Lapuerta, MM. T. von Danwitz (rapporteur) et S. Rodin, M^me^ K. Jürimäe, présidents de chambre, MM. A. Rosas, E. Juhász, A. Borg Barthet, J. Malenovský, D. Šváby, M^me^ M. Berger, MM. F. Biltgen et C. Lycourgos, juges,

avocat général: M. Y. Bot,

greffier: M^me^ L. Hewlett, administrateur principal,

vu la procédure écrite et à la suite de l'audience du 24 mars 2015,

considérant les observations présentées:

– pour M. Schrems, par M. N. Travers, SC, M. P. O'Shea, BL, et M. G. Rudden, solicitor, ainsi que par M^e^ H. Hofmann, Rechtsanwalt,

– pour le Data Protection Commissioner, par M. P. McDermott, BL, M^me^ S. More O'Ferrall et M. D. Young, solicitors,

– pour Digital Rights Ireland Ltd, par M. F. Crehan, BL, ainsi que par MM. S. McGarr et E. McGarr, solicitors,

– pour l'Irlande, par MM. A. Joyce et B. Counihan ainsi que par M^me^ E. Creedon, en qualité d'agents, assistés de M. D. Fennelly, BL,

– pour le gouvernement belge, par M. J.-C. Halleux et M^me^ C. Pochet, en qualité d'agents,

– pour le gouvernement tchèque, par MM. M. Smolek et J. Vláčil, en qualité d'agents,

– pour le gouvernement italien, par M^me^ G. Palmieri, en qualité d'agent, assistée de M. P. Gentili, avvocato dello Stato,

– pour le gouvernement autrichien, par MM. G. Hesse et G. Kunnert, en qualité d'agents,

– pour le gouvernement polonais, par M^mes^ M. Kamejsza et M. Pawlicka ainsi que par M. B. Majczyna, en qualité d'agents,

– pour le gouvernement slovène, par M^mes^ A. Grum et V. Klemenc, en qualité d'agents,

– pour le gouvernement du Royaume-Uni, par M. L. Christie et M^me^ J. Beeko, en qualité d'agents, assistés de M. J. Holmes, barrister,

– pour le Parlement européen, par MM. D. Moore et A. Caiola ainsi que par M^me^ M. Pencheva, en qualité d'agents,

– pour la Commission européenne, par MM. B. Schima, B. Martenczuk et B. Smulders ainsi que par M^me^ J. Vondung, en qualité d'agents,

– pour le Contrôleur européen de la protection des données (CEPD), par MM. C. Docksey, A. Buchta et V. Pérez Asinari, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 23 septembre 2015,

rend le présent

**Arrêt**

1 La demande de décision préjudicielle porte sur l'interprétation, au regard des articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»), des articles 25, paragraphe 6, et 28 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 L 281, p. 31), telle que modifiée par le règlement (CE) n° 1882/2003 du Parlement européen et du Conseil, du 29 septembre 2003 (JO L 284, p. 1, ci-après la «directive 95/46»), ainsi que, en substance, sur la validité de 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 L 215, p. 7).

2 Cette demande a été présentée dans le cadre d'un litige opposant M. Schrems au Data Protection Commissioner (commissaire à la protection des données, ci-après le «commissaire») au sujet du refus de ce dernier d'enquêter sur une plainte introduite par M. Schrems en raison du fait que Facebook Ireland Ltd (ci-après «Facebook Ireland») transfère aux États-Unis les données à caractère personnel de ses utilisateurs et les conserve sur des serveurs situés dans ce pays.

## Le cadre juridique

*La directive 95/46*

3 Les considérants 2, 10, 56, 57, 60, 62 et 63 de la directive 95/46 sont libellés comme suit:

«(2) [...] les systèmes de traitement de données sont au service de l'homme; [...] ils doivent, quelle que soit la nationalité ou la résidence des personnes physiques, respecter

les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au [...] bien-être des individus;

[...]

(10) [...] l'objet des législations nationales relatives au traitement des données à caractère personnel est d'assurer le respect des droits et libertés fondamentaux, notamment du droit à la vie privée reconnu également dans l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[, signée à Rome le 4 novembre 1950,] et dans les principes généraux du droit communautaire; […] pour cette raison, le rapprochement de ces législations ne doit pas conduire à affaiblir la protection qu'elles assurent mais doit, au contraire, avoir pour objectif de garantir un niveau élevé de protection dans la Communauté;

[...]

(56) [...] des flux transfrontaliers de données à caractère personnel sont nécessaires au développement du commerce international; [...] la protection des personnes garantie dans la Communauté par la présente directive ne s'oppose pas aux transferts de données à caractère personnel vers des pays tiers assurant un niveau de protection adéquat; [...] le caractère adéquat du niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts;

(57) [...] en revanche, [...] lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit;

[...]

(60) [...] en tout état de cause, les transferts vers les pays tiers ne peuvent être effectués que dans le plein respect des dispositions prises par les États membres en application de la présente directive, et notamment de son article 8;

[...]

(62) [...] l'institution, dans les États membres, d'autorités de contrôle exerçant en toute indépendance leurs fonctions est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel;

(63) [...] ces autorités doivent être dotées des moyens nécessaires à l'exécution de leurs tâches, qu'il s'agisse des pouvoirs d'investigation et d'intervention, en particulier lorsque les autorités sont saisies de réclamations, ou du pouvoir d'ester en justice; [...]»

4 Les articles 1er, 2, 25, 26, 28 et 31 de la directive 95/46 disposent:

*«Article premier*

Objet de la directive

1. Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

[...]

*Article 2*

Définitions

Aux fins de la présente directive, on entend par:

a) ‘données à caractère personnel’: toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d’identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale;

b) ‘traitement de données à caractère personnel’ (traitement): toute opération ou ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l’enregistrement, l’organisation, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l’interconnexion, ainsi que le verrouillage, l’effacement ou la destruction;

[...]

d) ‘responsable du traitement’: la personne physique ou morale, l’autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d’autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire;

[...]

*Article 25*

Principes

1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l’objet d’un traitement, ou destinées à faire l’objet d’un traitement après leur transfert, 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; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d’origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.

3. Les États membres et la Commission s’informent mutuellement des cas dans lesquels ils estiment qu’un pays tiers n’assure pas un niveau de protection adéquat au sens du paragraphe 2.

4. Lorsque la Commission constate, conformément à la procédure prévue à l’article 31 paragraphe 2, qu’un pays tiers n’assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les États membres prennent les mesures nécessaires en vue d’empêcher tout transfert de même nature vers le pays tiers en cause.

5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4.

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.

*Article 26*

Dérogations

1. Par dérogation à l'article 25 et sous réserve de dispositions contraires de leur droit national régissant des cas particuliers, les États membres prévoient qu'un transfert 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 peut être effectué, à condition que:

a) la personne concernée ait indubitablement donné son consentement au transfert envisagé

ou

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

ou

c) le transfert soit nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers

ou

d) le transfert soit nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice

ou

e) le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée

ou

f) le transfert intervienne au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

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.

3. L'État membre informe la Commission et les autres États membres des autorisations qu'il accorde en application du paragraphe 2.

En cas d'opposition exprimée par un autre État membre ou par la Commission et dûment justifiée au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, la Commission arrête les mesures appropriées, conformément à la procédure prévue à l'article 31, paragraphe 2.

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

[...]

*Article 28*

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente directive.

Ces autorités exercent en toute indépendance les missions dont elles sont investies.

2. Chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel.

3. 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.

Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

4. Chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande.

Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 de la présente directive sont d'application. La personne est à tout le moins informée de ce qu'une vérification a eu lieu.

[...]

6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre.

[...]

*Article 31*

[...]

2. Dans le cas où il est fait référence au présent article, les articles 4 et 7 de la décision 1999/468/CE [du Conseil, du 28 juin 1999, fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission (JO L 184, p. 23)] s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci.

[...]»

*La décision 2000/520*

5 La décision 2000/520 a été adoptée par la Commission sur le fondement de l'article 25, paragraphe 6, de la directive 95/46.

6 Les considérants 2, 5 et 8 de cette décision sont libellés comme suit:

«(2) La Commission peut constater qu'un pays tiers assure un niveau de protection adéquat. Dans ce cas, des données à caractère personnel peuvent être transférées sans que des garanties supplémentaires soient nécessaires.

[...]

(5) Le niveau de protection adéquat pour le transfert de données de la Communauté vers les États-Unis d'Amérique, reconnu conformément à la présente décision, devrait être obtenu si les organisations respectent les "principes de la 'sphère de sécurité' relatifs à la protection de la vie privée" (ci-après dénommés 'les principes') et les 'questions souvent posées' 'frequently asked questions' (FAQ) qui fournissent des orientations pour la mise en œuvre des principes publiés par le gouvernement des États-Unis le 21 juillet 2000. En outre, les organisations devraient divulguer leurs règles de confidentialité et relever de la compétence de la Commission fédérale du commerce [Federal Trade Commission (FTC)] au titre de la section 5 du Federal Trade Commission Act qui interdit les manœuvres et les pratiques déloyales ou frauduleuses dans le domaine du commerce, ou de tout autre organisme officiel assurant efficacement la mise en œuvre des principes conformément aux FAQ.

