CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES

Résumé de l'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'Union européenne et des entreprises établies sur son territoire»

(Le texte complet de l'avis en allemand, anglais et français est disponible sur le site internet du CEPD (www.edps.europa.eu))

(2014/C 116/04)

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» ([1]) (ci-après la «communication relative au rétablissement de la confiance»). Cette communication est accompagnée d'un rapport sur les conclusions des coprésidents de l'Union européenne du groupe de travail ad hoc UE-USA sur la protection des données (ci-après le «rapport» et le «groupe de travail»).

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'Union européenne et des entreprises établies sur son territoire» ([2]) (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'Union européenne, 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'Union européenne 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'Union européenne ou d'autres pays tiers avec les États-Unis.

5. Le rapport rassemble les conclusions des coprésidents de l'Union européenne 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'Union européenne et sur les données à caractère personnel des citoyens de l'Union européenne. Ce rapport analyse le cadre juridique américain ([3]), les modalités de la collecte et du traitement ultérieur des données ([4]), ainsi que les mécanismes de contrôle et de recours juridictionnel existants.

([1]) COM(2013) 846 final.

([2]) COM(2013) 847 final.

([3]) 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.

([4]) 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).

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'Union européenne peuvent saisir les autorités américaines de questions liées à la prétendue surveillance d'institutions et de missions diplomatiques de l'Union européenne, tandis que les États membres peuvent discuter avec les autorités américaines, dans un cadre bilatéral, des enjeux relatifs à leur sécurité nationale.

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'Union européenne.

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'Union européenne 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'Union européenne, et plus particulièrement à l'existence du panel de l'Union européenne 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'Union européenne, 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» ([1]) 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'Union européenne 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.

([1]) 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'Union européenne, du CEPD et de la Commission.

13. Cependant, les programmes, dont l'existence, dans certains cas, est clairement confirmée par le rapport ([1]), mettent à mal non seulement la confiance, mais aussi les droits des citoyens instaurés par le droit primaire et le droit secondaire de l'Union européenne 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 ([2]), tel qu'interprété par la Cour suprême des États-Unis ([3]). 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'Union européenne dans le cadre juridique américain ([4]).

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 ([5]), 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 ([6]) est l'affaiblissement 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'Union européenne, 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'Union européenne 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'Union européenne 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.

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'Union européenne 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'Union européenne 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 données entre l'Union européenne 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,

([1]) 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».

([2]) 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).

([3]) Voir p. 4 à 12 du rapport.

([4]) Voir p. 26 à 27 du rapport.

([5]) *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

([6]) 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 clôture à l'ISSE 2013: *The Cryptographic Year in Review* http://homes.esat.kuleuven.be/~preneel/preneel_isse13.pdf

— le CEPD partage pleinement l'avis de la Commission selon lequel, pour consolider et améliorer le cadre de l'Union européenne 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'Union européenne. 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'Union européenne 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'Union européenne 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'Union européenne devrait promouvoir des initiatives en matière de formation concernant la sécurité des données traitées sur l'internet.

Fait à Bruxelles, le 20 février 2014.

Peter HUSTINX

Contrôleur européen de la protection des données