COMMISSION EUROPÉENNE

SERVICE JURIDIQUE

Bruxelles, le 3 novembre 2014
sj f(2014)4003332

Documents de procédure juridictionnelle
ORIGINAL: EN

À MONSIEUR LE PRÉSIDENT ET AUX MEMBRES DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

Observations écrites

présentées par

LA COMMISSION EUROPÉENNE,

représentée par M. Ben Smulders, conseiller juridique principal, M. Bernd Martenczuk et M^me^ Julie Vondung, membres de son service juridique, en qualité d'agents, ayant élu domicile auprès de M^me^ Merete Clausen, également membre de son service juridique, Bâtiment Bech, 5 rue A. Weicker, 2721 Luxembourg, et consentant à la signification de tous les actes de procédure via e-Curia,

dans l'affaire C-362/14,

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

Maximilian Schrems

et

le Data Protection Commissioner

amicus curiae:

Digital Rights Ireland Ltd.

portant sur l'interprétation 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

TABLE DES MATIÈRES

LA COMMISSION EUROPEENNE A L'HONNEUR DE SOUMETTRE LES PRESENTES OBSERVATIONS ECRITES A LA COUR.

1. INTRODUCTION ET RESUME

1. Les questions préjudicielles portent sur les pouvoirs et obligations des autorités nationales chargées de la protection des données dans le cadre de la décision «sphère de sécurité»[1], à la suite des révélations d'Edward Snowden sur les programmes de surveillance à grande échelle mis en place par les agences américaines de sécurité nationale. Dans la décision «sphère de sécurité», la Commission européenne avait constaté en 2000 que des entreprises américaines ayant déclaré leur adhésion aux principes relatifs à la protection de la vie privée énoncés dans ladite décision assuraient un niveau adéquat de protection des données à caractère personnel, de sorte que de telles données pouvaient être transférées à ces entreprises conformément à la directive 95/46/CE relative à la protection des données à caractère personnel. Les programmes de surveillance, dont l'existence a été révélée en 2013 par le lanceur d'alertes Edward Snowden, permettent aux agences américaines de sécurité nationale d'accéder massivement et de manière non différenciée à des données à caractère personnel transférées à des entreprises américaines, dont Facebook Inc. À la suite de ces révélations, la Commission a entamé un réexamen, toujours en cours, de la décision «sphère de sécurité».

2. Le demandeur à l'action principale, M. Maximilian Schrems, conteste le refus du défendeur, à savoir le Data Protection Commissioner (autorité irlandaise chargée de la protection des données, ci-après le «Commissioner»), de poursuivre l'examen de la plainte dont il l'avait saisi concernant le transfert de ses données à caractère personnel par Facebook Ireland Ltd à Facebook Inc. aux États-Unis, une société ayant autocertifié son adhésion aux principes de la «sphère de sécurité». Il fait valoir que, du fait des programmes de surveillance (dont PRISM), un niveau de protection adéquat n'est plus garanti, rendant ce transfert illicite. Le Commissioner se dit lié par la constatation contraire énoncée par la Commission européenne dans la décision «sphère de sécurité». La juridiction de renvoi demande en substance si, à la lumière de la Charte des droits

---

[1] 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 (JO L 215 du 25.8.2000, p. 7).

fondamentaux, le Commissioner est effectivement absolument lié par cette constatation ou si, dans le cas contraire, il peut et/ou doit mener sa propre enquête en tenant compte des révélations faites par Edward Snowden.

3. La Commission estime que les révélations d'Edward Snowden suscitent, en effet, de graves inquiétudes en ce qui concerne l'application de la décision «sphère de sécurité». Elle a dès lors décidé d'agir et d'entamer le réexamen de ladite décision, ainsi que sera relaté plus en détail ci-après. Toutefois, aux yeux de la Commission, une autorité nationale chargée de la protection des données est liée par la constatation d'une protection adéquate faite par la Commission tant que la décision «sphère de sécurité» elle-même n'autorise pas de décision contraire, conformément à son article 3, paragraphe 1. En vertu du point b) de cette disposition, les autorités nationales chargées de la protection des données peuvent notamment suspendre les flux de données vers une organisation autocertifiée «*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*». Cependant, dans des circonstances telles que celles de l'affaire dont a été saisie la juridiction nationale, ces conditions ne sont que partiellement remplies. En effet, si, à la lumière des révélations d'Edward Snowden, il est «*fort probable que les principes sont violés*» et s'il y a bel et bien «*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*», rien n'indique que la poursuite du transfert des données à caractère personnel du demandeur par Facebook Ireland Limited à Facebook Inc. ferait courir «*un risque imminent de subir des dommages graves*» au demandeur.

2. LE CADRE JURIDIQUE

4. Le cadre juridique fixé par le droit de l'Union européenne pertinent en l'espèce se compose des articles 7, 8 et 47 de la Charte des droits fondamentaux, de l'article 25 de la directive 95/46/CE et de la décision «sphère de sécurité».