[...]

(8) Dans un souci de transparence et en vue de permettre aux autorités compétentes des États membres d'assurer la protection des individus en ce qui concerne le traitement des données à caractère personnel, il est nécessaire d'indiquer dans la décision dans quelles circonstances exceptionnelles la suspension de certains flux de données peut être justifiée, même si le niveau de protection fourni a été jugé adéquat.»

7 Aux termes des articles 1er à 4 de la décision 2000/520:

*«Article premier*

1. Aux fins de l'article 25 de la directive 95/46/CE, pour toutes les activités rentrant dans le domaine d'application de ladite directive, il est considéré que les "principes de la 'sphère de sécurité' relatifs à la protection de la vie privée" (ci-après dénommés 'les principes visés à l'annexe I de la présente décision'), appliqués conformément aux orientations fournies par les 'questions souvent posées' ['frequently asked questions' (FAQ)] publiées le 21 juillet 2000 par le ministère du commerce des États-Unis d'Amérique, visées à l'annexe II de la présente décision, assurent un niveau adéquat de protection des données à caractère personnel transférées depuis la Communauté vers des organisations établies aux États-Unis compte tenu des documents suivants émis par le ministère du commerce des États-Unis:

a) une étude relative à la mise en œuvre des principes de la sphère de sécurité, visée à l'annexe III;

b) un aide-mémoire sur la réparation des préjudices subis par suite d'atteintes à la vie privée et sur les autorisations explicites prévues par le droit américain, visé à l'annexe IV;

c) une lettre de la Commission fédérale du commerce, visée à l'annexe V;

d) une lettre du ministère des transports des États-Unis, visée à l'annexe VI.

2. En ce qui concerne chaque transfert de données, les conditions suivantes doivent être remplies:

a) l'organisation destinataire des données s'est clairement et publiquement engagée à observer les principes mis en œuvre conformément aux FAQ et

b) l'organisation est soumise aux pouvoirs légaux d'un organe administratif américain énuméré à l'annexe VII de la présente décision, habilité à instruire des plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées, quel que soit leur pays de résidence ou leur nationalité, en cas de non-respect des principes mis en œuvre conformément aux FAQ.

3. Les conditions indiquées au paragraphe 2 sont considérées comme remplies par chaque organisation qui a déclaré son adhésion aux principes mis en œuvre conformément aux FAQ à compter de la date à laquelle elle avise le ministère américain du commerce (ou son représentant) de la divulgation de l'engagement visé au paragraphe 2, point a), et de l'identité de l'organe administratif visé au paragraphe 2, point b).

*Article 2*

La présente décision concerne uniquement le caractère adéquat de la protection fournie aux États-Unis par les principes mis en œuvre conformément aux FAQ en vue de répondre aux exigences de l'article 25, paragraphe 1, de la directive 95/46/CE et n'affecte pas l'application d'autres dispositions de ladite directive qui se rapportent au traitement de données à caractère personnel dans les États membres, et notamment de son article 4.

*Article 3*

1. Sans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées en application de dispositions autres que celles de l'article 25 de la directive 95/46/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour suspendre les flux de données vers une organisation adhérant aux principes mis en œuvre conformément aux FAQ afin de protéger les individus en ce qui concerne le traitement de leurs données personnelles, et ce dans les cas:

a) où l'organe administratif américain visé à l'annexe VII de la présente décision, ou une instance indépendante de recours au sens du point a) du principe d'application visé à l'annexe I de la présente décision, a constaté que l'organisation viole les principes mis en œuvre conformément aux FAQ ou

b) où il est fort probable que les principes sont violés; où il y a tout lieu de croire que l'instance d'application concernée ne prend pas ou ne prendra pas en temps voulu les mesures qui s'imposent en vue de régler l'affaire en question; où la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves; et où les autorités compétentes des États membres se sont raisonnablement efforcées, compte tenu des circonstances, d'avertir l'organisation et de lui donner la possibilité de répondre.

La suspension cesse dès que le respect des principes mis en œuvre conformément aux FAQ est assuré et que les autorités compétentes de la Communauté en sont avisées.

2. Les États membres informent sans tarder la Commission de l'adoption de mesures fondées sur le paragraphe 1.

3. Les États membres et la Commission s'informent aussi mutuellement des cas dans lesquels les organismes chargés de faire respecter les principes mis en œuvre conformément aux FAQ aux États-Unis ne parviennent pas à s'acquitter de leur tâche.

4. Si les informations recueillies en application des paragraphes 1, 2 et 3 montrent qu'un quelconque organisme chargé de faire respecter les principes mis en œuvre conformément aux FAQ aux États-Unis ne remplit pas efficacement sa mission, la Commission informe le ministère américain du commerce et, si nécessaire, propose un projet des mesures à prendre, conformément à la procédure visée à l'article 31 de la directive 95/46/CE, en vue d'abroger ou de suspendre la présente décision ou d'en limiter la portée.

*Article 4*

1. La présente décision peut être adaptée à tout moment à la lumière de l'expérience acquise durant sa mise en œuvre et/ou si le niveau de protection assuré par les principes et les FAQ est dépassé par les exigences du droit américain. La Commission évalue, en tout état de cause, l'application de la présente décision, sur la base des informations disponibles, trois ans après sa notification aux États membres et communique au comité institué au titre de l'article 31 de la directive 95/46/CE toute constatation pertinente, y compris tout élément susceptible d'influer sur l'évaluation selon laquelle les dispositions de l'article 1er de la présente décision assurent un niveau de protection adéquat au sens de l'article 25 de la directive 95/46/CE et toute information montrant que la présente décision est appliquée de manière discriminatoire.

2. La Commission présente, si nécessaire, un projet des mesures à prendre conformément à la procédure visée à l'article 31 de la directive 95/46/CE.»

8 L'annexe I de la décision 2000/520 est ainsi libellée:

«Principes de la 'sphère de sécurité' relatifs à la protection de la vie privée

publiés par le ministère américain du commerce le 21 juillet 2000

[...]

[...] le ministère américain du commerce publie le présent document ('les principes') ainsi que les 'questions souvent posées' (FAQ) en vertu de son autorité légale afin de stimuler, de promouvoir et de développer le commerce international. Les principes ont été élaborés en concertation avec les entreprises et le grand public dans le but de faciliter le commerce et les relations d'affaires entre les États-Unis et l'Union européenne. Ils sont exclusivement destinés aux organisations américaines recevant des données à caractère personnel en provenance de l'Union européenne et doivent permettre à ces organisations de remplir les conditions relatives à la 'sphère de sécurité' de façon à bénéficier de la présomption de 'niveau de protection adéquat' que prévoit celle-ci. Comme les principes n'ont été conçus que pour servir cet objectif spécifique, leur adoption à d'autres fins peut s'avérer inadéquate. [...]

Toute organisation est libre de remplir ou non les conditions relatives à la 'sphère de sécurité' et dispose de plusieurs moyens pour s'y conformer. [...]

L'adhésion aux principes peut être limitée par: a) les exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect des lois des États-Unis; b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir; c) les exceptions ou les dérogations prévues par la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables. Conformément à l'objectif d'un renforcement de la protection de la vie privée, les organisations doivent s'efforcer d'appliquer ces principes de manière complète et transparente, y compris en indiquant – dans leurs codes de protection de la vie privée – dans quels domaines les exceptions visées au point b) ci-dessus s'appliqueront de façon régulière. Pour la même raison, lorsque les principes et/ou les lois des États-Unis permettent aux

organisations de faire un choix, celles-ci sont invitées à opter, dans la mesure du possible, pour le niveau de protection le plus élevé.

[...]»

9 L'annexe II de la décision 2000/520 est rédigée comme suit:

«Questions souvent posées (FAQ)

[...]

FAQ 6 – Autocertification

Q: *Comment une organisation autocertifie-t-elle qu'elle adhère aux principes de la 'sphère de sécurité'?*

R: Les avantages afférents à la 'sphère de sécurité' sont acquis à partir de la date à laquelle une organisation autocertifie au ministère américain du commerce (ou à la personne désignée par celui-ci) qu'elle adhère aux principes conformément aux modalités ci-dessous.

Pour autocertifier son adhésion à la 'sphère de sécurité', une organisation peut remettre au ministère américain du commerce (ou à la personne désignée par celui-ci) une lettre signée d'un cadre de ladite organisation contenant au moins les informations suivantes:

1) le nom de l'organisation, son adresse postale, son adresse électronique, ses numéros de téléphone et de télécopieur;

2) une description des activités de l'organisation relativement aux informations à caractère personnel en provenance de l'Union européenne;

3) une description des dispositions de protection de la vie privée appliquées par l'organisation auxdites informations, précisant: a) le lieu où le texte de ces dispositions peut être consulté par le public; b) la date de mise en œuvre de ces dispositions; c) le service à contacter en cas de plainte, pour des demandes d'accès et pour toute autre question relevant de la 'sphère de sécurité'; d) le nom de l'instance réglementaire spécifique qui est chargée de statuer sur les plaintes déposées, le cas échéant, contre l'organisation pour pratiques déloyales ou frauduleuses et pour infraction aux lois ou aux réglementations régissant la protection de la vie privée (et qui est mentionnée dans l'annexe aux principes); e) l'intitulé de tout programme relatif à la protection de la vie privée auquel participe l'organisation; f) la méthode de vérification (par exemple, en interne ou par des tiers) [...] et g) l'instance de recours indépendante qui pourra instruire les plaintes non résolues.

