Avis du Contrôleur européen de la protection des données

sur la communication de la Commission au Parlement européen et au Conseil relative au «rétablissement de la confiance dans les flux de données entre l'Union européenne et les États-Unis» et sur la 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'UE et des entreprises établies sur son territoire»

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu 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[1],

vu le règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[2], et notamment son article 41.

A ADOPTÉ L'AVIS SUIVANT:

I. INTRODUCTION

I.1. Consultation du CEPD

1. Le 27 novembre 2013, la Commission a adopté la communication de la Commission au Parlement européen et au Conseil relative au «rétablissement de la confiance dans les flux de données entre l'Union européenne et les États-Unis»3 (ci-après la «communication relative au rétablissement de la confiance»). Cette communication est accompagnée d'un rapport sur les conclusions des co-présidents de l'UE du groupe de travail ad hoc UE-USA sur la protection des données (ci-après le «rapport» et le «groupe de travail»).

[1] JO L 281, 23.11.1995, p. 31 (ci-après la «directive 95/46/CE»).
[2] JO L 8, 12.1.2001, p. 1 (ci-après le «règlement 45/2001»).
[3] COM(2013) 846 final.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
E-mail: edps@edps.europa.eu - Site Internet: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

2. À cette même date, la Commission a adopté une 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'UE et des entreprises établies sur son territoire»[4] (ci-après la «communication relative à la sphère de sécurité»).

3. Le CEPD se réjouit d'avoir eu la possibilité de faire part d'observations informelles à la Commission avant l'adoption des documents susmentionnés. Ces documents ont été adoptés par la Commission dans le sillage des révélations sur les programmes de surveillance mis en place par les services de renseignement américains. Compte tenu de l'incidence de ces programmes de surveillance sur le droit des personnes au respect de la vie privée et à la protection des données à caractère personnel les concernant dans l'UE, le CEPD a décidé de rendre le présent avis de sa propre initiative.

I.2. Objectif et portée des documents de la Commission

a) La communication relative au rétablissement de la confiance et le rapport

4. La communication propose des pistes pour l'avenir à la suite de la révélation de programmes américains de collecte de renseignements à grande échelle (ci-après les «programmes» ou les «programmes révélés») et traite de leur impact sur la confiance entre l'UE et les États-Unis. Elle ne fait pas référence aux révélations sur la conduite d'activités similaires et/ou à la collaboration d'États membres de l'UE ou d'autres pays tiers avec les États-Unis.

5. Le rapport rassemble les conclusions des co-présidents de l'UE du groupe de travail ad hoc UE-USA sur la protection des données qui a été mis en place après la réunion du COREPER du 18 juillet 2013, dans le but d'établir les faits concernant les programmes et leur incidence sur les droits fondamentaux dans l'UE et sur les données à caractère personnel des citoyens de l'UE. Ce rapport analyse le cadre juridique américain[5], les modalités de la collecte et du traitement ultérieur des données[6], ainsi que les mécanismes de contrôle et de recours juridictionnel existants.

6. Le rapport mentionne une «deuxième voie» qui a également été arrêtée au cours de la réunion du COREPER du 18 juillet 2013. Il affirme que, conformément à cette «deuxième voie», les institutions de l'UE peuvent saisir les autorités américaines de questions liées à la prétendue surveillance d'institutions et de missions diplomatiques de l'UE, tandis que les États membres peuvent discuter avec les autorités américaines, dans un cadre bilatéral, des enjeux relatifs à leur sécurité nationale.

[4] COM(2013) 847 final.

[5] En particulier la Constitution, telle qu'interprétée par la Cour suprême; la section 702 du Foreign Intelligence Surveillance Act (loi sur la surveillance et le renseignement extérieur) de 1978 (FISA) (tel que modifié par le FISA Amendments Act de 2008, 50 U.S.C. § 1881a); et la section 215 du USA PATRIOT Act de 2001 (modifiant également le FISA, 50 U.S.C. 1861) et le décret exécutif 12333.

[6] Sur la base des informations fournies par les États-Unis dans le cadre du groupe de travail et de documents déclassifiés, y compris des avis de la Foreign Intelligence Surveillance Court (ci-après la «FISC») et des documents rendus accessibles au public, tels que les Attorney General's Guidelines for Domestic FBI Operations (directives du Ministre de la justice américain concernant les opérations du FBI sur le territoire national).

7. Le rapport indique également que cette division a fixé certaines limitations aux discussions au sein du groupe de travail et aux informations communiquées en son sein. Le CEPD n'a reçu aucune information sur cette «deuxième voie» ou sur la création d'un groupe de travail parallèle sur ce sujet. La Commission est donc invitée à informer le CEPD des résultats de la «deuxième voie», notamment en ce qui concerne la prétendue surveillance des institutions et des missions diplomatiques de l'UE.

b) La communication relative à la sphère de sécurité

8. La communication relative à la sphère de sécurité analyse le fonctionnement de la sphère de sécurité, recense les défauts et propose des améliorations possibles. Elle fait état de l'augmentation du volume de données transférées entre l'UE et les États-Unis ainsi que du nombre croissant d'entreprises qui adhèrent aux principes de la sphère de sécurité. Après un bref rappel de la structure et du fonctionnement de la sphère de sécurité, la Commission insiste sur la nécessité d'améliorer l'application des principes par les entreprises qui y adhèrent mais aussi par leurs sous-traitants. D'après la communication, cela nécessiterait d'intégrer les principes de la sphère de sécurité de manière plus efficace dans les politiques de ces entreprises en matière de protection de la vie privée et de les rendre publics. La Commission fédérale du commerce (FTC) devrait adopter une démarche plus proactive en ce qui concerne le contrôle de l'application de ces principes. En outre, les autorités chargées de la protection des données devraient contribuer à la sensibilisation à la sphère de sécurité dans l'UE, et plus particulièrement à l'existence du panel de l'UE sur la protection des données. La Commission propose également des solutions visant à améliorer les mécanismes de règlement extrajudiciaire des litiges.

9. En ce qui concerne l'accès aux données transférées dans le cadre du régime de la sphère de sécurité et traitées ultérieurement par les autorités américaines, la Commission met l'accent sur le fait qu'il devrait être limité à ce qui est strictement nécessaire et proportionné. Elle exige également que l'application de limitations aux politiques de protection de la vie privée pour satisfaire à des exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois fasse l'objet d'un contrôle rigoureux, afin de s'assurer qu'elle ne porte pas atteinte à la protection accordée. Elle encourage aussi les entreprises qui adhèrent aux principes de la sphère de sécurité à être transparentes sur ces limitations et sur leur impact sur la confidentialité des communications, dans le but de sensibiliser les citoyens.

I.3. Portée et objectif du présent avis

10. Le présent avis porte sur la communication relative au rétablissement de la confiance, mais aussi, dans ce contexte, sur la communication relative à la sphère de sécurité. En conséquence, il ne traite pas directement des révélations concernant les États membres de l'UE, que ce soit seuls ou en collaboration avec les États-Unis, ni des activités de surveillance menées par des pays tiers autres que les États-Unis.

11. Cet avis commence par des observations sur l'approche générale de la communication relative au rétablissement de la confiance. La partie II analyse brièvement l'applicabilité du cadre juridique pertinent et ses conséquences, et contient des remarques sur la communication relative à la sphère de sécurité. Étant

donné que le Groupe de travail "Article 29"[7] examine actuellement le cadre juridique européen et international applicable, le présent avis ne traite pas en détail de ce volet. La partie III porte sur les recommandations de la Commission concernant les mesures à prendre.

