Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. YVES BOT
présentées le 23 septembre 2015 [1]

Affaire C-362/14

Maximillian Schrems
contre
Data Protection Commissioner

[demande de décision préjudicielle formée par la Haute Cour de justice (High Court, Irlande)]

«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 — Article 25 — Décision 2000/520/CE — Transfert de données à caractère personnel vers les États-Unis — Évaluation du caractère adéquat ou non du niveau de protection — Plainte d'une personne physique dont les données ont été transférées vers un pays tiers — Autorité nationale de contrôle — Pouvoirs»

I – Introduction

1. Ainsi que la Commission européenne l'a constaté dans sa communication du 27 novembre 2013 [2], «[l]es transferts de données à caractère personnel constituent un volet important et nécessaire des relations transatlantiques. Ils font partie intégrante des échanges commerciaux transatlantiques, notamment dans les nouveaux secteurs du numérique en pleine croissance, comme les médias sociaux ou l'informatique en nuage, qui supposent le transfert de grands volumes de données de l'Union européenne vers les États-Unis» [3].

2. Les échanges commerciaux font l'objet de la décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil 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 [4]. Cette décision fournit une base juridique pour le transfert de données à caractère personnel de l'Union vers des entreprises établies aux États-Unis qui adhèrent aux principes de la sphère de sécurité.

3. Ladite décision est aujourd'hui confrontée au défi consistant à permettre les flux de données entre l'Union et les États-Unis tout en garantissant un niveau élevé de protection à ces données, ainsi que le droit de l'Union l'exige.

1 — Langue originale: le français.

2 — Communication de la Commission au Parlement européen et au Conseil intitulée «Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique» [COM(2013) 846 final].

3 — Page 2.

4 — JO L 215, p. 7, et rectificatif JO 2001, L 115, p. 14.

4. En effet, un certain nombre de révélations ont récemment mis en lumière l'existence de programmes américains de collecte de renseignements à grande échelle. Ces révélations ont jeté le trouble sur le respect des normes du droit de l'Union lors de transferts de données à caractère personnel vers des entreprises établies aux États-Unis et sur les faiblesses du régime de la sphère de sécurité.

5. Le présent renvoi préjudiciel invite la Cour à préciser quelle attitude doivent adopter les autorités nationales de contrôle et la Commission lorsqu'elles sont confrontées à des dysfonctionnements dans l'application de la décision 2000/520.

6. 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 [5], prévoit, à son chapitre IV, des règles relatives au transfert de données à caractère personnel vers des pays tiers.

7. Au sein de ce chapitre, le principe posé à l'article 25, paragraphe 1, de cette directive est celui selon lequel 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 le pays tiers en question assure un niveau de protection adéquat à de telles données.

8. À l'inverse, ainsi que le législateur de l'Union l'indique au considérant 57 de ladite directive, 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.

9. Aux termes de l'article 25, paragraphe 2, de la directive 95/46, «[l]e 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 pris 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».

10. En vertu de l'article 25, paragraphe 6, de cette directive, la Commission peut constater qu'un pays tiers assure, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection adéquat aux données à caractère personnel. Dès lors que la Commission adopte une décision en ce sens, le transfert de données à caractère personnel vers le pays tiers concerné peut avoir lieu.

11. Faisant application de cette disposition, la Commission a adopté la décision 2000/520. Il résulte de l'article 1er, paragraphe 1, de cette décision que les «principes de la 'sphère de sécurité' relatifs à la protection de la vie privée», appliqués conformément aux orientations fournies par les «questions souvent posées» [6], sont considérés comme assurant un niveau de protection adéquat des données à caractère personnel transférées depuis l'Union vers des entreprises établies aux États-Unis.

12. En conséquence, la décision 2000/520 autorise le transfert de données à caractère personnel depuis les États membres vers des entreprises établies aux États-Unis qui se sont engagées à respecter les principes de la sphère de sécurité.

5 — JO L 281, p. 31. Directive telle que modifiée par le règlement (CE) nº 1882/2003 du Parlement européen et du Conseil, du 29 septembre 2003 (JO L 284, p. 1, ci-après la «directive 95/46»).

6 — Frequently asked questions, ci-après les «FAQ».

13. La décision 2000/520 énonce, à son annexe I, un certain nombre de principes auxquels les entreprises peuvent souscrire volontairement, assortis de limites et d'un système de contrôle spécifique. Le nombre des entreprises ayant souscrit à ce qui pourrait être qualifié de «code de conduite» dépassait le chiffre de 3 200 en 2013.

14. Le régime de la sphère de sécurité repose sur une solution mêlant l'autocertification ainsi que l'autoévaluation par les entreprises privées et l'intervention de la puissance publique.

15. Les principes de la sphère de sécurité 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 [...]. Ils sont exclusivement destinés aux organisations américaines recevant des données à caractère personnel en provenance de l'Union [...] 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» [7].

16. Les principes de la sphère de sécurité, figurant à l'annexe I de la décision 2000/520, prévoient, notamment:

— une obligation d'information selon laquelle «[t]oute organisation doit informer les personnes concernées des raisons de la collecte et de l'utilisation d'informations à caractère personnel, de la façon de la contacter pour toute demande ou plainte, des tiers auxquels les informations sont communiquées, des choix et des moyens qu'offre l'organisation aux personnes concernées pour limiter l'utilisation et la divulgation de ces données. La notification [...] doit être communiquée aux personnes concernées lorsque celles-ci sont invitées pour la première fois à fournir des informations à caractère personnel ou dès que possible après cette invitation et, en tout état de cause, avant que les données ne soient utilisées dans un but différent de celui pour lequel elles ont été initialement collectées ou traitées par l'organisation ayant effectué le transfert ou avant qu'elles ne soient diffusées pour la première fois à un tiers» [8];

— une obligation pour les organisations d'offrir aux personnes concernées la possibilité de décider si leurs données peuvent être divulguées à une tierce personne ou utilisées dans un but incompatible avec le ou les objectifs pour lesquels les données ont été initialement collectées ou dans un but approuvé ultérieurement par la personne concernée. S'agissant des données sensibles, «toute personne doit avoir positivement ou explicitement la possibilité de décider (consentement) si les données peuvent être divulguées à un tiers ou utilisées dans un but qui diffère de l'objectif initial de la collecte ou dans un but approuvé ultérieurement par la personne concernée exerçant son droit de consentement» [9];

— des règles relatives au transfert ultérieur des données. Ainsi, «[p]our divulguer des informations à un tiers, les organisations sont tenues d'appliquer les principes de notification et de choix» [10];

— quant à la sécurité des données, une obligation pour «[l]es organisations qui créent, gèrent, utilisent ou diffusent des données à caractère personnel [de] prendre les mesures nécessaires pour éviter la perte, l'utilisation abusive, la consultation illicite, la divulgation, la modification et la destruction de ces données» [11];

7 — Deuxième alinéa de l'annexe I de la décision 2000/520.

8 — Voir annexe I, sous «Notification».

9 — Voir annexe I, sous «Choix».

10 — Voir annexe I, sous «Transfert ultérieur».

11 — Voir annexe I, sous «Sécurité».

— quant à l'intégrité des données, une obligation pour les organisations de «prendre les mesures qui s'imposent [...] pour assurer la fiabilité des données par rapport à l'utilisation prévue ainsi que leur exactitude, leur exhaustivité et leur actualité» [12];

— qu'une personne dont les données sont détenues par une organisation doit, en principe, «avoir accès à ces données et doit pouvoir les corriger, les modifier ou les supprimer lorsqu'elles sont inexactes» [13];

— une obligation de prévoir «des mécanismes permettant d'assurer le respect des principes de la 'sphère de sécurité', de ménager un droit de recours aux personnes concernées par le non-respect des principes et de sanctionner les organisations qui n'ont pas appliqué les principes alors qu'elles s'y sont engagées» [14].

17. Une organisation américaine souhaitant adhérer aux principes de la sphère de sécurité est tenue de stipuler, dans sa politique de protection de la vie privée, qu'elle rend public le fait qu'elle adhère à ces principes et s'y conforme effectivement et de s'autocertifier en déclarant au ministère du Commerce des États-Unis qu'elle est en conformité avec lesdits principes [15].

18. Les organisations disposent de plusieurs moyens pour se conformer aux principes de la sphère de sécurité. Ainsi, elles peuvent, par exemple, «participe[r] à un programme sur la protection de la confidentialité géré par le secteur privé qui respecte ces principes [ou] intégrer la 'sphère de sécurité' en mettant au point ses propres règles en matière de protection des données, pour autant que celles-ci soient conformes auxdits principes. [...] En outre, lorsqu'une organisation est soumise à un ensemble de dispositions juridiques, réglementaires, administratives ou autres (ou encore à un ensemble de règles) qui assurent une protection efficace des données à caractère personnel, elle peut également bénéficier des avantages de la 'sphère de sécurité'» [16].

19. Plusieurs mécanismes, mêlant l'arbitrage privé et le contrôle par les pouvoirs publics, existent pour vérifier le respect des principes de la sphère de sécurité. Le contrôle peut ainsi être assuré par l'intermédiaire d'un système de règlement extrajudiciaire des litiges par un tiers indépendant. Par ailleurs, les entreprises peuvent s'engager à coopérer avec le panel de l'Union sur la protection des données. Enfin, la Commission fédérale du commerce (Federal Trade Commission, ci-après la «FTC»), sur la base des pouvoirs qui lui sont conférés en vertu de la section 5 de la loi sur la Commission fédérale du commerce (Federal Trade Commission Act), et le ministère du Transport (Department of Transportation), sur la base des pouvoirs qui lui sont conférés en vertu de la section 41712 du Code des États-Unis (United States Code) figurant à son titre 49, sont compétents pour traiter des plaintes.

20. Aux termes du quatrième alinéa de l'annexe I de la décision 2000/520, l'adhésion aux principes de la sphère de sécurité peut être limitée, notamment, par «les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis» et 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» [17].

12 — Voir annexe I, sous «Intégrité des données».

13 — Voir annexe I, sous «Accès».

14 — Voir annexe I, sous «Mise en œuvre».

15 — Article 1er, paragraphes 2 et 3, de la décision 2000/520. Voir, également, annexe II, FAQ 6.

16 — Troisième alinéa de l'annexe I.

17 — Voir, également, annexe IV, B.

21. En outre, la possibilité pour les autorités compétentes des États membres de suspendre des flux de données est soumise à plusieurs conditions qui sont prévues à l'article 3, paragraphe 1, de la décision 2000/520.

22. La présente demande de décision préjudicielle conduit à s'interroger sur la portée de la décision 2000/520, eu égard aux articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») ainsi qu'aux articles 25, paragraphe 6, et 28 de la directive 95/46. 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») conserve les données à caractère personnel de ses abonnés sur des serveurs situés aux États-Unis.

23. M. Schrems est un ressortissant autrichien et réside en Autriche. Il est abonné au réseau social Facebook depuis l'année 2008.

24. Il est demandé à tous les abonnés de Facebook résidant sur le territoire de l'Union de signer un contrat avec Facebook Ireland qui est une filiale de la société mère Facebook Inc., sise aux États-Unis (ci-après «Facebook USA»). Les données des abonnés de Facebook Ireland résidant sur le territoire de l'Union sont, en tout ou en partie, transférées sur des serveurs de Facebook USA, situés sur le territoire des États-Unis, où elles sont conservées.

25. M. Schrems a déposé, le 25 juin 2013, une plainte devant le commissaire en faisant valoir, en substance, que le droit et les pratiques des États-Unis n'offrent aucune protection réelle des données conservées sur le territoire des États-Unis contre la surveillance de l'État. Cela résulterait des révélations faites par M. Snowden à partir du mois de mai 2013 au sujet des activités des services de renseignement américains, et en particulier de celles de la National Security Agency (ci-après la «NSA»).

26. Il résulte, notamment, de ces révélations que la NSA aurait établi un programme dénommé «PRISM» dans le cadre duquel cette agence aurait obtenu un accès libre aux données de masse stockées sur des serveurs situés aux États-Unis, possédés ou contrôlés par une série de sociétés actives dans le domaine de l'Internet et de la technologie telles que Facebook USA.

27. Le commissaire a estimé qu'il n'était pas obligé d'enquêter sur la plainte, dans la mesure où celle-ci était dépourvue de fondement juridique. Il a considéré qu'il n'existait pas de preuves que la NSA ait accédé aux données de M. Schrems. En outre, la plainte devait, selon lui, être rejetée en raison de la décision 2000/520 par laquelle la Commission a constaté que les États-Unis assurent, dans le cadre du régime de la sphère de sécurité, un niveau de protection adéquat aux données à caractère personnel transférées. Toute question relative au caractère adéquat de la protection de ces données aux États-Unis devrait être tranchée en conformité avec cette décision qui l'empêcherait d'examiner le problème soulevé par la plainte.