2.1. La Charte des droits fondamentaux

5. L’article 7 de la Charte est libellé comme suit:

> Respect de la vie privée et familiale
>
> Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.

6. L’article 8 de la Charte prévoit ce qui suit:

> Protection des données à caractère personnel
>
> 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
>
> 2. 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. Toute personne a le droit d’accéder aux données collectées la concernant et d’en obtenir la rectification.
>
> 3. Le respect de ces règles est soumis au contrôle d’une autorité indépendante.

7. L’article 47 de la Charte dispose:

> Droit à un recours effectif et à accéder à un tribunal impartial
>
> Toute personne dont les droits et libertés garantis par le droit de l’Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article.
>
> Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable par un tribunal indépendant et impartial, établi préalablement par la loi. Toute personne a la possibilité de se faire conseiller, défendre et représenter.
>
> Une aide juridictionnelle est accordée à ceux qui ne disposent pas de ressources suffisantes, dans la mesure où cette aide serait nécessaire pour assurer l’effectivité de l’accès à la justice.

2.2. La directive 95/46/CE

8. La directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31) régit le transfert de données à caractère personnel à destination de pays tiers. Conformément à son article 25, un tel transfert ne peut, en principe, avoir lieu que si le pays tiers en question assure un niveau de protection adéquat. La Commission peut constater, en vertu de l’article 25, paragraphe 6, qu’un pays tiers assure un tel niveau de protection adéquat; les transferts de données à caractère personnel vers ce pays tiers sont dès lors autorisés sans que des garanties supplémentaires doivent être fournies. Les États membres sont tenus de se conformer à la décision de la Commission en ce qui concerne la reconnaissance du niveau de protection offert dans le pays en question (article 25, paragraphe 6, dernier alinéa).

9. L’article 25 de la directive 95/46/CE est rédigé dans les termes suivants:

> Principes
>
> 1. Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l’objet d’un traitement, ou destinées à faire l’objet d’un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.
>
> 2. Le caractère adéquat du niveau de protection offert par un pays tiers s’apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d’origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.
>
> 3. Les États membres et la Commission s’informent mutuellement des cas dans lesquels ils estiment qu’un pays tiers n’assure pas un niveau de protection adéquat au sens du paragraphe 2.
>
> 4. Lorsque la Commission constate, conformément à la procédure prévue à l’article 31 paragraphe 2, qu’un pays tiers n’assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les États membres prennent les mesures nécessaires en vue d’empêcher tout transfert de même nature vers le pays tiers en cause.
>
> 5. La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faite en application du paragraphe 4.
>
> 6. La Commission peut constater, conformément à la procédure prévue à l’article 31 paragraphe 2, qu’un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l’issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes.
>
> Les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

2.3. La décision 2000/520/CE (décision «sphère de sécurité»)

10. La décision relative à la sphère de sécurité est fondée sur l’article 25, paragraphe 6, de la directive 95/46/CE.

11. Conformément à son article 1er, la décision «sphère de sécurité» régit le transfert de données à caractère personnel au départ de l’Union européenne vers des organisations établies aux États-Unis ayant autocertifié leur adhésion aux principes de la «sphère de sécurité» relatifs à la protection de la vie privée, qui sont énoncés à l’annexe I de la décision et sont appliqués conformément aux orientations fournies par les «questions souvent posées» [«*Frequently Asked Questions*» (FAQ)] publiées par le ministère du commerce des États-Unis d’Amérique, figurant à l’annexe II de la décision. La décision de la Commission reconnaît, en son article 1er, paragraphe 1, que les principes de protection de la vie privée et les FAQ s’y rapportant assurent un niveau adéquat de protection des données à caractère personnel transférées vers des entreprises établies aux États-Unis.

12. Le quatrième alinéa du préambule aux Principes relatifs à la protection de la vie privée publiés par le ministère américain du commerce et figurant en annexe I de la décision «sphère de sécurité» est rédigé comme suit:

> L'adhésion aux principes peut être limitée par: a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis; [...]

13. L'annexe III de la décision présente une synthèse de la mise en œuvre des principes relatifs à la «sphère de sécurité». En vertu de l'annexe VII, la Commission fédérale du commerce (*Federal Trade Commission*) et le ministère du transport (*Department of Transportation*) sont habilités à instruire les plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées, quel que soit leur pays de résidence ou leur nationalité, en cas de non-respect des principes mis en œuvre conformément aux FAQ.

14. En outre, la décision «sphère de sécurité» définit et délimite les compétences respectives, d'une part, de la Commission européenne et, d'autre part, des autorités nationales chargées de la protection des données dans les États membres.

15. Les pouvoirs de la Commission sont évoqués au considérant 9 et définis à l'article 4 de la décision «sphère de sécurité».

16. Le considérant 9 indique ce qui suit:

> La «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.