I.4. Remarques sur l'approche de la communication relative au rétablissement de la confiance

12. La communication met l'accent sur le fait que la confiance entre les partenaires stratégiques que sont l'UE et les États-Unis a été ébranlée par les révélations sur les programmes et qu'il convient de la rétablir. Le CEPD se félicite de ce constat.

13. Cependant, les programmes, dont l'existence, dans certains cas, est clairement confirmée par le rapport[8], mettent à mal non seulement la confiance, mais aussi les droits des citoyens instaurés par le droit primaire et le droit secondaire de l'UE et du Conseil de l'Europe, notamment les droits au respect de la vie privée et à la protection des données. Ces programmes témoignent également de l'ampleur de la collecte de renseignements étrangers qui a lieu actuellement en vertu du cadre juridique américain[9], tel qu'interprété par la Cour suprême des États-Unis[10]. Le rapport confirme également l'absence de garanties, de mesures de protection, de droits, de mécanismes de contrôle et de voies de recours ouvertes aux citoyens de l'UE dans le cadre juridique américain[11].

14. Ainsi que la Commission l'a souligné à maintes reprises, la confiance des citoyens et des entreprises dans les communications sur internet dépend de la mise à disposition d'outils techniques efficaces pour la protection de la vie privée, et plus particulièrement de la confidentialité des communications. Cette nécessité a également été reconnue par le Groupe d'examen américain sur les technologies de renseignement et de communication[12], qui a formulé plusieurs recommandations visant à rétablir la confiance dans les outils de cryptage et les logiciels commerciaux, ainsi que dans le fonctionnement de mécanismes de correction rapide des vulnérabilités logicielles. Certains des experts les plus réputés dans le domaine de la sécurité considèrent que l'un des effets les plus préjudiciables des discussions récentes au sujet des opérations de renseignement de signaux[13] est l'affaiblissement

---

[7] Le Groupe de travail "Article 29" sur la protection des données, créé par la directive 95/46/CE, a un rôle consultatif et agit à titre indépendant. Il est composé de représentants des autorités nationales chargées de la protection des données dans l'UE, du CEPD et de la Commission.

[8] Voir p. 5, 10 et 26 du rapport, lequel, sur la base d'avis déclassifiés de la Foreign Intelligence Surveillance Court, affirme que «les agences de renseignement américaines ont recours à des méthodes de collecte en vertu de l'article 702 qui sont à grande échelle, telles que le programme PRISM qui collecte des données auprès des fournisseurs d'accès internet ou via la "collecte en amont" des données transitant par les États-Unis».

[9] Si les États-Unis ont confirmé qu'il existe d'autres bases juridiques autorisant la collecte de données de ressortissants non américains, ils n'ont pas fourni de précisions sur les autorités compétentes et les procédures applicables. Les bases juridiques pertinentes n'ont pas toutes été communiquées au GT (voir p. 13 du rapport).

[10] Voir p. 4 à 12 du rapport.

[11] Voir p. 26 à 27 du rapport.

[12] «Liberty and Security in a Changing World» (Liberté et sécurité dans un monde en pleine mutation), rapport et recommandations du Groupe d'examen du président sur les technologies de renseignement et de communication, notamment les recommandations 25, 29 et 30. http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[13] B Schneier, C Soghoian dans le rapport du 6 septembre 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; B. Preneel: discours de

de la confiance dans ces systèmes. Au vu de l'importance de la mise en place d'une cybersécurité efficace en Europe, il convient d'élaborer une réponse commune à ce défi technique et politique au niveau de l'UE, sur la base d'une initiative de la Commission.

15. Dans la section 3 de la communication, la Commission aborde les mesures à prendre pour rétablir la confiance dans les transferts de données entre l'UE et les États-Unis. Le CEPD se félicite de ce chapitre, qui s'intéresse à l'amélioration du cadre juridique existant et propose de nouveaux instruments. Toutefois, la Commission n'examine pas l'incidence des programmes sur les instruments nationaux, de l'UE et du Conseil de l'Europe applicables. Le CEPD estime que l'impact sur les instruments juridiques existants aurait dû faire l'objet d'une plus grande attention dans la communication.

II. REMARQUES SUR LE CADRE JURIDIQUE APPLICABLE

II.1. Cadres juridiques de l'UE et du Conseil de l'Europe en matière de protection des données

16. Les droits au respect de la vie privée et à la protection des données sont consacrés par le droit primaire, à l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (ci-après la «CEDH»), aux articles 7 et 8 de la Charte des droits de l'homme de l'UE (ci-après la «Charte») et à l'article 16 du traité sur le fonctionnement de l'UE (ci-après le «TFUE»). L'article 17 du Pacte international relatif aux droits civils et politiques (ci-après le «PIDVP»), qui a été ratifié par les États-Unis, prévoit également que «nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée». La Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel fournit davantage de précisions sur le droit à la protection des données.

17. En application du droit secondaire, la directive 95/46/CE, la décision-cadre du Conseil 2008/977[14], le règlement (CE) 45/2001 et la directive 2002/58/CE[15], tels qu'interprétés par la Cour de justice de l'UE, régissent l'exercice de ces droits. Conjointement avec l'article 8, paragraphe 2, de la CEDH et l'article 52, paragraphe 1, de la Charte, ils fixent les critères et les conditions pour en limiter l'exercice.

18. Les dispositions précitées du droit de l'UE ne s'appliquent pas à la sécurité nationale des États membres de l'UE car, conformément à l'article 4, paragraphe 2, du traité de l'Union européenne (ci-après le «TUE»), il s'agit d'une «fonction essentielle de l'État» qui relève de la «compétence exclusive» des États membres et est donc réglementée au niveau national.

---

clôture à l'ISSE 2013: «The Cryptographic Year in Review» http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf

[14] Décision-cadre du Conseil 2008/977/JHA du 27 novembre 2008 sur la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire dans des affaires criminelles. JO L 350, 30.12.2008, p.6.

[15] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). JO L 201, 31.07.2002, p.37.

II.1.1. Champ d'application des dérogations pour motif de sécurité nationale

a) Motifs de sécurité nationale limitant le champ d'application des instruments de l'UE

19. La communication affirme «qu'alors que l'UE peut prendre des mesures dans des domaines qui relèvent de sa compétence, notamment pour garantir l'application du droit de l'UE, la sécurité nationale reste une compétence exclusive de chaque État membre»[16]. Le CEPD se réjouit de ce rappel de la compétence de l'UE pour garantir l'application du droit de l'UE. Le CEPD relève également que la sécurité nationale des pays tiers n'étant ni une fonction essentielle, ni une compétence exclusive des États Membres de l'UE, elle n'est pas couverte par cette dérogation.

20. En tout état de cause, l'exclusion de la sécurité nationale des États membres du champ d'application du droit de l'UE ne signifie pas que la sécurité nationale constitue un domaine non réglementé, notamment au regard de la protection des droits fondamentaux. En effet, les instruments du Conseil de l'Europe susmentionnés[17] et les lois nationales sont, dans la plupart des cas, pleinement applicables à ce domaine[18].