28. La législation nationale ayant conduit le commissaire à rejeter la plainte est la suivante.

29. L'article 10, paragraphe 1, de la loi de 1988 sur la protection des données (Data Protection Act 1988), telle que modifiée par la loi de 2003 sur la protection des données [Data Protection (Amendment) Act 2003, ci-après la «loi sur la protection des données»] lui confère le pouvoir d'examiner les plaintes et énonce:

«a) Le commissaire peut examiner ou faire examiner si des dispositions de la présente loi ont été, sont ou risquent d'être enfreintes à l'endroit d'une personne donnée, soit que cette personne porte plainte devant lui pour une infraction à l'une quelconque de ces dispositions, soit que le commissaire estime qu'une telle infraction puisse exister.

b) Lorsqu'une personne porte plainte devant le commissaire en vertu du point a) du présent paragraphe, le commissaire:

i) instruit ou fait instruire la plainte, sauf s'il conclut qu'elle est futile ou vexatoire, et,

ii) si il ou elle ne peut, dans un délai raisonnable, obtenir des parties concernées un règlement amiable de l'objet de la plainte, il notifie par écrit au plaignant la décision qu'il prend sur celle-ci en indiquant que, si cette décision lui fait grief, le plaignant peut former contre elle un recours juridictionnel en vertu de l'article 26 de la présente loi, dans un délai de 21 jours à compter de la réception de la notification.»

30. En l'espèce, le commissaire a conclu que la plainte de M. Schrems était «futile ou vexatoire» en ce sens qu'elle était vouée à l'échec car dépourvue de fondement juridique. C'est à ce titre qu'il a refusé d'instruire cette plainte.

31. L'article 11 de la loi sur la protection des données régit le transfert des données à caractère personnel en dehors du territoire national. L'article 11, paragraphe 2, sous a), de celle-ci prévoit:

«Lorsque, dans toute procédure régie par la présente loi, une question est soulevée:

i) pour déterminer si le niveau de protection adéquat précisé au paragraphe 1 du présent article est assuré par un pays ou un territoire en dehors de l'Espace économique européen [(EEE)] vers lequel des données à caractère personnel vont être transférées, et

ii) une constatation de l'Union a été faite en ce qui concerne le type de transferts en question,

la question sera tranchée en conformité avec cette constatation.»

32. L'article 11, paragraphe 2, sous b), de la loi sur la protection des données définit la notion de constatation de l'Union dans les termes suivants:

«Au point a) du présent paragraphe, 'constatation de l'Union' signifie une constatation que la Commission [...] a faite aux fins du paragraphe 4 ou du paragraphe 6 de l'article 25 de la directive [95/46], dans le cadre de la procédure prévue à l'article 31, paragraphe 2, de [celle-ci] en vue de déterminer si le niveau de protection adéquat précisé au paragraphe 1 du présent article est assuré par un pays ou un territoire en dehors de l'[EEE].»

33. Le commissaire a observé que la décision 2000/520 était une «constatation de l'Union» aux fins de l'article 11, paragraphe 2, sous a), de la loi sur la protection des données, de sorte que, en vertu de cette loi, toute question relative au caractère adéquat de la protection des données dans le pays tiers où celles-ci sont transférées devait être tranchée en conformité avec cette constatation. Dans la mesure où il s'agissait de l'essentiel de la plainte de M. Schrems, à savoir que des données à caractère personnel étaient transférées vers un pays tiers qui, en pratique, n'assurait pas un niveau de protection adéquat, le commissaire a estimé que la nature et l'existence même de la décision 2000/520 l'empêchaient d'examiner cette question.

34. M. Schrems a introduit un recours devant la Haute Cour de justice contre la décision du commissaire de rejeter sa plainte. Après avoir examiné les preuves soumises dans la procédure au principal, cette juridiction a constaté que la surveillance électronique et l'interception des données à caractère personnel répondent à des finalités nécessaires et indispensables à l'intérêt public, à savoir le maintien de la sécurité nationale et la prévention des crimes graves. La Haute Cour de justice indique, à cet égard, que la surveillance et l'interception des données à caractère personnel transférées depuis l'Union vers les États-Unis servent des objectifs légitimes liés à la lutte contre le terrorisme.

35. Selon cette même juridiction, les révélations faites par M. Snowden ont cependant démontré que la NSA et d'autres organes similaires avaient commis des excès considérables. Si la Foreign Intelligence Surveillance Court (ci-après la «FISC»), qui intervient dans le cadre de la loi de 1978 sur la surveillance des services de renseignement étrangers (Foreign Intelligence Surveillance Act of 1978)[18], exerce une supervision, la procédure devant elle serait toutefois secrète et non contradictoire. De plus, outre le fait que les décisions relatives à l'accès aux données à caractère personnel seraient prises sur le fondement du droit américain, les citoyens de l'Union n'auraient aucun droit effectif d'être entendus sur la question de la surveillance et de l'interception de leurs données.

36. Il ressortirait clairement des documents volumineux accompagnant les déclarations solennelles rendues au principal que l'exactitude d'un bon nombre des révélations de M. Snowden n'est pas remise en cause. La Haute Cour de justice a, dès lors, conclu que, une fois que les données à caractère personnel sont transférées aux États-Unis, la NSA ainsi que d'autres agences de sécurité américaines telles que le Federal Bureau of Investigation (FBI) peuvent y accéder dans le cadre de la surveillance et d'interceptions de masse indifférenciées.

37. La Haute Cour de justice constate que, en droit irlandais, l'importance des droits constitutionnels à la vie privée et à l'inviolabilité du domicile exige que toute ingérence dans ces droits soit conforme aux exigences prévues par la loi et proportionnée. L'accès massif et indifférencié à des données à caractère personnel ne répondrait nullement à l'exigence de proportionnalité et devrait donc être considéré comme étant contraire à la Constitution irlandaise[19].

38. La Haute Cour de justice relève que, pour que des interceptions de communications électroniques puissent être considérées comme étant constitutionnelles, il faudrait démontrer que des interceptions déterminées de communications et la surveillance de certaines personnes ou de certains groupes de personnes sont objectivement justifiées dans l'intérêt de la sécurité nationale et de la répression de la criminalité et qu'il existe des garanties adéquates et vérifiables.

39. Dès lors, la Haute Cour de justice indique que, si la présente affaire devait être abordée uniquement sur le fondement du droit irlandais, un problème considérable se poserait quant à la question de savoir si les États-Unis «assurent un niveau de protection adéquat de la vie privée ainsi que des libertés et droits fondamentaux», au sens de l'article 11, paragraphe 1, de la loi sur la protection des données. Il s'ensuit que, sur le fondement du droit irlandais, et en particulier de ses exigences constitutionnelles, le commissaire n'aurait pas pu rejeter la plainte de M. Schrems, mais il aurait dû examiner cette question.

40. Toutefois, la Haute Cour de justice constate que l'affaire dont elle est saisie concerne la mise en œuvre du droit de l'Union au sens de l'article 51, paragraphe 1, de la Charte, de sorte que la légalité de la décision du commissaire devrait être appréciée au regard du droit de l'Union.

41. Le problème auquel le commissaire s'est trouvé confronté est expliqué de la manière suivante par la Haute Cour de justice. En vertu de l'article 11, paragraphe 2, sous a), de la loi sur la protection des données, le commissaire est tenu de trancher la question du caractère adéquat de la protection dans le pays tiers «en conformité» avec une constatation de l'Union faite par la Commission en application de l'article 25, paragraphe 6, de la directive 95/46. Il s'ensuit que le commissaire ne pourrait pas s'écarter

18 — Voir section 702 de cette loi, telle que modifiée par la loi de 2008 (Foreign Intelligence Surveillance Act of 2008). C'est en application de cette section que la NSA détient une base de données connue sous le nom de «PRISM» (voir report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection du 27 novembre 2013).

19 — La Haute Cour de justice fait référence, en particulier, au respect de la dignité humaine et à la liberté de la personne (préambule), à l'autonomie personnelle (article 40, paragraphe 3, points 1 et 2), à l'inviolabilité du domicile (article 40, paragraphe 5) et à la protection de la vie familiale (article 41).

d'une telle constatation. La Commission ayant, dans sa décision 2000/520, constaté que les États-Unis garantissent un niveau de protection adéquat concernant le traitement des données par des sociétés qui adhèrent aux principes de la sphère de sécurité, une plainte faisant état du caractère inadéquat d'une telle protection devrait nécessairement être rejetée par le commissaire.

42. Tout en constatant que le commissaire a ainsi fait preuve d'une fidélité scrupuleuse à la lettre de la directive 95/46 et de la décision 2000/520, la Haute Cour de justice relève que M. Schrems objecte en réalité plus aux termes du régime de la sphère de sécurité lui-même qu'à la manière dont le commissaire l'a appliqué, tout en soulignant qu'il n'a pas contesté directement la validité de la directive 95/46 ni celle de la décision 2000/520.

43. Selon la Haute Cour de justice, la question essentielle serait donc de savoir si, eu égard au droit de l'Union et compte tenu, en particulier, de l'entrée en vigueur postérieure des articles 7 et 8 de la Charte, le commissaire est absolument tenu par la constatation de la Commission énoncée dans la décision 2000/520 relative au caractère adéquat du droit et des pratiques en matière de protection des données à caractère personnel aux États-Unis.

44. La Haute Cour de justice précise, en outre, que, dans le recours dont elle est saisie, aucun grief n'a été avancé à propos des actions de Facebook Ireland et de Facebook USA en tant que telles. Or, l'article 3, paragraphe 1, sous b), de la décision 2000/520, qui permet aux autorités nationales compétentes d'ordonner à une entreprise de suspendre les flux de données vers un pays tiers, ne s'appliquerait, selon cette juridiction, que dans des circonstances où la plainte est dirigée contre le comportement de l'entreprise concernée, ce qui ne serait pas le cas en l'espèce.

45. La Haute Cour de justice souligne, dès lors, que la véritable objection est dirigée non pas contre le comportement de Facebook USA en tant que tel, mais plutôt contre le fait que la Commission a estimé que le droit et les pratiques en matière de protection des données aux États-Unis garantissent une protection adéquate, alors que les révélations de M. Snowden font clairement apparaître que les autorités américaines peuvent accéder en masse et de manière indifférenciée aux données à caractère personnel de la population vivant sur le territoire de l'Union [20].

46. Sur ce point, la Haute Cour de justice estime qu'il est difficile d'envisager comment la décision 2000/520 pourrait, en pratique, satisfaire aux exigences des articles 7 et 8 de la Charte, a fortiori si l'on tient compte des principes formulés par la Cour dans son arrêt Digital Rights Ireland e.a. [21]. En particulier, la garantie prévue à l'article 7 de la Charte et par les valeurs essentielles communes aux traditions des États membres serait compromise s'il était permis aux pouvoirs publics d'avoir accès aux communications électroniques de manière aléatoire et généralisée sans devoir fournir une motivation objective fondée sur des raisons de sécurité nationale ou de prévention de la criminalité liées spécifiquement aux individus concernés et sans aucune garantie adéquate et vérifiable. Comme le recours de M. Schrems suggère que la décision 2000/520 pourrait, in abstracto, être incompatible avec les articles 7 et 8 de la Charte, la Cour pourrait estimer qu'il est possible d'interpréter la directive 95/46, et notamment son article 25, paragraphe 6, ainsi que la décision 2000/520 dans un sens permettant aux autorités nationales de mener leurs propres enquêtes afin d'établir si le transfert de données à caractère personnel vers un pays tiers satisfait aux exigences découlant des articles 7 et 8 de la Charte.

20 — La Haute Cour de justice indique, à cet égard, que le principal moyen invoqué par M. Schrems devant elle consistait à affirmer que, compte tenu des récentes révélations de M. Snowden et du fait que des données à caractère personnel ont été mises à la disposition des services de renseignement des États-Unis à grande échelle, le commissaire ne pouvait pas valablement conclure qu'il existe, dans ce pays tiers, un niveau de protection adéquat de ces données.

21 — C-293/12 et C-594/12, EU:C:2014:238, points 65 à 69.

47. C'est dans ces conditions que la Haute Cour de justice a décidé de surseoir à statuer et de saisir la Cour des questions préjudicielles suivantes:

«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 saisi d'une plainte relative au transfert de données à caractère personnel vers un pays tiers (en l'occurrence 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?

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 2000/520?»

II – Notre analyse

48. Les deux questions formulées par la Haute Cour de justice invitent la Cour à préciser les pouvoirs dont disposent les autorités nationales de contrôle lorsqu'elles sont saisies d'une plainte concernant un transfert de données à caractère personnel vers une entreprise établie dans un pays tiers et qu'il est allégué, au soutien de cette plainte, que ce pays tiers ne garantit pas un niveau de protection adéquat aux données transférées, alors même que la Commission a, sur le fondement de l'article 25, paragraphe 6, de la directive 95/46, adopté une décision reconnaissant le caractère adéquat du niveau de protection assuré par ledit pays tiers.

49. Nous observons que la plainte déposée par M. Schrems auprès du commissaire comporte une double dimension. Elle vise à contester le transfert de données à caractère personnel de Facebook Ireland à Facebook USA. M. Schrems demande qu'il soit mis fin à ce transfert dans la mesure où, selon lui, les États-Unis n'assureraient pas un niveau de protection adéquat aux données à caractère personnel qui sont transférées dans le cadre du régime de la sphère de sécurité. Plus précisément, il reproche à ce pays tiers d'avoir mis en place le programme PRISM permettant à la NSA d'accéder librement aux données de masse stockées sur des serveurs situés aux États-Unis. Ainsi, la plainte concerne spécifiquement les transferts de données à caractère personnel de Facebook Ireland à Facebook USA tout en mettant en cause de façon plus générale le niveau de protection assuré à de telles données dans le cadre du régime de la sphère de sécurité.

50. Le commissaire a estimé que l'existence même d'une décision de la Commission reconnaissant que les États-Unis assurent, dans le cadre du régime de la sphère de sécurité, un niveau de protection adéquat, l'empêchait d'enquêter sur la plainte.