17. L'article 4 dispose, dans sa partie pertinente:

> 1. La présente décision peut être adaptée à tout moment à la lumière de l'expérience acquise durant sa mise en œuvre et/ou si le niveau de protection assuré par les principes et les FAQ est dépassé par les exigences du droit américain.
>
> La Commission évalue, en tout état de cause, l'application de la présente décision, sur la base des informations disponibles, trois ans après sa notification aux États membres et communique au comité institué au titre de l'article 31 de la directive 95/46/CE toute constatation pertinente, y compris tout élément susceptible d'influer sur l'évaluation selon laquelle les dispositions de l'article 1er de la présente décision assurent un niveau de protection adéquat au sens de l'article 25 de la directive 95/46/CE et toute information montrant que la présente décision est appliquée de manière discriminatoire.
>
> 2. La Commission présente, si nécessaire, un projet des mesures à prendre conformément à la procédure visée à l'article 31 de la directive 95/46/CE.

18. Les pouvoirs des autorités nationales chargées de la protection des données sont évoqués au considérant 8 et établis à l'article 3, paragraphe 1, de la décision «sphère de sécurité».

19. Le considérant 8 est rédigé en ces termes:

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

20. L'article 3, paragraphe 1, dispose, dans sa partie pertinente:

> 1. Sans préjudice de leurs pouvoirs de prendre des mesures visant à assurer le respect des dispositions nationales adoptées en application de dispositions autres que celles de l'article 25 de la directive 95/46/CE, les autorités compétentes des États membres peuvent exercer les pouvoirs dont elles disposent pour suspendre les flux de données vers une organisation adhérant aux principes mis en œuvre conformément aux FAQ afin de protéger les individus en ce qui concerne le traitement de leurs données personnelles, et ce dans les cas:
>
> a) [...] ou
>
> b) où il est fort probable que les principes sont violés; où il y a tout lieu de croire que l'instance d'application concernée ne prend pas ou ne prendra pas en temps voulu les mesures qui s'imposent en vue de régler l'affaire en question; où la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves; et où les autorités compétentes des États membres se sont raisonnablement efforcées, compte tenu des circonstances, d'avertir l'organisation et de lui donner la possibilité de répondre.
>
> La suspension cesse dès que le respect des principes mis en œuvre conformément aux FAQ est assuré et que les autorités compétentes de la Communauté en sont avisées.

21. En outre, l'article 3, paragraphe 2, impose expressément aux États membres d'informer sans tarder la Commission de l'adoption de mesures fondées sur le paragraphe 1.

3. LA PLAINTE DANS LE LITIGE AU PRINCIPAL ET LES QUESTIONS PREJUDICIELLES

22. Le demandeur, de nationalité autrichienne, conteste une décision du défendeur, le Commissioner, de ne pas poursuivre l'examen au fond de la plainte qu'il a introduite à la suite des révélations, en juin 2013, relatives à la surveillance généralisée des données internet et des télécommunications par les agences américaines de sécurité nationale (ci-après les «révélations d'Edward Snowden»). Le demandeur est un utilisateur du service de réseau social «Facebook», exploité par Facebook Ireland Ltd, depuis 2008. Facebook Ireland Ltd transfère tout ou partie des données de ses clients à sa société mère Facebook Inc., implantée aux États-Unis, laquelle a autocertifié son adhésion aux principes de la sphère de sécurité. Dans la plainte dont il a saisi le défendeur, M. Schrems alléguait, en

substance, qu'au vu des révélations d'Edward Snowden, le droit et les pratiques des États-Unis ne protégeaient pas efficacement les données transférées par la société Facebook Ireland à sa société mère américaine en ce qui concerne la surveillance par l'état. Il ne faisait pas état de conséquences particulières de cette surveillance à grande échelle en ce qui le concerne personnellement.

23. Lors de son examen de la plainte, le Commissioner n'a relevé aucune preuve attestant que les données à caractère personnel de M. Schrems avaient été divulguées aux États-Unis (*locus standi objection* / défaut d'intérêt à agir). Le Commissioner a par ailleurs estimé que la décision «sphère de sécurité» de la Commission européenne l'empêchait d'examiner la question du respect des normes de protection des données par les États-Unis.

24. La High Court, après avoir rejeté l'argument de *locus standi objection*, a constaté que le Commissioner avait «*fait preuve d'une fidélité scrupuleuse à la lettre de la directive de 1995 et de la décision "sphère de sécurité"*» et a souligné que ni la validité de la directive 95/46/CE ni celle de la décision n'avaient été contestées. Selon la juridiction de renvoi, l'article 3, paragraphe 1, point b), de la décision «sphère de sécurité» n'était pas applicable en l'espèce, la plainte n'étant pas dirigée contre le *comportement* de Facebook en tant que tel[2]. Les questions et doutes formulées par la juridiction de renvoi quant à l'approche adoptée par le Commissioner découlent des évolutions intervenues pendant les quatorze années qui se sont écoulées depuis l'adoption de la décision «sphère de sécurité», à savoir les avancées technologiques, les révélations d'Edward Snowden et, depuis 2009, le caractère contraignant de la Charte des droits fondamentaux de l'Union européenne, notamment ses articles 7, 8 et 47.