21. Ainsi, même si le droit de l'UE ne s'applique pas, la Convention européenne des droits de l'homme et la Convention 108 s'appliquent à un grand nombre des traitements concernés. En effet, l'application générale de ces conventions à la plupart de leurs parties[19] n'exclut pas la sécurité nationale dans son ensemble[20]. Ces instruments créent également une obligation positive pour les parties de garantir les droits de chacun au respect de la vie privée et à la protection des données sur leur territoire[21], mais aussi d'adopter des lois nationales mettant en application les principes de protection des données [22].

b) Motifs de sécurité nationale limitant les droits conférés par les instruments de l'UE et du Conseil de l'Europe

22. Lorsque les instruments de l'UE et du Conseil de l'Europe susmentionnés sont applicables, les droits au respect de la vie privée et à la protection des données peuvent être limités si nécessaire, afin de garantir la sécurité nationale ou la sécurité de l'État[23], entre autres motifs. Toutefois, ces restrictions doivent être interprétées

[16] Voir p. 4 de la communication.
[17] Seule une minorité des parties à la Convention 108 ont déposé des déclarations conformément à l'article 3, paragraphe 2, point a), affirmant que la Convention 108 ne s'appliquera pas aux «fichiers automatisés de données à caractère personnel» liés à la «sécurité d'État» ou aux «secrets d'État».
[18] Voir notamment la décision du Bundesverfassungsgericht dans l'affaire Rasterfahndung (BVerfG 1 BvR 518/02 du 4.4.2006).
[19] Voir la note de bas de page 17.
[20] Comme pour les instruments de l'UE, lorsque les instruments du Conseil de l'Europe sont applicables, ils prévoient des restrictions à certains droits, par exemple pour les besoins de la sécurité nationale. Toutefois, ces limitations doivent être interprétées restrictivement (voir notamment l'arrêt du 6 septembre 1978, CEDH, Klass et autres/Allemagne, série A nº 28).
[21] Voir les articles 1 et 8 de la CEDH.
[22] Voir l'article 4, paragraphe 1, de la Convention 108.
[23] Voir notamment l'article 8, paragraphe 2, de la CEDH, l'article 9, paragraphe 2, point a), et l'article 13, paragraphe 1, point a), de la directive 95/46/CE.

restrictivement[24] et toute limitation à la jouissance des droits conférés par ces instruments ne doit être permise que si elle est énoncée dans une législation[25] prévisible et accessible[26] au public et si elle est nécessaire dans une société démocratique[27].

23. Les dérogations prévues par les instruments susmentionnés pour les besoins de la sécurité nationale ne peuvent donc pas justifier des limitations à grande échelle aux droits fondamentaux, telles que celles prévues par les programmes, pour des raisons qui vont au-delà de la sécurité nationale, qui touchent principalement aux intérêts d'un pays tiers[28] et qui ne sont pas strictement nécessaires pour garantir la sécurité nationale[29].

II.1.2. Contrôle du respect du cadre juridique de l'UE et du Conseil de l'Europe

a) Contrôle du respect par le responsable du traitement

24. Les lois nationales mettant en œuvre la directive 95/46/CE sont applicables aux traitements effectués dans le cadre des activités d'un établissement du responsable du traitement dans l'UE[30]. Elles sont également applicables lorsqu'un responsable du traitement non européen est établi en un lieu où la loi nationale de l'État membre s'applique en vertu du droit international ou si le responsable du traitement recourt à des moyens dans l'UE[31]. Dans ces cas, les autorités de l'UE chargées de la protection des données ont donc compétence pour faire respecter directement leur législation nationale en matière de protection des données aux organisations ayant divulgué ou donné accès à des données à caractère personnel à des gouvernements de pays tiers en violation de la législation nationale en matière de protection des données.

25. Étant donné que le règlement 45/2001 est également applicable, le CEPD a entamé une discussion avec les institutions et organes de l'UE sur les risques pour la confidentialité des communications et la sécurité des traitements et sur l'adoption de mesures de sécurité techniques appropriées et efficaces.

---

[24] CEDH, Klass et autres, précité, au point 42.
[25] Voir l'article 52, paragraphe 1, de la Charte.
[26] CEDH, Rotaru/Roumanie, arrêt du 4 mai 2000, demande nº 28341/95, point 48.
[27] Idem.
[28] Selon la FISA, le «renseignement étranger» tel que défini par la FISA peut recouvrir des informations concernant les activités politiques d'individus ou de groupes ainsi que les activités d'organismes publics, à condition que ces informations soient susceptibles de présenter un intérêt pour la politique étrangère des États-Unis. Les représentants de l'UE au sein du GP ont demandé aux États-Unis de spécifier davantage la portée du «renseignement étranger», mais ceux-ci ont refusé de répondre au motif que de telles clarifications révéleraient des aspects opérationnels spécifiques des programmes. Voir p. 5 à 7 du rapport.
[29] En vertu de la section 702 FISA, les données des ressortissants non américains sont considérées comme des «renseignements étrangers» dès lors qu'elles se *rapportent* aux finalités poursuivies. En revanche, les données des ressortissants américains doivent être *nécessaires* aux finalités indiquées pour être considérées comme des «renseignements étrangers». Voir p. 26 du rapport.
[30] Voir l'article 4, paragraphe 1, point a), de la directive 95/46/CE.
[31] Voir l'article 4, paragraphe 1, points b à c), de la directive 95/46/CE et son interprétation par le Groupe de travail "Article 29" dans l'avis 8/2010 sur le droit applicable (WP 179), consultable sur http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

b) Contrôle du respect par les parties à la CEDH

26. Les articles 1 et 8 de la CEDH instaurent une obligation positive pour les parties à la Convention de protéger les droits au respect de la vie privée et à la protection des données. Au vu des programmes, cette obligation n'a pas été respectée. La Convention 108, qui s'applique aux traitements par le secteur public et privé dans les États parties à la Convention, n'a, de ce point de vue, pas été respectée non plus.

27. Les États Membres de l'UE et toute partie à la CEDH peuvent être déférés devant la Cour européenne des droits de l'homme (ci-après la «CEDH») pour non-respect de leur obligation de «reconnaître à toute personne relevant de leur juridiction les droits et libertés définis dans la Convention»[32], en particulier le droit au respect de la vie privée[33]. Le 4 septembre 2013, une plainte a été déposée contre le Royaume-Uni par Big Brother Watch et autres[34].

II.2. Instruments régissant les transferts

a) Instruments régissant les transferts de l'UE vers les États-Unis dans le secteur privé

28. Les échanges de données à caractère personnel entre des entreprises et des organisations privées établies dans l'UE et aux États-Unis sont facilités par plusieurs instruments adoptés sur le fondement des articles 25 et 26 de la directive 95/46/CE: décision de la Commission 2000/520/CE (ci-après la «décision relative à la sphère de sécurité»); décisions de la Commission 2001/497/CE, 2004/915/CE et 2010/87/UE (ci-après les «clauses contractuelles types») et une série de documents du Groupe de travail "Article 29" sur les règles d'entreprise contraignantes (ci-après les «REC»).

29. Certains de ces instruments (sphère de sécurité et clauses contractuelles types) prévoient une dérogation aux principes qu'ils instaurent lorsque cela est nécessaire dans une société démocratique, par exemple pour les besoins de la sécurité nationale. Dans certains cas (sphère de sécurité, clauses contractuelles types et règles d'entreprise contraignantes), ils prévoient l'obligation d'informer l'organe de l'UE transférant les données ou l'autorité compétente de l'UE chargée de la protection des données lorsque le droit national du pays du destinataire est en contradiction avec les principes prévus par ces instruments.