51. Il convient donc d'examiner ensemble les deux questions qui tendent, en substance, à savoir si l'article 28 de la directive 95/46, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'existence d'une décision adoptée par la Commission sur le fondement de l'article 25, paragraphe 6, de cette directive a pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat aux données à caractère personnel transférées et, le cas échéant, de suspendre le transfert de ces données.

52. L'article 7 de la Charte garantit le droit au respect de la vie privée, tandis que l'article 8 de celle-ci proclame expressément le droit à la protection des données à caractère personnel. Les paragraphes 2 et 3 de ce dernier article précisent que ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi, que toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification et que le respect de ces règles est soumis au contrôle d'une autorité indépendante.

A – *Sur les pouvoirs des autorités nationales de contrôle en cas de décision d'adéquation de la Commission*

53. Ainsi que l'indique M. Schrems dans ses observations, aux fins de la plainte en cause au principal, la question centrale est celle du transfert de données à caractère personnel de Facebook Ireland à Facebook USA à la lumière de l'accès généralisé par la NSA et d'autres agences de sécurité américaines aux données stockées chez Facebook USA en vertu des pouvoirs que leur confère la législation américaine.

54. Saisie d'une plainte visant à remettre en cause le constat selon lequel un pays tiers assure un niveau de protection adéquat aux données transférées, l'autorité nationale de contrôle a, selon M. Schrems, le pouvoir, si elle dispose d'éléments allant dans le sens du bien-fondé des allégations contenues dans cette plainte, d'ordonner la suspension du transfert de données opéré par l'entreprise désignée dans ladite plainte.

55. Compte tenu des obligations du commissaire de protéger les droits fondamentaux de M. Schrems, ce dernier soutient que le commissaire a une obligation non seulement d'enquêter, mais aussi, si la plainte est accueillie, d'utiliser ses pouvoirs pour suspendre le flux de données entre Facebook Ireland et Facebook USA.

56. Or, le commissaire a rejeté la plainte sur la base des dispositions de la loi sur la protection des données qui énumèrent ses pouvoirs. Cette conclusion était fondée sur le point de vue du commissaire qu'il était lié par la décision 2000/520.

57. Il s'ensuit que le problème central dans la présente affaire est celui de savoir si l'appréciation de la Commission quant au caractère adéquat du niveau de protection, contenue dans la décision 2000/520 lie de manière absolue l'autorité nationale de protection des données et l'empêche d'enquêter sur des allégations tendant à remettre en cause ce constat. Les questions préjudicielles portent donc sur l'étendue des pouvoirs d'enquête des autorités nationales de protection des données en présence d'une décision d'adéquation de la Commission.

58. Selon la Commission, il importe de tenir compte de l'articulation entre les pouvoirs de celle-ci et ceux des autorités nationales de protection des données. Les compétences de ces dernières seraient centrées sur l'application de la législation en cette matière dans des cas individuels, tandis que le réexamen général de l'application de la décision 2000/520, y compris toute décision comportant sa suspension ou son abrogation, relèverait de la compétence de la Commission.

59. La Commission fait valoir que M. Schrems n'aurait pas avancé d'arguments spécifiques donnant à penser qu'il courrait un risque imminent de subir des dommages graves en raison du transfert de données entre Facebook Ireland et Facebook USA. Au contraire, en raison de leur nature abstraite et générale, les inquiétudes exprimées par M. Schrems à propos des programmes de surveillance mis en œuvre par les agences de sécurité américaines seraient identiques à celles qui ont conduit la Commission à entamer le réexamen de la décision 2000/520.

60. Selon la Commission, les autorités nationales de contrôle empièteraient sur les compétences dont elle dispose pour renégocier les conditions de cette décision avec les États-Unis ou, au besoin, pour suspendre celle-ci, si elles prenaient des mesures sur la base de plaintes faisant uniquement état de préoccupations structurelles et abstraites.

61. Nous ne partageons pas l'opinion de la Commission. À notre avis, l'existence d'une décision adoptée par la Commission sur le fondement de l'article 25, paragraphe 6, de la directive 95/46 ne saurait annihiler ni même réduire les pouvoirs dont disposent les autorités nationales de contrôle en vertu de l'article 28 de cette directive. Contrairement à ce que fait valoir la Commission, si les

autorités nationales de contrôle sont saisies dans le cadre de plaintes individuelles, cela ne les empêche pas, selon nous, en vertu de leurs pouvoirs d'investigation et de leur indépendance, de se faire leur propre opinion sur le niveau général de protection assuré par un pays tiers et d'en tirer les conséquences lorsqu'elles statuent sur des cas individuels.

62. Il découle d'une jurisprudence constante de la Cour qu'il y a lieu, pour l'interprétation des dispositions du droit de l'Union, de tenir compte non seulement des termes de celles-ci, mais également de leur contexte et des objectifs poursuivis par la réglementation dont elles font partie [22].

63. Il ressort du considérant 62 de la directive 95/46 que «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».

64. Aux termes de l'article 28, paragraphe 1, premier alinéa, de cette directive, «[c]haque 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». L'article 28, paragraphe 1, second alinéa, de ladite directive dispose que «[c]es autorités exercent en toute indépendance les missions dont elles sont investies».

65. L'article 28, paragraphe 3, de la directive 95/46 énumère les pouvoirs dont dispose chaque autorité de contrôle, à savoir des pouvoirs d'investigation, des pouvoirs effectifs d'intervention lui permettant, notamment, d'interdire temporairement ou définitivement un traitement ainsi que le pouvoir d'ester en justice en cas de violations des dispositions nationales prises en application de cette directive ou le pouvoir de porter ces violations à la connaissance de l'autorité judiciaire.

66. Par ailleurs, aux termes de l'article 28, paragraphe 4, premier alinéa, de la directive 95/46, «[c]haque autorité de contrôle peut être saisie 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». L'article 28, paragraphe 4, second alinéa, de cette directive précise que «[c]haque 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 [ladite] directive sont d'application». Nous précisons que cette dernière disposition permet aux États membres de prendre des mesures législatives visant à limiter la portée de plusieurs obligations et droits prévus dans la directive 95/46, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder, notamment, la sûreté de l'État, la défense, la sécurité publique ainsi que la prévention, la recherche, la détection et la poursuite d'infractions pénales.

67. Ainsi que la Cour l'a déjà relevé, l'exigence de contrôle par une autorité indépendante du respect des règles du droit de l'Union relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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 [23]. Elle a également rappelé que «[l]'institution, dans les États membres, d'autorités de contrôle indépendantes constitue ainsi un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel» [24].

68. La Cour a aussi jugé que «l'article 28, paragraphe 1, second alinéa, de la directive 95/46 doit être interprété en ce sens que les autorités de contrôle compétentes pour la surveillance du traitement des données à caractère personnel doivent jouir d'une indépendance qui leur permette d'exercer leurs missions sans être soumises à une influence extérieure. Cette indépendance exclut notamment toute

22 — Voir, notamment, arrêt Koushkaki (C-84/12, EU:C:2013:862, point 34 et jurisprudence citée).

23 — Voir arrêts Commission/Autriche (C-614/10, EU:C:2012:631, point 36) et Commission/Hongrie (C-288/12, EU:C:2014:237, point 47).

24 — Voir, notamment, arrêt Commission/Hongrie (C-288/12, EU:C:2014:237, point 48 et jurisprudence citée). Voir également, en ce sens, arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 68 ainsi que jurisprudence citée).

injonction et toute autre influence extérieure sous quelque forme que ce soit, qu'elle soit directe ou indirecte, qui seraient susceptibles d'orienter leurs décisions et qui pourraient ainsi remettre en cause l'accomplissement, par lesdites autorités, de leur tâche consistant à établir un juste équilibre entre la protection du droit à la vie privée et la libre circulation des données à caractère personnel» [25].

69. La Cour a également précisé que «[l]a 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» [26]. Cette garantie d'indépendance a été établie «en vue de renforcer la protection des personnes et des organismes qui sont concernés par [les] décisions [de ces autorités nationales de contrôle]» [27].

70. Ainsi qu'il ressort notamment du considérant 10 et de l'article 1er de la directive 95/46, celle-ci vise à garantir, au sein de l'Union, «un niveau élevé de protection des libertés et des droits fondamentaux à l'égard du traitement de données à caractère personnel» [28]. Selon la Cour, «[l]es autorités de contrôle prévues à l'article 28 de la directive 95/46 sont donc les gardiennes desdits droits et libertés fondamentaux» [29].

71. Compte tenu de l'importance du rôle qu'occupent les autorités nationales de contrôle en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel, leurs pouvoirs d'intervention doivent demeurer entiers même lorsque la Commission a adopté une décision sur le fondement de l'article 25, paragraphe 6, de la directive 95/46.

72. Nous notons, à cet égard, que rien n'indique que les régimes de transfert de données à caractère personnel vers des pays tiers soient exclus du champ d'application matériel de l'article 8, paragraphe 3, de la Charte, lequel consacre au plus haut niveau de la hiérarchie des normes en droit de l'Union l'importance du contrôle exercé par une autorité indépendante en ce qui concerne le respect des règles relatives à la protection des données à caractère personnel.

73. Si les autorités nationales de contrôle étaient liées de manière absolue par les décisions adoptées par la Commission, cela limiterait inévitablement leur totale indépendance. Conformément à leur rôle de gardiennes des droits fondamentaux, les autorités nationales de contrôle doivent pouvoir enquêter, en toute indépendance, sur les réclamations qui leur sont soumises, dans l'intérêt supérieur de la protection des individus à l'égard du traitement des données à caractère personnel.

74. En outre, comme l'ont relevé à juste titre le gouvernement belge et le Parlement européen lors de l'audience, il n'existe aucun lien hiérarchique entre le chapitre IV de la directive 95/46 relatif au transfert de données à caractère personnel vers des pays tiers et le chapitre VI de celle-ci qui est consacré, notamment, au rôle des autorités nationales de contrôle. Rien dans ce chapitre VI ne suggère que les dispositions relatives aux autorités nationales de contrôle soient subordonnées d'une quelconque façon aux dispositions distinctes sur les transferts énoncées dans le chapitre IV de la directive 95/46.

75. Au contraire, il ressort expressément de l'article 25, paragraphe 1, de cette directive, figurant au chapitre IV de celle-ci, que l'autorisation du transfert de données à caractère personnel vers un pays tiers assurant un niveau de protection adéquat ne vaut que sous réserve du respect des dispositions nationales prises en application des autres dispositions de ladite directive.

25 — Voir, notamment, arrêt Commission/Hongrie (C-288/12, EU:C:2014:237, point 51 et jurisprudence citée).

26 — Arrêt Commission/Allemagne (C-518/07, EU:C:2010:125, point 25).

27 — Idem.

28 — Ibidem (point 22 et jurisprudence citée).

29 — Ibidem (point 23). Voir également, en ce sens, arrêts Commission/Autriche (C-614/10, EU:C:2012:631, point 52) et Commission/Hongrie (C-288/12, EU:C:2014:237, point 53).

76. Nous rappelons, à cet égard, que, en vertu de cette disposition, les États membres doivent prévoir dans leur législation nationale 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 directive 95/46, le pays tiers en question assure un niveau de protection adéquat.

77. Conformément à l'article 28, paragraphe 1, de cette directive, les autorités nationales de contrôle sont chargées de surveiller l'application, sur le territoire de chaque État membre, des dispositions adoptées par les États membres en application de ladite directive.

78. Le rapprochement entre ces deux dispositions permet de considérer que la règle énoncée à l'article 25, paragraphe 1, de la directive 95/46, selon laquelle le transfert de données à caractère personnel ne peut avoir lieu que si le pays tiers destinataire leur assure un niveau de protection adéquat, fait partie des règles dont les autorités nationales de contrôle doivent surveiller l'application.

79. Il convient d'interpréter largement, conformément à l'article 8, paragraphe 3, de la Charte, les pouvoirs des autorités nationales de contrôle pour enquêter en toute indépendance sur les réclamations dont elles sont saisies au titre de l'article 28 de la directive 95/46. Ces pouvoirs ne peuvent donc pas être limités par les pouvoirs conférés par le législateur de l'Union à la Commission, en vertu de l'article 25, paragraphe 6, de cette directive, afin de constater le caractère adéquat du niveau de protection offert par un pays tiers.

80. Eu égard à leur rôle essentiel en matière de protection des données à caractère personnel, les autorités nationales de contrôle doivent pouvoir enquêter lorsqu'elles sont saisies d'une plainte faisant état d'éléments qui pourraient être de nature à remettre en cause le niveau de protection assuré par un pays tiers, y compris lorsque la Commission a constaté, dans une décision prise sur le fondement de l'article 25, paragraphe 6, de la directive 95/46, que le pays tiers concerné assure un niveau de protection adéquat.

81. Si, au terme des investigations qui sont conduites par une autorité nationale de contrôle, celle-ci estime que le transfert de données contesté porte atteinte à la protection dont doivent bénéficier les citoyens de l'Union quant au traitement de leurs données, elle a le pouvoir de suspendre le transfert de données en cause, et ce quelle que soit l'évaluation générale faite par la Commission dans sa décision.

82. Il est, en effet, constant, aux termes de l'article 25, paragraphe 2, de la directive 95/46, que le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie en fonction d'un ensemble de circonstances tant factuelles que juridiques. Si l'une de ces circonstances évolue et apparaît comme étant de nature à remettre en cause le caractère adéquat du niveau de protection offert par un pays tiers, l'autorité nationale de contrôle saisie d'une plainte doit pouvoir en tirer les conséquences par rapport au transfert contesté.