25. En outre, la juridiction de renvoi déclarait que «*si cette affaire devait être tranchée <u>uniquement</u> au regard des exigences constitutionnelles irlandaises, en concluant sommairement qu'il n'y avait pas lieu d'enquêter, le Commissioner n'aurait pas exercé correctement les pouvoirs que lui confère l'article 10, paragraphe 1, sous a)*»[3]. Ainsi qu'elle le relevait, en vertu du droit irlandais, «*l'interception ou la surveillance de*

---

2 Voir le point 19 de l'ordonnance de renvoi.

3 Voir le point 15 de l'ordonnance de renvoi.

communications privées par les autorités met en cause le droit constitutionnel à la vie privée. En outre, les autorités qui interceptent ou surveillent des communications privées générées au domicile [...] *portent aussi clairement atteinte à l'inviolabilité du domicile garantie par l'article 40, paragraphe 5, de la Constitution*»[4]. Toutefois, la question étant régie par la législation de l'Union, qui prime le droit irlandais, la juridiction de renvoi a décidé de saisir la CJUE d'une demande de décision préjudicielle.

26. La High Court a donc sursis à statuer et posé les questions préjudicielles suivantes:

> «Eu égard aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne [2000(C) 364/01] et sans préjudice des dispositions de l'article 25, paragraphe 6, de la directive 95/46/CE, le Commissaire indépendant chargé d'appliquer la législation sur la protection des données saisi d'une plainte relative au transfert de données à caractère personnel vers un pays tiers (en l'occurrence les États-Unis d'Amérique) 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 de la Commission du 26 juillet 2000 (2000/520/CE)? Dans le cas contraire, peut-il ou doit-il mener sa propre enquête en s'instruisant de la manière dont les faits ont évolué depuis la première publication de la décision de la Commission?»

4. LA REACTION DE LA COMMISSION EUROPEENNE AUX ALLEGATIONS D'EDWARD SNOWDEN

27. Depuis juin 2013, l'existence de plusieurs programmes de surveillance américains reposant sur la collecte et le traitement à grande échelle de données à caractère personnel a été révélée. Ces programmes concernent plus particulièrement la collecte de données à caractère personnel auprès de fournisseurs américains de services internet et de télécommunications, ainsi que le contrôle de flux de données, à l'intérieur et en dehors des frontières des États-Unis. Compte tenu de la position centrale que ces sociétés américaines occupent sur le marché européen, de la transmission transatlantique d'une grande partie des flux électroniques de données et des communications, ainsi que des volumes de données transitant par l'Atlantique, un très grand nombre de citoyens européens – et très

---

4 Voir le point 9 de l'ordonnance de renvoi.

probablement la totalité des utilisateurs de l'internet en Europe – sont susceptibles d'être touchés par ces programmes.

28. À la suite de ces révélations, la Commission a immédiatement fait part de vives préoccupations et a demandé des explications aux États-Unis, à la fois oralement et par écrit, quant à l'incidence de ces programmes sur les droits fondamentaux des citoyens de l'Union, en particulier leurs droits au respect de la vie privée et à la protection des données à caractère personnel. Un groupe de travail ad hoc UE/États-Unis sur la protection des données[5] a notamment été mis sur pied, en juillet 2013, pour établir les faits entourant ces révélations. Il a publié son rapport le 27 novembre 2013 (annexe 1). [6] Les États-Unis ont confirmé qu'en vertu de la section 702 de la loi de 1978 sur la surveillance des services de renseignement étrangers (*Foreign Intelligence Surveillance Act* ou FISA), la NSA (l'agence américaine de sécurité nationale) dispose d'une base de données baptisée «PRISM», qui permet de collecter des données stockées par voie électronique. [7] Les autorités américaines ont également confirmé que cette même section 702 était la base juridique du système dit de la «collecte en amont» (*upstream collection*), à savoir l'interception des communications internet par la NSA à leur entrée ou pendant leur passage sur le territoire américain (par exemple, par le réseau câblé, à certains points des transmissions). Elles ont en outre indiqué que l'Executive Order 12333 constituait aussi une base juridique pour d'autres programmes de surveillance visant la collecte massive de données provenant de l'internet, ainsi que le cadre général pour la collecte de renseignements à l'intérieur et en dehors des frontières des États-Unis[8].

---

5 Ce groupe, présidé conjointement par la Commission et la présidence du Conseil, rassemblait notamment des membres du SEAE, des experts des États membres et des représentants des autorités gouvernementales américaines.