30. Toutefois, les programmes vont au-delà de ce qui est nécessaire, tout au moins en ce qui concerne les données des ressortissants non américains[35]. En tout état de cause, ces instruments n'étaient pas destinés à assurer une protection contre des transferts ultérieurs ou un accès à grande échelle du gouvernement de l'organisation destinataire. Le CEPD recommande donc d'améliorer ces instruments, notamment la sphère de sécurité, qui a été examinée à la fois dans la communication relative au rétablissement de la confiance et, de façon plus approfondie, dans la communication relative à la sphère de sécurité.

---

[32] Voir l'art. 1 CEDH.
[33] Voir l'art. 8 CEDH.
[34] Big Brother Watch et autres/Royaume-Uni, demande nº 58170/13, consultable sur http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-140713, dernier accès le 17.02.2014.
[35] Voir la note de bas de page 29.

b) Mise en œuvre de la sphère de sécurité

31. Le CEPD se réjouit de l'analyse et des recommandations formulées par la Commission sur la mise en œuvre de la sphère de sécurité. La communication relative à la sphère de sécurité affirme que la Commission a recensé des lacunes, notamment un manque de transparence et un contrôle insuffisant de l'application. Elle relève en outre que certaines entreprises autocertifiées au titre de la sphère de sécurité n'en appliquent pas les principes dans la pratique, ce qui entraîne, entre autres conséquences, une incidence négative sur les droits fondamentaux des citoyens de l'UE.

32. La communication relative à la sphère de sécurité aborde également la question de l'«accès aux données transférées dans le cadre du régime de la sphère de sécurité». La communication relative au rétablissement de la confiance soulève la question de savoir si la collecte et le traitement à grande échelle de données à caractère personnel dans le cadre des programmes respectent les exigences de la sphère de sécurité au regard des principes de nécessité et de proportionnalité. La Commission conclut que la sphère de sécurité sert d'«interface pour le transfert de données à caractère personnel de citoyens européens, de l'Union européenne vers les États-Unis, par les entreprises qui sont tenues de remettre des données aux agences américaines de renseignement».

33. À cet égard, le CEPD se réjouit aussi de la réaffirmation par la Commission du fait que «pour être valides, les limitations et restrictions à la jouissance des droits fondamentaux doivent être interprétées restrictivement; elles doivent être énoncées dans une législation accessible au public et être nécessaires et proportionnées dans une société démocratique»[36]. Dès lors, toute limitation aux règles de protection des données pour raison de sécurité nationale devrait remplir ces conditions. Cette exigence de «nécessité» est déjà énoncée dans la décision[37] relative à la sphère de sécurité, qui dispose que: «L'adhésion aux principes peut être limitée: (a) dans la mesure nécessaire aux exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois».

34. Toutefois, le CEPD regrette la conclusion de la Commission selon laquelle «l'accès à grande échelle des autorités américaines aux données traitées par les entreprises autocertifiées au titre de la sphère de sécurité risque» uniquement «de porter atteinte à la confidentialité des communications électroniques», sans préciser qu'un tel accès va au-delà des limites définies dans les principes de la sphère de sécurité. Le CEPD estime que l'ampleur des programmes et le fait que l'exigence de «nécessité» ne s'applique, en vertu du droit américain, qu'aux seules données des ressortissants américains[38] démontrent que les programmes ne répondent pas à la condition de nécessité au regard des ressortissants non américains[39].

[36] Voir p. 17, premier paragraphe de la communication relative à la sphère de sécurité.
[37] Voir l'annexe I, principes de la sphère de sécurité relatifs à la protection de la vie privée, paragraphe 4.
[38] Voir la note de bas de page 29.
[39] Voir également l'arrêt de la Cour de justice de l'UE dans l'affaire Huber, C-524/06.

c) Instruments régissant les transferts de l'UE vers les États-Unis aux fins du respect des lois

35. Outre les instruments susmentionnés, plusieurs accords régissent l'échange de données à caractère personnel entre l'UE et les États-Unis aux fins du respect des lois, y compris pour la prévention et la lutte contre le terrorisme:
- l'accord d'entraide judiciaire (ci-après le «MLAA»)[40],
- l'accord sur l'utilisation et le transfert des données des dossiers passagers (ci-après l'«accord PNR»)[41],
- l'accord sur le traitement et le transfert de données de messagerie financière aux fins du programme de surveillance du financement du terrorisme (ci-après l'«accord TFTP»)[42], et
- l'accord entre Europol et les États-Unis[43].

36. L'accès des autorités américaines aux données traitées sur le territoire de l'UE devrait intervenir exclusivement dans le cadre de ces accords.

37. Les révélations sur les programmes portent notamment sur de prétendues violations de l'accord PNR et de l'accord TFTP. D'après la Commission, ces allégations ne sont étayées par aucun élément de preuve[44]. Cependant, les événements récents invitent à faire preuve d'une plus grande prudence, notamment en ce qui concerne le TFTP au vu des inquiétudes exprimées par le conseil de surveillance commun (CSC) d'Europol[45] et de l'enquête conjointe menée par les autorités néerlandaises et belges chargées de la protection des données[46].

38. En ce qui concerne les échanges d'informations aux fins du respect des lois, la communication affirme que l'accord PNR et l'accord TFTP assurent un «niveau élevé de protection des données à caractère personnel». Ainsi que le CEPD l'a expliqué à plusieurs reprises[47], le niveau de protection assuré par ces accords est discutable, et une telle affirmation ne peut donc être formulée sans réserve[48].

---

[40] Décision du Conseil 2009/820/PESC du 23 octobre 2009 concernant la conclusion, au nom de l'Union européenne, de l'accord d'extradition entre l'Union européenne et les États-Unis d'Amérique et de l'accord d'entraide judiciaire entre l'Union européenne et les États-Unis d'Amérique, JO L 291, 7.11.2009, p. 40.

[41] Accord entre l'Union européenne et les États-Unis d'Amérique sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure (décision du Conseil 2012/472/UE du 26 avril 2012, JO L 215, 11.8.2012, p. 4).

[42] Accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (décision du Conseil du 13 juillet 2010, JO L 195, 27.7.2010, p. 3).

[43] Accord entre les États-Unis d'Amérique et l'Office européen de police du 6 décembre 2001, et accord complémentaire entre Europol et les États-Unis d'Amérique relatif à l'échange de données à caractère personnel et d'informations y afférentes du 20 décembre 2002.

[44] La communication affirme que le réexamen conjoint de la mise en œuvre de l'accord PNR et les consultations officielles ouvertes par la Commission sur l'accord TFTP n'ont révélé «aucun élément prouvant l'existence d'une violation de ces accords», et que les États-Unis ont donné l'assurance écrite qu'aucune collecte directe de données n'avait lieu en violation des dispositions de l'accord TFTP.

[45] Rapport du CSC du 18 mars 2013 sur la mise en œuvre de l'accord TFTP.

[46] Communiqué de presse conjoint des autorités belges et néerlandaises chargées de la protection des données du 14 novembre 2013.

[47] Voir l'avis du CEPD du 30 septembre 2013 sur les proposition de décision du Conseil sur la conclusion et la signature de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement des données des dossiers passagers; l'avis du 9 décembre 2011 sur la proposition de décision du Conseil sur la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers

39. Si la prétendue violation des accords PNR et TFTP n'a pas été démontrée, rien ne prouve non plus qu'une enquête soit en cours à ce sujet. Le CEPD peut réagir séparément au rapport de réexamen conjoint du PNR américain, à la communication sur le TFTS et au rapport de réexamen conjoint du TFTP.