83. Certes, comme l'Irlande l'a relevé, le commissaire, tout comme les autres autorités étatiques, est lié par la décision 2000/520. Il résulte, en effet, de l'article 288, quatrième alinéa, TFUE qu'une décision prise par une institution de l'Union est obligatoire dans tous ses éléments. Par conséquent, la décision 2000/520 s'impose aux États membres à qui elle est destinée.

84. Nous relevons, à cet égard, que la décision 2000/520 elle-même dispose, à son article 5, que «[l]es États membres prennent toutes les mesures nécessaires pour se conformer à [celle-ci] au plus tard quatre-vingt-dix jours après la date de sa notification aux États membres». En outre, l'article 6 de cette décision confirme que «[l]es États membres sont destinataires de [celle-ci]».

85. Cependant, nous estimons que, eu égard aux dispositions précitées de la directive 95/46 et de la Charte, l'effet obligatoire de la décision 2000/520 n'est pas de nature à exclure toute enquête du commissaire sur des plaintes alléguant que des transferts de données à caractère personnel effectués vers les États-Unis dans le cadre de cette décision ne présentent pas les garanties nécessaires de protection requises par le droit de l'Union. Autrement dit, un tel effet contraignant n'est pas de nature à imposer que toute plainte de ce genre soit rejetée sommairement, à savoir immédiatement et sans aucun examen de son bien-fondé.

86. Nous ajoutons qu'il ressort, en outre, de l'économie de l'article 25 de la directive 95/46 que le constat selon lequel un pays tiers assure ou non un niveau de protection adéquat peut être effectué soit par les États membres, soit par la Commission. Il s'agit donc d'une compétence partagée.

87. Il résulte de l'article 25, paragraphe 6, de cette directive que, dès lors que la Commission constate qu'un pays tiers assure un niveau de protection adéquat, au sens de l'article 25, paragraphe 2, de ladite directive, les États membres doivent prendre les mesures nécessaires pour se conformer à la décision de la Commission.

88. Une telle décision ayant pour effet de permettre les transferts de données à caractère personnel vers un pays tiers dont le niveau de protection est considéré par la Commission comme étant adéquat, les États membres doivent donc, en principe, permettre que de tels transferts soient effectués par les entreprises établies sur leur territoire.

89. L'article 25 de la directive 95/46 n'attribue cependant pas à la Commission l'exclusivité en matière de constat du niveau adéquat ou non de protection des données à caractère personnel transférées. L'économie de cet article témoigne de ce que les États membres occupent également un rôle en la matière. Une décision de la Commission joue, certes, un rôle important pour l'uniformisation des conditions de transfert valables au sein des États membres. Cependant, cette uniformisation ne peut perdurer qu'aussi longtemps que ce constat n'est pas remis en cause.

90. L'argument de la nécessaire uniformisation des conditions de transfert des données à caractère personnel vers un pays tiers trouve, à notre avis, sa limite dans une situation telle que celle en cause au principal où non seulement la Commission est informée de ce que son constat est sujet à critiques, mais également où c'est elle-même qui formule de telles critiques et conduit des négociations pour y remédier.

91. L'évaluation du caractère adéquat ou non du niveau de la protection offert par un pays tiers peut également donner lieu à une coopération entre les États membres et la Commission. L'article 25, paragraphe 3, de la directive 95/46 prévoit, à cet égard, que «[l]es 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». Ainsi que l'observe le Parlement, cela montre bien que les États membres et la Commission ont un rôle équivalent à jouer pour repérer les cas dans lesquels un pays tiers n'assure pas un niveau de protection adéquat.

92. La décision d'adéquation a pour objet d'autoriser le transfert de données à caractère personnel vers le pays tiers concerné. Cela n'implique pas que les autorités de contrôle ne peuvent plus être saisies par les citoyens de l'Union d'une demande visant à protéger leurs données à caractère personnel. Nous notons, à cet égard, que l'article 28, paragraphe 4, premier alinéa, de la directive 95/46, selon lequel «[c]haque autorité de contrôle peut être saisie 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 pas d'exception à ce principe en cas d'existence d'une décision adoptée par la Commission en application de l'article 25, paragraphe 6, de cette directive.

93. Ainsi, si une décision prise par la Commission en application des pouvoirs d'exécution qui lui sont conférés par cette dernière disposition a pour effet de permettre le transfert de données à caractère personnel vers un pays tiers, une telle décision ne saurait, en revanche, avoir pour effet d'ôter tout pouvoir aux États membres, et en particulier à leurs autorités nationales de contrôle, ou même seulement de restreindre leurs attributions, dès lors qu'elles se trouvent confrontées à des allégations de violations de droits fondamentaux.

94. Une autorité nationale de contrôle doit être en mesure d'exercer les pouvoirs prévus à l'article 28, paragraphe 3, de la directive 95/46, dont celui d'interdire temporairement ou définitivement un traitement de données à caractère personnel. Si l'énumération des pouvoirs, prévue à cette disposition, ne prévoit pas explicitement des pouvoirs relatifs à un transfert depuis un État membre vers un pays tiers, un tel transfert doit, à notre avis, être considéré comme constituant un traitement de données [30]. Ainsi qu'il résulte du libellé de ladite disposition, l'énumération n'est, en outre, pas exhaustive. En tout état de cause, eu égard au rôle essentiel joué par les autorités nationales de contrôle dans le système mis en place par la directive 95/46, celles-ci doivent disposer du pouvoir de suspendre un transfert de données en cas d'atteinte avérée ou de risque d'atteinte aux droits fondamentaux.

95. Nous ajoutons que priver l'autorité nationale de contrôle de ses pouvoirs d'investigation dans des circonstances telles que celles en cause dans la présente affaire serait contraire non seulement au principe d'indépendance, mais également à l'objectif de la directive 95/46 tel qu'il résulte de l'article 1er, paragraphe 1, de celle-ci.

96. Ainsi que la Cour l'a relevé, «[i]l ressort des considérants 3, 8 et 10 de la directive 95/46 que le législateur de l'Union a entendu faciliter la libre circulation des données à caractère personnel en rapprochant les législations des États membres tout en sauvegardant les droits fondamentaux des personnes, notamment le droit à la protection de la vie privée, et en garantissant un niveau élevé de protection dans l'Union. L'article 1er de cette directive prévoit ainsi que les États membres doivent assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel» [31].

97. Les dispositions de la directive 95/46 doivent donc être interprétées conformément à l'objectif de celle-ci visant à garantir un niveau élevé de protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel au sein de l'Union.

98. L'importance de cet objectif et le rôle que les États membres doivent jouer pour l'atteindre impliquent que, lorsque des circonstances particulières viennent à fonder un doute sérieux quant au respect des droits fondamentaux garantis par la Charte en cas de transfert de données à caractère personnel vers un pays tiers, les États membres, et donc, en leur sein, les autorités nationales de contrôle, ne peuvent être tenus de manière absolue par une décision d'adéquation de la Commission.

99. La Cour a déjà jugé que «les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui, selon une jurisprudence constante, font partie intégrante des principes généraux du droit dont la Cour assure le respect et qui sont désormais inscrits dans la Charte» [32].

30 — Voir conclusions de l'avocat général Léger dans l'affaire Parlement/Conseil et Commission (C-317/04, EU:C:2005:710, points 92 à 95). Voir, également, arrêt Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346, point 56).

31 — Voir, notamment, arrêt IPI (C-473/12, EU:C:2013:715, point 28 et jurisprudence citée).

32 — Voir, notamment, arrêt Google Spain et Google (C-131/12, EU:C:2014:317, point 68 et jurisprudence citée).

100. Nous nous référons, en outre, à la jurisprudence selon laquelle «il incombe aux États membres non seulement d'interpréter leur droit national d'une manière conforme au droit de l'Union, mais également de veiller à ne pas se fonder sur une interprétation d'un texte du droit dérivé qui entrerait en conflit avec les droits fondamentaux protégés par l'ordre juridique de l'Union ou avec les autres principes généraux du droit de l'Union» [33].

101. La Cour a ainsi jugé, dans son arrêt N. S. e.a. [34], qu'«une application du règlement [(CE)] nº 343/2003 [35] sur la base d'une présomption irréfragable que les droits fondamentaux du demandeur d'asile seront respectés dans l'État membre normalement compétent pour connaître de sa demande est incompatible avec l'obligation des États membres d'interpréter et d'appliquer le règlement nº 343/2003 d'une manière conforme aux droits fondamentaux» [36].

102. À cet égard, la Cour a admis, dans le contexte du statut des États membres en tant que pays d'origine sûrs les uns vis-à-vis des autres pour les questions juridiques et pratiques liées au droit d'asile, qu'il doit être présumé que le traitement réservé aux demandeurs d'asile dans chaque État membre est conforme aux exigences de la Charte, à la convention relative au statut des réfugiés, signée à Genève le 28 juillet 1951 [37], ainsi qu'à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 [38]. Cependant, la Cour a jugé qu'«[i]l ne saurait [...] être exclu que ce système rencontre, en pratique, des difficultés majeures de fonctionnement dans un État membre déterminé, de sorte qu'il existe un risque sérieux que des demandeurs d'asile soient, en cas de transfert vers cet État membre, traités d'une manière incompatible avec leurs droits fondamentaux» [39].

103. Par conséquent, la Cour a jugé qu'«il incombe aux États membres, en ce compris les juridictions nationales, de ne pas transférer un demandeur d'asile vers l'"État membre responsable" au sens du règlement nº 343/2003 lorsqu'ils ne peuvent ignorer que les défaillances systémiques de la procédure d'asile et des conditions d'accueil des demandeurs d'asile dans cet État membre constituent des motifs sérieux et avérés de croire que le demandeur courra un risque réel d'être soumis à des traitements inhumains ou dégradants au sens de l'article 4 de la Charte» [40].

104. L'apport de l'arrêt N. S. e.a. [41] nous paraît pouvoir être étendu à une situation telle que celle en cause au principal. Ainsi, une interprétation du droit dérivé de l'Union qui reposerait sur une présomption irréfragable que les droits fondamentaux seront respectés – que ce soit par un État membre, par la Commission ou par un pays tiers – doit être considérée comme étant incompatible avec l'obligation des États membres d'interpréter et d'appliquer le droit dérivé de l'Union d'une manière conforme aux droits fondamentaux. L'article 25, paragraphe 6, de la directive 95/46 n'impose donc pas une telle présomption irréfragable de respect des droits fondamentaux en ce qui concerne l'appréciation par la Commission du caractère adéquat du niveau de protection offert par un pays tiers. Au contraire, la présomption, sous-tendant cette disposition, que le transfert de données vers un pays tiers respecte les droits fondamentaux doit être considérée comme réfragable [42]. Par conséquent, ladite disposition ne devrait pas être interprétée comme remettant en cause les garanties figurant notamment à l'article 28, paragraphe 3, de la directive 95/46 et à l'article 8, paragraphe 3, de la Charte, visant à la protection et au respect du droit à la protection des données à caractère personnel.

33 — Voir, notamment, arrêt N. S. e.a. (C-411/10 et C-493/10, EU:C:2011:865, point 77 ainsi que jurisprudence citée).

34 — C-411/10 et C-493/10, EU:C:2011:865.

35 — Règlement du Conseil du 18 février 2003 établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers (JO L 50, p. 1).

36 — Point 99 de cet arrêt.

37 — *Recueil des traités des Nations unies,* vol. 189, p. 150, nº 2545 (1954).

38 — Voir arrêt N. S. e.a. (C-411/10 et C-493/10, EU:C:2011:865, point 80).

39 — Ibidem (point 81).

40 — Ibidem (point 94).

41 — C-411/10 et C-493/10, EU:C:2011:865.

42 — Point 104 de cet arrêt.

105. Nous déduisons donc dudit arrêt que, en cas de défaillances systémiques constatées dans le pays tiers vers lequel des données à caractère personnel sont transférées, les États membres doivent pouvoir prendre les mesures nécessaires à la sauvegarde des droits fondamentaux protégés par les articles 7 et 8 de la Charte.

106. Par ailleurs, comme l'a relevé le gouvernement italien dans ses observations, l'adoption par la Commission d'une décision d'adéquation ne saurait avoir pour effet de réduire la protection des citoyens de l'Union à l'égard du traitement de leurs données lorsque celles-ci sont transférées vers un pays tiers par rapport au niveau de protection dont ces personnes jouiraient si leurs données faisaient l'objet d'un traitement au sein de l'Union. Les autorités nationales de contrôle doivent, par conséquent, être en mesure d'intervenir et d'exercer leurs pouvoirs à l'égard de transferts de données vers des pays tiers faisant l'objet d'une décision d'adéquation. Dans le cas contraire, les citoyens de l'Union seraient moins bien protégés qu'en cas de traitement de leurs données au sein de l'Union.

107. Ainsi, l'adoption par la Commission d'une décision en application de l'article 25, paragraphe 6, de la directive 95/46 a uniquement pour effet de lever l'interdiction générale d'exportation des données à caractère personnel vers des pays tiers garantissant un niveau de protection comparable à celui qu'offre cette directive. Autrement dit, il ne s'agit pas de créer un régime spécial d'exception et moins protecteur pour les citoyens de l'Union par rapport au régime général prévu par ladite directive pour les traitements de données qui s'opèrent à l'intérieur de l'Union.