Une organisation peut étendre les avantages de la 'sphère de sécurité' à des informations de type 'ressources humaines' qui sont transférées depuis l'Union européenne afin d'être utilisées dans le cadre de relations de travail, lorsque l'une des instances réglementaires mentionnées dans l'annexe aux principes est compétente pour statuer sur les plaintes déposées, le cas échéant, contre ladite organisation dans le domaine des informations de type 'ressources humaines'. [...]

Le ministère (ou la personne désignée par celui-ci) tiendra une liste de l'ensemble des organisations qui suivent cette procédure, garantissant ainsi les avantages de la 'sphère de sécurité', et mettra à jour cette liste sur la base des lettres et notifications reçues chaque année en conformité avec la FAQ 11. [...]

[...]

FAQ 11 — Résolution des litiges et application des décisions

Q: *Comment les exigences en matière de résolution des litiges formulées dans le principe d'application doivent-elles être mises en œuvre et comment le non-respect persistant des principes de la part d'une organisation sera-t-il traité?*

R: Le principe d'application définit les exigences sur lesquelles repose la mise en œuvre de la 'sphère de sécurité'. La FAQ sur la vérification (FAQ 7) explique la manière de satisfaire les exigences énoncées au point b) du principe. La présente FAQ 11 traite des points a) et c), qui nécessitent tous deux des instances de recours indépendantes. Ces instances peuvent prendre différentes formes, mais doivent répondre aux exigences du principe d'application. Les organisations participant à la 'sphère de sécurité' peuvent les satisfaire: 1) en participant à des programmes du secteur privé en matière de protection de la vie privée intégrant dans leurs règles les principes de la 'sphère de sécurité' et comportant des mécanismes de mise en œuvre efficaces, de même nature que ceux qui sont décrits dans le principe d'application; 2) en se conformant aux instructions des organes légaux ou statutaires de surveillance qui assurent le traitement des plaintes de particuliers et la résolution des litiges; 3) en s'engageant à coopérer avec les autorités chargées de la protection des données au sein de la Communauté européenne ou avec leurs représentants autorisés. La présente liste a valeur indicative et n'est pas restrictive. Le secteur privé peut concevoir d'autres mécanismes de mise en application, pour autant que ceux-ci répondent aux exigences du principe d'application et des FAQ. Il convient de remarquer que les exigences du principe d'application s'ajoutent à l'exigence énoncée au paragraphe 3 de l'introduction aux principes, selon laquelle les initiatives d'autoréglementation doivent être exécutoires conformément à la section 5 du Federal Trade Commission Act ou à une loi similaire.

Instances de recours

Les consommateurs devraient être encouragés à soumettre toute plainte éventuelle à l'organisation concernée avant de faire appel à des instances de recours indépendantes. [...]

[...]

Action de la FTC

La FTC s'est engagée à examiner en priorité les cas soumis par les organisations d'autoréglementation, telles que BBBOnline et TRUSTe, ainsi que par les États membres de l'Union européenne en ce qui concerne le non-respect des principes de la 'sphère de sécurité', afin de déterminer s'il y a eu une violation de la section 5 du Federal Trade Commission Act, qui interdit les actions ou pratiques déloyales ou frauduleuses dans le commerce. [...]

[...]»

10 Aux termes de l'annexe IV de la décision 2000/520:

«Confidentialité et dommages-intérêts, autorisations légales et fusions et acquisitions suivant la législation des États-Unis

Le présent document répond à la demande de la Commission européenne visant à la clarification de la législation américaine en ce qui concerne a) les demandes de compensations pour violations de la confidentialité, b) 'les autorisations explicites' prévues par la législation américaine pour utilisation d'informations à caractère personnel d'une façon contredisant les principes de la 'sphère de sécurité' et c) l'effet des fusions et acquisitions sur les obligations contractées conformément aux principes de la sphère de sécurité.

[...]

B. Autorisations légales explicites

Les principes de la 'sphère de sécurité' contiennent une exception lorsque le droit écrit, les réglementations ou la jurisprudence créent 'des obligations conflictuelles ou des autorisations

explicites, à condition que, dans l'exercice de ces autorisations, une organisation puisse démontrer que sa non-conformité aux principes est limitée dans la mesure nécessaire à la satisfaction des intérêts légitimes principaux favorisés par cette autorisation'. Il est clair que lorsque la législation américaine impose une obligation conflictuelle, les organisations américaines faisant ou non partie de la 'sphère de sécurité' doivent se plier à cette législation. Quant aux autorisations explicites, si les principes de la 'sphère de sécurité' sont destinés à combler le fossé séparant les régimes américain et européen de protection de la vie privée, nous devons respecter les prérogatives législatives de nos législateurs élus. L'exception limitée au strict respect des principes de la 'sphère de sécurité' s'efforce d'établir un équilibre pour tenir compte des intérêts légitimes de chaque partie.

L'exception est limitée aux cas où existe une autorisation explicite. Par conséquent, en tant que cas limite, la législation, la réglementation ou la décision de justice pertinente doivent autoriser affirmativement une conduite particulière des organisations adhérant à la 'sphère de sécurité'. En d'autres termes, l'exception ne s'appliquera pas lorsque la loi est silencieuse. De surcroît, l'exception ne s'appliquera que si l'autorisation explicite contredit le respect des principes de la 'sphère de sécurité'. Même dans ces conditions, l'exception 'est limitée dans la mesure nécessaire à la satisfaction des intérêts légitimes principaux favorisés par cette autorisation'. À titre d'illustration, lorsque la loi autorise simplement une société à fournir des informations à caractère personnel à des organismes gouvernementaux, l'exception ne s'appliquera pas. À l'inverse, lorsque la loi autorise spécifiquement la société à fournir des informations à caractère personnel à des organismes gouvernementaux sans le consentement de la personne, cela constituerait une 'autorisation explicite' d'agir d'une manière contredisant les principes de la 'sphère de sécurité'. Par ailleurs, les exceptions spécifiques aux exigences de notification et de consentement entreraient dans le cadre de l'exception (car cela équivaudrait à une autorisation spécifique de révéler l'information sans notification et consentement). Par exemple, un texte de loi autorisant les médecins à fournir les dossiers médicaux de leurs patients aux fonctionnaires sanitaires sans l'autorisation préalable de ces patients pourrait permettre une exception aux principes de notification et de choix. Cette autorisation ne laisserait pas la possibilité à un médecin de fournir les mêmes dossiers médicaux aux caisses de maladie ou aux laboratoires de recherche pharmaceutique, car cela irait au-delà de l'objectif autorisé par la loi et donc au-delà du champ de l'exception [...]. L'autorisation en question peut être une autorisation 'autonome' de faire des choses déterminées avec des informations personnelles, mais, comme l'illustrent les exemples ci-dessous, il est plus probable qu'il s'agisse d'une exception à une loi plus large qui interdit la collecte, l'utilisation ou la divulgation d'informations à caractère personnel.

[...]»

*La communication COM(2013) 846 final*

11 Le 27 novembre 2013, la Commission a adopté la communication au Parlement européen et au Conseil, intitulée «Rétablir la confiance dans les flux des données entre l'Union européenne et les États-Unis d'Amérique» [COM(2013) 846 final, ci-après la «communication COM(2013) 846 final»]. Cette communication était accompagnée d'un rapport, également daté du 27 novembre 2013, contenant les «conclusions des coprésidents de l'Union européenne du groupe de travail ad hoc Union européenne-États-Unis sur la protection des données à caractère personnel» («Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection»). Ce rapport avait été élaboré, ainsi que l'indique son point 1, en coopération avec les États-Unis d'Amérique à la suite de la révélation de l'existence, dans ce pays, de plusieurs programmes de surveillance incluant la collecte et le traitement à grande échelle de données à caractère personnel. Ledit rapport contenait notamment une analyse détaillée de l'ordre juridique des États-Unis en ce qui concerne, en particulier, les bases légales autorisant l'existence de programmes de surveillance ainsi que la collecte et le traitement de données à caractère personnel par des autorités américaines.

12 Au point 1 de la communication COM(2013) 846 final, la Commission a précisé que «les échanges commerciaux font l'objet de la décision [2000/520]», ajoutant que «[c]ette décision fournit une base juridique aux fins du transfert de données à caractère personnel de l'Union européenne vers des entreprises établies aux États-Unis qui adhèrent aux principes de la sphère de sécurité». En outre, à ce même point 1, la Commission a mis en exergue l'importance croissante des flux de données à caractère personnel, liée notamment au développement de l'économie numérique, celui-ci ayant en effet «entraîné une croissance

exponentielle de la quantité, de la qualité, de la diversité et de la nature des activités de traitement de données».

13 Au point 2 de cette communication, la Commission a fait observer que «le niveau de protection des données à caractère personnel des citoyens de l'[Union] qui sont transférées vers les États-Unis dans le cadre de la sphère de sécurité suscite de plus en plus d'inquiétude» et que «[l]e caractère volontaire et déclaratoire de la sphère de sécurité a attiré une attention accrue sur sa transparence et sa mise en œuvre».