III. REMARQUES SPÉCIFIQUES SUR LES MESURES À PRENDRE

III.1. Adoption rapide de la réforme des règles de l'UE en matière de protection des données

40. Dans ce contexte, le CEPD partage le point de vue de la Commission sur l'importance des propositions en vue d'un nouveau cadre juridique de protection des données (ci-après les «propositions»)[49]. La communication mentionne en particulier cinq éléments du train de mesures proposé: l'extension du champ d'application territorial, la clarification des conditions de transferts, l'harmonisation et le renforcement du contrôle de l'application des règles par les autorités de l'UE chargées de la protection des données, la mise en place de règles claires concernant les obligations et les responsabilités des sous-traitants, et enfin l'établissement d'un «ensemble complet de règles» pour protéger les données à caractère personnel traitées à des fins répressives.[50]

41. À cet égard, le CEPD souhaite mettre l'accent sur deux éléments supplémentaires qui sont en cours d'examen par les co-législateurs: (i) aborder la question du traitement à des fins répressives des données à caractère personnel collectées à l'origine pour des finalités commerciales, et (ii) traiter la question des conflits de droit internationaux.

42. Le premier de ces éléments supplémentaires est lié au fait que, malgré les possibilités offertes par la nouvelle base juridique instaurée par l'article 16 TFUE, le train de mesures en matière de protection des données n'est pas constitué par une seule proposition complète, mais par deux propositions ayant chacune un champ d'application matériel différent. Cela risque de créer une certaine insécurité juridique lorsque des données à caractère personnel relevant initialement de la proposition de règlement en matière de protection des données sont ensuite traitées à des fins et par

---

passagers et leur transfert au ministère américain de la sécurité intérieure; l'avis du 15 juillet 2011 sur la proposition de décision du Conseil sur la conclusion d'un accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières; l'avis du 19 octobre 2010 sur l'approche globale suivie en matière de transferts des données des dossiers passagers (données PNR) vers les pays tiers; l'avis du 15 juin 2005 sur la proposition de décision du Conseil sur la conclusion d'un accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations anticipées sur les voyageurs (API)/dossiers passagers (PNR); tous consultables sur www.edps.europa.eu.

[48] Voir également les avis du Groupe de travail "Article 29" sur les accords PNR entre l'UE et les pays tiers, consultables sur http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

[49] Proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [COM(2012)11 final] et proposition de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données [COM(2012)10 final].

[50] Voir p. 5 et 6 de la communication relative au rétablissement de la confiance.

des autorités relevant du champ d'application de la proposition de directive relative à la protection des données. Ce problème avait déjà été soulevé par la Commission dans l'analyse d'impact[51], mais il n'est pas réglé par les propositions. Le CEPD recommande que les co-législateurs corrigent cette omission et régulent ces situations.

43. En ce qui concerne les conflits de droit internationaux, il convient d'indiquer clairement que toutes les activités de traitement relevant du champ d'application du paquet de mesures en matière de protection des données doivent respecter ces mesures, à moins qu'un accord international contraignant prévoyant des garanties de protection des données adéquates ne dispose autrement, ou à moins qu'une autorité judiciaire ou une autorité chargée de la protection des données n'accorde une dérogation.

44. Le CEPD souscrit à l'observation finale de la communication, rappelant que les récents événements ont «fait prendre conscience à l'Union et à ses États membres qu'il y avait lieu de progresser rapidement et avec ambition dans la réforme de la protection des données».

III.2. Renforcer la sphère de sécurité

45. Dans la communication relative au rétablissement de la confiance, la Commission propose de renforcer la sphère de sécurité. Si le CEPD se réjouit de cette proposition, il aurait préféré une formule plus affirmative. Ainsi que cela est indiqué plus haut, le CEPD insiste également sur la nécessité de tirer les conclusions juridiques appropriées concernant l'application insuffisante des principes de la sphère de sécurité.

46. En particulier, le renforcement du régime devrait constituer le *résultat* du réexamen de son fonctionnement et non l'inverse. Même si la communication relative au rétablissement de la confiance met en avant plusieurs raisons justifiant le maintien du régime, le choix final devrait dépendre des modalités de mise en œuvre effective des recommandations formulées dans le rapport. En cas d'échec, la suspension ou l'abrogation du régime pourrait toujours être envisagée.

47. Différents scénarios pourraient ainsi être envisagés, y compris d'éventuelles actions en fonction du résultat du réexamen. Ces scénarios devraient prévoir une analyse approfondie de l'éventuelle application de l'article 3 et/ou de l'article 4 de la décision relative à la sphère de sécurité et expliquer dans quels cas et dans quelles conditions la suspension pourrait être une option envisageable, et dans quels cas l'article 4 servirait de base pour mieux définir les principes de la sphère de sécurité, notamment l'étendue exacte de la dérogation pour motif de sécurité nationale par rapport à d'autres intérêts qui ne relèvent pas du champ d'application de cette dérogation.

48. À cet égard, le CEPD considère que la communication relative au rétablissement de la confiance aurait gagné à proposer une définition plus ambitieuse des mesures à prendre. En effet, le texte ne fixe aucun délai précis, hormis la définition de mesures visant à «combler les lacunes» d'ici à l'été 2014 et leur mise en œuvre «le plus

[51] Voir l'annexe III, p. 4 de l'analyse d'impact accompagnant les propositions [SEC(2012) 72 final].

rapidement possible»[52]. L'objet de ces mesures n'est pas clairement défini. Le rapport et la communication recensent les mesures à prendre pour améliorer le fonctionnement du régime, et le CEPD recommande que la Commission indique plus précisément comment ces mesures pourraient être mises en œuvre dans la pratique. En outre, le contenu et le calendrier du «processus plus large de réexamen» devraient être mieux définis.

49. S'agissant des pistes possibles pour améliorer la sphère de sécurité, le CEPD partage l'avis de la Commission selon lequel toute réforme devrait porter sur les lacunes structurelles liées à la transparence et au contrôle de la mise en œuvre, les principes matériels de la sphère de sécurité et l'application de la dérogation pour motif de sécurité nationale.

50. En particulier, le CEPD se réjouit des affirmations selon lesquelles (a) le contrôle et la surveillance par les autorités américaines du respect des principes de la sphère de sécurité devraient être plus efficaces et plus systématiques, (b) la transparence des politiques des entreprises certifiées en matière de respect de la vie privée devrait être améliorée, (c) l'existence et l'accessibilité de mécanismes de règlement des litiges devraient être garanties aux citoyens de l'UE, et (d) la dérogation pour motif de sécurité nationale ne devrait être appliquée que dans la mesure où cela est strictement nécessaire et proportionné.

51. Quelle que soit l'option politique retenue, les organisations actuellement autocertifiées au titre de la sphère de sécurité devraient respecter tous les principes du régime, y compris la transparence. Par ailleurs, les agences de renseignement américaines ne devraient pas adresser de demandes aux membres de la sphère de sécurité allant au-delà de ce qui est strictement nécessaire et proportionné pour des motifs de sécurité nationale.