108. Certes, la Cour a indiqué, au point 63 de son arrêt Lindqvist [43], que «[l]e chapitre IV de la directive 95/46, dans lequel figure l'article 25, met en place un régime spécial». Toutefois, cela ne signifie pas, selon nous, qu'un tel régime doit être moins protecteur. Au contraire, afin d'atteindre l'objectif de protection des données fixé à l'article 1er, paragraphe 1, de la directive 95/46, l'article 25 de celle-ci impose une série d'obligations aux États membres et à la Commission [44] et cet article 25 pose le principe selon lequel 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 [45].

109. S'agissant plus spécifiquement du régime de la sphère de sécurité, la Commission n'envisage l'intervention des autorités nationales de contrôle et la suspension par elles des flux de données que dans le cadre tracé par l'article 3, paragraphe 1, sous b), de la décision 2000/520.

110. Selon le considérant 8 de cette décision, «[d]ans 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».

111. Dans le cadre de la présente affaire, c'est plus particulièrement l'application de l'article 3, paragraphe 1, sous b), de ladite décision qui a été discutée. Ainsi, en vertu de cette disposition, la suspension de flux de données peut être décidée par les autorités nationales de contrôle dans les cas «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».

43 — C-101/01, EU:C:2003:596.

44 — Point 65.

45 — Point 64.

112. Ladite disposition pose plusieurs conditions qui ont fait l'objet de diverses interprétations par les parties au cours de la présente procédure [46]. Sans entrer dans le détail de ces interprétations, il en ressort que ces conditions encadrent de manière stricte le pouvoir des autorités nationales de contrôle de suspendre des flux de données.

113. Or, contrairement à ce que fait valoir la Commission, l'article 3, paragraphe 1, sous b), de la décision 2000/520 doit être interprété conformément à l'objectif de protection des données à caractère personnel que poursuit la directive 95/46 ainsi qu'à la lumière de l'article 8 de la Charte. L'impératif d'interprétation conforme aux droits fondamentaux milite en faveur d'une interprétation large de cette disposition.

114. Il s'ensuit que les conditions qui sont prévues à l'article 3, paragraphe 1, sous b), de la décision 2000/520 ne sauraient, à notre avis, empêcher une autorité nationale de contrôle d'exercer, en toute indépendance, les pouvoirs dont elle est investie en vertu de l'article 28, paragraphe 3, de la directive 95/46.

115. Comme l'ont indiqué, en substance, les gouvernements belge et autrichien lors de l'audience, l'issue de secours que constitue l'article 3, paragraphe 1, sous b), de la décision 2000/520 est tellement étroite qu'elle est difficile à mettre en pratique. Elle exige des critères cumulatifs et place la barre trop haut. Or, à la lumière de l'article 8, paragraphe 3, de la Charte, il est impossible que la marge de manœuvre des autorités nationales de contrôle concernant les prérogatives qui procèdent de l'article 28, paragraphe 3, de la directive 95/46 soit limitée de telle sorte que celles-ci ne pourraient plus être exercées.

116. À cet égard, le Parlement a, à juste titre, fait remarquer que c'est le législateur de l'Union qui a décidé quels étaient les pouvoirs qui devaient revenir aux autorités nationales de contrôle. 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 n'affecte pas les pouvoirs conférés par ce même législateur aux autorités nationales de contrôle à l'article 28, paragraphe 3, de cette directive. Autrement dit, la Commission ne dispose pas de la compétence de restreindre les pouvoirs des autorités nationales de contrôle.

117. Par conséquent, pour assurer une protection appropriée des droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel, les autorités nationales de contrôle doivent être habilitées, en cas d'allégations faisant état de violations de ces droits, à mener des enquêtes. Si, à l'issue de telles investigations, ces autorités considèrent qu'il existe dans un pays tiers couvert par une décision d'adéquation des indices sérieux d'atteinte au droit des citoyens de l'Union à la protection de leurs données à caractère personnel, elles doivent pouvoir suspendre le transfert de données vers le destinataire établi dans ce pays tiers.

118. Autrement dit, les autorités nationales de contrôle doivent pouvoir mener leurs investigations et, le cas échéant, suspendre un transfert de données, indépendamment des conditions restrictives fixées à l'article 3, paragraphe 1, sous b), de la décision 2000/520.

46 — Selon M. Schrems, la première condition, selon laquelle «il est fort probable que les principes sont violés», ne serait pas remplie. Or, il n'est pas allégué que Facebook USA, en tant qu'organisme autocertifié auquel des données sont transférées, aurait elle-même violé les principes de la sphère de sécurité du fait de l'accès de masse et indifférencié par les autorités américaines aux données qu'elle détient. En effet, les principes de la sphère de sécurité sont expressément limités par le droit américain, que l'annexe I, quatrième alinéa, de la décision 2000/520 définit en renvoyant aux textes législatifs, aux règlements administratifs et aux décisions jurisprudentielles.

119. Par ailleurs, en vertu de leur pouvoir d'ester en justice en cas de violations des dispositions nationales prises en application de la directive 95/46 ou de leur pouvoir de porter ces violations à la connaissance de l'autorité judiciaire, prévus à l'article 28, paragraphe 3, de cette directive, les autorités nationales de contrôle devraient pouvoir, lorsqu'elles ont connaissance de faits démontrant qu'un pays tiers n'assure pas un niveau de protection adéquat, saisir un juge national qui, lui-même, pourra décider, le cas échéant, d'opérer un renvoi préjudiciel devant la Cour aux fins d'apprécier la validité d'une décision d'adéquation de la Commission.

120. Il résulte de l'ensemble de ces éléments que l'article 28 de la directive 95/46, lu à la lumière des articles 7 et 8 de la Charte, doit être interprété en ce sens que l'existence d'une décision adoptée par la Commission sur le fondement de l'article 25, paragraphe 6, de cette directive n'a pas pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat aux données à caractère personnel transférées et, le cas échéant, de suspendre le transfert de ces données.

121. Même si la Haute Cour de justice souligne, dans sa décision de renvoi, que M. Schrems n'a contesté formellement dans le recours au principal ni la validité de la directive 95/46 ni celle de la décision 2000/520, il ressort de cette décision de renvoi que la critique principale formulée par M. Schrems vise à remettre en cause le constat selon lequel les États-Unis assurent, dans le cadre du régime de la sphère de sécurité, un niveau de protection adéquat aux données à caractère personnel transférées.

122. Il ressort également des observations du commissaire que la plainte de M. Schrems vise à mettre directement en cause la décision 2000/520. En déposant cette plainte, ce dernier a voulu attaquer les termes et le fonctionnement du régime de la sphère de sécurité en tant que tel au motif que la surveillance de masse des données à caractère personnel transférées aux États-Unis démontrerait qu'il n'existe pas de véritable protection de ces données dans le droit et dans les pratiques en vigueur dans ce pays tiers.

123. De plus, la juridiction de renvoi observe elle-même que la garantie offerte par l'article 7 de la Charte et par les valeurs essentielles communes aux traditions constitutionnelles des États membres serait compromise si l'on permettait aux pouvoirs publics d'avoir accès aux communications électroniques de manière aléatoire et généralisée sans devoir fournir une motivation objective fondée sur des raisons de sécurité nationale ou de prévention de la criminalité liées spécifiquement aux individus concernés et sans aucune garantie adéquate et vérifiable [47]. La juridiction de renvoi émet ainsi indirectement des doutes sur la validité de la décision 2000/520.

124. L'appréciation du point de savoir si les États-Unis, dans le cadre du régime de la sphère de sécurité, garantissent un niveau de protection adéquat aux données à caractère personnel transférées conduit donc nécessairement à se pencher sur la validité de cette décision.

125. À cet égard, il convient de relever que, dans le cadre de l'instrument de coopération entre la Cour et les juridictions nationales institué par l'article 267 TFUE, la Cour, même exclusivement saisie à titre préjudiciel d'une question d'interprétation du droit de l'Union, peut, dans certaines circonstances particulières, être amenée à examiner la validité de dispositions de droit dérivé.

126. Partant, la Cour a, à plusieurs reprises, déclaré d'office invalide un acte dont seule l'interprétation lui était demandée [48]. Elle a également jugé que, «lorsqu'il apparaît que le véritable objet des questions posées par une juridiction nationale relève de l'examen de la validité plus que de l'interprétation des actes [de l'Union], il appartient à la Cour d'éclairer immédiatement ladite juridiction sans l'obliger à

47 — Point 24 de la décision de renvoi.

48 — Voir, notamment, arrêts Strehl (62/76, EU:C:1977:18, points 10 à 17); Roquette Frères (145/79, EU:C:1980:234, point 6), ainsi que Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, points 32 à 39).

un formalisme purement dilatoire incompatible avec la nature propre des mécanismes institués par l'article [267 TFUE]» [49]. La Cour a, par ailleurs, déjà considéré que les doutes manifestés par une juridiction de renvoi sur la compatibilité d'un acte de droit dérivé avec les règles relatives à la protection des droits fondamentaux devaient être compris comme mettant en cause la validité de cet acte au regard du droit de l'Union [50].

127. Nous rappelons également qu'il résulte de la jurisprudence de la Cour que les actes des institutions, des organes et des organismes de l'Union jouissent d'une présomption de validité, ce qui implique que ceux-ci produisent 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. La Cour est seule compétente pour constater l'invalidité d'un acte de l'Union, compétence ayant pour objet de garantir la sécurité juridique en assurant l'application uniforme du droit de l'Union. À défaut de déclaration d'invalidité, de modification ou d'abrogation par la Commission, la décision demeure obligatoire dans tous ses éléments et directement applicable dans tout État membre [51].

128. Afin de fournir une réponse complète à la juridiction de renvoi et de lever les doutes exprimés au cours de la présente procédure sur la validité de la décision 2000/520, nous sommes d'avis que la Cour devrait donc procéder à une appréciation de validité de cette décision.

129. Cela étant, il importe également de préciser que l'examen du point de savoir si la décision 2000/520 est ou non valide doit être circonscrit aux griefs qui ont fait l'objet d'un débat dans le cadre de la présente procédure. En effet, tous les aspects relatifs au fonctionnement du régime de la sphère de sécurité n'ont pas été débattus dans ce cadre, c'est pourquoi il ne nous semble pas possible de nous livrer ici à un examen exhaustif des insuffisances de ce régime.

130. En revanche, la question de savoir si l'accès généralisé et non ciblé des services de renseignement américains aux données transférées est susceptible d'affecter la légalité de la décision 2000/520 a fait l'objet d'un débat devant la Cour dans le cadre de la présente procédure. La validité de cette décision peut donc être appréciée sous cet angle.

B – *Sur la validité de la décision 2000/520*

1. Sur les éléments à prendre en compte pour apprécier la validité de la décision 2000/520

131. Il convient de rappeler la jurisprudence selon laquelle, «dans le cadre d'un recours en annulation, la légalité d'un acte doit être appréciée en fonction des éléments de fait et de droit existant à la date où l'acte a été adopté, l'appréciation de la Commission ne pouvant être censurée que si elle apparaît manifestement erronée au vu des éléments dont elle disposait au moment de l'adoption de l'acte en cause» [52].

49 — Arrêt Schwarze (16/65, EU:C:1965:117, p. 1094).

50 — Voir arrêt Hauer (44/79, EU:C:1979:290, point 16).

51 — Voir, notamment, arrêt CIVAD (C-533/10, EU:C:2012:347, points 39 à 41 et jurisprudence citée).

52 — Voir, notamment, arrêt BVGD/Commission (T-104/07 et T-339/08, EU:T:2013:366, point 291), se référant à l'arrêt IECC/Commission (C-449/98 P, EU:C:2001:275, point 87).

132. Dans son arrêt Gaz de France – Berliner Investissement [53], la Cour a rappelé le principe selon lequel «l'appréciation de la validité d'un acte, à laquelle il appartient à la Cour de procéder dans le cadre d'un renvoi préjudiciel, doit normalement être fondée sur la situation qui existe au moment de l'adoption de l'acte» [54]. Elle a, cependant, semblé admettre que «la validité d'un acte puisse, dans certains cas, être appréciée en fonction d'éléments nouveaux survenus postérieurement à son adoption» [55].

133. Cette ouverture ainsi esquissée par la Cour nous paraît particulièrement pertinente dans le cadre de la présente affaire.

134. En effet, les décisions adoptées par la Commission sur le fondement de l'article 25, paragraphe 6, de la directive 95/46 présentent des caractéristiques particulières. Elles sont destinées à évaluer si le niveau de protection des données à caractère personnel qui est offert par un pays tiers présente ou non un caractère adéquat. Il s'agit là d'une appréciation qui est destinée à évoluer en fonction du contexte factuel et juridique qui prévaut dans le pays tiers.

135. Eu égard au fait que la décision d'adéquation constitue un type particulier de décision, la règle selon laquelle l'appréciation de validité de celle-ci ne pourrait être effectuée qu'en fonction des éléments qui existaient au moment de son adoption doit être nuancée en l'espèce. Une telle règle conduirait sinon à ce que, plusieurs années après l'adoption d'une décision d'adéquation, l'appréciation de validité à laquelle la Cour doit procéder ne puisse prendre en compte des événements qui se sont produits ultérieurement, et ce alors même qu'un renvoi préjudiciel en appréciation de validité n'a pas de limite dans le temps et que son déclenchement peut précisément être la conséquence de faits postérieurs qui révèlent les insuffisances de l'acte en cause.