14 En outre, elle a indiqué, à ce même point 2, que «[l]es données à caractère personnel des citoyens de l'[Union] transférées aux États-Unis dans le cadre de la sphère de sécurité peuvent, en effet, être consultées et traitées par les autorités américaines d'une manière incompatible avec les motifs pour lesquels elles avaient été initialement collectées dans l'[Union] et avec les finalités de leur transfert vers les États-Unis» et que «[l]a majorité des entreprises américaines du secteur de l'internet, qui semblent être plus directement concernées par [les] programmes [de surveillance], sont certifiées dans le cadre de la sphère de sécurité».

15 Au point 3.2 de la communication COM(2013) 846 final, la Commission a relevé l'existence d'un certain nombre d'insuffisances quant à la mise en œuvre de la décision 2000/520. Elle y a fait état, d'une part, de ce que des entreprises américaines certifiées ne respectaient pas les principes visés à l'article 1er, paragraphe 1, de la décision 2000/520 (ci-après les «principes de la sphère de sécurité») et que des améliorations devaient être apportées à cette décision concernant «les lacunes structurelles liées à la transparence et au contrôle de la mise en œuvre, les principes matériels de la sphère de sécurité et l'application de la dérogation pour motif de sécurité nationale». D'autre part, elle a fait observer que la «sphère de sécurité sert également d'interface pour le transfert de données à caractère personnel de citoyens européens, de l'[Union] vers les États-Unis, par les entreprises qui sont tenues de remettre des données aux agences américaines de renseignement dans le cadre de programmes américains de collecte de renseignements».

16 La Commission a conclu, à ce même point 3.2, que, si, «[c]ompte tenu des insuffisances recensées, la sphère de sécurité ne peut plus être mise en œuvre telle qu'elle l'est actuellement, [...] sa suppression porterait [toutefois] préjudice aux intérêts des entreprises qui en sont membres dans l'[Union] et aux États-Unis». Enfin, toujours audit point 3.2, la Commission a ajouté qu'elle entendait «entamer de toute urgence un dialogue avec les autorités américaines afin d'examiner les lacunes mises en évidence».

*La communication COM(2013) 847 final*

17 À cette même date du 27 novembre 2013, la Commission a adopté la communication au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire [COM(2013) 847 final, ci-après la «communication COM(2013) 847 final»]. Ainsi qu'il ressort de son point 1, cette communication était fondée, notamment, sur les informations reçues par le groupe de travail ad hoc Union européenne-États-Unis et faisait suite à deux rapports d'analyse d'impact de la Commission publiés, respectivement, en 2002 et en 2004.

18 Le point 1 de cette communication précise que le fonctionnement de la décision 2000/520 «repose sur les engagements pris par les entreprises qui décident d'y souscrire et l'autocertification de celles-ci» et ajoute que «[l]'adhésion revêt un caractère volontaire, mais [que] les règles sont contraignantes pour les entreprises qui y souscrivent».

19 En outre, il ressort du point 2.2 de la communication COM(2013) 847 final que, à la date du 26 septembre 2013, 3 246 entreprises, relevant de nombreux secteurs de l'économie et des services, étaient certifiées. Ces entreprises fournissaient, principalement, des services sur le marché intérieur de l'Union, en particulier dans le secteur de l'Internet, et une partie d'entre elles étaient des entreprises de l'Union ayant des filiales aux États-Unis. Certaines de ces entreprises traitaient les données de leurs salariés employés en Europe, lesquelles étaient transférées vers ce pays à des fins de gestion des ressources humaines.

20 À ce même point 2.2, la Commission a souligné que «tout défaut [de transparence] et toute lacune [dans la mise en œuvre] du côté américain [avaient] pour effet de reporter la responsabilité sur les autorités européennes chargées de la protection des données et sur les entreprises qui appliquent ce régime».

21 Il ressort, notamment, des points 3 à 5 et 8 de la communication COM(2013) 847 final que, en pratique, un nombre important d'entreprises certifiées ne respectaient pas, ou pas entièrement, les principes de la sphère de sécurité.

22 En outre, au point 7 de cette communication, la Commission a fait état de ce que «toutes les entreprises participant au programme PRISM [programme de collecte de renseignements à grande échelle], qui permettent aux autorités américaines d'avoir accès à des données stockées et traitées aux États-Unis semblent être certifiées dans le cadre de la sphère de sécurité» et que celle-ci «est donc devenue l'une des voies par lesquelles les autorités américaines du renseignement ont accès à la collecte des données à caractère personnel initialement traitées dans l'[Union]». À cet égard, la Commission a constaté, au point 7.1 de ladite communication, «qu'un certain nombre de bases juridiques prévues par la législation américaine permettent la collecte et le traitement à grande échelle des données à caractère personnel stockées ou traitées par des sociétés établies aux États-Unis» et que «[c]es programmes étant à grande échelle, il est possible que les données transférées dans le cadre de la sphère de sécurité soient accessibles aux autorités américaines et traitées par celles-ci au-delà de ce qui est strictement nécessaire et proportionné à la protection de la sécurité nationale, comme le prévoit l'exception énoncée dans la décision [2000/520]».

23 Au point 7.2 de la communication COM(2013) 847 final, intitulé «Limitations et voies de droit», la Commission a souligné que «ce sont principalement les ressortissants des États-Unis et les personnes qui y résident légalement qui bénéficient des garanties prévues en droit américain» et qu'«[i]l n'existe, en outre, aucune possibilité, que ce soit pour les personnes concernées de l'[Union] ou des États-Unis, d'obtenir l'accès, la rectification ou la suppression de données ou d'exercer des voies de droit administratives ou judiciaires si, dans le cadre des programmes de surveillance des États-Unis, des données à caractère personnel les concernant sont collectées et traitées ultérieurement».

24 Selon le point 8 de la communication COM(2013) 847 final, figuraient parmi les entreprises certifiées «les sociétés du web, telles que Google, Facebook, Microsoft, Apple et Yahoo», celles-ci ayant «des centaines de millions de clients en Europe» et transférant des données à caractère personnel vers les États-Unis aux fins de leur traitement.

25 La Commission a conclu, à ce même point 8, que «l'accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États-Unis soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États-Unis».

**Le litige au principal et les questions préjudicielles**

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

27 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.

28 Le 25 juin 2013, M. Schrems a saisi le commissaire d'une plainte par laquelle il demandait en substance à celui-ci d'exercer ses compétences statutaires en interdisant à Facebook Ireland de transférer ses données à caractère personnel vers les États-Unis. Il y faisait 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. M. Schrems se référait à cet égard aux révélations faites par M. Edward Snowden concernant les activités des services de renseignement des États-Unis, notamment celles de la National Security Agency (ci-après la «NSA»).

29 Considérant qu'il n'était pas tenu de procéder à une enquête sur les faits dénoncés par M. Schrems dans sa plainte, le commissaire a rejeté celle-ci comme étant dépourvue de fondement. Ce dernier a, en effet, estimé qu'il n'existait pas de preuves que la NSA ait accédé aux données à caractère personnel de l'intéressé. Le commissaire a ajouté que les griefs soulevés par M. Schrems dans sa plainte ne pouvaient être utilement avancés, puisque toute question relative au caractère adéquat de la protection des données à caractère personnel aux États-Unis devait être tranchée en conformité avec la décision 2000/520 et que, dans cette décision, la Commission avait constaté que les États-Unis d'Amérique assuraient un niveau adéquat de protection.

30 M. Schrems a introduit un recours devant la High Court (Haute Cour de justice) contre la décision en cause au principal. Après avoir examiné les preuves soumises par les parties au principal, cette juridiction a constaté que la surveillance électronique et l'interception des données à caractère personnel transférées depuis l'Union vers les États-Unis répondaient à des finalités nécessaires et indispensables à l'intérêt public. Toutefois, ladite juridiction a ajouté que les révélations de M. Snowden avaient démontré que la NSA et d'autres organes fédéraux avaient commis des «excès considérables».

31 Or, selon cette même juridiction, les citoyens de l'Union ne disposeraient d'aucun droit effectif à être entendus. La supervision des actions des services de renseignement serait effectuée dans le cadre d'une procédure secrète et non contradictoire. Une fois les données à caractère personnel transférées vers les États-Unis, la NSA et d'autres organes fédéraux, tels que le Federal Bureau of Investigation (FBI), pourraient accéder à ces données dans le cadre de la surveillance et des interceptions indifférenciées qu'ils pratiquent à grande échelle.

32 La High Court (Haute Cour de justice) a constaté que le droit irlandais interdit le transfert des données à caractère personnel hors du territoire national, à l'exception des cas où le pays tiers en cause assure un niveau de protection adéquat de la vie privée ainsi que des droits et libertés fondamentaux. L'importance des droits au respect de la vie privée et à l'inviolabilité du domicile, garantis par la Constitution irlandaise, exigerait que toute ingérence dans ces droits soit proportionnée et conforme aux exigences prévues par la loi.