6 Report of the Findings by the EU Co-Chairs of the Ad Hoc EU-US Working Group on Data Protection (en anglais uniquement): http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

7 Voir le point 2.1.1 du rapport du groupe de travail ad hoc UE/États-Unis. Le programme PRISM permet de collecter des données stockées sous forme électronique, y compris du contenu, au moyen de directives adressées aux principaux fournisseurs de services internet et entreprises technologiques américains proposant des services en ligne, dont – selon ce qui ressort des documents classifiés divulgués dans la presse, sans confirmation de la part des autorités américaines – Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype et YouTube.

8 Voir le point 2.3 du rapport du groupe de travail ad hoc UE/États-Unis.

29. À la même date, la Commission a publié deux communications: la première évaluait le fonctionnement de la sphère de sécurité[9] (annexe 2) et la seconde énonçait une série de mesures à prendre en vue de rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis[10] (annexe 3). La communication sur le fonctionnement de la sphère de sécurité comportait treize recommandations à l'intention des États-Unis visant à renforcer le régime de la sphère de sécurité à la lumière des évolutions intervenues depuis son adoption. Les onze premières recommandations portent sur des obligations fondamentales de la sphère de sécurité et s'articulent autour des trois axes suivants: transparence, recours et mise en œuvre. Les deux dernières portent sur la nécessité de régler la question de l'accès, par les autorités américaines, aux données de la sphère de sécurité à des fins de sécurité nationale, en particulier dans le contexte de la dérogation pour des raisons de sécurité nationale, prévue par les dispositions actuelles relatives à la sphère de sécurité. La douzième recommandation est libellée comme suit: «*Les politiques de protection de la vie privée adoptées par les entreprises autocertifiées doivent comporter des informations sur la mesure dans laquelle la législation des États-Unis permet aux autorités publiques de collecter et de traiter des données transférées selon les principes de la sphère de sécurité. En particulier, les entreprises devraient être encouragées à indiquer, dans leurs politiques de protection de la vie privée, si elles dérogent auxdits principes pour répondre à des exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois.*» La treizième recommandation mentionne: «*Il importe que la dérogation pour raison de sécurité nationale prévue par la décision relative à la sphère de sécurité ne soit utilisée que dans la mesure où cela est strictement nécessaire et proportionné.*[11]»

30. Dans sa communication visant à rétablir la confiance dans les flux de données entre l'Union et les États-Unis, la Commission présentait trois options envisageables pour la

---

9 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 du 27.11.2013].

10 Communication de la Commission au Parlement européen et au Conseil, Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique [COM(2013)846 du 27.11.2013]. Les principales mesures préconisées sont les suivantes: 1) adopter rapidement la réforme des règles de l'Union en matière de protection des données, 2) rendre la sphère de sécurité plus sûre, 3) renforcer les garanties en matière de protection des données dans le cadre de la coopération entre les services répressifs (accord-cadre), 4) recourir aux accords sectoriels et d'entraide judiciaire pour obtenir des données, 5) répondre aux préoccupations européennes dans le cadre de la réforme en cours aux États-Unis sur les activités de renseignement et 6) promouvoir des normes de protection de la vie privée au niveau international.

11 COM(2013) 847, p. 23.

sphère de sécurité: 1) le maintien du statu quo, 2) le renforcement de la sphère de sécurité et la révision approfondie de son fonctionnement ou 3) la suspension ou l'abrogation de la décision relative à la sphère de sécurité. La Commission participe activement à des discussions avec les autorités américaines sur la mise en œuvre, par les États-Unis, des treize recommandations figurant dans la communication. Les questions en cause étant particulièrement sensibles et complexes, ces échanges sont toujours en cours.

5. ANALYSE JURIDIQUE

5.1. Observations générales

31. Conformément à l'article 25, paragraphe 6, dernier alinéa, de la directive 95/46/CE, les décisions constatant le caractère adéquat de la protection offerte sont, en principe, contraignantes pour tous les États membres. L'article 3, paragraphe 1, point b), de la décision «sphère de sécurité» autorise les autorités nationales de protection des données à suspendre les flux de données vers les États-Unis sous certaines conditions. Il s'agit là d'une exception au principe de l'application uniforme de la décision de la Commission constatant un niveau adéquat de protection, qu'il convient dès lors, en principe, d'interpréter de manière restrictive. Dans le même temps, elle doit être interprétée à la lumière de la Charte, en particulier de ses articles 7 et 8.

32. En outre, aux fins de l'interprétation de l'article 3, paragraphe 1, point b), il importe de tenir compte de l'articulation des pouvoirs respectifs de la Commission et des autorités nationales de protection des données. Concrètement, comme expliqué plus en détail ci-après, les compétences des autorités nationales chargées de la protection des données sont 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 «sphère de sécurité», y compris toute décision comportant sa suspension ou son abrogation, relève de la compétence de la Commission.