52. Le CEPD estime également qu'il convient de:
    a. réexaminer les FAQ des principes de la sphère de sécurité afin d'en clarifier l'application et d'expliquer les répercussions pratiques des principes pour les entreprises qui décident d'y adhérer. Ce sera aussi l'occasion de clarifier les modalités d'application pour les sous-traitants, notamment en cas de transfert ultérieur des données, et de renforcer l'obligation pour les responsables du traitement européens de veiller à l'application effective des principes de la sphère de sécurité par les entreprises établies aux États-Unis qui prétendent les appliquer ;
    b. impliquer les autorités européennes chargées de la protection des données dans une vaste campagne de communication sur la sphère de sécurité après le réexamen des FAQ;
    c. encourager la FTC à procéder à des contrôles in situ et à augmenter le niveau des sanctions en cas de non-respect;
    d. insister sur le fait que les principes de la sphère de sécurité n'ont pas vocation à permettre un accès à grande échelle des autorités de renseignement américaines aux données transférées sur leur territoire.

[52] Voir p. 7.

III.3. Renforcer les garanties en matière de protection des données dans le cadre de la coopération entre les services répressifs

53. D'après la communication relative au rétablissement de la confiance[53], la décision du Conseil autorisant la Commission à négocier un accord global UE - États-Unis pour l'échange de données à des fins répressives (ci-après l'«accord-cadre»), qui n'a pas été rendue publique, vise à assurer «un niveau élevé de protection en conformité avec l'acquis de l'UE sur la protection des données».

54. Le CEPD se réjouit de cet objectif, car un tel accord permettrait non seulement éventuellement d'établir un cadre plus clair pour les échanges de données qui ont déjà lieu ou qui auront lieu à l'avenir, mais aussi de mettre en place des garanties accrues en matière de protection des données. Toutefois, ainsi que le CEPD l'a souligné précédemment, «un tel cadre pourrait légitimer des transferts de données massifs dans un domaine — la répression — où les conséquences pour les personnes sont particulièrement graves et où des garanties strictes et fiables sont, de ce fait, d'autant plus nécessaires»[54].

55. Par ailleurs, ainsi que le CEPD l'a relevé précédemment[55], par souci de cohérence l'UE devrait d'abord procéder à la réforme de ses instruments internes de protection des données, puis, à partir de ce cadre, négocier des accords avec les pays tiers. Par la suite, un accord global UE - États-Unis sur l'échange de données à caractère personnel à des fins répressives devrait servir de base à la négociation d'accords sectoriels spécifiques (comme le PNR et le TFTP), et non l'inverse.

56. Compte tenu du contexte actuel, le CEPD recommande de veiller à ce que le futur cadre de protection des données s'applique aux accords existants en matière d'échange de données à caractère personnel à des fins répressives, tant au niveau général qu'au niveau sectoriel. En particulier, ainsi qu'il l'affirme dans son avis sur la réforme de la protection des données, le CEPD recommande que la non-applicabilité du paquet de mesures en matière de protection des données soit limitée dans le temps afin de s'appliquer uniquement aux accords internationaux déjà existants. En outre, la proposition de règlement et la proposition de directive devraient comporter une clause transitoire prévoyant le réexamen de ces accords internationaux dans un délai fixé afin de les mettre en adéquation avec le paquet de mesures. Cette clause devrait être incluse dans le préambule[56] mais aussi dans les dispositions de fond de chaque proposition.

57. Ainsi que cela est indiqué ci-dessus, le CEPD met aussi en question l'affirmation réitérée dans la communication relative au rétablissement de la confiance selon laquelle les accords PNR et TFTP fixent des conditions strictes pour le transfert de données et prévoient des garanties pour les citoyens de l'UE.

---

[53] Voir p. 8.

[54] Voir l'avis du CEPD du 11 novembre 2008 sur le rapport final du groupe de contact à haut niveau UE - États-Unis sur le partage d'informations et la protection de la vie privée et des données à caractère personnel, consultable sur www.edps.europa.eu.

[55] Voir notamment l'avis du CEPD sur la communication de la Commission relative à l'approche globale des transferts des données des dossiers passagers (PNR) aux pays tiers précitée.

[56] Voir l'avis du CEPD du 7 mars 2012 sur le paquet de mesures pour une réforme de la protection des données, consultable sur www.edps.europa.eu.

58. Il est ainsi indiqué dans la communication relative au rétablissement de la confiance que «les négociations offrent l'occasion de préciser que les données à caractère personnel détenues par des entreprises privées situées dans l'UE ne seront pas directement accessibles aux services répressifs américains ni ne leur seront transférées en dehors des canaux officiels de coopération». Le CEPD se félicite de cette assurance. Toutefois, le texte indique ensuite que «tout accès par d'autres moyens doit être exclu, à moins qu'il ne s'agisse de cas exceptionnels clairement définis et susceptibles de faire l'objet d'un contrôle juridictionnel». Le CEPD recommande de spécifier dans la communication que toute dérogation ne devrait être appliquée que dans la mesure où elle est strictement nécessaire, proportionnée et conforme à la jurisprudence constante de la Cour européenne des droits de l'homme et de la Cour de justice.

59. En ce qui concerne la notion de sécurité nationale, qui peut différer de l'autre côté de l'Atlantique, le CEPD se réjouit du fait que la Commission affirme que les dérogations fondées sur des motifs de sécurité nationale devraient être définies d'une manière restrictive et que des garanties et des limitations devraient être convenues à cet égard.

60. S'agissant des garanties mentionnées dans la communication et de celles qui n'y figurent pas, telles que les voies de recours juridictionnel, le CEPD soutient l'objectif de la Commission d'obtenir des engagements sur les droits opposables, y compris les mécanismes de recours juridictionnel ouverts aux citoyens de l'UE ne résidant pas aux États-Unis.

III.4. Répondre aux préoccupations européennes dans le cadre de la réforme en cours aux États-Unis

61. La communication relative au rétablissement de la confiance[57] cite d'éventuelles améliorations du cadre juridique américain, notamment afin d'étendre aux citoyens de l'UE ne résidant pas aux États-Unis les garanties dont bénéficient les ressortissants et résidents américains. Elle plaide aussi pour une plus grande transparence et pour le renforcement des contrôles. Ces modifications devraient bien entendu être approuvées et encouragées dans la mesure où elles sont à même de garantir une protection accrue et plus efficace des citoyens de l'UE et des droits fondamentaux en cause, notamment au regard des mécanismes de recours juridictionnel.

62. À cet égard, le rapport du Privacy and Civil Liberties Oversight Board du 23 janvier 2014, le discours du président Obama du 17 janvier 2014 et les directives présidentielles adoptées ce même jour vont dans le bon sens. Ces modifications supplémentaires que nous appelons de nos vœux non seulement renforceraient la confiance et réduiraient l'impact des programmes sur les Européens, comme l'affirme la communication, mais permettraient également de réduire les situations dans lesquelles les organisations peuvent être confrontées à des conflits de juridictions.

[57] Voir p. 9.

63. La communication précise que ces modifications «pourraient réduire le traitement des données à caractère personnel concernant des Européens qui ne sont pas pertinentes aux fins de la protection de la sécurité nationale». Comme mentionné ci-dessus, le CEPD note que cette norme est inadéquate et que les données à caractère personnel des Européens ne devraient être traitées aux fins de la protection de la sécurité nationale que dans la mesure où cela est strictement nécessaire et proportionné.

64. L'UE devrait également encourager et soutenir les efforts du gouvernement américain et du Congrès américain visant à promulguer une loi générale en matière de respect de la vie privée, qui prévoie des garanties solides et des contrôles adéquats, notamment dans les domaines où il n'existe pas de mécanisme substantiel en matière de protection des droits au respect de la vie privée.