33 Or, l'accès massif et indifférencié à des données à caractère personnel serait évidemment contraire au principe de proportionnalité et aux valeurs fondamentales protégées par la Constitution irlandaise. Pour que des interceptions de communications électroniques puissent être considérées comme conformes à cette Constitution, la preuve devrait être rapportée que ces interceptions présentent un caractère ciblé, que la surveillance de certaines personnes ou de certains groupes de personnes soit objectivement justifiée dans l'intérêt de la sécurité nationale ou de la répression de la criminalité et qu'il existe des garanties adéquates et vérifiables. Ainsi, selon la High Court (Haute Cour de justice), si l'affaire au principal devait être tranchée sur la base du seul droit irlandais, il conviendrait alors de constater que, compte tenu de l'existence d'un doute sérieux sur le fait que les États-Unis d'Amérique assurent un niveau de protection adéquat des données à caractère personnel, le commissaire aurait dû procéder à une enquête sur les faits dénoncés par M. Schrems dans sa plainte et que c'est à tort qu'il a rejeté cette dernière.

34 Toutefois, la High Court (Haute Cour de justice) considère que cette affaire concerne la mise en œuvre du droit de l'Union au sens de l'article 51 de la Charte, de sorte que la légalité de la décision en cause au principal doit être appréciée au regard du droit de l'Union. Or, selon cette juridiction, la décision 2000/520 ne satisfait pas aux exigences découlant tant des articles 7 et 8 de la Charte que des principes énoncés par la Cour dans l'arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238). Le droit au respect de la vie privée, garanti par l'article 7 de la Charte et par les valeurs essentielles communes aux traditions des États membres, serait privé de toute portée si les pouvoirs publics étaient autorisés à accéder aux communications électroniques de manière aléatoire et généralisée sans aucune justification objective fondée sur des raisons de sécurité nationale ou de prévention de la criminalité, liées

spécifiquement aux individus concernés, et sans que ces pratiques soient entourées de garanties adéquates et vérifiables.

35 La High Court (Haute Cour de justice) observe, en outre, que M. Schrems, à l'occasion de son recours, dénonce en réalité la légalité du régime de la «sphère de sécurité» mis en place par la décision 2000/520 et dont procède la décision en cause au principal. Ainsi, même si M. Schrems n'a formellement contesté la validité ni de la directive 95/46 ni de la décision 2000/520, la question est posée, selon cette juridiction, de savoir si, du fait de l'article 25, paragraphe 6, de cette directive, le commissaire était lié par la constatation effectuée par la Commission dans cette décision, selon laquelle les États-Unis d'Amérique assurent un niveau de protection adéquat, ou si l'article 8 de la Charte autorisait le commissaire à s'affranchir, le cas échéant, d'une telle constatation.

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

«1) Eu égard aux articles 7, 8 et 47 de la Charte et sans préjudice des dispositions de l'article 25, paragraphe 6, de la directive 95/46, le Commissaire indépendant chargé d'appliquer la législation sur la protection des données saisi d'une plainte relative au transfert de données à caractère personnel vers un pays tiers (en l'occurrence vers les États-Unis), dont le plaignant soutient que le droit et les pratiques n'offriraient pas des protections adéquates à la personne concernée, est-il absolument lié par la constatation contraire de l'Union contenue dans la décision 2000/520?

2) Dans le cas contraire, peut-il ou doit-il mener sa propre enquête en s'instruisant de la manière dont les faits ont évolué depuis la première publication de la décision de la Commission?»

**Sur les questions préjudicielles**

37 Par ses questions préjudicielles, qu'il convient d'examiner conjointement, la juridiction de renvoi demande, en substance, si et dans quelle mesure l'article 25, paragraphe 6, de la directive 95/46, lu à la lumière des articles 7, 8 et 47 de la Charte, doit être interprété en ce sens qu'une décision adoptée au titre de cette disposition, telle que la décision 2000/520, par laquelle la Commission constate qu'un pays tiers assure un niveau de protection adéquat, fait obstacle à ce qu'une autorité de contrôle d'un État membre, au sens de l'article 28 de cette directive, puisse examiner la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant qui ont été transférées depuis un État membre vers ce pays tiers, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans celui-ci n'assurent pas un niveau de protection adéquat.

*Sur les pouvoirs des autorités nationales de contrôle, au sens de l'article 28 de la directive 95/46, en présence d'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de cette directive*

38 Il convient de rappeler, à titre liminaire, que les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptible de porter atteinte aux libertés fondamentales et, en particulier, au droit au respect de la vie privée doivent nécessairement être interprétées à la lumière des droits fondamentaux garantis par la Charte (voir arrêts Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 68; Google Spain et Google, C-131/12, EU:C:2014:317, point 68, ainsi que Ryneš, C-212/13, EU:C:2014:2428, point 29).

39 Il résulte de l'article 1er ainsi que des considérants 2 et 10 de la directive 95/46 que celle-ci vise à garantir non seulement une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit fondamental au respect de la vie privée à l'égard du traitement des données à caractère personnel, mais également un niveau élevé de protection de ces libertés et droits fondamentaux. L'importance tant du droit fondamental au respect de la vie privée, garanti par l'article 7 de la Charte, que du droit fondamental à la protection des données à caractère personnel, garanti par l'article 8 de celle-

ci, est en outre soulignée dans la jurisprudence de la Cour (voir arrêts Rijkeboer, C-553/07, EU:C:2009:293, point 47; Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 53, ainsi que Google Spain et Google, C-131/12, EU:C:2014:317, points 53, 66 et 74 et jurisprudence citée).

40 S'agissant des pouvoirs dont disposent les autorités de contrôle nationales à l'égard des transferts de données à caractère personnel vers des pays tiers, il convient de relever que l'article 28, paragraphe 1, de la directive 95/46 impose aux États membres d'instituer une ou plusieurs autorités publiques chargées de contrôler, en toute indépendance, le respect des règles de l'Union relatives à la protection des personnes physiques à l'égard du traitement de telles données. Cette exigence résulte également du droit primaire de l'Union, notamment de l'article 8, paragraphe 3, de la Charte et de l'article 16, paragraphe 2, TFUE (voir, en ce sens, arrêts Commission/Autriche, C-614/10, EU:C:2012:631, point 36, et Commission/Hongrie C-288/12, EU:C:2014:237, point 47).

41 La garantie d'indépendance des autorités nationales de contrôle vise à assurer l'efficacité et la fiabilité du contrôle du respect des dispositions en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel et doit être interprétée à la lumière de cet objectif. Elle a été établie en vue de renforcer la protection des personnes et des organismes qui sont concernés par les décisions de ces autorités. L'institution, dans les États membres, d'autorités de contrôle indépendantes constitue donc, ainsi que le relève le considérant 62 de la directive 95/46, un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel (voir arrêts Commission/Allemagne, C-518/07, EU:C:2010:125, point 25, ainsi que Commission/Hongrie C-288/12, EU:C:2014:237, point 48 et jurisprudence citée).

42 Pour garantir cette protection, les autorités nationales de contrôle doivent, notamment, assurer un juste équilibre entre, d'une part, le respect du droit fondamental à la vie privée et, d'autre part, les intérêts qui commandent une libre circulation des données à caractère personnel (voir, en ce sens, arrêts Commission/Allemagne, C-518/07, EU:C:2010:125, point 24, et Commission/Hongrie C-288/12, EU:C:2014:237, point 51).

43 À cet effet, ces autorités disposent d'un large éventail de pouvoirs et ceux-ci, énumérés de façon non exhaustive à l'article 28, paragraphe 3, de la directive 95/46, constituent autant de moyens nécessaires à l'exécution de leurs tâches, comme le souligne le considérant 63 de cette directive. Ainsi, lesdites autorités jouissent, notamment, de pouvoirs d'investigation, tels que celui de recueillir toutes les informations nécessaires à l'accomplissement de leur mission de contrôle, de pouvoirs effectifs d'intervention, tels que celui d'interdire temporairement ou définitivement un traitement de données, ou encore du pouvoir d'ester en justice.

44 Certes, il ressort de l'article 28, paragraphes 1 et 6, de la directive 95/46 que les pouvoirs des autorités nationales de contrôle concernent les traitements de données à caractère personnel effectués sur le territoire de l'État membre dont ces autorités relèvent, de sorte qu'elles ne disposent pas de pouvoirs, sur le fondement de cet article 28, à l'égard des traitements de telles données effectués sur le territoire d'un pays tiers.

45 Toutefois, 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 2, sous b), de la directive 95/46 (voir, en ce sens, arrêt Parlement/Conseil et Commission, C-317/04 et C-318/04, EU:C:2006:346, point 56) effectué sur le territoire d'un État membre. En effet, cette disposition définit le «traitement de données à caractère personnel» comme «toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel» et cite, à titre d'exemple, «la communication par transmission, diffusion ou toute autre forme de mise à disposition».

46 Le considérant 60 de la directive 95/46 précise que les transferts de données à caractère personnel vers les pays tiers ne peuvent être effectués que dans le plein respect des dispositions prises par les États membres en application de cette directive. À cet égard, le chapitre IV de ladite directive, dans lequel figurent les articles 25 et 26 de celle-ci, a institué un régime visant à assurer un contrôle par les États membres des transferts de données à caractère personnel vers les pays tiers. Ce régime est complémentaire du régime général mis

en place par le chapitre II de cette même directive prévoyant les conditions générales de licéité des traitements de données à caractère personnel (voir, en ce sens, arrêt Lindqvist, C-101/01, EU:C:2003:596, point 63).