5.2. Les conditions de l'article 3, paragraphe 1, point b), de la décision «sphère de sécurité» ne sont que partiellement remplies

33. L'article 3, paragraphe 1, point b), de la décision «sphère de sécurité» fixe quatre conditions qui doivent toutes être remplies pour que les autorités chargées de la protection des données puissent décider de suspendre certains flux de données.

5.2.1. Première condition: il est fort probable que les principes sont violés

34. De l'avis de la Commission, une forte probabilité que les principes de la sphère de sécurité ont été violés existe bel et bien. Le caractère indifférencié et l'application à très grande échelle des programmes de surveillance américains sont effectivement incompatibles avec l'exemption strictement circonscrite à des besoins de sécurité nationale que prévoient les principes de la sphère de sécurité, au quatrième alinéa du préambule aux principes relatifs à la protection de la vie privée.

35. Cette conclusion résulte d'une interprétation de la décision «sphère de sécurité» à la lumière de la Charte des droits fondamentaux et de la jurisprudence pertinente de la Cour. En vertu de l'article 52, paragraphe 1, de la Charte, «[*t*]*oute limitation de l'exercice des droits et des libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées 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 libertés d'autrui.*» De même, aux termes de la Convention européenne des droits de l'homme,«[*i*]*l ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit*» au respect de la vie privée et familiale, qui inclut le droit à la protection des données, «*que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui*» (article 8, paragraphe 2). Conformément à la jurisprudence de la Cour sur le droit au respect de la vie privée:

«[...] *la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, 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*»[12].

---

[12] Arrêt Digital Rights Ireland, C−293/12, EU:C:2014:238, point 52.

36. Par conséquent, la décision «sphère de sécurité», qui précise que ces restrictions ne sont autorisées que pour répondre à des exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois, doit être interprétée *de manière stricte*.

37. Ainsi que la Cour l'a déclaré à plusieurs reprises, l'exception prévue à l'article 4, paragraphe 2, TUE, selon laquelle la sécurité nationale reste de la seule responsabilité de chaque État membre, ne saurait entraîner l'inapplicabilité du droit de l'Union (arrêt *ZZ contre Secretary of State for the Home Department*, C-300/11, point 38[13]). Par ailleurs, la Cour a également estimé que les limitations visées à l'article 52, paragraphe 1, de la Charte des droits fondamentaux s'appliquaient également dans ce domaine du droit; voir, par exemple, les points 49 et 51 de l'arrêt *ZZ /Secretary of State for the Home Department* (C-300/11):

«*Ce n'est qu'à titre de dérogation que l'article 30, paragraphe 2, de la directive 2004/38 autorise les États membres à limiter l'information transmise à l'intéressé pour des motifs relevant de la sûreté de l'État. En tant que dérogation à la règle énoncée au point précédent, cette disposition doit faire l'objet d'une interprétation stricte sans toutefois priver celle-ci de son effet utile.* [...] *Notamment, il convient de prendre en considération que, si, certes, l'article 52, paragraphe 1, de la Charte admet des limitations à l'exercice des droits consacrés par celle-ci, cette disposition exige toutefois que toute limitation doit notamment respecter le contenu essentiel du droit fondamental en cause et requiert, en outre, que, dans le respect du principe de proportionnalité, toute limitation soit nécessaire et réponde effectivement à des objectifs d'intérêt général reconnus par l'Union.*»

38. Ce raisonnement est d'autant plus valable que l'espèce concerne l'application d'une exemption pour des raisons de sécurité nationale en faveur *d'un pays tiers*, en l'occurrence les États-Unis, qui fait l'objet d'une décision de la Commission européenne. La présente affaire ne porte donc pas sur le rôle des États membres dans la sauvegarde de leur sécurité nationale.

39. L'arrêt rendu par la Cour dans l'affaire *Digital Rights Ireland* (C-293/12) est aussi pertinent dans ce contexte, et notamment son point 37:

---

13 EU:C:2013:363.

«*Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave. En outre, la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.* »

40. En outre, par analogie dans le contexte particulier de l'application du droit pénal, au point 51 du même arrêt, la Cour a dit pour droit que:

«*la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte».*

41. Dans ces circonstances, la Cour a considéré qu'il y avait eu une violation manifeste du principe de proportionnalité et, partant, une ingérence illégale dans le droit à la protection des données à caractère personnel, dans la mesure où:

a) la conservation de données à caractère personnel concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales (point 58);

b) la directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes

qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves (point 59);

c) à cette absence générale de limites s'ajoute le fait que la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence (point 60).