65. Tout comme la Commission, le CEPD se réjouirait d'un renforcement du cadre juridique national des États-Unis, et notamment de l'adoption du «Consumer Privacy Bill of Rights» (déclaration de droits sur la protection de la vie privée des consommateurs) présentée par le président Obama en 2012[58]. Le CEPD encourage les institutions de l'UE à soutenir activement l'adoption d'un cadre global en matière de protection des données aux États-Unis, qui facilite les flux transatlantiques de données tout en assurant un niveau de protection élevé.

66. Le gouvernement américain et le secteur privé américain, en tant que parties prenantes aux discussions, ont alimenté le débat sur la réforme du cadre de l'UE en matière de protection des données. De même, afin de renforcer la compréhension et la confiance, et compte tenu de l'importance des transferts de données entre l'UE et les États-Unis, les institutions de l'UE devraient faire part activement de leurs points de vue sur le débat législatif en cours aux États-Unis concernant le respect de la vie privée.

III.5. Négociations sur le TTIP

67. La Commission fait référence aux négociations menées entre l'UE et les États-Unis en vue d'un partenariat transatlantique en matière de commerce et d'investissements (ci-après le «TTIP») et affirme que les normes de protection des données ne seront pas négociées dans le cadre du TTIP, qui «respectera pleinement les règles de protection des données».

68. Le CEPD invite la Commission à s'assurer du respect de cet engagement et à veiller à ce que les questions négociées dans le cadre du TTIP, telles que les «flux de données transfrontières»[59], les normes et les certificats liés aux exigences relatives à l'informatique en nuage[60] ou à la sécurité des données[61], n'aient pas d'incidence

[58] Voir le document «Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy», la Maison-Blanche, février 2012, consultable sur: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[59] Voir les observations de la Commission à la p. 4 du rapport sur le Dialogue avec la société civile - mise à jour sur le TTIP du 16.07.2013, consultable sur http://trade.ec.europa.eu/doclib/docs/2013/july/tradoc_151656.pdf, dernier accès le 31.03.2014.

[60] Voir les observations de la Commission à la p. 2 du rapport sur le TTIP Stakeholders Event du 12.06.2013, http://ec.europa.eu/digital-agenda/en/news/ttip-ict-stakeholders-event-report, dernier accès le 31.03.2014.

négative sur la protection des données à caractère personnel. En particulier, sur la base de l'article XIV du GATS, le texte de l'accord devrait comporter une disposition prévoyant son application sans préjudice de la législation applicable en matière de protection des données.

69. Par ailleurs, la Commission devrait envisager la possibilité de fixer un objectif commun de développement progressif vers une plus grande interopérabilité des cadres juridiques en matière de respect de la vie privée et de protection des données, objectif auquel les États-Unis pourraient contribuer selon les modalités mentionnées aux points 63 et 64.

III.6. Promouvoir des normes internationales de protection de la vie privée

70. Le CEPD soutient l'idée de la Commission[62] de promouvoir au niveau international les règles de l'UE en matière de collecte, de traitement et de transfert de données. En particulier, le CEPD soutient l'adoption d'un instrument international exigeant le respect des normes de protection des données par les services de renseignement. Cet instrument pourrait être adopté au niveau de l'ONU sur la base de l'article 17 du Pacte international relatif aux droits civils et politiques[63].

71. En ce qui concerne les discussions actuelles au sujet de la Convention sur la cybercriminalité du Conseil de l'Europe, le CEPD rappelle que l'accès des services répressifs des pays tiers aux données sur le territoire de l'UE devrait se conformer aux exigences de l'UE relatives à la protection des données[64].

72. Le CEPD soutient le point de vue de la Commission selon lequel, afin de promouvoir des normes internationales de protection de la vie privée, il conviendrait de favoriser l'adhésion des États-Unis à la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel («convention 108»), laquelle est ouverte aux pays qui ne sont pas membres du Conseil de l'Europe.

73. Le CEPD estime que ces efforts devraient s'accompagner d'un renforcement de la coopération entre les autorités chargées de la protection des données et les autorités chargées du respect de la vie privée à l'échelle mondiale[65]. Le développement de mécanismes de coopération internationale entre les services répressifs devrait faciliter l'application des lois nationales, régionales et internationales en matière de respect de la vie privée et de protection des données dans le cadre des transferts de données transfrontières.

---

[61] Voir le communiqué de presse de la Commission du 20/12/2013 sur le troisième cycle de négociations, consultable sur http://trade.ec.europa.eu/doclib/press/index.cfm?id=1007, dernier accès le 31.03.2014.
[62] Voir p. 9 de la communication relative au rétablissement de la confiance.
[63] Voir la résolution sur l'inscription de la protection des données et de la protection de la vie privée dans le droit international, adoptée par la Conférence internationale des commissaires à la protection des données et à la vie privée (Varsovie, 23-26 septembre 2013).
[64] Voir la lettre du WP29 au comité sur la cybercriminalité du Conseil de l'Europe du 5 décembre 2013, consultable sur http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2013/20131205_wp29_letter_to_cybercrime_committee.pdf.
[65] Voir la résolution sur la coordination de l'application de la loi à l'échelle internationale, adoptée par la Conférence internationale des commissaires à la protection des données et à la vie privée (Varsovie, 23-26 septembre 2013).

III.7. La nécessité de soumettre les activités de renseignement à des garanties appropriées

74. Les services de renseignement et les entités liées au renseignement opèrent dans un cadre très souple dans lequel les exigences de nécessité et de proportionnalité sont plus importantes que jamais. Toutefois, ces exigences ne sont pas toujours assorties de garanties et de mécanismes juridiques suffisants pour assurer une responsabilité et un contrôle adéquats. Le recours croissant aux réseaux de télécommunications par les usagers du monde entier et le déploiement de moyens techniques de collecte et de stockage massifs des données de plus en plus puissants ont considérablement augmenté la capacité des services de renseignement à récolter des données. La mise en place de garanties solides à tous les niveaux pertinents est essentielle pour contenir ce pouvoir accru tout en veillant à ce que la surveillance soit nécessaire et que l'immixtion dans le droit à la protection de la vie privée soit proportionnée.

75. Selon le CEPD, l'une des garanties permettant de s'assurer que les activités de surveillance ne vont pas au-delà de ce qui est nécessaire et proportionné consiste à renforcer le contrôle des activités de renseignement. Ce contrôle pourrait prendre des formes diverses et intervenir à différents stades:

- Lors de la mise en œuvre d'une activité de surveillance impliquant un nouveau traitement, la nécessité d'une autorisation de l'activité par un juge ou toute autre autorité indépendante réduirait le risque d'abus en garantissant que la nécessité et la proportionnalité soient déterminées au moment de prendre des décisions qui affectent la vie privée des citoyens. Cette autorisation devrait comporter une évaluation de la nécessité et de la proportionnalité de la mesure, prévoir éventuellement des garanties appropriées et être limitée dans le temps.

- La totalité du traitement devrait faire l'objet d'un contrôle approprié et effectif par les parlements ou d'autres organes indépendants compétents. Le mandat des organes de contrôle devrait être élargi de façon que ceux-ci puissent inspecter tous les aspects des traitements effectués par l'ensemble des agences de renseignement.

- L'échange de données entre des agences de renseignement de différents pays devrait, elle aussi, faire l'objet d'un contrôle indépendant.