47 Les autorités nationales de contrôle étant, conformément à l'article 8, paragraphe 3, de la Charte et à l'article 28 de la directive 95/46, chargées du contrôle du respect des règles de l'Union relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, chacune d'entre elles est donc 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 la directive 95/46.

48 Tout en reconnaissant, à son considérant 56, que des transferts de données à caractère personnel depuis les États membres vers des pays tiers sont nécessaires au développement du commerce international, la directive 95/46 pose comme principe, à son article 25, paragraphe 1, que de tels transferts ne peuvent avoir lieu que si ces pays tiers assurent un niveau de protection adéquat.

49 En outre, le considérant 57 de ladite directive précise que des transferts de données à caractère personnel vers des pays tiers n'assurant pas un niveau de protection adéquat doivent être interdits.

50 Afin de contrôler les transferts de données à caractère personnel vers les pays tiers en fonction du niveau de protection accordé à celles-ci dans chacun de ces pays, l'article 25 de la directive 95/46 impose une série d'obligations aux États membres et à la Commission. Il ressort, notamment, de cet article que la constatation selon laquelle un pays tiers assure ou n'assure pas un niveau de protection adéquat peut, comme l'a relevé M. l'avocat général au point 86 de ses conclusions, être effectuée soit par les États membres soit par la Commission.

51 La Commission peut adopter, sur le fondement de l'article 25, paragraphe 6, de la directive 95/46, une décision constatant qu'un pays tiers assure un niveau de protection adéquat. Une telle décision a, conformément au second alinéa de cette disposition, pour destinataires les États membres qui doivent prendre les mesures nécessaires pour se conformer à celle-ci. En vertu de l'article 288, quatrième alinéa, TFUE, elle a un caractère contraignant pour tous les États membres destinataires et s'impose donc à tous leurs organes (voir, en ce sens, arrêts Albako Margarinefabrik, 249/85, EU:C:1987:245, point 17, et Mediaset, C-69/13, EU:C:2014:71, point 23), en ce qu'elle a pour effet d'autoriser des transferts de données à caractère personnel depuis les États membres vers le pays tiers visé par celle-ci.

52 Ainsi, aussi longtemps que la décision de la Commission 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, certes, 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. En effet, les actes des institutions de l'Union jouissent, en principe, d'une présomption de légalité et produisent, dès lors, des effets juridiques aussi longtemps qu'ils n'ont pas été retirés, annulés dans le cadre d'un recours en annulation ou déclarés invalides à la suite d'un renvoi préjudiciel ou d'une exception d'illégalité (arrêt Commission/Grèce, C-475/01, EU:C:2004:585, point 18 et jurisprudence citée).

53 Toutefois, une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de la directive 95/46, telle que la décision 2000/520, ne saurait empêcher les personnes dont les données à caractère personnel ont été ou pourraient être transférées vers un pays tiers de saisir les autorités nationales de contrôle d'une demande, au sens de l'article 28, paragraphe 4, de cette directive, relative à la protection de leurs droits et libertés à l'égard du traitement de ces données. De même, une décision de cette nature ne saurait, ainsi que l'a relevé M. l'avocat général notamment aux points 61, 93 et 116 de ses conclusions, 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 28 de ladite directive.

54 Ni l'article 8, paragraphe 3, de la Charte ni l'article 28 de la directive 95/46 n'excluent du domaine de compétence des autorités nationales de contrôle le contrôle des transferts de

données à caractère personnel vers des pays tiers ayant fait l'objet d'une décision de la Commission au titre de l'article 25, paragraphe 6, de cette directive.

55 En particulier, l'article 28, paragraphe 4, premier alinéa, de la directive 95/46, qui dispose que les autorités nationales de contrôle peuvent être saisies par «toute personne [...] d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel», ne prévoit aucune exception à cet égard dans l'hypothèse où la Commission aurait adopté une décision au titre de l'article 25, paragraphe 6, de cette directive.

56 En outre, il serait contraire au système mis en place par la directive 95/46 ainsi qu'à la finalité des articles 25 et 28 de celle-ci qu'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de ladite directive ait pour effet d'empêcher une autorité nationale de contrôle d'examiner la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de ses données à caractère personnel qui ont été ou pourraient être transférées depuis un État membre vers un pays tiers visé par cette décision.

57 Au contraire, l'article 28 de la directive 95/46 s'applique, par sa nature même, à tout traitement de données à caractère personnel. Ainsi, même en présence d'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de cette directive, les autorités nationales de contrôle, saisies par une personne d'une demande relative à la protection de ses droits et libertés à l'égard du traitement des données à caractère personnel la concernant, doivent pouvoir examiner, en toute indépendance, si le transfert de ces données respecte les exigences posées par ladite directive.

58 S'il en était autrement, les personnes dont les données à caractère personnel ont été ou pourraient être transférées vers le pays tiers concerné seraient privées du droit, garanti à l'article 8, paragraphes 1 et 3, de la Charte, de saisir les autorités nationales de contrôle d'une demande aux fins de la protection de leurs droits fondamentaux (voir, par analogie, arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 68).

59 Une demande, au sens de l'article 28, paragraphe 4, de la directive 95/46, par laquelle une personne dont les données à caractère personnel ont été ou pourraient être transférées vers un pays tiers fait valoir, comme dans l'affaire au principal, 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 25, paragraphe 6, de cette directive, 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 et des libertés et droits fondamentaux des personnes.

60 À cet égard, il convient de rappeler la jurisprudence constante de la Cour selon laquelle l'Union est une Union de droit dans laquelle tout acte de ses institutions est soumis au contrôle de la conformité avec, notamment, les traités, les principes généraux du droit ainsi que les droits fondamentaux (voir, en ce sens, arrêts Commission e.a./Kadi, C-584/10 P, C-593/10 P et C-595/10 P, EU:C:2013:518, point 66; Inuit Tapiriit Kanatami e.a./Parlement et Conseil, C-583/11 P, EU:C:2013:625, point 91, ainsi que Telefónica/Commission, C-274/12 P, EU:C:2013:852, point 56). Les décisions de la Commission adoptées au titre de l'article 25, paragraphe 6, de la directive 95/46 ne sauraient donc échapper à un tel contrôle.

61 Cela étant, la Cour est seulecompétente pour constater l'invalidité d'un acte de l'Union, tel qu'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de la directive 95/46, le caractère exclusif de cette compétence ayant pour objet de garantir la sécurité juridique en assurant l'application uniforme du droit de l'Union (voir arrêts Melki et Abdeli, C-188/10 et C-189/10, EU:C:2010:363, point 54, ainsi que CIVAD, C-533/10, EU:C:2012:347, point 40).

62 Si les juridictions nationales sont, certes, en droit d'examiner la validité d'un acte de l'Union, tel qu'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de la directive 95/46, elles ne sont toutefois pas dotées de la compétence pour constater elles-mêmes l'invalidité d'un tel acte (voir, en ce sens, arrêts Foto-Frost, 314/85, EU:C:1987:452, points 15 à 20, ainsi que IATA et ELFAA, C-344/04, EU:C:2006:10, point 27). A fortiori, lors de l'examen d'une demande, au sens de l'article 28, paragraphe 4, de cette directive, portant sur la compatibilité d'une décision de la Commission adoptée au titre de

l'article 25, paragraphe 6, de ladite directive avec la protection de la vie privée et des libertés et droits fondamentaux des personnes, les autorités nationales de contrôle ne sont pas en droit de constater elles-mêmes l'invalidité d'une telle décision.

63 Eu égard à ces considérations, lorsqu'une personne, dont les données à caractère personnel ont été ou pourraient être transférées vers un pays tiers ayant fait l'objet d'une décision de la Commission au titre de l'article 25, paragraphe 6, de la directive 95/46, saisit une autorité nationale de contrôle d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de ces données et conteste, à l'occasion de cette demande, comme dans l'affaire au principal, la compatibilité de cette décision avec la protection de la vie privée et des libertés et droits fondamentaux des personnes, il incombe à cette autorité d'examiner ladite demande avec toute la diligence requise.

64 Dans l'hypothèse où ladite autorité parvient à la conclusion que les éléments avancés au soutien d'une telle demande sont dépourvus de fondement et rejette, de ce fait, cette dernière, la personne ayant introduit ladite demande doit, ainsi qu'il résulte de l'article 28, paragraphe 3, second alinéa, de la directive 95/46, lu à la lumière de l'article 47 de la Charte, avoir accès aux voies de recours juridictionnelles lui permettant de contester une telle décision lui faisant grief devant les juridictions nationales. Eu égard à la jurisprudence citée aux points 61 et 62 du présent arrêt, ces juridictions sont tenues de surseoir à statuer et de saisir la Cour d'une procédure de renvoi préjudiciel en appréciation de validité lorsqu'elles considèrent qu'un ou plusieurs moyens d'invalidité avancés par les parties ou, le cas échéant, soulevés d'office sont fondés (voir, en ce sens, arrêt T & L Sugars et Sidul Açúcares/Commission, C-456/13 P, EU:C:2015:284, point 48 et jurisprudence citée).