136. En l'espèce, le maintien en vigueur de la décision 2000/520 depuis environ quinze ans témoigne de la confirmation implicite par la Commission de son évaluation faite en 2000. Lorsque, dans le cadre d'un renvoi préjudiciel, la Cour est amenée à apprécier la validité d'une évaluation maintenue dans le temps par la Commission, il est, dès lors, non seulement possible, mais également approprié qu'elle puisse confronter cette évaluation aux circonstances nouvelles qui sont intervenues depuis l'adoption de la décision d'adéquation.

137. Compte tenu de la nature particulière de la décision d'adéquation, celle-ci doit faire l'objet d'un réexamen régulier par la Commission. Si, à la suite de nouveaux événements intervenus entre-temps, la Commission ne modifie pas sa décision, c'est qu'elle confirme implicitement, mais nécessairement, l'appréciation effectuée initialement. Elle réitère ainsi son constat selon lequel le pays tiers concerné assure un niveau de protection adéquat aux données à caractère personnel transférées. Il revient à la Cour d'examiner si ce constat continue à être valable malgré les circonstances intervenues postérieurement.

138. Afin d'assurer un contrôle juridictionnel effectif de ce type de décision, l'appréciation de la validité de celle-ci doit donc, à notre avis, être effectuée en tenant compte du contexte factuel et juridique actuel.

53 — C-247/08, EU:C:2009:600.

54 — Point 49 et jurisprudence citée.

55 — Point 50 et jurisprudence citée. Voir, en ce sens, Lenaerts, K., Maselis, I., et Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, qui énoncent que, «in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court» (point 10.16, p. 471).

2. Sur la notion de niveau de protection adéquat

139. L'article 25 de la directive 95/46 repose tout entier sur le principe selon lequel le transfert de données à caractère personnel vers un pays tiers ne peut avoir lieu à moins que ce pays tiers ne garantisse un niveau de protection adéquat à de telles données. L'objectif de cet article est ainsi d'assurer la continuité de la protection conférée par cette directive en cas de transfert de données à caractère personnel vers un pays tiers. Il convient, à cet égard, de rappeler que ladite directive offre un niveau élevé de protection des citoyens de l'Union à l'égard du traitement de leurs données à caractère personnel.

140. Compte tenu du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée, un tel niveau élevé de protection doit, dès lors, être garanti, y compris en cas de transfert de données à caractère personnel vers un pays tiers.

141. C'est pourquoi nous considérons que la Commission ne peut constater, sur le fondement de l'article 25, paragraphe 6, de la directive 95/46, qu'un pays tiers assure un niveau de protection adéquat que lorsque, au terme d'une évaluation d'ensemble du droit et de la pratique dans le pays tiers en question, elle est en mesure d'établir que ce pays tiers offre un niveau de protection substantiellement équivalent à celui offert par cette directive, même si les modalités de cette protection peuvent être différentes de celles qui ont généralement cours au sein de l'Union.

142. Bien que le terme anglais «adequate» puisse être compris, d'un point de vue linguistique, comme désignant un niveau de protection tout juste satisfaisant ou suffisant, et avoir ainsi un champ sémantique différent du terme français «adéquat», il convient d'observer que le seul critère qui doit guider l'interprétation de ce terme est l'objectif d'atteindre un niveau élevé de protection des droits fondamentaux, comme le requiert la directive 95/46.

143. L'examen du niveau de protection offert par un pays tiers doit s'intéresser à deux éléments fondamentaux, à savoir le contenu des règles applicables et les moyens d'assurer le respect de ces règles [56].

144. Selon nous, pour atteindre un niveau de protection substantiellement équivalent à celui en vigueur au sein de l'Union, le régime de la sphère de sécurité, qui repose en grande partie sur l'autocertification et sur l'autoévaluation par les entreprises participant volontairement à ce régime, devrait être assorti de garanties adéquates et d'un mécanisme de contrôle suffisant. Ainsi, les transferts de données à caractère personnel vers des pays tiers ne devraient pas bénéficier d'une protection plus faible que les traitements qui sont effectués au sein de l'Union.

145. À cet égard, nous relevons, d'emblée, que, au sein de l'Union, prévaut la conception selon laquelle un dispositif de contrôle externe sous la forme d'une autorité indépendante constitue un élément nécessaire de tout système visant à assurer le respect des règles relatives à la protection des données à caractère personnel.

146. Par ailleurs, afin d'assurer l'effet utile de l'article 25, paragraphes 1 à 3, de la directive 95/46, il convient de tenir compte du fait que le caractère adéquat du niveau de protection offert par un pays tiers est une situation évolutive qui peut changer au fil du temps en fonction d'une série de facteurs. Les États membres et la Commission doivent, dès lors, être constamment attentifs à tout changement de circonstances susceptible de rendre nécessaire une réévaluation du caractère adéquat du niveau de

56 — Voir p. 5 du document de travail WP 12 de la Commission, intitulé «Transferts de données personnelles vers des pays tiers: Application des articles 25 et 26 de la directive relative à la protection des données», adopté par le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel le 24 juillet 1998.

protection offert par un pays tiers. Une évaluation du caractère adéquat de ce niveau de protection ne peut nullement être fixée à un moment donné et, ensuite, être maintenue indéfiniment, indépendamment de tout changement de circonstances montrant que, en réalité, le niveau de protection offert n'est plus adéquat.

147. L'obligation pour le pays tiers d'assurer un niveau de protection adéquat constitue ainsi une obligation continue. Si l'évaluation est faite à un moment donné, le maintien de la décision d'adéquation suppose qu'aucune circonstance intervenue depuis ne soit de nature à remettre en cause l'évaluation initiale effectuée par la Commission.

148. En effet, il ne faut pas perdre de vue que l'objectif de l'article 25 de la directive 95/46 est d'éviter que les données à caractère personnel ne soient transférées vers un pays tiers qui n'assure pas un niveau de protection adéquat, en violation du droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte.

149. Il importe de souligner que le pouvoir conféré par le législateur de l'Union à la Commission, à l'article 25, paragraphe 6, de la directive 95/46, de constater qu'un pays tiers assure un niveau de protection adéquat est expressément conditionné à l'exigence que ce pays tiers assure un tel niveau au sens du paragraphe 2 de cet article. Si de nouvelles circonstances sont de nature à remettre en cause l'évaluation initiale de la Commission, cette dernière devrait adapter sa décision en conséquence.

3. Notre appréciation

150. Nous rappelons que, en vertu de l'article 25, paragraphe 6, de la directive 95/46, «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». Lu en liaison avec l'article 25, paragraphe 2, de cette directive, l'article 25, paragraphe 6, de celle-ci signifie que, pour constater qu'un pays tiers assure un niveau de protection adéquat, la Commission doit procéder à une évaluation d'ensemble des règles de droit en vigueur dans ce pays tiers ainsi que de leur application.

151. Nous avons vu que le maintien par la Commission de sa décision 2000/520, malgré la survenance d'éléments factuels et juridiques nouveaux, doit être compris comme une volonté de sa part de confirmer son évaluation initiale.

152. Il n'appartient pas à la Cour, dans le cadre d'un renvoi préjudiciel, d'apprécier les faits qui sont à l'origine du litige ayant conduit la juridiction nationale à opérer ce renvoi [57].

153. Nous nous appuierons donc sur les faits indiqués par la juridiction de renvoi dans sa demande de décision préjudicielle, faits qui, au demeurant, sont largement admis par la Commission elle-même comme étant établis [58].

154. Les éléments qui ont été avancés devant la Cour pour contester l'évaluation de la Commission selon laquelle le régime relatif à la sphère de sécurité assure un niveau de protection adéquat aux données à caractère personnel transférées depuis l'Union vers les États-Unis peuvent être ainsi décrits.

57 — Voir, notamment, arrêt Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, point 22 et jurisprudence citée).

58 — Voir communication de la Commission mentionnée à la note en bas de page 2 et communication de la Commission 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].

155. Dans sa demande de décision préjudicielle, la juridiction de renvoi part des deux constats factuels suivants. D'une part, les données à caractère personnel transférées par des entreprises telles que Facebook Ireland à leur société mère établie aux États-Unis sont, ensuite, susceptibles d'être consultées par la NSA ainsi que par d'autres agences de sécurité américaines au cours d'activités de surveillance et d'interception massives et non ciblées. En effet, à la suite des révélations de M. Snowden, aucune autre conclusion plausible ne saurait, à l'heure actuelle, être tirée des éléments de preuve disponibles [59]. D'autre part, les citoyens de l'Union ne disposeraient d'aucun droit effectif d'être entendus sur la question de la surveillance et de l'interception de leurs données par la NSA et par d'autres agences de sécurité américaines [60].

156. Les constats factuels ainsi effectués par la Haute Cour de justice sont étayés par les constatations effectuées par la Commission elle-même.

157. Ainsi, dans sa communication relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, susmentionnée, la Commission est partie du constat que, dans le courant de l'année 2013, des informations sur l'ampleur et la portée des programmes de surveillance américains ont suscité des préoccupations concernant la continuité de la protection des données à caractère personnel légalement transférées aux États-Unis au titre de la sphère de sécurité. Elle a relevé que toutes les entreprises participant au programme PRISM, 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. Selon elle, la sphère de sécurité est donc devenue l'une des voies par lesquelles les autorités américaines de renseignement ont accès à la collecte des données à caractère personnel initialement traitées au sein de l'Union [61].

158. Il résulte de ces éléments que le droit et la pratique des États-Unis permettent de collecter, à large échelle, les données à caractère personnel de citoyens de l'Union qui sont transférées dans le cadre du régime de la sphère de sécurité, sans que ces derniers bénéficient d'une protection juridictionnelle effective.

159. Ces constats factuels démontrent, à notre avis, que la décision 2000/520 ne contient pas suffisamment de garanties. En raison de ce défaut de garanties, cette décision a été mise en œuvre d'une manière qui ne répond pas aux exigences requises par la Charte ainsi que par la directive 95/46.

160. Or, une décision adoptée par la Commission sur le fondement de l'article 25, paragraphe 6, de la directive 95/46 a pour objet de constater qu'un pays tiers «assure» un niveau de protection adéquat. Le terme «assure», conjugué au temps présent, implique que, pour pouvoir être maintenue, une telle décision doit concerner un pays tiers qui continue, après l'adoption de ladite décision, à garantir un niveau de protection adéquat.

161. En réalité, les révélations dont il est fait état sur les agissements de la NSA qui utiliserait des données transférées dans le cadre du régime de la sphère de sécurité ont jeté la lumière sur les faiblesses de la base légale que constitue la décision 2000/520.

162. Les insuffisances qui ont été mises en exergue au cours de la présente procédure figurent plus particulièrement à l'annexe I, quatrième alinéa, de cette décision.

59 — Point 7, sous c), de la décision de renvoi.

60 — Point 7, sous b), de la décision de renvoi.

61 — Page 19 de sa communication.

163. Nous rappelons que, aux termes de cette disposition, «[l]'adhésion aux principes [de la sphère de sécurité] peut être limitée par: a) les exigences relatives à la sécurité nationale, l'intérêt public et le 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».

164. Le problème vient essentiellement de l'utilisation qui est faite par les autorités américaines des dérogations prévues à ladite disposition. En raison de leur formulation trop générale, la mise en œuvre de ces dérogations par ces autorités n'est pas limitée à ce qui est strictement nécessaire.

165. À cette formulation trop générale s'ajoute la circonstance que les citoyens de l'Union ne disposent pas de voie de recours adaptée contre le traitement de leurs données à caractère personnel à d'autres fins que celles pour lesquelles elles ont été initialement collectées, puis transférées vers les États-Unis.

166. Les dérogations prévues par la décision 2000/520 à l'application des principes de la sphère de sécurité, notamment pour des exigences de sécurité nationale, auraient dû être accompagnées par la mise en place d'un mécanisme de contrôle indépendant propre à éviter les atteintes constatées au droit à la vie privée.

167. Ainsi, les révélations sur les pratiques des services de renseignement américains quant à la surveillance généralisée des données transférées dans le cadre de la sphère de sécurité ont mis en lumière certaines insuffisances propres à la décision 2000/520.

168. Les allégations dont il est fait état dans le cadre de la présente affaire ne sont pas constitutives d'une violation par Facebook des principes de la sphère de sécurité. Si une entreprise certifiée, telle que Facebook USA, donne aux autorités américaines accès aux données qui lui ont été transférées depuis un État membre, il peut être considéré qu'elle le fait pour se conformer à la législation américaine. Eu égard au fait qu'une telle situation est expressément admise par la décision 2000/520, en raison de la formulation large des dérogations qu'elle contient, c'est, en réalité, la question de la compatibilité de telles dérogations avec le droit primaire de l'Union qui est soulevée dans le cadre de la présente affaire.

169. Il convient, à cet égard, de souligner qu'il ressort d'une jurisprudence constante de la Cour que le respect des droits de l'homme constitue une condition de la légalité des actes de l'Union et que ne sauraient être admises dans l'Union des mesures incompatibles avec le respect de ceux-ci [62].

170. Il résulte, par ailleurs, de la jurisprudence de la Cour que la communication des données à caractère personnel collectées à des tiers, publics ou privés, constitue une ingérence dans le droit au respect de la vie privée «quelle que soit l'utilisation ultérieure des informations ainsi communiquées» [63]. En outre, dans son arrêt Digital Rights Ireland e.a. [64], la Cour a confirmé que le fait d'autoriser les autorités nationales compétentes à avoir accès à de telles données constitue une atteinte supplémentaire à ce droit fondamental [65]. De plus, toute forme de traitement des données à caractère personnel est visée à l'article 8 de la Charte et constitue une ingérence dans le droit à la protection de

62 — Voir, notamment, arrêt Kadi et Al Barakaat International Foundation/Conseil et Commission (C-402/05 P et C-415/05 P, EU:C:2008:461, point 284 ainsi que jurisprudence citée).