42. Les révélations d'Edward Snowden sur la surveillance à grande échelle (dont la véracité et la gravité ont été reconnues par la juridiction de renvoi), la parution dans la presse d'une série de documents officiels, y compris de documents classifiés, dont un certain nombre ont par la suite été déclassifiés et rendus publics par les autorités américaines, ainsi que les conclusions du groupe de travail ad hoc UE/États-Unis mettent en évidence une surveillance généralisée d'une ampleur qui, pour reprendre les termes de la juridiction de renvoi elle-même, «*témoigne d'une ingérence massive de la part des autorités chargées de la sécurité, avec une indifférence quasi délibérée à l'égard de la vie privée des citoyens ordinaires, qui ont fait l'objet d'atteintes graves à leurs droits à la protection des données par des programmes de surveillance à grande échelle, en grande partie non supervisée*»[14]. Les programmes de surveillance ne comportent aucune limitation quant aux personnes concernées ou au type de données à caractère personnel collectées. Du fait de l'ampleur de ces programmes, il est effectivement possible que les autorités américaines aient accès à des données transférées dans le cadre de la sphère de sécurité et les soumettent éventuellement à un traitement ultérieur, au-delà de ce qui est strictement nécessaire et proportionné pour la sauvegarde de la sécurité nationale, comme le requiert l'exception prévue par la décision «sphère de sécurité».

---

[14] Arrêt de la High Court du 18 juin 2014, Schrems/Data Protection Commissioner [2014] IECCA 68, point 8.

43. En outre, Facebook a autocertifié son adhésion aux principes de la sphère de sécurité et elle est concernée par le programme PRISM[15]. Dans ce contexte – contrairement à l'avis de la juridiction de renvoi[16] –, il importe peu de savoir si Facebook Inc. a elle-même (directement ou sciemment) enfreint les principes en vigueur. Au regard de la protection des droits des personnes concernées de l'Union, le seul aspect pertinent est de déterminer si le niveau de protection qu'un constat d'adéquation est censé garantir a été compromis, indépendamment de savoir si cette situation est le fait d'une entreprise ou d'une autorité publique.

44. À la lumière de ces faits, on doit constater qu'une forte probabilité existe 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. Les 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.

45. En conséquence, compte tenu de ce qui précède et eu égard à la nature et à l'ampleur des programmes de surveillance en cause, il est fort probable que les principes énoncés dans la décision «sphère de sécurité» ont été violés dans des circonstances telles que celles décrites dans l'affaire au principal.

5.2.2. Deuxième condition: 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

46. La deuxième condition énoncée à l'article 3, paragraphe 1, point b), de la décision «sphère de sécurité» requiert qu'il y ait tout lieu de croire que l'instance d'application concernée

---

15 Voir le point 2.1.1 du rapport du groupe de travail ad hoc UE/États-Unis. Le programme PRISM permet de collecter des données stockées sous forme électronique, y compris du contenu, au moyen de directives adressées aux principaux fournisseurs de services internet et entreprises technologiques américains proposant des services en ligne, dont – selon ce qui ressort des documents classifiés divulgués dans la presse, sans confirmation de la part des autorités américaines – Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype et YouTube: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf.

16 Voir ci-dessus au point 23.

ne prend pas ou ne prendra pas en temps voulu les mesures qui s'imposent en vue de régler l'affaire en question.

47. Le contrôle de l'application de la décision «sphère de sécurité» incombe principalement à la Commission fédérale du commerce des États-Unis (*US Federal Trade Commission*). Toutefois, l'instance d'application de la sphère de sécurité n'a pas le pouvoir d'intervenir à l'égard des programmes de surveillance en général et, en particulier, pour déterminer si la condition de nécessité prévue par l'exemption est respectée. Le champ d'application des programmes de surveillance et les conditions dans lesquelles ils sont mis en œuvre sont fixés par les agences américaines de sécurité nationale, sous l'autorité du directeur des services nationaux de renseignement; seuls certains programmes sont soumis au contrôle juridictionnel du US Foreign Intelligence Surveillance Court (cour fédérale de surveillance des services de renseignement étrangers, FISC). Il convient de rappeler que les procédures devant le FISC ne sont pas contradictoires et que les personnes concernées ne peuvent se faire représenter devant lui pour défendre leurs intérêts lors de l'examen d'une demande d'injonction[17]. Il résulte de ce qui précède que l'instance d'application n'est pas en mesure de prendre en temps voulu les mesures adéquates pour régler les questions liées à la surveillance éventuelle des données à caractère personnel du plaignant figurant sur Facebook par les programmes de surveillance des agences américaines de sécurité nationale.

48. Par conséquent, 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 dans la situation en cause dans l'affaire au principal.

5.2.3. Troisième condition: la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves

49. En vertu de la troisième condition énoncée à l'article 3, paragraphe 1, point b), de la décision «sphère de sécurité», la poursuite du transfert des données à caractère personnel doit faire courir aux personnes concernées un risque imminent de dommages graves.

---

[17] Voir le rapport du groupe de travail ad hoc UE-États-Unis sur la protection des données (point 4.3).