65 Dans l'hypothèse contraire, où ladite autorité estime fondés les griefs avancés par la personne l'ayant saisie d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de ses données à caractère personnel, cette même autorité doit, conformément à l'article 28, paragraphe 3, premier alinéa, troisième tiret, de la directive 95/46, lu à la lumière notamment de l'article 8, paragraphe 3, de la Charte, pouvoir ester en justice. À cet égard, il incombe au législateur national de prévoir des voies de recours permettant à l'autorité nationale de contrôle concernée de faire valoir les griefs qu'elle estime fondés devant les juridictions nationales afin que ces dernières procèdent, si elles partagent les doutes de cette autorité quant à la validité de la décision de la Commission, à un renvoi préjudiciel aux fins de l'examen de la validité de cette décision.

66 Eu égard aux considérations qui précèdent, il y a lieu de répondre aux questions posées que l'article 25, paragraphe 6, de la directive 95/46, lu à la lumière des articles 7, 8 et 47 de la Charte, doit être interprété en ce sens qu'une décision adoptée au titre de cette disposition, telle que la décision 2000/520, par laquelle la Commission constate qu'un pays tiers assure un niveau de protection adéquat, ne fait pas obstacle à ce qu'une autorité de contrôle d'un État membre, au sens de l'article 28 de cette directive, examine la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant qui ont été transférées depuis un État membre vers ce pays tiers, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans celui-ci n'assurent pas un niveau de protection adéquat.

*Sur la validité de la décision 2000/520*

67 Ainsi qu'il ressort des explications de la juridiction de renvoi relatives aux questions posées, M. Schrems fait valoir, dans la procédure au principal, que le droit et les pratiques des États-Unis n'assurent pas un niveau de protection adéquat au sens de l'article 25 de la directive 95/46. Comme l'a relevé M. l'avocat général aux points 123 et 124 de ses conclusions, M. Schrems émet des doutes, que cette juridiction paraît d'ailleurs partager en substance, concernant la validité de la décision 2000/520. Dans de telles circonstances, eu égard aux constatations faites aux points 60 à 63 du présent arrêt, et afin de donner une réponse complète à ladite juridiction, il convient d'examiner si cette décision est conforme aux exigences découlant de cette directive, lue à la lumière de la Charte.

Sur les exigences découlant de l'article 25, paragraphe 6, de la directive 95/46

68 Ainsi qu'il a été déjà relevé aux points 48 et 49 du présent arrêt, l'article 25, paragraphe 1, de la directive 95/46 interdit les transferts de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat.

69 Toutefois, aux fins du contrôle de tels transferts, l'article 25, paragraphe 6, premier alinéa, de cette directive dispose que la Commission «peut constater [...] qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 [de cet article], en raison de sa législation interne ou de ses engagements internationaux [...], en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes».

70 Certes, ni l'article 25, paragraphe 2, de la directive 95/46 ni aucune autre disposition de celle-ci ne contiennent de définition de la notion de niveau de protection adéquat. En particulier, l'article 25, paragraphe 2, de ladite directive se borne à énoncer que 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 transfert de données» et énumère, de façon non exhaustive, les circonstances devant être prises en considération lors d'une telle appréciation.

71 Toutefois, d'une part, ainsi qu'il ressort des termes mêmes de l'article 25, paragraphe 6, de la directive 95/46, cette disposition exige qu'un pays tiers «assure» un niveau de protection adéquat en raison de sa législation interne ou de ses engagements internationaux. D'autre part, également selon cette disposition, le caractère adéquat de la protection assurée par le pays tiers s'apprécie «en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes».

72 Ainsi, l'article 25, paragraphe 6, de la directive 95/46 met en œuvre l'obligation explicite de protection des données à caractère personnel, prévue à l'article 8, paragraphe 1, de la Charte, et vise à assurer, comme l'a relevé M. l'avocat général au point 139 de ses conclusions, la continuité du niveau élevé de cette protection en cas de transfert de données à caractère personnel vers un pays tiers.

73 Certes, le terme «adéquat» figurant à l'article 25, paragraphe 6, de la directive 95/46 implique qu'il ne saurait être exigé qu'un pays tiers assure un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union. Toutefois, comme l'a relevé M. l'avocat général au point 141 de ses conclusions, l'expression «niveau de protection adéquat» doit être comprise 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 droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte. En effet, à défaut d'une telle exigence, l'objectif mentionné au point précédent du présent arrêt serait méconnu. En outre, le niveau élevé de protection garanti par la directive 95/46, lue à la lumière de la Charte, pourrait facilement être contourné par des transferts de données à caractère personnel depuis l'Union vers des pays tiers aux fins de leur traitement dans ces pays.

74 Il ressort du libellé exprès de l'article 25, paragraphe 6, de la directive 95/46 que c'est l'ordre juridique du pays tiers visé par la décision de la Commission qui doit assurer un niveau de protection adéquat. Même si les moyens auxquels ce pays tiers a recours, à cet égard, pour assurer un tel niveau de protection peuvent être différents de ceux mis en œuvre au sein de l'Union afin de garantir le respect des exigences découlant de cette directive, lue à la lumière de la Charte, ces moyens doivent néanmoins s'avérer, en pratique, effectifs afin d'assurer une protection substantiellement équivalente à celle garantie au sein de l'Union.

75 Dans ces conditions, lors de l'examen du niveau de protection offert par un pays tiers, la Commission est tenue d'apprécier le contenu des règles applicables dans ce pays résultant de la législation interne ou des engagements internationaux de celui-ci ainsi que la pratique visant à assurer le respect de ces règles, cette institution devant, conformément à l'article 25, paragraphe 2, de la directive 95/46, prendre en compte toutes les circonstances relatives à un transfert de données à caractère personnel vers un pays tiers.

76 De même, au regard du fait que le niveau de protection assuré par un pays tiers est susceptible d'évoluer, il incombe à la Commission, après l'adoption d'une décision au titre de l'article 25, paragraphe 6, de la directive 95/46, de vérifier de manière périodique si la

constatation relative au niveau de protection adéquat assuré par le pays tiers en cause est toujours justifiée en fait et en droit. Une telle vérification s'impose, en tout état de cause, lorsque des indices font naître un doute à cet égard.

77 En outre, ainsi que l'a relevé M. l'avocat général aux points 134 et 135 de ses conclusions, lors de l'examen de la validité d'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de la directive 95/46, il doit être également tenu compte des circonstances intervenues postérieurement à l'adoption de cette décision.

78 À cet égard, il convient de constater que, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, du nombre important de personnes dont les droits fondamentaux sont susceptibles d'être violés en cas de transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat, le pouvoir d'appréciation de la Commission quant au caractère adéquat du niveau de protection assuré par un pays tiers s'avère réduit, de sorte qu'il convient de procéder à un contrôle strict des exigences découlant de l'article 25 de la directive 95/46, lu à la lumière de la Charte (voir, par analogie, arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 47 et 48).

Sur l'article 1er de la décision 2000/520

79 La Commission a considéré, à l'article 1er, paragraphe 1, de la décision 2000/520, que les principes visés à l'annexe I de celle-ci, appliqués conformément aux orientations fournies par les FAQ visées à l'annexe II de ladite décision, assurent un niveau adéquat de protection des données à caractère personnel transférées depuis l'Union vers des organisations établies aux États-Unis. Il ressort de cette disposition que tant ces principes que ces FAQ ont été publiés par le ministère du Commerce américain.

80 L'adhésion d'une organisation aux principes de la sphère de sécurité est effectuée sur la base d'un système d'autocertification, ainsi qu'il ressort de l'article 1er, paragraphes 2 et 3, de cette décision, lu en combinaison avec la FAQ 6 figurant à l'annexe II de ladite décision.

81 Si le recours, par un pays tiers, à un système d'autocertification n'est pas, par lui-même, contraire à l'exigence prévue à l'article 25, paragraphe 6, de la directive 95/46, selon laquelle le pays tiers concerné doit assurer un niveau de protection adéquat «en raison de [la] législation interne ou [des] engagements internationaux» de ce pays, la fiabilité d'un tel système, au regard de cette exigence, repose essentiellement sur la mise en place de mécanismes efficaces de détection et de contrôle permettant d'identifier et de sanctionner, en pratique, d'éventuelles violations des règles assurant la protection des droits fondamentaux, notamment du droit au respect de la vie privée ainsi que du droit à la protection des données à caractère personnel.

82 En l'occurrence, les principes de la sphère de sécurité sont, en vertu de l'annexe I, deuxième alinéa, de la décision 2000/520, «exclusivement destinés aux organisations américaines recevant des données à caractère personnel en provenance de l'Union européenne et doivent permettre à ces organisations de remplir les conditions relatives à la 'sphère de sécurité' de façon à bénéficier de la présomption de 'niveau de protection adéquat' que prévoit celle-ci». Ces principes sont donc uniquement applicables aux organisations américaines autocertifiées recevant des données à caractère personnel depuis l'Union, sans qu'il soit exigé que les autorités publiques américaines soient soumises au respect desdits principes.

83 En outre, en vertu de l'article 2 de la décision 2000/520, cette dernière «concerne uniquement le caractère adéquat de la protection fournie aux États-Unis par les principes [de la sphère de sécurité] mis en œuvre conformément aux FAQ en vue de répondre aux exigences de l'article 25, paragraphe 1, de la directive [95/46]», sans pour autant contenir les constatations suffisantes quant aux mesures par lesquelles les États-Unis d'Amérique assurent un niveau de protection adéquat, au sens de l'article 25, paragraphe 6, de cette directive, en raison de leur législation interne ou de leurs engagements internationaux.