63 — Arrêt Österreichischer Rundfunk e.a. (C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 74).

64 — C-293/12 et C-594/12, EU:C:2014:238.

65 — Point 35.

telles données [66]. L'accès dont disposent les services de renseignement américains aux données transférées est donc également constitutif d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte, puisqu'un tel accès constitue un traitement de ces données.

171. À l'instar de ce que la Cour a constaté dans cet arrêt, l'ingérence ainsi identifiée est d'une vaste ampleur et doit être considérée comme particulièrement grave, eu égard au nombre important d'utilisateurs concernés et des quantités de données transférées. Ces éléments, associés au caractère secret de l'accès par les autorités américaines aux données à caractère personnel transférées vers les entreprises établies aux États-Unis, rendent l'ingérence extrêmement sérieuse.

172. À cela s'ajoute la circonstance que les citoyens de l'Union, utilisateurs de Facebook, ne sont pas informés du fait que leurs données à caractère personnel seront d'une manière générale accessibles pour les agences de sécurité américaines.

173. Il convient également de mettre l'accent sur le fait que la juridiction de renvoi a constaté que, aux États-Unis, les citoyens de l'Union n'ont aucun droit effectif d'être entendus sur la question de la surveillance et de l'interception de leurs données. La FISC exerce une supervision, mais la procédure devant elle est secrète et non contradictoire [67]. Nous considérons qu'il s'agit là d'une ingérence dans le droit des citoyens de l'Union à un recours effectif protégé par l'article 47 de la Charte.

174. L'ingérence que permettent les dérogations aux principes de la sphère de sécurité figurant à l'annexe I, quatrième alinéa, de la décision 2000/520 dans les droits fondamentaux protégés par les articles 7, 8 et 47 de la Charte est donc constituée.

175. Il y a lieu, à présent, de vérifier si cette ingérence est ou non justifiée.

176. Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi et doit respecter le contenu essentiel de ces droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées auxdits droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui.

177. Au vu des conditions ainsi posées pour pouvoir admettre des limitations à l'exercice des droits et des libertés protégés par la Charte, nous doutons fortement que les limitations qui sont en cause dans la présente affaire puissent être considérées comme respectant le contenu essentiel des articles 7 et 8 de la Charte. En effet, l'accès des services de renseignement américains aux données transférées semble s'étendre au contenu des communications électroniques, ce qui porterait atteinte au contenu essentiel du droit fondamental au respect de la vie privée et des autres droits consacrés à l'article 7 de la Charte. De plus, dans la mesure où la formulation large des limitations prévues à l'annexe I, quatrième alinéa, de la décision 2000/520 permet potentiellement d'écarter l'application de l'ensemble des principes de la sphère de sécurité, il pourrait être considéré que ces limitations portent atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel [68].

66 — Point 36.

67 — Point 7, sous b), de la décision de renvoi.

68 — Voir, à cet égard, arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, points 39 et 40).

178. Quant à la question de savoir si l'ingérence constatée répond à un objectif d'intérêt général, nous rappelons, d'abord, que, aux termes de l'annexe I, quatrième alinéa, sous b), de la décision 2000/520, l'adhésion aux principes de la sphère de sécurité peut être limitée 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».

179. Force est de constater que les «intérêts légitimes» dont il est fait mention à cette disposition ne sont pas précisés. Il en résulte une incertitude quant au champ d'application, potentiellement extrêmement large, de cette dérogation à l'application des principes de la sphère de sécurité par les entreprises adhérentes.

180. La lecture des explications contenues au titre B de l'annexe IV de la décision 2000/520, intitulé «Autorisations légales explicites», confirme cette impression, en particulier l'affirmation selon laquelle «[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». Il est, par ailleurs, indiqué, s'agissant des autorisations explicites, que, «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».

181. Il en résulte que, à notre avis, cette dérogation est contraire aux articles 7, 8 et 52, paragraphe 1, de la Charte dans la mesure où elle ne poursuit pas un objectif d'intérêt général défini de façon suffisamment précise.

182. En tout état de cause, la facilité et la généralité avec lesquelles la décision 2000/520 elle-même, à ses annexes I, quatrième alinéa, sous b), et IV, B, prévoit que les principes de la sphère de sécurité peuvent être écartés en application de normes du droit américain sont incompatibles avec la condition selon laquelle les dérogations aux règles relatives à la protection des données à caractère personnel doivent être limitées à ce qui est strictement nécessaire. Il est, certes, fait mention de la condition de nécessité mais, outre que la démonstration de cette condition est mise à la charge de l'entreprise concernée, nous ne voyons pas comment une telle entreprise pourrait se soustraire à une obligation d'écarter les principes de la sphère de sécurité qui découle de règles de droit qu'elle est tenue d'appliquer.

183. Nous sommes, dès lors, d'avis que la décision 2000/520 doit être déclarée invalide dans la mesure où l'existence d'une dérogation qui permet d'une manière aussi générale et imprécise d'écarter les principes du régime de la sphère de sécurité empêche par elle-même de considérer que ce régime assure un niveau de protection adéquat aux données à caractère personnel qui sont transférées aux États-Unis depuis l'Union.

184. S'agissant, maintenant, de la première catégorie de limites prévues à l'annexe I, quatrième alinéa, sous a), de la décision 2000/520 en raison d'exigences relatives à la sécurité nationale, de l'intérêt public et du respect des lois américaines, seul le premier objectif nous paraît être suffisamment précis pour être considéré comme un objectif d'intérêt général reconnu par l'Union au sens de l'article 52, paragraphe 1, de la Charte.

185. Il y a lieu, à présent, de vérifier la proportionnalité de l'ingérence constatée.

186. À cet égard, il convient de rappeler que «le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs» [69].

187. En ce qui concerne le contrôle juridictionnel du respect de ces conditions, «dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci» [70].

188. Nous sommes d'avis que les décisions que la Commission adopte sur le fondement de l'article 25, paragraphe 6, de la directive 95/46 sont soumises au contrôle complet de la Cour quant à la proportionnalité de l'évaluation effectuée par cette institution relative au caractère adéquat du niveau de protection offert par un pays tiers du fait «de sa législation interne ou de ses engagements internationaux».

189. Il convient, à cet égard, de noter que, dans son arrêt Digital Rights Ireland e.a. [71], la Cour a jugé 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, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive [en cause], le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict» [72].

190. Une telle ingérence doit être apte à réaliser l'objectif poursuivi par l'acte de l'Union en cause et être nécessaire pour atteindre cet objectif.

191. À cet égard, «s'agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour [...], que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire» [73].

192. Dans son contrôle, la Cour tient également compte de la circonstance que «la protection des données à caractère personnel, résultant de l'obligation explicite prévue à l'article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci» [74].

193. Selon la Cour, qui se réfère, à cet égard, à la jurisprudence de la Cour européenne des droits de l'homme, «la réglementation de l'Union en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre

69 — Arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 46 ainsi que jurisprudence citée).

70 — Ibidem (point 47 et jurisprudence citée).

71 — C-293/12 et C-594/12, EU:C:2014:238.

72 — Point 48.

73 — Arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 52 ainsi que jurisprudence citée).

74 — Ibidem (point 53).

tout accès et toute utilisation illicites de ces données» [75]. La Cour indique que «[l]a 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» [76].

194. Il existe, selon nous, une analogie entre l'annexe I, quatrième alinéa, sous a), de la décision 2000/520 et l'article 13, paragraphe 1, de la directive 95/46. À la première disposition, il est indiqué que l'adhésion aux principes de la sphère de sécurité peut être limitée par les «exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis». À la seconde, il est prévu que les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus aux articles 6, paragraphe 1, 10, 11, paragraphe 1, 12 et 21 de cette directive, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder, notamment, la sûreté de l'État, la défense, la sécurité publique ainsi que la prévention, la recherche, la détection et la poursuite d'infractions pénales.

195. Comme la Cour l'a relevé dans son arrêt IPI [77], il ressort du libellé de l'article 13, paragraphe 1, de la directive 95/46 que les États membres peuvent prévoir les mesures visées à cette disposition uniquement lorsque celles-ci sont nécessaires. Le caractère «nécessaire» des mesures conditionne ainsi la faculté accordée aux États membres par ladite disposition [78]. Pour les traitements de données à caractère personnel à l'intérieur de l'Union, les limites prévues à l'article 13 de cette directive doivent s'entendre comme étant cantonnées à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi. Il doit, à notre avis, en aller de même s'agissant des limites aux principes de la sphère de sécurité qui sont prévues à l'annexe I, quatrième alinéa, de la décision 2000/520.

196. Or, force est de constater que toutes les versions linguistiques ne font pas mention du critère de nécessité dans le libellé de l'annexe I, quatrième alinéa, sous a), de la décision 2000/520. Il en va, notamment, ainsi de la version en langue française qui indique que «[l]'adhésion aux principes peut être limitée par [...] les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis», alors que, à titre d'exemple, les versions en langues espagnole, allemande et anglaise indiquent que les limitations instaurées doivent être nécessaires pour atteindre les objectifs susmentionnés.

197. Quoi qu'il en soit, les éléments factuels qui sont avancés par la juridiction de renvoi ainsi que par la Commission dans ses communications susmentionnées montrent clairement que, en pratique, la mise en œuvre de ces limitations n'est pas cantonnée à ce qui est strictement nécessaire pour atteindre les objectifs visés.

198. Nous observons, à cet égard, que l'accès aux données à caractère personnel transférées dont disposent les services de renseignement américains couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données transférées, y compris le contenu des communications, sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif d'intérêt général poursuivi [79].

199. En effet, l'accès des services de renseignement américains aux données transférées concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques sans qu'il soit exigé que les personnes concernées présentent une menace pour la sécurité nationale [80].

75 — Ibidem (point 54 et jurisprudence citée).

76 — Ibidem (point 55 et jurisprudence citée).

77 — C-473/12, EU:C:2013:715.

78 — Point 32.

79 — Voir, par analogie, arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 57 et jurisprudence citée).

80 — Ibidem (points 58 et 59).

200. Une telle surveillance massive et non ciblée est disproportionnée par nature et constitue une ingérence injustifiée dans les droits garantis par les articles 7 et 8 de la Charte.

201. Comme l'a relevé, à juste titre, le Parlement dans ses observations, puisqu'il est impossible pour le législateur de l'Union ou pour les États membres d'adopter des dispositions législatives qui, en violation de la Charte, prévoiraient une surveillance massive et non ciblée, il s'ensuit nécessairement que, a fortiori, des pays tiers ne sauraient en aucun cas être réputés assurer un niveau de protection adéquat aux données à caractère personnel des citoyens de l'Union lorsque leur réglementation autorise effectivement la surveillance et l'interception massives et non ciblées de ce type de données.

202. Il importe, en outre, de souligner que le régime de la sphère de sécurité tel qu'il est défini par la décision 2000/520 ne contient pas les garanties propres à éviter un accès massif et généralisé aux données transférées.

203. Nous observons, à cet égard, que la Cour a mis en exergue, dans son arrêt Digital Rights Ireland e.a. [81], l'importance de prévoir des «règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte» [82]. Une telle ingérence doit, selon la Cour, être «précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire» [83]. La Cour a également, dans cet arrêt, mis l'accent sur la nécessité de prévoir «des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données [à caractère personnel] contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données» [84].

204. Or, force est de constater que les mécanismes d'arbitrage privé et la FTC, en raison de son rôle limité aux litiges de nature commerciale, ne constituent pas des moyens de contester l'accès des services de renseignement américains aux données à caractère personnel transférées depuis l'Union.

205. La compétence de la FTC couvre les actions et les pratiques déloyales ou frauduleuses dans le domaine du commerce et ne s'étend donc pas à la collecte et à l'utilisation d'informations personnelles à des fins non commerciales [85]. Le domaine de compétence limité de la FTC restreint le droit des particuliers à la protection de leurs données à caractère personnel. La FTC a été mise en place non pas pour assurer, comme c'est le cas au sein de l'Union pour les autorités nationales de contrôle, la protection du droit individuel à la vie privée, mais pour garantir un commerce loyal et fiable pour les consommateurs, ce qui limite, de facto, ses capacités d'intervention dans la sphère relative à la protection des données à caractère personnel. La FTC ne joue donc pas un rôle comparable à celui des autorités nationales de contrôle prévues à l'article 28 de la directive 95/46.

206. Les citoyens de l'Union dont les données ont été transférées peuvent s'adresser à des organismes d'arbitrage spécialisés établis aux États-Unis comme TRUSTe et BBBOnline pour demander des précisions sur le point de savoir si l'entreprise qui détient leurs données à caractère personnel viole les conditions du régime d'autocertification. L'arbitrage privé assuré par des organismes comme TRUSTe ne peut pas traiter les violations du droit à la protection des données à caractère personnel qui sont commises par des organismes ou des autorités autres que les entreprises autocertifiées. Ces organismes d'arbitrage n'ont aucune compétence pour statuer sur la légalité des activités des agences de sécurité américaines.

81 — C-293/12 et C-594/12, EU:C:2014:238.

82 — Point 65.