50. Il convient, pour interpréter cette condition, d'avoir à l'esprit les observations générales formulées ci-dessus concernant l'interprétation de l'article 3, paragraphe 1, point b). Puisqu'elle constitue une exception au principe de l'application uniforme de la décision de la Commission constatant un niveau adéquat de protection, cette disposition doit, en principe, être interprétée de manière restrictive. En outre, comme il a déjà été observé, il importe de tenir compte, pour interpréter l'article 3, paragraphe 1, point b), de l'articulation des pouvoirs respectifs de la Commission et des autorités nationales de protection des données. Notamment, les compétences des autorités nationales chargées de la protection des données sont 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 «sphère de sécurité», y compris toute décision prévoyant sa suspension ou son abrogation, relève de la compétence de la Commission. Il en résulte, en particulier, que les conditions énoncées à l'article 3, paragraphe 1, point b), doivent être remplies dans les circonstances spécifiques en cause, ainsi que le mentionne le considérant 8 de la décision «sphère de sécurité» («*suspension de certains flux de données*»).

51. À cet égard, il y a lieu de souligner que la notion de «dommages graves» désigne un niveau de dommage ou de préjudice plus élevé que la simple violation du droit à la protection des données à caractère personnel. La formulation de la disposition indique qu'il doit s'agir d'un préjudice caractérisé. De plus, une lecture combinée de la première condition en liaison avec la troisième montre bien qu'une simple violation du droit à la protection des données à caractère personnel ne suffirait pas car, dans le cas contraire, la troisième condition serait superfétatoire.

52. Ensuite, l'existence d'un risque imminent de dommages graves doit être appréciée d'après la situation concrète du ou des plaignants. Ainsi qu'il a été exposé ci-dessus, les conditions de l'article 3, paragraphe 1, point b), doivent être réunies dans le cas d'espèce. Or, le plaignant n'a pas avancé d'arguments spécifiques donnant à penser qu'il courrait un risque imminent de subir des dommages graves. 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 américaines de sécurité nationale sont tout à fait identiques à celles qui ont conduit la Commission à entamer le réexamen de la décision «sphère de sécurité». Les autorités nationales de protection des données empiéteraient sur les compétences dont dispose la Commission pour renégocier les conditions de ladite décision avec les États-Unis ou, au besoin, suspendre celle-ci si elles

prenaient des mesures sur la base de plaintes faisant uniquement état de préoccupations structurelles et abstraites.

Cela dit, la Commission n'exclut pas que, dans d'autres cas particuliers, lorsqu'un risque imminent de dommages graves pour les plaignants est démontré, les autorités nationales de protection des données puissent agir.

5.2.4. Quatrième condition: 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

53. Comme la troisième condition de l'article 3, paragraphe 1, point b), n'est pas remplie, il n'est en principe pas nécessaire d'examiner la quatrième condition. Toutefois, si la Cour aboutissait à une autre conclusion relativement à la troisième condition, la Commission tient à faire observer que le Commissioner avait bel et bien soulevé les allégations concernant le programme PRISM auprès de Facebook Ireland, avant même d'être saisi de la plainte de M. Schrems, et s'était déclaré satisfait des réponses fournies, notamment que l'entreprise «*avait mis en place des procédures appropriées pour le traitement des demandes d'accès adressées par les agences chargées de la sécurité en général*» [appendice 1, observations présentées par le défendeur (Commissioner), point 66]. On pourrait en conclure que la quatrième condition est remplie. Toutefois, la Commission constate également que ces discussions avec l'organisation concernée ne suffisent peut-être pas pour remédier aux problèmes posés par l'accès à des données à caractère personnel par des agences américaines de sécurité nationale, ce qui conforte la Commission dans son idée que la meilleure manière de procéder en la matière passe par le réexamen, par la Commission, de la décision «sphère de sécurité».

5.3. L'autorité de protection des données n'a pas de pouvoir d'enquête

54. Si, comme dans des circonstances telles que celles de l'affaire au principal, les conditions cumulatives de l'article 3, paragraphe 1, point b), ne sont pas réunies, l'autorité chargée de la protection des données n'a pas le pouvoir de poursuivre l'examen de la plainte en question. Elle est au contraire liée par la constatation du caractère adéquat du niveau de protection fait par la Commission dans la décision «sphère de sécurité». Ceci dit, la Commission n'exclut pas que, dans d'autres cas particuliers, lorsqu'un risque imminent de

dommages graves pour les plaignants est démontré, les autorités nationales chargées de la protection des données puissent agir.

6. CONCLUSION

55. Eu égard aux considérations qui précèdent, la Commission a l'honneur de proposer à la Cour de répondre comme suit aux questions préjudicielles dont elle a été saisie par la High Court d'Irlande:

Dans des circonstances telles que celles de l'affaire au principal, l'autorité de protection des données est liée par la constatation du caractère adéquat du niveau de protection fait par la Commission dans la décision 2000/520/CE (décision «sphère de sécurité»).

Ben Smulders Bernd Martenczuk Julie Vondung

Agents de la Commission