76. Les organes de contrôle devraient se voir confier la mission de superviser l'application des principes de protection des données aux activités de renseignement, et ils devraient être investis des pouvoirs nécessaires à cet effet. Le contrôle de l'application des principes de protection des données devrait reposer sur les éléments suivants:

- la mise en place de contrôles stricts de la qualité des données: un risque d'erreur peut survenir lorsque l'on mélange des bases de données privées et publiques (cf. PNR), et l'exploitation de données soulève un problème de précision qui doit être traité;

- il conviendrait de procéder à un examen régulier des échanges de données à caractère personnel afin de contrôler la destination des données, la finalité de l'échange, la qualité des destinataires des données, ainsi que la proportionnalité de l'échange au regard de son incidence sur les droits fondamentaux;

- les organes de contrôle devraient coopérer entre eux. Pour cela, il convient d'aider le réseau d'organes de contrôle existants à se réunir et à échanger des informations sur des problèmes communs et sur les solutions à ces problèmes.

III.8. Garantir une sécurité informatique efficace

77. La communauté des experts d'Internet reconnaît les dangers d'une surveillance à grande échelle et s'est engagée à concevoir et à mettre en place des infrastructures qui offrent une meilleure protection contre l'interception[66]. Des chercheurs européens ont d'ores et déjà jeté les fondations de la plupart des mécanismes cryptographiques les plus importants. Outre le cryptage, les développeurs de logiciels, notamment sur l'internet, devraient être conscients des risques que posent leurs produits en matière de vie privée et recourir à des méthodes de conception concrètes qui permettent de les éviter ou tout au moins de les réduire.

78. L'UE devrait analyser ses forces et ses faiblesses dans ce domaine et réexaminer ses projets de recherche, de développement et de formation, afin de s'assurer, d'une part, de la mise en place d'outils de sécurité efficaces et fiables pour tous, et, d'autre part, de la formation de développeurs capables de concevoir des systèmes de protection de la vie privée. Le CEPD encourage les échanges sur ce sujet avec les parties prenantes concernées[67].

IV. CONCLUSIONS

79. Si le CEPD se réjouit des mesures envisagées par la Commission, il constate néanmoins que les révélations relatives aux activités des agences de renseignement américaines n'affectent pas seulement la confiance dans les flux de données entre l'UE et les États-Unis. En effet, elles ont également un impact sur les droits opposables des citoyens européens au respect de la vie privée et à la protection des données à caractère personnel les concernant, droits qui sont consacrés par le droit primaire et le droit secondaire de l'UE et du Conseil de l'Europe. Dès lors, le CEPD regrette que la communication relative au rétablissement de la confiance n'ait pas accordé davantage d'attention à l'incidence sur les instruments juridiques existants.

80. Le CEPD souhaiterait à plusieurs égards que la Commission soit plus ambitieuse dans la définition des mesures à prendre et estime que:

    - l'application correcte de l'actuel cadre juridique européen en matière de protection des données est non seulement exigée par la loi, mais elle serait aussi une contribution essentielle au rétablissement de la confiance. Cela vaut également pour les instruments régissant les transferts internationaux de

[66] Vancouver IETF, https://www.ietf.org/media/2013-11-07-internet-privacy-and-security.html;
[67] https://www.w3.org/2014/strint/papers/64.pdf

données entre l'UE et les États-Unis, y compris les principes existants de la sphère de sécurité;

- la Commission devrait rappeler que les dérogations ou restrictions aux droits fondamentaux accordées pour motif de sécurité nationale ne sont justifiées et admissibles que dans la mesure où elles sont strictement nécessaires, proportionnées et conformes à la jurisprudence de la CEDH et de la Cour de justice;

- le CEPD partage pleinement l'avis de la Commission selon lequel, pour consolider et améliorer le cadre de l'UE en matière de protection des données, il convient d'adopter rapidement les propositions de réforme de la protection des données et de se doter de dispositions adéquates garantissant une protection plus solide, plus efficace et plus systématique des données à caractère personnel et de la vie privée en pleine conformité avec le droit de l'UE. Cette réforme devrait également prévoir une protection adéquate des données en cas de traitement ultérieur à des fins répressives et de conflit de compétence international;

- les principes de la sphère de sécurité devraient être réexaminés et renforcés dans les termes indiqués par la Commission. Le CEPD recommande de fixer des délais plus stricts pour la mise en œuvre de ces actions, avec la mise en place notamment d'un suivi adéquat pour remédier aux éventuelles lacunes qui pourraient subsister;

- il convient de renforcer les garanties de protection des données appliquées à la coopération des services répressifs de l'UE et des États-Unis. Les négociations en cours sur un «accord-cadre» devraient non pas légitimer des transferts de données massifs, mais respecter le cadre existant en matière de protection des données et les conclusions de l'actuel processus de réexamen. En particulier, des mécanismes de recours juridictionnel efficaces devraient être accessibles à toutes les personnes concernées, indépendamment de leur nationalité. Ces mécanismes devraient, à terme, également s'appliquer aux accords internationaux en vigueur, si nécessaire sur la base de clauses transitoires appropriées;

- la Commission devrait soutenir les efforts du gouvernement et du Congrès américains tendant à promulguer une loi générale en matière de respect de la vie privée prévoyant des garanties solides et des contrôles adéquats, notamment dans les domaines où il n'existe pas de mécanisme substantiel de protection de la vie privée;

- les négociations qui ont lieu actuellement en vue de l'adoption d'un TTIP ne devraient pas avoir d'impact négatif sur la protection des données à caractère personnel des citoyens. Par ailleurs, la Commission devrait envisager la possibilité de fixer un objectif commun de développement progressif vers une plus grande interopérabilité des cadres juridiques en matière de respect de la vie privée et de protection des données, objectif auquel les États-Unis pourraient contribuer comme mentionné ci-dessus;

- la promotion internationale de normes de protection de la vie privée devrait viser à:
    i. favoriser la pleine conformité des nouveaux instruments internationaux avec le cadre juridique européen en matière de protection des données;
    ii. encourager l'adhésion des pays tiers, et en particulier des États-Unis, à la Convention 108 du Conseil de l'Europe;
    iii. soutenir l'adoption d'un instrument international exigeant le respect des normes de protection des données par les activités de renseignement. Cet instrument pourrait être adopté au niveau de l'ONU sur la base de l'article 17 du PIDCP;

- les services de surveillance devraient être obligés de respecter en permanence l'État de droit et les principes de nécessité et de proportionnalité dans une société démocratique. Les cadres juridiques devraient donc être précisés, et, le cas échéant, complétés à tous les niveaux pertinents. Ces cadres devraient comporter des mécanismes de contrôle appropriés et suffisamment solides;

- en tant que responsables du traitement, les institutions de l'UE et toutes les entités concernées des États membres sont directement responsables du maintien d'une sécurité informatique efficace. Cette responsabilité suppose de procéder à une évaluation des risques pour la sécurité des données au niveau adapté. Elle nécessite aussi d'encourager la recherche sur les mécanismes de cryptage, de sensibiliser les responsables du traitement et les citoyens aux risques pour la vie privée liés aux produits vendus ou utilisés, et enfin d'exiger des développeurs qu'ils utilisent des méthodes de conception ciblées pour éviter ou, tout au moins, réduire ces risques. L'UE devrait promouvoir des initiatives en matière de formation concernant la sécurité des données traitées sur l'internet.

Fait à Bruxelles, le 20 février 2014

(**signé**)

Peter HUSTINX
Contrôleur européen de la protection des données