83 — Idem.

84 — Ibidem (point 66).

85 — Voir, à cet égard, annexe II, FAQ 11, de la décision 2000/520, sous «Action de la FTC», et annexes III, V et VII de celle-ci.

207. Ni la FTC ni les organismes d'arbitrage privé n'ont donc de compétence pour contrôler les possibles violations des principes de protection des données à caractère personnel commises par des acteurs publics tels que les agences de sécurité américaines. Une telle compétence serait, cependant, essentielle pour garantir pleinement le droit à la protection effective de ces données. La Commission ne pouvait donc pas constater, en adoptant la décision 2000/520 et en maintenant celle-ci en vigueur, qu'il y aurait pour l'ensemble des données à caractère personnel qui seraient transférées vers les États-Unis une protection adéquate du droit accordé par l'article 8, paragraphe 3, de la Charte, c'est-à-dire qu'une autorité indépendante exercerait un contrôle effectif du respect des exigences de protection et de sécurité de ces données.

208. Il y a lieu, par conséquent, de constater l'absence, au sein du régime de la sphère de sécurité prévu par la décision 2000/520, d'une autorité indépendante qui pourrait contrôler que la mise en œuvre des dérogations aux principes de la sphère de sécurité est limitée au strict nécessaire. Or, nous avons vu qu'un tel contrôle par une autorité indépendante constitue, du point de vue du droit de l'Union, un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel [86].

209. Il convient, à cet égard, de souligner le rôle qu'occupent, dans le système de protection des données à caractère personnel en vigueur au sein de l'Union, les autorités nationales de contrôle dans le contrôle des limitations prévues à l'article 13 de la directive 95/46. Aux termes de l'article 28, paragraphe 4, second alinéa, de cette directive, «[c]haque 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». Par analogie, nous estimons que la mention de limites à l'application des principes de la sphère de sécurité à l'annexe I, quatrième alinéa, de la décision 2000/520 aurait dû être accompagnée par la mise en place d'un mécanisme de contrôle assuré par une autorité indépendante spécialisée en matière de protection des données à caractère personnel.

210. L'intervention d'autorités de contrôle indépendantes est, en effet, au cœur du système européen de protection des données à caractère personnel. C'est donc naturellement que l'existence de telles autorités a été considérée, d'emblée, comme l'une des conditions nécessaires au constat d'adéquation du niveau de protection offert par les pays tiers. Il s'agit là d'une condition pour que les flux de données depuis le territoire des États membres vers celui de pays tiers ne soient pas interdits conformément à l'article 25 de la directive 95/46 [87]. Comme le note le document de discussion adopté par le groupe de travail institué par l'article 29 de cette directive, il existe en Europe un large consensus selon lequel «un dispositif de 'contrôle externe', sous la forme d'une autorité indépendante, constitue un élément nécessaire de tout système visant à assurer le respect des règles sur la protection des données» [88].

211. Nous relevons, en outre, que la FISC n'offre pas un recours juridictionnel effectif aux citoyens de l'Union dont les données à caractère personnel sont transférées aux États-Unis. En effet, les protections contre la surveillance par les services gouvernementaux dans le cadre de la section 702 de la loi de 1978 sur la surveillance des services de renseignement étrangers s'appliquent uniquement aux citoyens américains ainsi qu'aux citoyens étrangers qui résident légalement et de manière permanente aux États-Unis. Comme la Commission l'a elle-même relevé, le contrôle des programmes américains de

86 — Voir arrêt Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238, point 68 ainsi que jurisprudence citée).

87 — Voir Poullet, Y., «L'autorité de contrôle: 'vues' de Bruxelles», *Revue française d'administration publique*, n° 89, janvier-mars 1999, p. 69, spécialement p. 71.

88 — Voir p. 7 du document de travail WP 12 de la Commission mentionné à la note en bas de page 56.

collecte de renseignements pourrait être amélioré en renforçant le rôle de la FISC et en instaurant des voies de recours pour les particuliers. Ces mécanismes pourraient réduire le traitement des données à caractère personnel concernant des citoyens de l'Union qui ne sont pas pertinentes aux fins de la protection de la sécurité nationale [89].

212. Par ailleurs, la Commission a elle-même indiqué que les citoyens de l'Union n'ont aucune possibilité 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 américains, des données à caractère personnel les concernant sont collectées et traitées ultérieurement [90].

213. Il convient, enfin, de mentionner que les normes américaines relatives à la protection de la vie privée peuvent faire l'objet d'une application différenciée entre les citoyens américains et les citoyens étrangers [91].

214. Il résulte de ce qui précède que la décision 2000/520 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette décision et l'application qui en est faite comportent une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.

215. En adoptant la décision 2000/520, puis en maintenant celle-ci en vigueur, la Commission a donc excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte. À cela s'ajoute le constat d'une ingérence non justifiée dans le droit des citoyens de l'Union à un recours effectif protégé par l'article 47 de la Charte.

216. Cette décision doit, par conséquent, être déclarée invalide dans la mesure où, en raison des violations des droits fondamentaux précédemment décrites, il ne saurait être considéré que le régime de la sphère de sécurité qu'elle instaure assure un niveau de protection adéquat aux données à caractère personnel qui sont transférées depuis l'Union vers les États-Unis dans le cadre de ce régime.

217. Face à un tel constat de violations des droits fondamentaux des citoyens de l'Union, nous estimons que la Commission aurait dû suspendre l'application de la décision 2000/520.

218. Cette décision a une durée indéterminée. Or, la présente affaire démontre que le caractère adéquat du niveau de protection offert par un pays tiers peut évoluer avec le temps en fonction du changement des circonstances à la fois factuelles et juridiques qui ont fondé ladite décision.

219. Nous relevons que la décision 2000/520 elle-même contient des dispositions prévoyant la possibilité pour la Commission d'adapter celle-ci en fonction des circonstances.

220. Ainsi, il résulte du considérant 9 de cette décision que «[l]a 'sphère de sécurité' créée par les principes et les FAQ peut devoir être revue à la lumière de l'évolution de la protection de la vie privée, dans des circonstances où la technologie rend de plus en plus faciles le transfert et le traitement de données à caractère personnel, ainsi qu'à la lumière de rapports de mise en œuvre élaborés par les autorités compétentes».

89 — Pages 10 et 11 de la communication de la Commission mentionnée à la note en bas de page 2.

90 — Voir point 7.2, p. 20, de la communication de la Commission mentionnée à la note en bas de page 58.

91 — Voir, sur cette question, Kuner, C., «Foreign Nationals and Data Protection Law: A Transatlantic Analysis», *Data Protection Anno 2014: How To Restore Trust?* Intersentia, Cambridge, 2014, p. 213, spécialement p. 216 et suiv.

221. De même, aux termes de l'article 3, paragraphe 4, de ladite décision, «[s]i 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 [...] en vue d'abroger ou de suspendre la présente décision ou d'en limiter la portée».

222. En outre, selon l'article 4, paragraphe 1, de la décision 2000/520, celle-ci «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[...] 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». Aux termes de l'article 4, paragraphe 2, de la décision 2000/520, «[l]a Commission présente, si nécessaire, un projet des mesures à prendre conformément à la procédure visée à l'article 31 de la directive 95/46».

223. La Commission a constaté, dans ses observations, qu'il existe «une forte probabilité [...] que l'adhésion aux principes de la sphère de sécurité a été limitée d'une manière qui ne répond plus aux conditions strictement circonscrites de l'exemption prévue en matière de sécurité nationale» [92]. Elle observe, à cet égard, que «[l]es révélations en question font apparaître un degré de surveillance indifférenciée à grande échelle qui n'est pas compatible avec le critère de nécessité prévu dans cette exemption ni, de manière plus générale, avec le droit à la protection des données à caractère personnel consacré à l'article 8 de la Charte» [93]. La Commission a, par ailleurs, constaté elle-même que «[l]a portée [des] programmes de surveillance, associée au traitement inégal des citoyens de l'[Union], remet en question le niveau de protection offert par la sphère de sécurité» [94].

224. De plus, la Commission a expressément reconnu, lors de l'audience, que, dans le cadre de la décision 2000/520, telle qu'elle est appliquée actuellement, il n'y a pas de garantie que le droit des citoyens de l'Union à la protection de leurs données sera assuré. Ce constat n'est cependant, selon elle, pas de nature à rendre invalide cette décision. Si la Commission est d'accord avec l'affirmation selon laquelle elle doit agir face à des circonstances nouvelles, elle considère qu'elle a pris des mesures qui sont appropriées et proportionnées en entamant des négociations avec les États-Unis afin de réformer le régime de la sphère de sécurité.

225. Nous ne sommes pas de cet avis. En effet, dans l'intervalle, les transferts de données à caractère personnel vers les États-Unis doivent pouvoir être suspendus à l'initiative des autorités nationales de contrôle ou à la suite de plaintes déposées auprès d'elles.

226. Par ailleurs, nous estimons que, face à de tels constats, la Commission aurait dû suspendre l'application de la décision 2000/520. En effet, l'objectif de protection des données à caractère personnel que poursuivent la directive 95/46 ainsi que l'article 8 de la Charte fait peser des obligations non seulement sur les États membres, mais également sur les institutions de l'Union, ainsi qu'il résulte de l'article 51, paragraphe 1, de la Charte.

92 — Point 44.

93 — Idem.

94 — Voir p. 5 de la communication de la Commission mentionnée à la note de bas de page 2.

227. Dans son évaluation du niveau de protection offert par un pays tiers, la Commission doit examiner non seulement la législation interne et les engagements internationaux de ce pays tiers, mais également la manière dont la protection des données à caractère personnel est assurée en pratique. Si l'examen de la pratique révèle des dysfonctionnements, la Commission doit réagir et, le cas échéant, suspendre et/ou adapter sans délai sa décision.

228. Comme nous l'avons vu dans nos développements précédents, l'obligation qui pèse sur les États membres consiste principalement à assurer, par l'action de leurs autorités nationales de contrôle, le respect des règles prévues par la directive 95/46.

229. L'obligation qui pèse sur la Commission est de suspendre l'application d'une décision qu'elle a adoptée sur le fondement de l'article 25, paragraphe 6, de cette directive en cas de manquements avérés de la part du pays tiers concerné, pendant qu'elle conduit des négociations avec ce pays tiers en vue de mettre fin à ces manquements.

230. Nous rappelons qu'une décision adoptée par la Commission sur le fondement de cette disposition a pour objet de constater qu'un pays tiers «assure» un niveau de protection adéquat aux données à caractère personnel qui font l'objet d'un transfert vers ce pays tiers. Le terme «assure» conjugué au temps présent implique que, pour pouvoir être maintenue, une telle décision doit concerner un pays tiers qui continue, après l'adoption de ladite décision, à garantir un tel niveau de protection adéquat.

231. Selon le considérant 57 de la directive 95/46, «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».

232. Aux termes de l'article 25, paragraphe 4, de cette directive, «[l]orsque 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». Par ailleurs, l'article 25, paragraphe 5, de ladite directive dispose que «[l]a Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4».

233. Il résulte de cette dernière disposition que, dans le système mis en place par l'article 25 de la directive 95/46, les négociations entamées avec un pays tiers ont pour but de remédier à une absence de niveau de protection adéquat constatée conformément à la procédure prévue à l'article 31, paragraphe 2, de cette directive. Dans le cas qui nous occupe, la Commission n'a pas formellement constaté, conformément à cette procédure, que le régime de la sphère de sécurité n'assurait plus un niveau de protection adéquat. Cela étant, si la Commission a décidé d'entamer des négociations avec les États-Unis, c'est bien que, au préalable, elle a considéré que le niveau de protection assuré par ce pays tiers n'était plus adéquat.

234. Alors qu'elle avait connaissance de dysfonctionnements dans l'application de la décision 2000/520, la Commission n'a ni suspendu ni adapté cette dernière, entraînant ainsi la poursuite de la violation des droits fondamentaux des personnes dont les données à caractère personnel ont été et continuent à être transférées dans le cadre du régime de la sphère de sécurité.

235. Or, la Cour a déjà jugé, certes dans un autre contexte, qu'il appartient à la Commission de veiller à une adaptation de la réglementation aux données nouvelles [95].

95 — Voir, en ce sens, arrêt Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, point 40).

236. Un tel défaut d'agir de la part de la Commission, qui porte directement atteinte aux droits fondamentaux protégés par les articles 7, 8 et 47 de la Charte, constitue, à notre avis, un motif supplémentaire de déclarer invalide la décision 2000/520 dans le cadre du présent renvoi préjudiciel [96].

III – Conclusion

237. Eu égard aux développements qui précèdent, nous proposons à la Cour de répondre aux questions posées par la Haute Cour de justice de la manière suivante:

L'article 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, lu à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que l'existence d'une décision adoptée par la Commission européenne sur le fondement de l'article 25, paragraphe 6, de la directive 95/46 n'a pas pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat aux données à caractère personnel transférées et, le cas échéant, de suspendre le transfert de ces données.

La décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil 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, est invalide.

96 — Si la Cour a jugé, dans son arrêt T. Port (C-68/95, EU:C:1996:452), que «le traité n'a pas prévu la possibilité d'un renvoi par lequel une juridiction nationale demanderait à la Cour de constater à titre préjudiciel la carence d'une institution» (point 53), il semble qu'elle a adopté une position plus favorable à cette possibilité dans son arrêt Ten Kate Holding Musselkanaal e.a. (C-511/03, EU:C:2005:625, point 29).