84 À cela s'ajoute que, conformément à l'annexe I, quatrième alinéa, de la décision 2000/520, l'applicabilité desdits principes peut être limitée par, notamment, «les exigences relatives à la

sécurité nationale, [à] l'intérêt public et [au] respect des lois des États-Unis», ainsi que par «les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir».

85 À cet égard, sous le titre B de son annexe IV, la décision 2000/520 souligne, s'agissant des limites auxquelles est soumise l'applicabilité des principes de la sphère de sécurité, qu'«[i]l est clair que lorsque la législation américaine impose une obligation conflictuelle, les organisations américaines faisant ou non partie de la 'sphère de sécurité' doivent se plier à cette législation».

86 Ainsi, la décision 2000/520 consacre la primauté des «exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect des lois des États-Unis» sur les principes de la sphère de sécurité, primauté en vertu de laquelle les organisations américaines autocertifiées recevant des données à caractère personnel depuis l'Union sont tenues d'écarter, sans limitation, ces principes lorsque ces derniers entrent en conflit avec ces exigences et s'avèrent donc incompatibles avec celles-ci.

87 Eu égard au caractère général de la dérogation figurant à l'annexe I, quatrième alinéa, de la décision 2000/520, celle-ci rend ainsi possible 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. À cet égard, il importe peu, pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence (arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 33 et jurisprudence citée).

88 Au surplus, la décision 2000/520 ne comporte aucune constatation quant à l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union vers les États-Unis, ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la sécurité nationale.

89 À cela s'ajoute le fait que la décision 2000/520 ne fait pas état de l'existence d'une protection juridique efficace contre des ingérences de cette nature. Ainsi que l'a relevé M. l'avocat général aux points 204 à 206 de ses conclusions, les mécanismes d'arbitrage privé et les procédures devant la Commission fédérale du commerce, dont les pouvoirs, décrits notamment dans les FAQ 11 figurant à l'annexe II de cette décision, sont limités aux litiges commerciaux, portent sur le respect, par les entreprises américaines, des principes de la sphère de sécurité et ne peuvent être mis en œuvre dans le cadre des litiges portant sur la légalité d'ingérences dans les droits fondamentaux résultant de mesures d'origine étatique.

90 Par ailleurs, l'analyse de la décision 2000/520 qui précède est corroborée par l'appréciation que la Commission a elle-même faite de la situation résultant de la mise en œuvre de cette décision. En effet, en particulier aux points 2 et 3.2 de la communication COM(2013) 846 final ainsi qu'aux points 7.1, 7.2 et 8 de la communication COM(2013) 847 final, dont la teneur est exposée respectivement aux points 13 à 16 ainsi qu'aux points 22, 23 et 25 du présent arrêt, cette institution a constaté que les autorités américaines pouvaient accéder aux données à caractère personnel transférées à partir des États membres vers les États-Unis et traiter celles-ci d'une manière incompatible, notamment, avec les finalités de leur transfert, et au-delà de ce que qui était strictement nécessaire et proportionné à la protection de la sécurité nationale. De même, la Commission a constaté qu'il n'existait pas, pour les personnes concernées, de voies de droit administratives ou judiciaires permettant, notamment, d'accéder aux données les concernant et, le cas échéant, d'obtenir leur rectification ou leur suppression.

91 S'agissant du niveau de protection des libertés et droits fondamentaux garanti au sein de l'Union, une réglementation de celle-ci comportant une ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte doit, selon la jurisprudence constante de la Cour, prévoir des règles claires et précises régissant la portée et l'application d'une

mesure et imposant un minimum d'exigences, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement leurs données contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55 ainsi que jurisprudence citée).

92 En outre et surtout, la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 52 et jurisprudence citée).

93 Ainsi, n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données [voir en ce sens, en ce qui concerne la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54), arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, points 57 à 61].

94 En particulier, une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte (voir, en ce sens, arrêt Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 39).

95 De même, 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. En effet, l'article 47, premier alinéa, de la Charte exige que toute personne dont les droits et 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. À cet égard, 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 (voir, en ce sens, arrêts Les Verts/Parlement, 294/83, EU:C:1986:166, point 23; Johnston, 222/84, EU:C:1986:206, points 18 et 19; Heylens e.a., 222/86, EU:C:1987:442, point 14, ainsi que UGT-Rioja e.a., C-428/06 à C-434/06, EU:C:2008:488, point 80).

96 Ainsi qu'il a été constaté notamment aux points 71, 73 et 74 du présent arrêt, l'adoption par la Commission d'une décision au titre de l'article 25, paragraphe 6, de la directive 95/46 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, tel qu'il ressort notamment des points précédents du présent arrêt.

97 Or, il y a lieu de relever que la Commission n'a pas fait état, dans la décision 2000/520, de ce que les États-Unis d'Amérique «assurent» effectivement un niveau de protection adéquat en raison de leur législation interne ou de leurs engagements internationaux.

98 Par suite, et sans qu'il soit besoin d'examiner les principes de la sphère de sécurité quant à leur contenu, il convient de conclure que l'article 1er de cette décision méconnaît les exigences fixées à l'article 25, paragraphe 6, de la directive 95/46, lu à la lumière de la Charte, et qu'il est de ce fait invalide.

Sur l'article 3 de la décision 2000/520

99 Il ressort des considérations exposées aux points 53, 57 et 63 du présent arrêt que, au regard de l'article 28 de la directive 95/46, lu à la lumière notamment de l'article 8 de la Charte, les autorités nationales de contrôle doivent pouvoir examiner, en toute indépendance, toute demande relative à la protection des droits et libertés d'une personne à l'égard du traitement de données à caractère personnel la concernant. Il en va en particulier ainsi lorsque, à l'occasion d'une telle demande, cette personne soulève des interrogations quant à la compatibilité d'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de cette directive avec la protection de la vie privée et des libertés et droits fondamentaux des personnes.

100 Cependant, l'article 3, paragraphe 1, premier alinéa, de la décision 2000/520 prévoit une réglementation spécifique quant aux pouvoirs dont disposent les autorités nationales de contrôle au regard d'une constatation effectuée par la Commission relativement au niveau de protection adéquat, au sens de l'article 25 de la directive 95/46.

101 Ainsi, aux termes de cette disposition, ces autorités peuvent, «[s]ans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées en application de dispositions autres que celles de l'article 25 de la directive [95/46], […] suspendre les flux de données vers une organisation adhérant aux principes [de la décision 2000/520]», dans des conditions restrictives établissant un seuil élevé d'intervention. Si cette disposition ne porte pas préjudice aux pouvoirs de ces autorités de prendre des mesures visant à assurer le respect des dispositions nationales adoptées en application de cette directive, elle exclut, en revanche, la possibilité pour lesdites autorités de prendre des mesures visant à assurer le respect de l'article 25 de cette même directive.

102 L'article 3, paragraphe 1, premier alinéa, de la décision 2000/520 doit donc être compris comme privant les autorités nationales de contrôle des pouvoirs qu'elles tirent de l'article 28 de la directive 95/46, dans le cas où une personne avance, à l'occasion d'une demande au titre de cette disposition, des éléments susceptibles de remettre en cause la compatibilité avec la protection de la vie privée et des libertés et droits fondamentaux des personnes d'une décision de la Commission ayant constaté, sur le fondement de l'article 25, paragraphe 6, de cette directive, qu'un pays tiers assure un niveau de protection adéquat.

103 Or, le pouvoir d'exécution accordé par le législateur de l'Union à la Commission à l'article 25, paragraphe 6, de la directive 95/46 ne confère pas à cette institution la compétence de restreindre les pouvoirs des autorités nationales de contrôle visés au point précédent du présent arrêt.

104 Dans ces conditions, il y a lieu de constater que, en adoptant l'article 3 de la décision 2000/520, la Commission a outrepassé la compétence qui lui est attribuée à l'article 25, paragraphe 6, de la directive 95/46, lu à la lumière de la Charte, et qu'il est de ce fait invalide.

105 Les articles 1er et 3 de la décision 2000/520 étant indissociables des articles 2 et 4 ainsi que des annexes de celle-ci, leur invalidité a pour effet d'affecter la validité de cette décision dans son ensemble.

106 Eu égard à l'ensemble des considérations qui précèdent, il convient de conclure que la décision 2000/520 est invalide.

**Sur les dépens**

107 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 25, paragraphe 6, 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, telle que modifiée par le règlement (CE) n° 1882/2003 du Parlement européen et du Conseil, du 29 septembre 2003, lu à la lumière des articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'une décision adoptée au titre de cette disposition, telle que 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, par laquelle la Commission européenne constate qu'un pays tiers assure un niveau de protection adéquat, ne fait pas obstacle à ce qu'une autorité de contrôle d'un État membre, au sens de l'article 28 de cette directive, telle que modifiée, examine la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant qui ont été transférées depuis un État membre vers ce pays tiers, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans celui-ci n'assurent pas un niveau de protection adéquat.**

2) **La décision 2000/520 est invalide.**

Signatures

---

* Langue de procédure: l'anglais.